BAB II

LANDASAN TEORI

2.1. Sistem Informasi

2.1.1. Pengertian Sistem

Menurut Reynolds & Stair (2012) "*System is a set of elements or components that interact to acomplish goals"* yang berarti bahwa sistem adalah seperangkat element atau komponen yang berinteraksi untuk mencapai tujuan.

Menurut Gelinas & Dull (2012) "*A system is generally consists of an intergrated 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.

2.1.2 Pengertian Informasi

Menurut Gilenas & Dull (2012) "*Information is data presented in a form that is useful in a decision making activity"* yang berarti bahwa informasi adalah data yang disajikan dalam sebuah bentuk form, yang bermanfaat dalam membuat sebuah keputusan.

Menurut Reynold & Stair (2012) *"Information is a collection of fact organized and processed so that they have addictional value beyond the value of the individuals fact"* yang berarti bahwa sistem informasi adalah kumplulan fakta yang terorganisir dan diproses sehingga memiliki nilai tambah melebihi nilai dari fakta individu.

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

2.1.3 Pengertian Sistem Informasi

Menurut Gupta (2011) "*system information can be seen as an organized combination of people, hardware, software, communication network, data resources, policies and procedures, that stores, retrieves, transforms and dissesminates information in an organization"* yang dapat diartikan bahwa sistem informasi dapat dilihat sebagai sebuah kombinasi yang teroganisir dari pengguna, perangkat keras, perangkat lunak, jaringan komunikasi, sumber data, kebijakan dan prosedur, yang disimpan, diambil, diubah dan menyebarkannya dalam bentuk sebuah informasi.

Menurut Moscove, Simkin, & Bagranoff (2009) "*an system information is a set of interrelated subsystem that work together to collect, process, store, transform and distribute information for planning, decision making and control"* yang dapat diartikan bahwa sebuah sistem informasi adalah seperangkat subsistem

yang saling terkait yang bekerja sama untuk mengumpulkan, mengolah, menyimpan, mengubah, dan mendistribusikan informasi untuk pencernaan, pengambilan keputusan dan pengendalian.

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

2.2. Audit

2.2.1. Pengertian Audit

Beberapa pengertian audit yang diberikan dari banyak ahli dibidang akuntansi, antara lain :

Menurut Arens, Elder, & Beasley (2012) *"Auditing is the accumulation and evaluation of evidence about information and establish criteria, auditing should be done by a competent, independent person"* yang dapat diartikan bahwa audit merupakan akumulasi dan evaluasi bukti mengenai informasi untuk menentukan dan melaporkan derajat kesesuaian antara informasi dan kriteria yang ditetapkan. Audit harus dilakukan oleh orang yang berwenang, bebas atau tidak terkait.

Menurut Gramling, Johnstone, & Rittenberg (2012) *"Systematic process of objectively obtaining and evaluating evidence regarding assertion 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 berati bahwa audit merupakan proses sistematis yang secara objektif mendapatkan evaluasi bukti pernyataan tentang tindakan dan pristiwa ekonomi untuk memastikan tingkat korespondensi antara pernyataan dan kriteria yang telah di tetapkan dan mengkomunikasikan hasilnya kepada para penguna yang tertarik.

Dari kedua pendapat ahli di atas dapat disimpulkan bahwa audit merupakan proses akumulasi yang secara objektif mendapatkan dan mengevaluasi bukti mengenai informasi atau pernyataan tentang tindakan dan pristiwa ekonomi untuk menentukan dan melaporkan derajat kesesuaian antara informasi dan kriteria yang telah di tetapkan dan mengkomunikasikan hasil dari audit tersebut yang dilakukan oleh orang berwenang, bebas dan tidak terkait kepara pada penguna.

2.1.2 Opini Audit

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

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

Dengan pendapat wajar tanpa pengecualian, pedoman terbaik telah diikuti dan di otomisasi pada sistem berdasarkan proses yang telah terencana dan telah didokumentasikan, 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 mengharukan auditor untuk menambahkan paragraf penjelasan (atau bahasa penjelasan lain) dalam laporan auditor bentuk baku. Keadaan tersebut terjadi ketika proses komputerisasi telah dimonitor dan dievaluasi dengan baik, management 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 independent lain.

b. Jika terdapat kondisi dan pristiwa yang semula menyebabkan auditor yakin tentang adanya kesangsian mengenai kelangsungan hidup entitas, namun setelah mempertimbangkan rencana management, auditor berkesimpulan bahwa rencana management tersebut dapat secara efektif dilaksanakan dan pengungkapan mengenai hal itu telah memadai.

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

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

Auditor menyatakan bahwa sistem informasi perusahaan 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 perusahaan secara wajar atau baik. Pendapat ini dinyatakan bila, menurut pertimbangan auditor, sistem informasi secara keseluruhan masih banyak terdapat 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 tentang kewajaran sistem informasi sesuai standar SPAP. Jika auditor menyatakan tidak memberikan pendapat, laporan auditor harus memberikan semua alasan substantif yang mendukung pernyataan tersebut.

2.3. Audit Sistem Informasi

2.3.1. Sejarah Audit Sistem Informasi

Audit informasi teknologi pada awalnya dikenal sebagai *EDP* audit *(Electronic Data Processing)* telah mengalami perkembangan yang pesat. Perkembangan Audit *IT* ini didorong oleh kemajuan teknologi dalam sistem keuangan, meningkatkan kebutuhan akan kontrol *IT*, dan pengaruh dari komputer itu sendiri untuk menyelesaikan tugas penting. Pemanfaatan teknologi komputer kedalam sistem keuangan telah mengubah cara kerja sistem keuangan, yaitu dalam penyimpanan data, pengambilan kembali data, dan pengendalian. Sistem keuangan pertama yang mengunakan teknologi komputerisasi muncul pertama kali tahun 1954. Selama periode 1954 sampai dengan 1960-an profesi audit masih mengunakan komputer.

Pada pertengahan tahun 1960-an terjadi perubahan pada mesin komputer, dari *mainframe* menjadi komputer yang lebih kecil dan murah. Pada tahun 1968, *American Institute of Certified Public Association (AICPA)* ikut mendukung

pengembangan *EDP* auditing, sekitar periode ini pula para auditor bersama – sama mendirikan *Electronic Data Processing Auditor Association (EDPAA),* tujuan lembaga ini adalah untuk membuat suatu pedoman, prosedur, dan standar bagi audit *EDP*.

Menurut Gondodiyoto (2007) audit sistem informasi sebagai audit tersendiri dan merupakan bagian dari audit laporan keuangan, perlu dilakukan untuk memeriksa tingkat kematangan dan kesiapan suatu organisasi dalam melakukan pengelolaan teknologi informasi (*IT Governance).*

Tingkat kesiapan *(level of maturity)* dapat dilihat dari tata kelola informasi, tingkat kepedulian seluru *Stakeholder* tentang posisi sekarang dan arah yang diinginkan di masa yang akan datang. Sehingga perencanaan teknologi hendaknya dilakukan tidak asal-asalan. Oleh karenanya, audit sistem informasi (berbasis teknologi informasi) ini mencakup dua hal, yaitu:

1. Audit sistem informasi atau yang dilaksanakan dalam rangka audit laporan keuangan *(General Financial Audit)* adalah pemeriksaan terhadap aspek – aspek teknologi informasi pada sistem informasi akuntansi. Paduan yang digunakan adalah Standar Profesional Akuntan (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 management dan pengelolaan sumber daya informasi dan audit terhadap kehandalan sistem informasi berbasis TI mengenai aspek efektivitas, efesiensi, ekonomis tidak fungsional sistem informasi, *data integrity, safeguarding assets, realibility, confidenciality, avaibility* dan *security.* Paduan yang digunakan adalah standar atesasi. Sedangkan model referensi sistem pengendalian internal lazimnya ialah *control Objective for Information and Related Technology* (CobIT).

Dan besarnya peranan audit dalam tata kelolah teknologi informasi diantaranya untuk pendeteksian terhadap :

1. Komputer yang dikelolah secara kurang terarah, tidak adanya visi dan misi, perencanaan teknologi informasi, pucuk pimpinan organisasi kurang perduli, tidak ada pelatihan dan pola karier personil yang baik dan sebagainya.

2. Resiko kehilangan data atau aset.

3. Resiko kesalahan dalam pengambilan keputusan akibat informasi hasil proses sistem komputerisasi yang salah / lambat / tidak lengkap.

4. Resiko kebocoran data.

5. Penyalahgunaan komputer *(fraud)*

6. Kerugian akibat kesalahan proses perhitungan

7. Keamanan aset perusahaan kerena tingginya nilai investasi perangkat keras dan perangkat lunak

8. Peningkatan pengendalian pengunaan 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 wether a computer system safeguard assets, maintains data integrity, achieves organization goals effetively, and consumes resources effeciently".*

Yang berarti *EDP* audit adalah sebuah proses pengumpulan data dan evaluasi bukti untuk menentukan apakah sistem komputer dapat mengunakan aset, memelihara integritas data, dan dapat mencapai tujuan perusahaan secara efektif dan mengunakan 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 berlangsung, tetapi hanya berfokus pada *input* dan *output* dari sistem komputer. Diasumsikan bahwa jika *input* 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 ditelusuri secara manual.

b. Tidak menciptakan saran bagi auditor untuk mengayati dan mendalami lebih mantap tentang komputer.

c. Cara ini mengabaikan pengendalian sistem dalam pengelolaan 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 penyelengaraan 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 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 tingkat kepercayaan terhadap kendali kehandalan 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 Computer*

Pendekatan ini dilakukan dengan mengunakan komputer dan perangkat lunak digunakan untuk mengotomitasi prosedur pelaksanaan audit. Pendekatan ini merupakan cara audit yang sangat bermanfaat, khususnya dalam pengujian substantif atas data dan *record* perusahaan. *Software* audit yang digunakan merupakan aplikasi komputer auditor untuk membantu dalam pengujian dan evaluasi kehandalan data, *file* dan *record* perusahaan.

Keungulan 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 untuk diuji dengan komputer lain.

2.3.4. Jenis Audit Sistem Informasi

Menurut Gondodiyoto (2007), sesunguhnya 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 resiko 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 *reability 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 bentuk dari audit operasional. Tetapi kini audit sistem informasi sudah dikenal sebagai satuan audit tersendiri yang tujuan utamanya untuk lebih meningkatkan *IT Governance.*

Sebagai suatu audit operasional terhadap management sumber daya informasi, yaitu efektivitas, efesiensi dan ekonomis tidaknya unit fungsional unit fungsional sistem informasi pada pengelolaan sistem informasi pada suatu organisasi.

Paduan yang digunakan dalam audit SI ini untuk di indonesia adalah standar – standar atestasi dan aturan – aturan yang dikeluarkan oleh AIA. Sedangkan model referensi sistem pengendalian internal lazimnya ialah *control Objective for Information and Related Technology* (CobIT).

Audit objektif dalam audit terhadap *IT Governance* menurut CobIT adalah *effectiveness, confidentiality, data integrity, avaibility, effeciency,* dan *reability.*

2.3.5. Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Weber (2009), dapat disimpulkan secara garis besar terbagi menjadi empat tahap, yaitu:

1. Meningkatkan keamanan aset – aset perusahaan

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

2. Menjaga integritas data yakni menjaga suatu konsep dasar informasi

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

4. Efesiensi sistem menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang menandai.

2.3.6. Standar Audit Sistem Informasi

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

1. *Audit Chapter*

1.1. *Responsibility, Authority & Accountability*

Definisi dari tanggungjawab, otoritas, & *accountability* dari fungsi 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 *Organization Relationship*

Fungsi audit sistem informasi harus berada independen dari area yang diaudit untuk mencapai tujuan objektifitas 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 System 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 memantain 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 aditor sistem informasi harus mendapatkan bukti yang tepat, dapat dipercaya, relavan 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 kualifikasi 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 terhahulu untuk mendefenisikan 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 dan strawswer, 2008) adalah "*internal control is a process, affected by an entity's board of directors, management and other personel, designed to provided reasonable assurance regarding the achievement of objective in the following three categories Reliability of financial reporting, effectiveness and effeciency 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 menandai tentang pencapaian tujuan entitas dalam tiga kategori yaitu, keandalan laporan keuangan, efektivitas, dan efesiensi operasi, dan kepatuhan terhadap hukum dan peraturan yang berlaku.

2.4.2. Komponen Pengendalian Internal Menurut *COSO*

1. *Control Envriomen*t

Lingkungan pengendalian memberikan nada pada suatu organisasi, mempengaruhi kesadaran pengendalian dari para angotanya. Lingkungan pengendalian internal lainnya, memberikan displin dan stuktur. Faktor pengendalian termasuk:

a. Integritas, nilai etika dan kemampuan orang – orang dalam entitas

b. Filosofi management dan gaya operasi

c. Cara management untuk menentukan wewenang dan tanggung jawab, mengorganisasikan dan mengembangkan orang – orangnya

d. Perhatian dan arahan yang diberikan dewan direksi.

2. *Risk Assesment*

Seluruh entitas menghadapi berbagai macam resiko dari luar dan dalam yang harus ditaksir. Persyaratan dari *Risk Assesment* adalah penegakan tujuan, yang terhubung antara tingkatan yang berbeda, dan konsisten secara internal.

Risk Assesment 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 management bahwa arahnya 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 akuntansi yang termasuk metode dan catatan yang digunakan untuk memcatat, memproses, merangkum, dan melaporkan transaksi – transaksi perusahaan serta menjaga akuntanbilitas untuk aset, hutang, dan modal perusahaan. Sistem akuntansi harus fokus dalam menjaga aset, 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* dapat dilaporkan kepada management dan kemudian dapat dilakukan tindakan korektif.

5. *Monitoring*

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

2.4.3. Pengendalian Umum *(General Control)*

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

Arens, Elder, & Beasley	IAI, SA 319
a. *Administration of IT Function* b. *Separation Of IT Duties* c. *System Development* d. *Physical and Online Security* e. *Backup and Contingency Planning* f. *Hardware Control*	a. Pengendalian Organisasi dan manajemen b. Pengendalian pengembangan dan pemeliharaan sistem aplikasi c. Pengendalian sistem aplikasi d. Pengendalian perangkat lunak e. Pengendalian Keamanan IT

Tabel 2.1 Perbandingan Defenisi Pengendalian Umum

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

2.4.4. Pengendalian Aplikasi *(Aplication Control)*

Menurut Gondodiyoto (2007), pengendalian aplikasi *(aplication 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 dasar nya terdiri dari :

1. Pengendalian batasan sistem *(boundary controls)*
2. Pengendalian masukan *(input controls)*
3. Pengendalian proses pengelolaan data *(process controls)*
4. Pengendalian keluaran *(output goal)*
5. Pengendalian data *(file / database controls)*
6. Pengendalian komunikasi aplikasi *(communication controls)*

2.4.4.1. Pengendalian Batasan Sistem *(Boundary Controls)*

Menurut Gondodiyoto (2007), yang dimaksud dengan *boundary* adalah tampilan antara penguna *(users)* dengan sistem berbasis teknologi informasi. Tujuan utama *boundary contols* antara lain :

a. Untuk mengenal identitas dan otentik *(authentic)* atau tidaknya penguna sistem, artinya suatu sistem yang dirancang 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 Controls)*

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

Mekanisme masukan data dan *input* kedalam sistem dapat dikategorikan dalam dua cara, yaitu:

a. *Batch System (Delayed Processing System)*

Pada sistem pengelolaan data secara *batch processing sistem,* tiap transaksi (misalnya formulir sensus, kartu dari pemilihan umum, atau kertas jawaban ujian) dibundel dalam jumlah lembar tertentuk untuk direkam. Demikian pula sistem *batch* dalam siklus akuntansi keuangan *(book keeping)* untuk mencatat transaksi kedalam jurnal, *posting* kebuku besar dan buku pembantu, tidak pada saat transaksi itu terjadi.

Sistem pengelolaan data lebih bersifat *back office system,* yaitu semata – mata untuk mengelola data dokumen – dokumen akuntansi yang transaksinya sudah lewat (yang lalu), jadi pengelolahan datanya tertunda *(delayed processing).* Pada sistem *batch* ini orientasi utamanya adalah sistem pengelolaan data (dahulu disebut sistem pengelolahan data elektronik, *electronic data processing).*

Data *inputi* yang akan dimasukan kedalam sistem informasi berbasis teknologi pada dasarnya dapat dikelompokan menjadi tiga tahapan, yaitu :

1. *Data Capture* (penangkapan data, pengisian dokumen sumber atau *resource document*),

2. *Data Preparation* (penyiapan data untuk dimasukan), serta

3. *Data Entry* (pemasukan data)

Tiga tahapan diatas merupakan proses merekam atau memasukan data ke komputer, suatu proses mengubah data kedalam bentuk yang dapat dibaca oleh mesin *(machine readable form).*

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

Cara pemrosesan data *input* yang lain yang lebih lazin pada saat ini adalah dengan *on-line transaction processing system.* Pada sistem tersebut data masukan dientri dengan *workstation* atau *terminal* atau bisa juga dengan media *input device* seperti *Automatic Teller Machine (ATM)* dan *point of sales (POS).* Meskipun *online* dikaitkan dengan *real time system,* artinya *uploading* data di komputer bersamaan dengan terjadinya transaksi, data yang di*input* ke sistem komputer harus divalidasi terlebih dahulu.

2.4.4.3. Pengendalian Proses *(Process Control)*

Menurut Gondodiyoto (2007), pengendalian proses *(process controls)* adalah pengendalian intern untuk mendeteksi jangan sampai data (khususnya data yang sesunghuhnya sudah valid) menjadi *error* karena adanya kesalahan proses. Tujuan pengendalian pengelolahan ini adalah untuk mencegah agar tidak terjadi kesalahan – kesalahan selama proses pengelolahan data.

Kemungkinan terbesar untuk menimbulkan terjadinya *error* adalah kesalahan logika program, salah rumus, salah urutan program, ketidakterpaduan antara subsistem ataupun kesalahan teknis lainnya. Kemungkinan terjadinya kesalahan yang lain ialah *programer* salah menerjemahkan spesifikasi yang diberikan oleh sistem analis, aplikasi dibuat dengan tidak mengikuti standar (struktur, *language,* tidak dites dengan memadai). Tipe kesalahan yang tingkatnya tinggi adalah jika sistem aplikasi (dan program – programnya) tidak dibuat sesuai dengan kebutuhan pemakai *(user).*

Pengendalian proses merupakan bentuk pengendalian yang diterapkan setelah berada pada sistem aplikasi komputer. Menurut IAI (SA341, par.08) pengendalian ini didesain untuk pengendalian ini dirancang 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 pengelolaan dapat diidentifikasi dan dikoreksi secara tepat waktu.

2.4.4.4. Pengendalian Keluaran *(Output Controls)*

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

a. Rekonsiliasi keluaran dengan masukan dan pengelolaan, rekonsiliasi dilakukan dengan cara membandingkan hasil keluaran dari sistem dengan dokumen asal.

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

c. Pendistribusian keluaran, pengendalian ini dirancang untuk memastikan bahwa keluaran didistribusikan kepada pihak yang berhak dilakukan secara tepat waktu dan hanya keluaran yang diperlukan saja yang di distribusikan.

2.5. CobIT

Menurut *ICASA (information systems audit and control associaton)* CobIT *(control objective for information and related technology)* adalah sebuah alat yang diterima secara internasional yang diorganisir menjadi sebuah kerangka kerja *(framework)* yang dapat digunakan para eksklusif untuk memastikan bahwa teknologi informasi yang mereka miliki membantu mereka dalam mencapai sasaran dan tujuan.

CobIT memastikan bahwa teknologi informasi bekerja secara efektif memungkinkan untuk memaksimalkan sesiko TI yang terkait dan memastikan keuntungan dari investasi ekonomi.

CobIT disusun oleh *The IT Governance Institute (ITG)* 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* 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 meberikan informasi yang dibutuhkan perusahaan untuk mencapai tujuannya, investasi yang diperlukan perusahaan, serta mengelola dan mengendalikan sumber daya IT mengunakan seperangkat proses yang terstruktur untuk memberikan layanan informasi yang dibutuhkan perusahaan.

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

Menurut CobIT, untuk memenuhi tujun bisnis 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, benar, konsisten, dan dapat dipercaya.

2. *Effeciency* (Efisiensi)

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

3. *Confidentially* (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 ekspetasi.

5. *Avaibility* (Ketersediaan)

Fokus terhadap ketersediaan informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun dimasa 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 / kontak untuk proses bisnis.

7. *Reliability* (Handal)

Pemberian informasi yang tepat bagi management 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 pada pengukuran *(measurement driven)*. CobIT *Framework* 4.1 terdiri dari 34 *high level control objectives* dan kemudian mengelompokan proses tersebut menjadi 4 *domain*, keempat *domain* tersebut adalah *planning and organization (10 process), acquisition and implementation (7 process), delivery and support (13 process),* dan *monitoring and evaluation (4 process),* yang mencakup :

1. *Plant and Organize* (Perencanaan dan Organisir)

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

a. Apakah proses TI dan stategi bisnis telah sesuai?

b. Apakah perusahaan mencapai pengunaan yang optimum dengan sumber dayanya?

c. apakah setiap karyawan diperusahaan memahami tujuan TI?

d. Apakah resiko TI dipahami dan di kelolah?

e. Apakah kualitas sistem TI sesuai dengan kebutuhan bisnis

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

Untuk merealisasikan strategi TI, perlu dilakukan pengidentifikasian, pengembangan dan perolehan solusi TI, sesuai dengan yang akan diimplementasikan dan diintegrasikan kedalam proses bisnis. Domain ini meliputi pernyataan – pernyataan sebagai berikut:

a. Apakah proyek baru berkemungkinan 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 menganggu operasi bisnis yang sedang berjalan?

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

Domain ini berfokus terhadap penyampaian jasa yang sesunguhnya diperlukan, termasuk penyediaan layanan, management keamanan dan kontinuitasnya, jasa dukungan kepada penguna dan management data dan fasilitas operasi. Domain ini meliputi pertanyaan – pertanyaan sebagai berikut:

a. Apakah jasa TI yang disampaikan sejalan dengan priotitas bisnis?

b. Apakah biaya TI teroptimalisasi?

c. Apakah sistem TI 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 management 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 management memastikan bahwa *internal control* efektif dan efisien?

c. Dapatkah kinerja TI dihubungkan dengan tujuan perusahaan?

d. Apakah terdapat control demi kerahasiaan, integritas dan ketersediaan yang cukup baik terhadap keamanan informasi?

2.5.2. Manfaat penerapan CobIT

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

a. Pengunaan bahasa yang umum bagi para eksekutif, management dan profesional TI.

b. Pemahaman yang lebih baik tentang bagaimana bisnis dan TI dapat bekerja sama untuk keberhasilan pengiriman inisiatif TI.

c. Peningkatan efesiensi dan optimalisasi biaya.

d. Mengurangi resiko operasional.

e. Pengembangan kebijakan yang jelas.

f. Audit yang lebih efisien dan sukses.

g. Kepemilikan dan tangguna 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), diantaranya:

a. Skala 0 – *Not Existance*

perusahaan tidak menyadari pentingnya membuat perencanaan strategis dibidang 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 dibidang teknologi informasi. Namun, tidak ada proses yang distandarisasi, perencanaan, perancangan dan management masih belum teroganisir dengan baik. Dalam skala ini keperluan untuk dijadikan tamuan, 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 terorganisir.

f. Skala 5 – *Optimised*

Best Prectices (pedoman terbaik) telah diikuti dan di otomatisasi pada sistem berdasarkan proses yang terencana, terorganisir dan mengunakan metodologi yang tepat.

2.6. Database

2.6.1. Pengertian *Database*

Menurut Connolly, dan Begg (2010), Database ada

lah logikal data yang saling terhubung dan dirancang untuk memenuhi kebutuhan informasi dari suatu organisasi. Database digunakandalam kehidupan sehari-hari baik secara sadar maupun tidak sadar, contoh database yang sering kita gunakan dalam kehidupan sehari-hari yaitu:

1. Pembayaran kartu kredit
2. Pembayaran liburan pada agen travel
3. Pembayaran belanja di supermarket
4. Mencari buku diperpustakaan
5. Peminjaman DVD
6. Penggunaaan internet.

2.6.2 Pengertian DBMS

Menurut Connolly, dan Begg (2010,p66), Database Management

System adalah sistem software yang memungkinkan pengguna untuk mendefinisikan, membuat, memelihara, dan kontrol akses ke database. DBMS adalah software yang berinteraksi dengan program aplikasi dan 11 pengguna database Biasanya DBMS menyediakan fasilitas sebagai berikut :

1. DDL (Data Definition Language)

DDL memungkinkan pengguna untuk menentukan tipe data dan struktur dan kendala pada data yang akan disimpan dalam database.

2.DML(Data ManipulationLanguage)

Ini memungkinkan pengguna untuk memasukkan, update, menghapus dan mengambil data dari database biasanya meskipun memanipulasi data bahasa (DML).

3. Memberikan akses kontrol ke database:

1. Keamanan sistem: yang mencegah pengguna yang tidak berhak mengakses database.
2. Integritas system : yang menjaga konsistensi data yang tersimpan.
3. Concurrency control system : yang memungkinkan berbagi akses database.
4. Pemulihan sistem control: yang mengembalikan database ke keadaan yang konsisten sebelumnya setelah perangkat keras atau kegagalan software.
5. User-diakses katalog, yang berisi deskripsi dari data dalam database.