BAB II

LANDASAN TEORI

2.1.Audit

2.1.1. Pengertian Audit

Beberapa pengertian audit yang diberikan oleh beberapa ahli di bidang akuntansi, antara lain:

Menurut Arens, Elder, & Beasley (2012): "*Auditing is the accumulation and evaluation of evidence aboutinformation todetermine and report on the degree of correspondencebetween the information and established criteria. Auditing should bedone by a competent, independent person.*"

Yang berarti audit merupakan akumulasi dan evaluasi bukti mengenai informasi untuk menentukan dan melaporkan derajat kesesuaian antara informasi dan criteria yang ditetapkan. Audit harus dilakukan oleh orang yang berwenang, bebas atau tidak terikat.

Sedangkan menurut Gramling, Johnstone, & Rittenberg (2012): "*Systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the result to interested users*".

Yang berarti Audit merupakan proses sistematis yang secara objektif mendapatkan dan mengevaluasi bukti mengenai pernyataan tentang tindakan dan peristiwa ekonomi untuk memastikan tingkat korespondensi antara pernyataan

dan kriteria yang telah ditetapkan dan mengkomunikasikan hasilnya kepada para pengguna yang tertarik.

Dari kedua pengertian tersebut dapat disimpulkan bahwa audit merupakan proses akumulasi yang secara objektif mendapatkan dan mengevaluasi bukti mengenai informasi atau pernyataan tentang tindakan dan peristiwa ekonomi untuk menentukan dan melaporkan derajat kesesuaian antara informasi dan kriteria yang telah ditetapkan dan mengkomunikasikan hasil dari audit tersebut yang dilakukan oleh orang yang berwenang, bebas dan tidak terikat kepada para pengguna.

2.1.2. Opini Audit

Berdasarkan SPAP (2011) - PSA 29 SA Seksi 508, terdapat lima jenis opini auditor yang telah disesuaikan dengan audit sistem infromasi, yaitu :

1. Pendapat Wajar Tanpa Pengecualian (*Unqualified Opinion*).

Dengan pendapat wajar tanpa pengecualian, pedoman terbaik telah diikuti dan diotomatisasi pada sistem berdasarkan proses yang terencana dan telah di dokumentasikan, dikomunikasikan dan dilaksanakan berdasarkan suatu metode tertentu.

2. Pendapat Wajar Tanpa Pengecualian dengan Bahasa Penjelasan yang Ditambahkan dalam Laporan Auditor Bentuk Baku (*Unqualified Opinion With Explanatory Language*).

Auditor menyatakan bahwa keadaan tertentu sering kali mengharuskan auditor untuk menambahkan paragraf penjelasan (atau bahasa penjelasan lain) dalam laporan auditor bentuk baku. Keadaan tersebut terjadi ketika proses

komputerisasi telah dapat dimonitor dan dievaluasi dengan baik, manajemen proyek pengembangan sistem komputerisasi sudah dijalankan dengan lebih terorganisir tetapi belum menerapkan pedoman terbaik sehingga masih terdapat beberapa kelemahan yang sifatnya tidak material dan dibutuhkan penambahan pengendalian:

a. Pendapat auditor sebagian didasarkan atas laporan auditor independen lain.
b. Jika terdapat kondisi dan peristiwa yang semula menyebabkan auditor yakin tentang adanya kesangsian mengenai kelangsungan hidup entitas, namun setelah mempertimbangkan rencana manajemen, auditor berkesimpulan bahwa rencana manajemen tersebut dapat secara efektif dilaksanakan dan pengungkapan mengenai hal itu telah memadai.

Selain itu, auditor dapat menambahkan paragraf penjelasan untuk menekankan suatu hal tentang laporan audit sistem informasi.

1. Pendapat Wajar Dengan Pengecualian (*Qualified Opinion*).

Auditor menyatakan bahwa sistem informasi perusahan secara wajar, seluruh proses telah didokumentasikan dan dikomunikasikan, serta dilaksanakan berdasarkan metode pengembangan sistem komputerisasi yang baik, namun belum terdapat proses evaluasi terhadap sistem tersebut, sehingga masih ada kemungkinan terjadinya penyimpangan.

2. Pendapat Tidak Wajar (*Adverse Opinion*).

Auditor menyatakan bahwa sistem informasi suatu perusahaan tidak berjalan secara wajar atau baik. Pendapat ini dinyatakan bila, menurut pertimbangan

auditor, sistem informasi secara keseluruhan masih terdapat banyak kesalahan dan tidak diterapkan secara wajar sesuai dengan standar SPAP di Indonesia.

3. Pernyataan Tidak Memberikan Pendapat (*Disclaimer Opinion*).

Auditor tidak memberikan pendapat atas suatu sistem informasi perusahaan. Auditor dapat tidak menyatakan suatu pendapat bilamana ia tidak dapat merumuskan atau tidak merumuskan suatu pendapat tentang kewajaran sistem informasi sesuai dengan standar SPAP. Jika auditor menyatakan tidak memberikan pendapat, laporan auditor harus memberikan semua alasan substantif yang mendukung pernyataannya tersebut.

2.2. Sistem Informasi

2.2.1. Pengertian Sistem

Menurut Reynolds & Stair (2012): *" System is a set of elements or components that interact to accomplish goals. "*

Yang berarti bahwa Sistem adalah seperangkat elemen atau komponen yang berinteraksi untuk mencapai tujuan.

Menurut Gelinas & Dull (2012):*" A system is generally consists of an integrated set of computer-based components and manual components establish to collect, store, and manage data to provide output information to users. "*

Yang berarti bahwa sebuah sistem umumnya terdiri dari sebuah kesatuan yang terintegrasi oleh komponen dasar komputer dan komponen manual untuk mengumpulkan, menyimpan, dan me-*manage* data untuk menghasilkan *output* berupa informasi kepada pengguna.

2.2.2. Pengertian Informasi

Menurut Gelinas & Dull (2012): *" Information is data presented in a form that is useful in a decision making activiy."*

Yang berarti bahwa informasi adalah data yang disajikan dalam sebuah bentuk form yang bermanfaat dalam kegiatan pengambilan keputusan.

Sedangkan menurut Reynolds & Stair (2012):*"Information is a collection of facts organized and processed so that they have additional value beyond the value of the individual facts"*

Yang berarti bahwa sistem informasi adalah kumpulan fakta yang terorganisir dan diproses sehingga memiliki nilai tambah melebihi nilai dari fakta individu.

Jadi dapat disimpulkan bahwa informasi adalah kumpulan fakta atau data yang terorganisir yang diolah atau diproses sehingga memiliki nilai tambah yang berguna bagi penggunanya.

2.2.3. Pengertian Sistem Informasi

Menurut Gupta (2011):

" system information can be seen as the organized combination of people, hardware, software, communication network, data resources, policies and procedures, that stores, retrieves, transforms and disseminates information in an organization. "

Yang diartikan bahwa sistem informasi dapat dilihat sebagai sebuah kombinasi yang terorganisir dari orang, perangkat keras, perangkat lunak, jaringan

komunikasi, sumber data, kebijakan dan prosedur, yang disimpan, diambil, diubah, dan menyebarkan informasi dalam sebuah informasi.

Sedangkan menurut Moscove, Simkin, & Bagranoff (2009): *" An system information is a set of interrelated subsystems that work together to collect, processs, store, transform, and distribute information for planning, decision making and control."*

Yang diartikan bahwa Sebuah sistem informasi adalah seperangkat subsistem yang saling terkait yang bekerja sama untuk mengumpulkan, mengolah, menyimpan, mengubah, dan mendistribusikan informasi untuk perencanaan, pengambilan keputusan dan pengendalian

Jadi dapat disimpulkan bahwa sistem informasi merupakan sebuah kombinasi dari seperangkat subsistem yang saling terkait yang terdiri dari orang, *hardware, software,* jaringan komunikasi dan data yang saling bekerja sama untuk mengumpulkan, mengolah, menyimpan, dan menyebarkan informasi untuk mendukung perencanaan, pengambilan keputusan, dan pengendalian.

2.3. Audit Sistem Informasi

2.3.1. Sejarah Audit Sistem Informasi

Audit *IT* yang pada awalnya lebih dikenal sebagai *EDP* Audit (*Electronic Data Processing*) telah mengalami perkembangan yang pesat. Perkembangan Audit *IT* ini didorong oleh kemajuan teknologi dalam sistem keuangan, meningkatnya kebutuhan akan kontrol *IT*, dan pengaruh dari komputer itu sendiri untuk menyelesaikan tugas penting. Pemanfaatan teknologi komputer ke dalam sistem keuangan telah mengubah cara kerja sistem keuangan, yaitu dalam

penyimpanan data, pengambilan kembali data, dan pengendalian. Sistem keuangan pertama yang menggunakan teknologi komputer muncul pertama kali tahun 1954. Selama periode 1954 sampai dengan 1960-an profesi audit masih menggunakan komputer. Pada pertengahan 1960-an terjadi perubahan pada mesin komputer, dari *mainframe* menjadi komputer yang lebih kecil dan murah. Pada tahun 1968, *American Institute of Certified Public Accountants (AICPA)* ikut mendukung pengembangan *EDP auditing*. Sekitar periode ini pula para auditor bersama-sama mendirikan *Electronic Data Processing Auditors Association (EDPAA)*. Tujuan lembaga ini adalah untuk membuat suatu tuntunan, prosedur, dan standar bagi audit *EDP*. Pada tahun 1977, edisi pertama *Control Objectives* diluncurkan. Publikasi ini kemudian dikenal sebagai *Control Objectives for Information and Related Technology* (CobIT). Tahun 1994, *EDPAA* mengubah namanya menjadi *Information System Audit (ISACA)*. Selama periode akhir 1960-an sampai saat ini teknologi TI telah berubah dengan cepat dari mikrokomputer dan jaringan ke internet. Pada akhirnya perubahan-perubahan tersebut ikut pula menentukan perubahan pada audit *IT*.

Menurut Gondodiyoto (2007), pada hakekatnya, audit sistem informasi sebagai audit tersendiri dan merupakan bagian dari audit laporan keuangan, perlu dilakukan untuk memeriksa tingkat kematangan atau kesiapan suatu organisasi dalam melakukan pengelolaan teknologi informasi *(IT governance)*. Tingkat kesiapan *(level of maturity)* dapat dilihat dari tata kelola informasi, tingkat kepedulian seluruh *stakeholders* tentang posisi sekarang dan arah yang dinginkan di masa yang akan datang. Sehingga perencanaan teknologi informasi hendaknya

dilakukan tidak asal-asalan. Oleh karenanya, audit sistem informasi (berbasis teknologi informasi) ini mencakup 2 hal, yaitu:

1. Audit sistem informasi atau yang dilaksanakan dalam rangka audit laporan keuangan *(general financial audit),* adalah pemeriksaan terhadap aspek-aspek TI pada sistem informasi akuntansi. Panduan yang digunakan adalah Standar Profesional Akuntan Publik (SPAP). Audit *objectives*-nya ialah kesesuaian dengan standar akuntansi keuangan dan tidak adanya salah saji yang material pada laporan keuangan. Sedangkan referensi model sistem pengendalian internal lazimnya adalah *Committee of Sponsoring Organization (COSO).*
2. Audit sistem informasi yang dilakukan dalam kaitannya dengan *IT Governance,* adalah audit operasional terhadap manajemen atau pengelolaan sumber daya informasi atau audit terhadap kehandalan sistem informasi berbasis TI mengenai aspek-aspek: efektivitas, efisiensi, ekonomis tidak unit fungsional sistem informasi, *data integrity, safeguarding assets, reliability, confidenciality, availability* dan *security.* Panduan yang digunakan adalah standar atestasi. Sedangkan model referensi sistem pengendalian internal lazimnya ialah *Control Objective for Information and related Technology* (CobIT).

Dan besarnya peranan audit dalam tata kelola TI diantaranya untuk pendeteksian terhadap:

1. Komputer yang tidak dikelola secara kurang terarah, tidak ada visi-misi, perencanaan TI, pucuk pimpinan organisasi kurang peduli, tidak ada pelatihan dan pola karier personil yang baik, dan sebagainya.

2. Risiko kehilangan data
3. Risiko kesalahan dalam pengambilan keputusan akibat informasi hasil proses sistem komputerisasi salah/lambat/ tidak lengkap.
4. Risiko kebocoran data
5. Penyalahgunaan komputer *(fraud)*
6. Kerugian akibat kesalahan proses perhitungan
7. Keamanan aset perusahaan karena tingginya nilai investasi *hardware* dan *software*.
8. Peningkatan pengendalian penggunaan komputer agar tidak terjadi pemborosan.

2.3.2. Pengertian Audit Sistem Informasi

Menurut Weber(1999), *EDP* Audit *(Electronic Data Processing)* atau yang biasa disebut audit sistem informasi adalah:*"EDP auditing is the process of collecting and evaluating evidence to determine whether a computer systems safeguard assets, maintains data integrity,achieves organizational goals effectively, and consumes resources efficiently."*

Yang berarti *EDP* auditing adalah sebuah proses pengumpulan dan evaluasi bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dan dapat mencapai tujuan perusahaan secara efektif dan menggunakan sumber daya secara efisien.

2.3.3. Pendekatan Audit Sistem Informasi

Menurut Weber (1999), metode audit antara lain :

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 pemrosesan juga benar dan tidak melakukan pengecekan terhadap pemrosesan komputer secara langsung.

Pendekatan ini mengandung beberapa kelemahan, antara lain :

a. Umumnya database mencakup jumlah data yang banyak dan suka di telusuri secara manual.
b. Tidak menciptakan saran bagi auditor untuk mengayati dan mendalami lebih mantap tentang komputer.
c. Cara ini mengabaikan pengendalian sistem dalam pengolahan komputer itu sendiri, sehingga rawan terhadap adanya kelemahan dan kesalahan potensial didalamnya.
d. Kemampuan komputer sebagai fasilitas penunjang pelaksanaan audit menjadi sia-sia.
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 pada pendekatan ini adalah dapat meningkatkan kekuatan terhadap pengujian sistem aplikasi secara efektif dimana ruang lingkup dan kemampuan dari pengujian yang dilakukan dapat diperluas sehingga tinggkat kepercayaan terhadap keandalan dari pengumpulan dan pengevaluasian bukti dapat di tingkatkan. 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 *relative* 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 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 *substantive* atas *file* dan *record* perusahaan. *Software* audit yang digunakan merupakan program

komputer auditor untuk membantu 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.

2.3.4. Jenis Audit Sistem Informasi

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

1. Audit Laporan Keuangan (*general audit on financial statement*)

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

Audit objektifnya yaitu memeriksa kesesuaian *financial statement* dengan standar akuntansi keuangan yang ada atau tidak adanya salah saji material pada laporan keuangan. Audit TI dilaksanakan dalam rangka memeriksa program dan sistem aplikasinya serta memeriksa data pada *database*.

Panduan yang dipergunakan dalam audit ini untuk di Indonesia adalah Standar Profesional Akuntan Publik (SPAP) dan aturan-aturan yang dikeluarkan oleh IAI. Referensi model sistem pengendalian intern yang dipakai lazimnya adalah model *COSO (Committee of Sponsoring*

Organization). Dalam menilai risiko dan pengendalian intern, auditor menilai risiko dan pengendalian internya: *general control* dan *application control.* Auditor melakukan evaluasi untuk memperoleh kesimpulan atau keyakinan bahwa *internal control* telah mendorong *safeguarding assets, information processing, integritas data,* dan *reliability of financial reporting.* Pendekatan auditnya adalah *audit around the computer* (memeriksa *input* dan *output*).

2. Audit Sistem Informasi (SI)

Sebagai kegiatan tersendiri, terpisah dari audit keuangan. Audit SI pada hakekatnya merupakan salah satu dari bentuk audit operasional, tetapi kini audit SI sudah dikenal sebagai satuan jenis audit tersendiri yang tujuan utamanya lebih untuk meningkatkan *IT Governance*. Sebagai suatu audit operasional terhadap manajemen sumber daya informasi, yaitu efektivitas, efisiensi, dan ekonomis tidaknya unit fungsional sistem informasi pada pengelolaan sistem informasi pada suatu organisasi.

Panduan yang digunakan dalam audit SI ini untuk di Indonesia adalah Standar Atestasi dan aturan-aturan yang dikeluarkan oleh IAI. Model referensi sistem pengendalian intern lazimnya adalah *CobIT (Control Objectives for Information and Related Technology).* Audit objektif dalam audit terhadap *IT governance* menurut CobIT adalah *effectiveness, confidentiality, data integrity, availability, efficiency,* dan *realibility*)

2.3.5. Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Weber (1999), dapat disimpulkan secara garis besar terbagi menjadi empat tahap, yaitu:

1. Meningkatkan Keamanan Aset-Aset Perusahaan

   Aset informasi suatu perusahaan seperti *hardware, software*, sumber data, *file* data harus dijaga oleh suatu sistem pengendalian intern yang baik agar tidak terjadi penyalahgunaan aset perusahaan.

2. Menjaga Integritas Data

   Integritas data adalah suatu konsep dasar informasi.

3. Efektifitas Sistem

   Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan.

4. Efisiensi Sistem

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

2.3.6. Standar Audit Sistem Informasi

Adapun menurut *Information Systems Audit and Control Association (ISACA)* (dalam Gondodiyoto, 2007) standar untuk audit sistem informasi adalah:

1. Audit Chapter

1.1 Responsibility, Authority and Accountability

Definisi dari tanggungjawab, otoritas, dan *accountability* dari fugsi audit sistem informasi lebih tepat bila di dokumentasi dalam suatu surat perjanjian.

2. *Independence*

2.1 Professional Independence

Dalam permasalahan yang berkaitan dengan audit, auditor sistem informasi harus bersikap independen dalam tingkah laku dan tindakannya.

2.2 Organizational Relationship

Fungsi audit sistem informasi harus berada independen dari area yang diaudit untuk mencapai tujuan objektivitas dari suatu proses audit.

3. *Professional Ethics and Standards*

3.1 Code Of Professional Ethics

Auditor dari sistem informasi harus menghormati dan menaati etika profesional dari *Information Systems Audit and Control Association.*

3.2 Due Professional Care

Standard auditing profesional harus diterapkan dalam segala aspek dalam pekerjaan yang dilakukan oleh auditor sistem informasi.

4. *Competence*

4.1 Continuing Professional Education

Auditor sistem informasi harus memaintain kompetensi teknikal melalui pendidikan lanjut profesional.

5. *Planning*

5.1 Audit Planning

Auditor sistem informasi harus merencanakan perencanaan audit sistem untuk menempatkan tujuan audit dan melengkapi standar profesional

audit.

6. *Performance of Audit Work*

6.1 Supervision

Staf dari audit sistem informasi harus tepat untuk dapat menjamin tujuan dari audit dijalankan dan standar profesional auditing dapat terpenuhi.

6.2 Evidence

Selama masa pekerjaan audit auditor sistem infromasi harus mendapatkan bukti yang tepat, dapat dipercaya, relevan dan berguna untuk mencapai tujuan objektif dari suatu audit.

7. *Reporting*

7.1 Report Content and Form

Auditor sistem informasi harus menyediakan *report* dalam bentuk yang tepat pada saat penyelesaian tugas audit. Laporan audit berupa lingkup, tujuan, periode audit, dan lingkungan dimana audit dijalankan. Laporan audit harus mengidentifikasi permasalahan yang terjadi dalam jangka waktu audit. Laporan audit juga memberikan rekomendasi dari layanan atau kualisifikasi yang diberikan auditor terhadap tugas audit yang dijalankan.

8. *Follow Up Activities*

8.1 Follow Up

Auditor sistem informasi harus meminta dan mengevaluasi informasi yang sesuai dari penemuan yang terdahulu dan rekomendasi yang

dihasilkan pada periode audit terdahulu untuk mendefinisikan tindakan yang tepat yang harus diimplementasikan dalam suatu periode tertentu.

2.4. Pengendalian Internal

2.4.1. Pengertian Pengendalian Internal

Pengendalian internal menurut *COSO* (*Committee of Sponsoring Organization*) (dalam Louwers, Ramsay, Sinason, & Strawswer, 2008) adalah:

" Internal Control is a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objective in the following three categories: Reliability of financial reporting, Effectiveness and efficiency of operation, Compliance with applicable laws and regulations. "

Yang berarti Pengendalian internal adalah sebuah proses yang dipengaruhi oleh dewan direksi entitas, manajemen dan personil lainnya yang dirancang untuk memberikan keyakinan yang memadai tentang pencapaian tujuan entitas dalam tiga kategori yaitu, keandalan laporan keuangan, efektivitas dan efisiensi operasi, dan kepatuhan terhadap hukum dan peraturan yang berlaku.

2.4.2. Komponen Pengendalian Internal Menurut *COSO*

1. *Control Environment*

Lingkungan pengendalian memberikan nada pada suatu organisasi, mempengaruhi kesadaran pengendalian dari para anggotanya. Lingkungan pengendalian merupakan dasar bagi komponen Pengendalian Internal lainnya, memberikan disiplin dan struktur. Faktor lingkungan pengendalian termasuk :

a) Integritas, nilai etika dan kemampuan orang-orang dalam entitas;

b) Filosofi manajemen dan gaya operasi;

c) Cara manajemen untuk menentukan wewenang dan tanggung jawab, mengorganisasikan dan mengembangkan orang-orangnya;

d) Perhatian dan arahan yang diberikan dewan direksi.

2. *Risk Assessment*

Seluruh entitas menghadapi berbagai macam resiko dari luar dan dalam yang harus ditaksir. Prasyarat dari *risk assessment* adalah penegakan tujuan, yang terhubung antara tingkatan yang berbeda, dan konsisten secara internal. *Risk assessment* adalah proses identifikasi dan menganalisis resiko-resiko yang relevan dalam pencapaian tujuan, membentuk sebuah basis untuk menentukan bagaimana resiko dapat diatur.

3. *Control Activities*

Control activities adalah kebijakan dan prosedur membantu meyakinkan manajemen bahwa arahannya telah dijalankan. *Control activities* membantu meyakinkan bahwa tindakan yang diperlukan telah diambil dalam menghadapi resiko sehingga tujuan entitas dapat tercapai.

4. *Information and Communication*

Istilah informasi mengarah kepada sistem akuntasi yang termasuk metode dan catatan yang digunakan untuk mencatat, memproses, merangkum, dan melaporkan transaksi-transaksi perusahaan serta menjaga akuntabilitas untuk aset, hutang, dan modal perusahaan. Sistem akuntansi harus fokus dalam menjaga aset dan memeriksa keakuratan dan keandalan data akuntansi.

Sedangkan komunikasi mengarah kepada penyediaan personil perusahaan dengan pemahaman mengenai peran dan tanggung jawab yang berkaitan dengan pengendalian *internal* terhadap laporan keuangan. Dengan jaringan komunikasi yang terbuka, diharapkan semua pengecualian yang terdapat didalam sistem pengendalian *internal* dapat dilaporkan kepada manajemen dan kemudian dapat dilakukan tindakan korektif.

5. *Monitoring*

Monitoring merupakan proses yang menilai kualitas dari performa pengendalian *internal* dari waktu ke waktu yang melibatkan evaluasi dari rancangan dan operasi pengendalian berdasarkan waktu ke waktu dan melakukan tindakan korektif ketika pengendalian spesifik tidak berjalan dengan baik.

2.4.3. Pengendalian Umum *(General Control)*

Menurut Arens, Elder, & Beasley (2012) Pengendalian Umum (*General Control*) memberikan keyakinan yang memadai bahwa semua pengendalian aplikasi telah efektif. Menurut beberapa pakar, pengendalian umum diklasifikasikan sebagai berikut:

Arens, Elder, & Beasley	IAI, SA 319
a. Administration of the IT function *b. Separation of IT duties*	a. Pengendaliam organisasi dan manajemen b. Pengendalian pengembangan

c. *System development* d. *Physical and online security* e. *Backup and contingency planning* f. *Hardware controls*	dan pemeliharaan sistem aplikasi c. Pengendalian operasi sistem d. Pengendalian perangkat lunak e. Pengendalian keamanan TI

Tabel 2.1 : Perbandingan Definisi Pengendalian Umum

Penulis dalam melakukan audit terhadap pengendalian umum, memakai standar IAI, PSA 319.

2.4.4. Pengendalian Aplikasi *(Application Control)*

Menurut Gondodiyoto (2007), pengendalian aplikasi (*application control*) adalah sistem pengendalian *internal* (*internal control)* pada sistem informasi berbasis teknologi informasi yang berkaitan dengan pekerjaan atau kegiatan atau aplikasi tertentu (setiap aplikasi memiliki karakteristik dan kebutuhan pengendalian yang berbeda).

Terdapat beberapa unsur dalam pengendalian aplikasi, pengendalian aplikasi pada dasarnya terdiri dari:

1. Pengendalian batasan sistem (*boundary controls*).
2. Pengendalian masukan (*input controls*).
3. Pengendalian proses pengolahan data (*process controls*).
4. Pengendalian keluaran (*output controls*).

5. Pengendalian *file/database* (*file/ database controls*).
6. Pengendalian komunikasi aplikasi (*communication controls*)

2.4.4.1 Pengendalian Batasan Sistem *(Boundary Control)*

Menurut Gondodiyoto (2007), yang dimaksud *boundary* adalah *interface* antara pengguna (*users*) dengan sistem berbasis teknologi informasi. Tujuan utama *boundary controls* adalah antara lain :

a. Untuk mengenal identitas dan otentik (*authentic*) atau tidaknya *user*atau pemakai sistem, artinya suatu sistem yang didesain dengan baik seharusnya dapat mengidentifikasi dengan tepat siapa *user* tersebut, dan apakah identitas diri yang dipakainya otentik.
b. Untuk menjaga agar sumber daya informasi digunakan oleh *user* dengan cara yang ditetapkan.

2.4.4.2 Pengendalian Masukan *(Input Control)*

Menurut Gondodiyoto (2007), pengendalian masukan (*input controls*) dirancang dengan tujuan untuk mendapat keyakinan bahwa data transaksi *input* adalah valid, lengkap, serta bebas dari kesalahan dan penyalahgunaan. *Input controls* ini merupakan pengendalian aplikasi yang penting, karena *input* yang salah akan menyebabkan *output* juga keliru.

Mekanisme masuknya data *input* ke sistem dapat dikategorikan ke dalam dua cara, yaitu :

a. *Batch System (Delayed Processing Systems)*

Pada sistem pengolahan data secara *batch processing system*, tiap transaksi (misalnya formulir sensus, kartu coblosan pemilihan umum, atau *answer sheet* ujian calon mahasiswa) dibundel dalam jumlah lembar tertentu untuk direkam. Demikian pula sistem *batch* dalam siklus akuntansi keuangan (*book – keeping* untuk mencatat transaksi ke dalam jurnal, *posting* ke buku besar dan buku pembantu, serta pengolahan untuk menghasilkan laporan keuangan) dilakukan tidak pada saat transaksi itu terjadi. Sistem pengolahan data lebih bersifat *back office system*, yaitu semata-mata untuk mengolah data dokumen-dokumen akuntansi yang transaksinya sudah lewat (yang lalu). Jadi pengolahan datanya tertunda *(delayed processing).* Pada sistem *batch* ini orientasi utamanya adalah sistem pengolahan data (dahulu disebut sistem pengolahan data elektronik, *electronic data processing (EDP).* Data *input* yang akan dimasukkan ke sistem informasi berbasis teknologi pada hakikatnya dapat dikelompokan dalam tiga tahapan, yaitu: 1. *data capture* (penangkapan data, pengisian dokumen sumber atau *source document*), 2. *data preparation* (penyiapan data untuk di *entry*), serta 3. *data entry* (pemasukkan data) merupakan proses merekam atau memasukkan data ke komputer, suatu proses mengubah data ke dalam bentuk yang dapat dibaca oleh mesin (*machine readable form*).

b. *On-line Real Time Entry & Validation*

Cara pemrosesan data *input* yang lain yang lebih lazim pada saat ini adalah dengan *on-line transaction processing system.* Pada sistem tersebut data masukan dientri dengan *workstation* atau *terminal* atau jenis *input device*

seperti *ATM* (*Automatic Teller Machine*) dan *point of sales (POS).* Meskipun *online* dikaitkan dengan *real time system,* artinya *updating* data di komputer bersamaan dengan terjadinya transaksi. Data yang di*input*kan ke sistem komputer harus divalidasi lebih dahulu.

2.4.4.3 Pengendalian Proses *(Process Control)*

Menurut Gondodiyoto (2007), pengendalian proses (*processing controls*) ialah pengendalian intern untuk mendeteksi jangan sampai data (khususnya data yang sesungguhnya sudah valid) menjadi *error* karena adanya kesalahan proses. Tujuan pengendalian pengolahan adalah untuk mencegah agar tidak terjadi kesalahan-kesalahan selama proses pengolahan data. Kemungkingan terbesar untuk menimbulkan terjadinya *error* adalah kesalahan logika program, salah rumus, salah urutan program, ketidakterpaduan antar subsistem ataupun kesalahan teknis lainnya. Kemungkinan terjadinya kesalahan yang lain ialah *programmer* salah menterjemahkan spesifikasi yang diberikan oleh sistem analis, program dibuat dengan tidak mengikuti standar (struktur, *language,* tidak dites dengan memadai. Tipe kesalahan yang "*level*nya tinggi" adalah jika sistem aplikasi (dan program-programnya) dibuat tidak sesuai dengan kebutuhan pemakai (*user*nya).

Pengendalian proses merupakan bentuk pengendalian yang diterapkan setelah data berada pada sistem aplikasi komputer. Menurut IAI (SA341, par.08) pengendalian ini didesain untuk memberikan keyakinan memadai bahwa:

a) Transaksi, termasuk transaksi yang dipicu melalui sistem, diolah semestinya oleh komputer.
b) Transaksi tidak hilang, ditambah, digandakan, atau diubah tidak semestinya.

c) Kekeliruan pengolahan dapat diidentifikasi dan dikoreksi secara tepat waktu.

2.4.4.4 Pengendalian Keluaran *(Output Control)*

Menurut Gondodiyoto (2007), pengendalian keluaran merupakan pengendalian yang dilakukan untuk menjaga *output* sistem agar akurat, lengkap, dan digunakan sebagaimana mestinya. Pengendalian keluaran (*output controls*) ini didesain untuk menjamin agar *output* atau informasi dapat disajikan secara akurat, lengkap, mutakhir, dan didistribusikan kepada orang – orang yang berhak (para pengguna) secara cepat dan tepat waktu. Yang termasuk pengendalian keluaran antara lain adalah :

a. Rekonsiliasi Keluaran dengan Masukan dan Pengolahan.

   Rekonsiliasi keluaran dilakukan dengan cara membandingkan hasil keluaran dari sistem dengan dokumen asal.

b. Penelaahan dan Pengujian Hasil – Hasil Pengolahan.

   Pengendalian ini dilakukan dengan cara melakukan penelaahan, pemeriksaan dan pengujian terhadap hasil – hasil pengolahan dari sistem. Proses penelaahan dan pengujian ini biasanya dilakukan oleh atasan langsung pegawai.

c. Pendistribusian Keluaran.

   Pengendalian ini didesain untuk memastikan bahwa keluaran didistribusikan kepada pihak yang berhak, dilakukan secara tepat waktu dan hanya keluaran yang diperlukan saja yang didistribusikan.

2.5. CobIT

Menurut *ISACA (Information Systems Audit and Control Association)* CobIT *(Control Objective for Information and Related Technology)* adalah sebuah alat yang telah diterima secara internasional yang diorganisir menjadi sebuah kerangka kerja *(framework)* yang dapat digunakan para eksekutif untuk memastikan bahwa Teknologi Informasi yang mereka miliki membantu mereka dalam mencapai sasaran dan tujuannya. CobIT memastikan bahwa Teknologi Informasi bekerja secara efektif memungkinkan untuk meminimalkan risiko TI yang terkait dan memaksimalkan keuntungan dari investasi teknologi.

CobIT disusun oleh *The IT Governance Institute (ITGI)* dan *Information System Audit and Control Foundation (ISACF)* pada tahun 1992. Edisi pertama CobIT dipublikasikan pada tahun 1996, kemudian edisi kedua dari CobIT diterbitkan pada tahun 1998. Pada tahun 2000 dirilis cobIT 3.0, CobIT 4.0 pada tahun 2005 dan cobIT 4.1 pada tahun 2007. Kemudian terakhir CobIT 5.0 pada tahun 2012. CobIT merupakan kombinasi dari prinsip-prinsip yang telah ditanamkan dilengkapi dengan *balance scorecard* dan dapat digunakan sebagai acuan model (seperti *COSO*) dan disejajarkan dengan standar industri, seperti *ITIL, CMM, BS779, ISO9000.*

CobIT difokuskan pada apa yang diperlukan untuk mencapai pengelolaan dan pengendalian TI yang memadai, dan diposisikan pada tingkat tinggi. CobIT *framework* didasarkan pada prinsip untuk memberikan informasi yang dibutuhkan perusahaan untuk mencapai tujuannya, invenstasi yang diperlukan perusahaan,

serta mengelola dan mengendalikan sumber daya IT menggunakan seperangkat proses yang terstruktur untuk meberikan layanan informasi yang dibutuhkan perusahaan.

CobIT berguna bagi Auditor untuk mendukung atau memperkuat opini yang dihasilkan dan memberikan saran kepada manajemen atas pengendalian internal yang ada. Bagi Manajemen untuk membantu mereka menyeimbangkan antara resiko dan investasi pengendalian dalam sebuah lingkungan TI yang sering tidak dapat diprediksi. Sedangkan bagi *user*, CobIT berguna untuk memperoleh keyakinan atas kehandalan sistem aplikasi yang digunakan.

Menurut CobIT, untuk memenuhi tujuan bisnis perusahaan informasi harus sesuai dengan kriteria pengendalian tertentu yang disebut sebagai kriteria informasi CobIT, yaitu :

1. *Effectiveness* (Efektifitas)

   Informasi yang diperoleh harus relevan dan berkaitan dengan proses bisnis, disampaikan tepat waktu, tepat, konsisten, dan dapat dipercaya.

2. *Efficiency* (Efisiensi)

   Penyediaan informasi melalui penggunaan sumber daya (yang paling produktif dan ekonomis) yang optimal.

3. *Confidentiality* (Kerahasiaan)

   Berkaitan dengan proteksi pada informasi penting dari pengungkapan yang tidak sah atau pihak-pihak yang tidak memiliki otorisasi.

4. *Integrity* (Integritas)

   Berkaitan dengan keakuratan dan kelengkapan informasi serta validitas yang sesuai dengan nilai-nilai bisnis dan ekspektasi.

5. *Availability* (Ketersediaan)

   Fokus terhadap ketersediaan informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun di masa yang akan datang. Ini juga terkait dengan pengamanan sumber daya yang diperlukan dan terkait.

6. *Compliance* (Kepatuhan)

   Pemenuhan informasi yang sesuai dengan ketentuan hukum, peraturan dan rencana perjanjian/kontrak untuk proses bisnis.

7. *Reliability* (Handal)

   Pemberian informasi yang tepat bagi manajemen untuk mengoperasikan perusahaan dan pemenuhan kewajiban mereka untuk membuat laporan keuangan dan tanggung jawab kepada pemerintah.

2.5.1. Komponen CobIT

Framework CobIT disusun dengan karakteristik yang berfokus pada bisnis (*business-focused*), berorientasi pada proses (*process-oriented*), berbasis pada pengendalian (*controls-based*) dan terarah kepada pengukuran (*measurement-driven*). CobIT *framework*4.1terdiri dari 34 *high level control objectives* dan kemudian mengelompokan proses tersebut menjadi 4 *domain*, keempat *domain* tersebut adalah: *Planning and Organization* (10 proses), *Acquisition and*

Implementation (7 proses), *Delivery and Support* (13 proses), dan *Monitoring and Evaluation* (4 proses), yang mencakup:

1. *Plan and Organise* (Perencanaan dan Organisasi)

   Mencakup strategi, taktik dan identifikasi kontribusi terbaik TI demi pencapaian tujuan perusahaan. Domain ini meliputi pertanyaan-pertanyaan sebagai berikut :

   a) Apakah proses TI dan strategi bisnis telah sesuai?
   b) Apakah perusahaan mencapai penggunaan yang optimum dengan sumber dayanya?
   c) Apakah setiap karyawan di perusahaan memahami tujuan TI?
   d) Apakah risiko TI dipahami dan dikelola?
   e) Apakah kualitas sistem TI sesuai dengan kebutuhan bisnis.

2. *Acquire and Implement (*Pengadaan dan Implementasi*)*

   Untuk merealisasikan strategi TI, perlu dilakukan pengidentifikasian, pengembangan dan perolehan solusi TI, sesuai dengan yang akan diimplementasikan dan diinteregasikan ke dalam proses bisnis. Domain ini meliputi pertanyaan-pertanyaan sebagai berikut :

   a) Apakah proyek baru kemungkinan akan memberikan solusi yang dibutuhkan?
   b) Apakah proyek baru kemungkinan akan dikirim tepat waktu sesuai dengan anggaran?
   c) Apakah sistem baru dapat bekerja dengan baik ketika diimplementasikan?

d) Apakah perubahan dilakukan tanpa menggangu operasi bisnis yang sedang berjalan?

3. *Deliver and Support* (Pengiriman Layanan dan Dukungan)

Domain ini berfokus terhadap penyampaian jasa yang sesungguhnya diperlukan, termasuk penyediaan layanan, manajemen keamanan dan kontinuitasnya, jasa dukungan kepada *user* dan manajemen data dan fasilitas operasi. Domain ini meliputi pertanyaan-pertanyaan sebagai berikut :

a) Apakah jasa TI yang disampaikan sejalan dengan prioritas bisnis?

b) Apakah biaya TI teroptimalisasi?

c) Apakah sistem TI sistem bekerja secara produktif dan aman?

d) Apakah terdapat kontrol demi kerahasiaan, integritas dan ketersediaan yang baik terhadap keamanan informasi?

4. *Monitor and Evaluate* (Pengawasan dan Evaluasi)

Berkenaan dengan manajemen kinerja, pemantauan *internal control*, kepatuhan terhadap regulasi dan pelaksanaan tata kelola. Domain ini meliputi pertanyaan-pertanyaan sebagai berikut:

a) Apakah kinerja TI diukur untuk mendeteksi permasalahan sebelum terlambat?

b) Apakah pihak manajemen memastikan bahwa *internal control* efektif dan efisien?

c) Dapatkah kinerja TI dihubungkan dengan tujuan perusahaan?

d) Apakah terdapat kontrol demi kerahasiaan, integritas dan ketersediaan yang baik terhadap keamanan informasi?

2.5.2. Manfaat Penerapan CobIT

Menurut *The IT Governance Institute (ITGI),* manfaat dari penerapan CobIT sebagai kerangka tata kelola TI meliputi:

a) Penggunan bahasa yang umum bagi para eksekutif, manajemen dan profesional TI.
b) Pemahaman yang lebih baik tentang bagaimana bisnis dan TI dapat bekerja sama untuk keberhasilan pengiriman inisiatif TI.
c) Peningkatan efisiensi dan optimalisasi biaya.
d) Mengurangi risiko operasional.
e) Pengembangan kebijakan yang jelas.
f) Audit yang lebih efisien dan sukses.
g) Kepemilikan dan tanggung jawab yang jelas, berdasarkan proses orientasi.

2.5.3. *Maturity Model*

Menurut *ISACA maturity model* merupakan alat bantu yang dapat digunakan untuk memetakan status *maturity* proses (dalam skala 0-5), diantarany :

a. Skala 0 – *Not Existence*

Perusahaan tidak menyadari pentingnya membuat perencanaan strategis di bidang teknologi informasi.Dalam skala ini penting untuk dilakukan evaluasi pengendalian dan dijadikan sebagai temuan yang penting.

b. Skala 1 – *Initial*

Perusahaan telah menyadari akan pentingnya pembuatan perencanaan strategis di bidang teknologi informasi. Namun, tidak ada proses yang distandarisasi; perencanaan, perancangan dan manajemen masih belum teroganisir dengan baik.Dalam skala ini keperluan untuk dijadikan temuan, karena tingkat kemungkinan terjadinya resiko tidak sebesar skala 0.

c. Skala 2 – *Repeatable*

Perusahaan telah menetapkan prosedur untuk dipatuhi oleh karyawan, namun belum dikomunikasikan dan belum adanya pemberian latihan formal kepada setiap karyawan mengenai prosedur dan tanggung jawab diberikan sepenuhnya kepada individu sehingga pemberian kepercayaan sepenuhnya kemungkinan dapat terjadi penyalahgunaan.

d. Skala 3 – *Defined*

Proses telah didokumentasikan dan telah dikomunikasikan, serta dilaksanakan berdasarkan metode pengembangan sistem komputerisasi yang baik, namun belum ada proses evaluasi terhadap sistem tersebut, sehingga masih ada kemungkinan terjadinya penyimpangan.

e. Skala 4 – *Managed*

Proses komputerisasi telah dapat dimonitor dan dievaluasi dengan baik, manajemen proyek pengembangan sistem komputerisasi sudah dijalankan dengan lebih teroganisir.

f. Skala 5 – *Optimised*

Best Practices (pedoman terbaik) telah diikuti dan diotomatisasi pada sistem berdasarkan proses yang terencana, teroganisir dan menggunakan metodologi yang tepat.