2.1 Pengendalian Internal

2.1.1 Tujuan Pengendalian Internal

According to Cascarino (2007, p59), overall, internal control objectives in detail are mentioned below, which are:

a. Reliability and Integrity of Information

“If management cannot trust the reliability and integrity of the information held and processed within the IS, then all information must be deemed suspect and, in some cases, this may be more detrimental to the organization than a loss of information systems.”

b. Compliance with Policies, Plans, Procedures, Laws, and Regulation

“Laws and Regulation are imposed externally and must be complied with. Inadequate information systems may lead to the organization inadvertently breaching the laws of the country with result of losses in terms of fines, penalties, and possibly imprisonment for corporate officers.

The organization’s internal policies, plans, and procedures are designed to ensures planned, systematic, and orderly operation. From time to time the manager may be required to evaluate the adequacy of such policies, plans, and procedures since the nature of the business may have changed, risk may have to be reassessed and control objectives re-prioritized.”
c. Safeguarding of Assets

“Loss of assets is typically one of the most visible risk an organization can face and typically these lead to the implementation of the most visible controls, such as locks on doors, safes, security guards and so forth. In an IS-dependent organization asset control may also include non-tangibles such as dual custody, segregation of duties, and computer authentication techniques. Few organizations would be in position to declare the information held as a corporate asset on the balance sheet. Nevertheless, the corporate information warehouse may be the largest asset the organization can claim if leveraged appropriately. In addition, for many organizations the financial records held within the computer systems are indeed actual assets in that, for example, the total value of inventory is commonly taken to be whatever the computer system says the inventory value is. Similarly, debtors and creditors valuations are largely based upon the information contained within the appropriate computer systems.”

d. Effectiveness and Efficiency of Operations

“Effectiveness involves the achievement of established objectives and should be the ultimate focus of all operations and controls. Many information systems, at the time of the original design, were focused upon achieving the corporate objectives. Over time these objectives may have changed and the information system may become counter-productive to achieving those objectives. Computer systems therefore required constant monitoring as to their alignment with corporate strategic directions and intent.”
Dengan demikian, tujuan dari pengendalian internal adalah menjaga kehandalan dan integritas informasi, melindungi aset perusahaan, meningkatkan efisiensi dan efektivitas operasi, serta pemenuhan terhadap kebijakan, prosedur, hukum yang berlaku. Maksudnya adalah informasi yang digunakan oleh perusahaan harus terjamin kehandalan dan integritasnya karena informasi memegang peranan sangat penting untuk kelangsungan sistem informasi yang dijalankan perusahaan. Selain itu, pengendalian internal juga membantu perusahaan dalam melindungi segala aset yang ada dalam perusahaan, baik aset fisik maupun aset sistem informasi.

2.1.2 Tipe Pengendalian Internal

According to Cascarino (2007, p61), types of internal control are classified into five types:

a. Preventative Controls

“Which occur before the fact but can never be 100% effective and therefore cannot be wholly relied upon. These could include controls such as restriction on users, requirement for password, and separate authorization of transaction.”

b. Detective Controls

“Which detect irregularities after occurrence and may be cheaper than checking every transaction with a preventative control. Such controls could include effective use of audit trails and the use of exception reports.”

c. Corrective Controls

“Ensures the correction of problem identified by detective controls and normally require human intervention within the IS. Control in this area may include such processes as disaster recovery plan and transaction reversal capabilities. Corrective
controls are themselves highly error-prone because they occur in unusual circumstances and typically require are human decision to be made, and an action decided upon and implemented. At each stage in the process a subsequent error will have a multiplier effect and may compound the original mistake.”

d. Directive Controls

“Are designed to produce positive result and encourage acceptable behavior. They do not themselves prevent undesirable behavior and are normally used where there is human discretion in a situation. Thus, informing all users of personal computers that it is their responsibility to ensure adequate back ups are taken and stored appropriately does not, of itself, enforce compliance. Nevertheless, such a directives control can be monitored and action taken where the control is breached.”

e. Compensating Controls

“Can be seen to exist where a weakness in one control maybe compensated by a control elsewhere. There are used to limit risk exposure and may trap unwary evaluator. This is particularly true where the auditor are faced with complex integrated systems and the control structures involves a mixture of system-driven and human controls scattered over a variety of operational areas.”

Tipe-tipe pengendalian internal dapat diklasifikasikan menjadi 5, pengendalian pencegahan, pengendalian deteksi, pengendalian korektif, pengendalian direktif, dan pengendalian kompensasi. Pengendalian pencegahan dilakukan sebelum kejadian berlangsung atau terjadi. Pengendalian deteksi dilakukan untuk mendeksi penyimpangan setelah kejadian berlangsung karena lebih murah daripada memeriksa setiap transaksi yang ada dalam perusahaan. Pengendalian korektif berfokus pada memastikan koreksi
dari masalah yang telah teridentifikasi sebelumnya. Pengendalian direktif dilakukan di tempat ditemukannya masalah atau resiko tersebut ditemukan. Sedangkan pengendalian kompensasi maksudnya adalah ada kelemahan dalam satu pengendalian yang mungkin dikompensasi oleh pengendalian di tempat lain.

### 2.1.3 Fungsi Internal Auditor

Menurut Hunton et al., dalam Basalamah (2011, p17), seorang auditor TI sebaiknya mampu melakukan pekerjaan-kerjaan sebagai berikut:

1. Mengevaluasi pengendalian atas aplikasi-aplikasi tertentu, yang mencakup analisis terhadap risiko dan pengendalian atas aplikasi-aplikasi seperti e-business, sistem perencanaan sumber daya perusahaan (Enterprise Resource Planning atau ERP) atau program-program lainnya.

2. Memberikan asersi (assurance) atas proses-proses tertentu, seperti audit dengan prosedur-prosedur tertentu yang disepakati bersama dengan auditan mengenai lingkup asersi.

3. Memberikan asersi atas aktivitas pengolahan data pihak ketiga, dengan tujuan untuk memberikan asersi bagi pihak lain yang memerlukan informasi mengenai aktivitas pengolahan data yang dilakukan oleh pihak ketiga tersebut.

4. Pengujian penetrasi, yaitu upaya untuk mengakses sumber daya informasi guna menemukan kelemahan-kelemahan yang ada dalam pengolahan data tersebut.

5. Memberikan dukungan atas pekerjaan audit keuangan, yang mencakup evaluasi atas risiko dan pengendalian TI yang dapat mempengaruhi kehandalan sistem pelaporan keuangan.
6. Mencari kecurangan yang berbasis TI, yaitu menginvestigasi catatan-catatan komputer dalam investigasi kecurangan.

2.2 Audit Sistem Informasi

2.2.1 Pengertian Audit Sistem Informasi

Menurut Basalamah (2011, p16), audit sistem informasi adalah suatu proses pengumpulan dan penilaian bukti untuk menentukan apakah suatu sistem komputer melindungi aktiva, mempertahankan integritas data, serta memungkinkan bagi tercapainya tujuan organisasi secara efektif dan penggunaan sumber daya secara efisien.


Audit yang dilakukan dengan mengumpulkan dan mengevaluasi bukti untuk menentukan apakah sistem informasi dan sumber daya terkait cukup melindungi asset serta memelihara data dan integritas sistem, penyediaan informasi yang relevan dan dapat diandalkan, pencapaian tujuan organisasi secara efektif, penggunaan sumber daya secara efisien. Audit Sistem Informasi mempunyai dampak pada kontrol internal yang menyediakan kepastian yang layak bahwa bisnis, operasional dan objektif kontrol dipenuhi serta kejadian yang tidak diinginkan akan dapat dicegah, atau dideteksi dan dikoreksi dengan tepat waktu.
2.2.2 Manfaat Audit Sistem Informasi

According to Dube and Gulati (2005, p12), the importance of control in an organization cannot be ignored at any given point of time. IS Auditors are regarded as control advocates in the entire lifecycle of the software and hardware, auditors perform important duties, which benefit the organization in several ways. Some of the benefits organizations receive are:

1. **Mapping business control with IT application**

   An IS auditor can help the organization in ensuring that the necessary business controls are mapped into the application control. Whether the IS auditor should be involved at the project stage of the application or not is a matter of debate, but from the perspective of control it is advisable to involve the internal auditor at the project stage. This way, he/she can help in ensuring that necessary controls are built into the system at the development stage itself. It must, however, be ensured that the same auditor is not allowed to conduct a post implementation review/audit of that application.

2. **Business Process Re-engineering (BPR)**

   The basic difference between automation and computerization is that while in the case of automation, the existing manual process is automated using computers, in the case of computerization; the manual process is re-engineered and then automated using computers. In the latter case, while the absorption of IT is more effectively achieved, there is every likelihood that some basic control may be missed or forgotten in the computerization process, which can have serious ramifications for the organization. For this reason, the IS auditor should be a part of the BPR
exercise to ensure that the basic controls required for the business exist in the re-engineered processes.

3. The IT security policy

An IS auditor due to extensive engagement with an organization, is able to say which parts of the policy are complied with and can also offer suggestions on improving compliance or making suitable changes to the policy. The IS auditor also comes across systems or situations that may not adequately addressed in the policy and offers guidance on the areas. Proactive IS audit function can make all the difference between an effective IT security policy and control perspective, an organization without an IT security policy would be considered relatively more secure than an organization with a dormant, non-implementable, IT security policy.

4. Security awareness

An effective IS auditor helps increase levels of security awareness and compliance with security measures among IT users. This also provides motivation to the security officers and system administrators to their jobs effectively. Consequently, business continuity preparedness also remains at a high level.

5. Better Return of Investment (ROI)

IS auditors today, are concerned not just with security and controls, but also with IT governance, which includes performance measurement, value for IT investments, and alignment of IT and business. The profession of IS audit is gradually being aligned to the profession of IT Governance. Therefore, and IS auditor for an organization helps in effective and efficient use of IT for fulfilling business objectives. Thus, management concerns, like ROI, are taken care of by IS auditor while prescribing IT contracts.
6. Risk management

The domain of IS auditing is gradually moving towards encompassing the domain of risk management and an internal IS auditor is increasingly being seen as a risk management professional particularly in the area of operational risk. Effective risk management is vital for an enterprise’s success and therefore, the role of the IS auditor is seen as crucial.

Dari kutipan di atas, dapat disimpulkan bahwa manfaat audit sistem informasi adalah dapat membantu organisasi dalam memastikan pengenalan bisnis yang diperlukan untuk memetakan pengendalian aplikasi. Selain itu, audit sistem informasi juga dapat melihat perbedaan antara kebijakan TI yang efektif dan perspektif kontrol serta sebagai manajemen resiko dalam suatu perusahaan.

2.2.3 Metode Audit Sistem Informasi

Menurut Sarno (2009, p33), metodologi dalam Audit SI terdiri atas beberapa tahapan antara lain:

1. Analisis kondisi eksisting

Merupakan aktivitas dalam memahami kondisi saat ini dari perusahaan yang diaudit termasuk hukum dan regulasi yang berpengaruh terhadap operasional proses bisnis.

2. Penentuan tingkat risiko

Dengan mengklarifikasikan proses bisnis yang tingkat risikonya tinggi (proses bisnis utama) maupun proses bisnis pendukung. Hasil penentuan tingkat risiko tersebut kemudian dijadikan sebagai bahan dalam penyusunan ruang lingkup pelaksanaan audit yang diarahkan kepada proses bisnis yang didukung oleh TI.
3. Pelaksanaan audit SI

Dengan mengacu kerangka kerja COBIT yang akan didahului dengan proses penentuan ruang lingkup dan tujuan audit (scope dan objective) berdasarkan hasil penentuan tingkat risiko pada tahapan sebelumnya.

4. Penentuan rekomendasi

Berisi laporan dari hasil audit yang dilakukan.

2.2.4 Prosedur Audit Sistem Informasi

According to Cannon (2011, p137), the audit program policy informs everyone that the overall auditing program is important. We use standards as a uniform rule of measurement, and each standard is supported by a set of procedures. The audit program is run in the same manner as an ISO 9001 quality management program. Every auditor needs to ensure that the following procedures are in the toolkit: a) Audit planning; b) Scheduling audits; c) Assuring competence of auditors and audit team leaders; d) Selecting appropriate audit teams; e) Assigning roles and responsibilities; f) Conducting audits; g) Maintaining audit program(me) records; h) Monitoring performance and effectiveness; i) Complaint tracking; j) Reporting to top management an overall achievements

Jadi dapat disimpulkan bahwa prosedur audit meliputi beberapa kegiatan, yaitu perencanaan audit, penjadwalan audit, memastikan kompetensi dari auditor dan pimpinan tim audit, pemilihan tim audit yang sesuai, menetapkan peran serta tanggung jawab, melakukan audit, mempertahankan catatan program audit, memantau kinerja dan
efektivitas, pelacakan pengaduan, serta melaporkan kepada manajemen puncak mengenai prestasi keseluruhan.

2.2.5 Teknik Audit Sistem Informasi

Menurut Restianto dan Bawono (2011, p20), audit sistem informasi dapat dilaksanakan dengan salah satu dari tiga teknik pendekatan, yaitu:

1. Audit di Sekitar Komputer (Audit Around the Computer)

   Auditor menelaah struktur pengendalian internal, menguji transaksi dan prosedur verifikasi saldo akun dengan cara yang sama seperti dalam sistem manual/bukan teknologi informasi. Auditor tidak menguji pengendalian pada sistem informasi tetapi sebatas pada masukan dan keluaran sistem informasi. Berdasarkan penilaian pada kualitas masukan dan keluaran sistem tersebut, auditor mengambil kesimpulan tentang kualitas pemrosesan data dalam sistem. Oleh karena itu, auditor harus mendapatkan dokumen sumber dan dokumen keluaran yang cukup dalam bentuk cetakan (hardcopy) atau dalam bentuk yang mudah dibaca oleh pemakai. Dalam pendekatan ini, sistem komputer dapat diibaratkan sebagai sebuah kotak hitam (black box).

   Keunggulan audit di sekitar komputer adalah kesederhanaannya sehingga auditor yang memiliki pengetahuan minimal di bidang komputer dapat terlatih dengan mudah untuk melaksanakan audit. Sementara itu, kelemahan metode ini adalah jika terjadi perubahan lingkungan organisasi, ada kemungkinan bahwa sistem itupun akan berubah sehingga auditor tidak dapat menilai dan menelaah sistem yang baik. Oleh karena itu, auditor harus dapat menilai kemampuan sistem informasi dalam menyesuaikan diri dengan perubahan lingkungan.
2. Audit Melalui Komputer (*Audit Through the Computer*)

Pendekatan ini digunakan untuk melakukan audit pada lingkungan sistem yang kompleks (*complex automated processing systems*). Dalam pendekatan ini, auditor menggunakan komputer untuk menguji logika dan pengendalian yang ada dalam sistem komputer dan keluaran yang dihasilkan oleh sistem. Besar kecilnya peranan komputer dalam audit tergantung pada kompleksitas dari sistem komputer yang diaudit. Dalam pendekatan ini, fokus perhatian auditor langsung tertuju pada operasi pemrosesan data di dalam sistem komputer.

Keunggulan pendekatan audit melalui komputer adalah sebagai berikut:

a. Auditor akan memperoleh bukti-bukti audit yang memadai.

b. Auditor lebih efektif dalam menguji sistem komputer.

c. Auditor akan memiliki keyakinan yang lebih memadai terhadap kualitas auditnya.

d. Auditor dapat menilai kemampuan sistem komputer dalam menghadapi perubahan lingkungan.

Sedangkan kelemahan dari pendekatan ini adalah dibutuhkannya biaya yang relatif besar dan dibutuhkannya tenaga ahli yang terampil, tidak hanya di bidang auditing, tetapi di bidang komputer, pengembangan sistem, komunikasi data, dan bidang lain yang terkait dengan teknologi informasi.

3. Audit dengan Komputer (*Audit With the Computer*)

Pada pendekatan audit dengan komputer, audit dilakukan dengan menggunakan komputer dan perangkat lunak audit untuk menjalankan prosedur audit secara otomatis. Pendekatan ini menggunakan beberapa jenis *Computer Assisted Audit Techniques* (CAAT), seperti *System Control Audit Review File* (SCARF) dan...
pemotretan (*snapshot*). Pendekatan audit dengan komputer sangat bermanfaat dalam pengujian substantif atas file-file basis data (*database*).

Perangkat lunak audit dapat digolongkan menjadi dua jenis, yaitu perangkat lunak audit terspesialisasi (*Specialized Audit Software* [SAS]) dan perangkat lunak audit tergeneralisasi (*Generalized Audit Software* [GAS]).

a. *Specialized Audit Software* (SAS)

SAS merupakan program khusus yang dirancang oleh auditor agar sesuai dengan situasi audit tertentu. SAS jarang digunakan karena penyusunannya membutuhkan waktu dan biaya yang relatif tinggi. Selain itu, keahlian auditor di bidang komputer juga diperlukan, meskipun auditor tidak harus membuat sendiri aplikasi SAS karena dapat diserahkan pada pemrogram komputer, namun paling tidak auditor harus mengetahui konsep pemrograman secara umum.

b. *Generalized Audit Software* (GAS)

Perangkat lunak audit tergeneralisasi atau umum adalah program aplikasi komputer yang dapat melakukan berbagai macam fungsi pemrosesan data atau manipulasi data. GAS dapat digunakan oleh auditor untuk berbagai penugasan audit yang berbeda-beda. Saat ini auditor tidak harus membuat sendiri aplikasi GAS karena telah banyak aplikasi GAS yang dapat dibeli dari *vendor* atau pengembang perangkat lunak.

2.2.6 **Perangkat Lunak Audit Sistem Informasi**


Perangkat lunak penganalisis data umumnya disebut sebagai Perangkat Lunak Audit dan yang paling sering digunakan diantara empat klasifikasi CAAT. Beberapa fitur didalam perangkat lunak tersebut antara lain: kueri data, stratifikasi data, ekstraksi sampel serta perhitungan dan analisis statistik. Adapun prasyarat penggunaan perangkat lunak tersebut adalah koneksi data dan akses terhadap data, pengetahuan akan aplikasi dan data serta keahlian auditan dan pengidentifikasi kontrol yang terkait dengan aplikasi dan data (Sayana, Using CAATs to Support IS Audit, 2003).

Keberadaan Perangkat Lunak Audit akan membantu pengaudit SI dalam melakukan uji secara substantif (substantive test) sehingga mampu menyediakan kepastian yang lebih menyeluruh atau penemuan kesalahan yang lebih tepat selama pelaksanaan audit. Lebih jauh lagi, pelaksanaan audit dapat dilakukan dengan biaya dan tenaga yang minimal dengan jaminan keakuratan yang tinggi karena dilakukan secara komputerisasi.

Dengan demikian, manfaat dari penggunaan perangkat lunak tersebut adalah uji yang dilakukan dapat lebih cermat terutama yang berkaitan dengan data transaksi yang besar. Jika audit untuk menguji data tersebut dilakukan secara manual akan membutuhkan waktu yang lama dan tenaga yang besar dengan tingkat kesalahan yang tinggi. Selain itu, perangkat lunak tersebut menyediakan tampilan yang user friendly serta fitur-fitur seperti: penyimpanan catatan uji (log) sehingga dapat ditinjau oleh pihak manajemen serta penggunaan fungsi untuk meningkatkan kecepatan dan efisiensi audit.
2.2.7 Tahapan Evaluasi Audit Sistem Informasi

Menurut Sarno (2009, p151), tujuan tahapan evaluasi audit sistem informasi adalah untuk mendapatkan prosedur tertulis dan memperkirakan jika prosedur yang ada telah menghasilkan struktur kontrol yang efektif.

Output dari tahapan evaluasi ini adalah bahwa pengaudit Sistem Informasi seharusnya mampu:

a. Mengevaluasi hukum, regulasi dan kriteria organisasi sebagai bahan yang dapat digunakan untuk penilaian/evaluasi kepatutan prosedur.

b. Mengevaluasi *compensating control* yang digunakan untuk memperkuat prosedur yang lemah.

c. Menyimpulkan temuan *(findings)* berdasarkan penilaian kepatutan yang dilakukan terhadap prosedur tertulis maupun standar pengelolaan. Proses TI yang berlangsung, *compensating control* yang mendukung proses, maupun pemisahan tanggung jawab akan pengelolaan proses terkait.

2.2.8 Standar Audit Sistem Informasi

Standar audit merupakan pedoman bagi auditor dalam menjalankan tanggung jawab profesionalnya. Standar-standar ini meliputi pertimbangan mengenai kualitas profesional mereka, seperti keahlian dan independensi, persyaratan pelaporan dan bahan bukti. Dalam audit sistem informasi, penulis menggunakan standar COBIT (*Control Objectives for Information and related Technology*) yang dikembangkan oleh *Information Technology Governance Institute* (ITGI) kemudian dipublikasikan oleh ISACA (*Information Systems Audit and Control Association*). ISACA merupakan sebuah asosiasi profesional dalam audit sistem informasi, pengendalian, keamanan dan
governance. ISACA yang beranggotakan auditor sistem informasi internasional mempunyai fungsi sebagai sumber informasi, pihak yang memberikan panduan-panduan praktek bagi auditor sistem informasi serta menyediakan standar, panduan (guidelines), dan prosedur dalam hal audit, pengendalian dan keamanan sistem informasi bagi para profesional auditor sistem informasi di seluruh dunia.

2.3 Laporan Audit Sistem Informasi

2.3.1 Ruang Lingkup Audit Sistem Informasi

Menurut Sarno (2009, p192), ruang lingkup audit sistem informasi merupakan sekumpulan aktivitas yang terdiri dari pendefinisian tujuan audit (audit objective), sifat, dan isi dari prosedur audit yang akan diselenggarakan, periode waktu serta aktivitas terkait yang tidak diaudit dengan tujuan untuk melukiskan batasan audit.

2.3.2 Bukti Audit Sistem Informasi

Menurut Sarno (2009, p149), bukti audit adalah informasi yang dikumpulkan oleh pengaudit dalam pelaksanaan audit sistem informasi. Bukti akan relevan jika berkaitan dengan tujuan audit yang memiliki hubungan logis terhadap temuan (findings) dan kesimpulan yang digunakan untuk mendukung temuan.

Beberapa teknik yang dapat dilakukan dalam mengumpulkan bukti-bukti audit sistem informasi antara lain:

a. Peninjauan terhadap struktur organisasi TI.
b. Peninjauan terhadap kebijakan dan prosedur yang terkait dengan TI.
c. Peninjauan terhadap standar yang terkait dengan TI.
d. Peninjauan dokumentasi yang terkait dengan pengelolaan SI.
e. Wawancara kepada personel yang tepat.

f. Pengobservasian proses dan kinerja karyawan.

2.3.3 Temuan dan Rekomendasi Audit Sistem Informasi

Menurut Sarno (2009, p194), temuan adalah pernyataan yang berhubungan dengan kondisi aktual perusahaan. Temuan dalam audit muncul setelah dilakukan perbandingan antara apa yang seharusnya dilakukan dengan proses yang berlangsung di perusahaan.

Sedangkan, rekomendasi adalah tindakan yang dilakukan untuk memberikan opini berdasarkan hasil pelaksanaan audit mengenai perbaikan kondisi eksisting atau meningkatkan operasional di perusahaan. (Sarno, p191)

Menurut Gallegos dalam Sarno (2009, p51) aktivitas audit seharusnya menghasilkan kesimpulan dan temuan yang akan mengarahkan pada rekomendasi yang mencerminkan penuhan terhadap tujuan objektif yang berbasis waktu, kinerja dan biaya. Hal tersebut seharusnya disertai dengan laporan awal yang menggambarkan temuan awal dalam aktivitas audit sebelum disusun ke dalam laporan akhir sehingga pihak manajemen mendapatkan gambaran mengenai kondisi eksisting perusahaannya serta gambaran rekomendasi yang akan diberikan oleh pengaudit SI (Gallegos, *IT Audit Report and Follow-up: Methods and Techniques for Communicating Audit Findings and Recommendation*, 2002)

2.3.4 Dokumentasi Audit Sistem Informasi

Menurut Sarno (2009, p50), agar dapat digunakan, dokumentasi audit seharusnya mencakup kriteria-kriteria sebagai berikut:
a. Seluruh dokumentasi seharusnya terkait dengan tujuan pelaksanaan audit.

b. Dokumentasi dapat berupa poin catatan dalam wawancara yang dengan jelas menyatakan topik diskusi, pihak yang diwawancara, posisi dan jabatan serta waktu dan tempat dilakukannya wawancara.

c. Dokumentasi dapat berupa catatan observasi saat pengaudit melihat kinerja yang mungkin mencakup tempat dan waktu, alasan dilakukan observasi dan pihak yang terlibat.

d. Dokumentasi dapat berupa laporan dan data yang dikumpulkan dari sistem secara langsung oleh pengaudit atau disediakan oleh staf perusahaan. Pengaudit SI perlu memastikan bahwa laporan tersebut jelas sumber, waktu dan cakupan informasinya.

e. Sering ditemui bahwa pengaudit SI bekerja dengan template kosong dan mengisinya saat pelaksanaan audit. Untuk meningkatkan dokumentasi tersebut pengaudit kemudian mengisikan informasi-informasi seperti yang telah dijelaskan sebelumnya.

f. Pengaudit SI dapat menambahkan komentar dan klarifikasi, keraguan dan kebutuhan akan informasi tambahan dalam penyajian yang berbeda. Pengaudit seharusnya kembali ke bagian tersebut dan memberikan informasi bagaimana dan dimana hal tersebut dipenuhi.

g. Laporan draft dan final dari audit seharusnya mengacu pada hasil dokumentasi audit yang disusun.

2.3.5 Laporan Hasil Audit Sistem Informasi

Menurut Sarno (2009, p166), laporan hasil audit merupakan hasil akhir dari pekerjaan audit SI yang berisikan temuan dan rekomendasi kepada manajemen.
Hal yang utama dari hasil audit adalah kesimpulan dan opini terhadap kelengkapan terhadap kontrol yang telah diperiksa, detail dari temuan dan rekomendasi yang diberikan untuk perbaikan proses.

Dengan demikian, Laporan Audit Sistem Informasi sebaiknya mencakup:

a. Perencanaan dan persiapan audit SI yang mencakup ruang lingkup dan tujuan audit (scope dan objective).

b. Kondisi eksisting sistem informasi.

c. Program audit SI yang dilakukan.

d. Langkah audit SI yang dilakukan dan bukti (evidence) audit SI yang dikumpulkan.

e. Temuan audit (findings) dan tingkat kedewasaan proses TI.

f. Kesimpulan dan hasil temuan.

g. Laporan-laporan terkait sebagai hasil dari pekerjaan audit SI.

h. Tinjauan pengawasan berupa rekomendasi untuk perbaikan berkelanjutan.

2.4 COBIT

2.4.1 Pengembangan COBIT

According to Boonen and Brand (2008, p21), The Control Objectives for Information and related Technology (COBIT), were developed started in 1994, with a first version published in 1996, and subsequent versions in 1998, 2000, and 2005. Originally, COBIT targeted auditors, end-users and management. In the current version of COBIT a clear shift is visible from a control framework toward an IT governance framework.
COBIT is a model for control of the IT environment. In developing COBIT, standards from different sources have been used, each covering a part of the information.

COBIT supports IT governance by providing a comprehensive description of the control objectives for IT processes and by offering the possibility of examining the maturity of these processes.

Hal tersebut mengartikan bahwa COBIT membantu dalam memahami, menilai, dan mengelola risiko bersama-sama dengan manfaat yang terkandung dengan informasi dan TI. COBIT memberi dan menyediakan instrumen tata kelola TI yang memungkinkan bagi manajer untuk menjembatani kesenjangan yang berhubungan
dengan pengendalian SI dan TI serta risiko bisnis, dan mengembangkan kebijakan yang jelas dan praktik yang baik untuk mengendalikan organisasi TI.

2.4.2 Sasaran COBIT

According to Brand and Boonen (2008, p23), the main target groups are described in the following paragraphs:

a. Managers

Within organizations managers are the ones that hold execute responsibility for operation of the operation of the enterprise. They need information in order to order to control the internal operations and to direct business processes. IT is an integral part of business operations. COBIT can help both business and IT managers to balance risk and control investment in an often unpredictable IT environment.

b. End-Users

Most organizations realize that having the right IT services is the responsibility of the business process owner. This is even the case when delivery of IT services is delegated to internal or external service providers. COBIT offers a framework to obtain assurance on the security and controls of IT services provided by internal or external parties.

c. Auditors

In order to provide independent assurance of the quality and applicability of controls, organizations employ auditors. Often an audit committee at the board or Top Management Level directs auditing. COBIT helps auditors to structure and substantiate their opinions and provides advice to management on how to improve internal controls.
d. **Business and IT Consultants**

New frameworks and methods, e.g. on IT governance often originate outside the enterprise. Business and IT consultants can bring this knowledge into the enterprise and thus provide advice to business and IT management on improving IT governance.

e. **IT Service Management Professionals**

In the IT service management community, Information Technology Infrastructure Library (ITIL) is the dominant framework. COBIT helps to further improve IT service management by providing a framework that covers the complete lifecycle of IT systems and services.

COBIT terutama ditujukan untuk manajemen, pengguna bisnis TI dan auditor. Gunanya, bisnis dan konsultan TI dapat memberikan manajemen dengan saran pada kontrol dan tata kelola manajemen layanan IT professional.

---

**Gambar 2.2  Possible Target Groups**

2.4.3 Kerangka Kerja COBIT

COBIT merupakan IT Governance Best Practices yang membantu auditor, manajemen, pengguna untuk menjembatani aspek bisnis, kebutuhan kontrol dan aspek teknis TI.

According to Anand (2006, p186), the COBIT framework provides a guidance for the IT controls that must be established and integrated to achieve financial reporting and disclosure objectives. The IT controls should consider the overall governance framework in supporting the quality and integrity of information.

According to Moeller (2009, p90), the COBIT framework is often described as a pentagon covering five broad and interconnected areas of internal controls. COBIT’s major areas of emphasis are arranged around the important core concept of IT governance:

a. Strategic Alignment

Efforts should be in place to align IT operations and activities with all other enterprise operations. These include establishing linkages between enterprise business operations and IT plans as well as processes for defining, maintaining, and validating quality and value relationships.

b. Value Delivery

Processes should be in place to ensure that IT and other operating units deliver promised benefits throughout a delivery cycle and with a strategy that optimizes costs while emphasizing the intrinsic values of IT and related activities.

c. Risk Management

Management, at all levels, should have a clear understanding of an enterprise’s appetite for risk, compliance requirements, and the impact of significant risks. Both
IT and other operations have their own and joint risk management responsibilities that may individually or jointly impact the entire enterprise.

d. Resource Management

With an emphasis on IT, there should be an optimal investment in, and the proper management of, critical IT resources, applications, information, infrastructure, and people. Effective IT governance depends on the optimization of knowledge and infrastructure.

e. Performance Measurement

Processes should be in place to track and monitor strategy implementation, project completions, resource usage, process performance, and service delivery. IT governance mechanisms should translate implementation strategies into actions and measurements to achieve these goals.

Jadi, kerangka COBIT sering digambarkan sebagai segilima yang mencakup lima bidang yang luas dan saling menghubungkan area pengendalian internal. Bidang utama COBIT dari penekanan yang diatur di sekitar inti penting dari tata kelola TI adalah Alignment Strategisc, nilai pengiriman, manajemen risiko, manajemen sumber daya dan pengukuran kinerja.
2.4.4 Hubungan antar komponen COBIT

According to Gelinas and Dull (2008, p247), IT resources must be managed by IT control process to ensure that an organization has the information it needs to achieve its objectives. COBIT thus supports IT governance by providing a framework to ensure that: a) IT is aligned with the business; b) IT enables the business and maximizes benefits; c) IT resources are used responsibly; d) IT risks are managed appropriately.

According to Moeller (2008, p122), IT processes and their supporting software applications and hardware devices are key activities in any modern enterprise today. Whether a small retail business, with a need to keep track of its inventory and pay employees, or an large enterprise, all need a wide set of interconnected and often complex IT processes that are closely tied to their business operations. (COBIT
component interrelationships) shows the relationship at a high level, with business processes providing the requirements to build and construct IT processes and IT then providing the information necessary to operate those business processes. All business processes and their supporting IT resources work in that relationship. IT cannot and certainly should not tell business operations what types of IT processes and systems they should consider implementing. In the very early days of IT systems, technical managers sometimes felt they had lots of answer and promoted systems solutions to their businesses, sometimes with very counterproductive results. However, this relationship has changed today and IT and business operations generally should have a close mutual relationship of shared requirements and information.

Dijelaskan bahwa sumber daya TI harus dikelola oleh proses pengendalian TI untuk memastikan bahwa suatu organisasi memiliki informasi yang dibutuhkan untuk mencapai tujuannya. Keterkaitan komponen COBIT menunjukkan hubungan dengan proses bisnis yang memberikan persyaratan untuk membangun proses TI, kemudian menyediakan informasi yang diperlukan untuk mengoperasikan proses bisnis tersebut. Semua proses bisnis dan sumber daya pendukung TI bekerja dalam hubungan keterkaitan komponen COBIT tersebut. Hal ini menunjukkan bahwa TI memiliki tanggung jawab atas serangkaian area proses terkait lainnya dan memiliki hubungan yang saling terkait antar satu dengan yang lainnya.
2.4.5 Empat Domain Proses Pengendalian TI

*According to Gelinas and Dull (2008, p251), there are four IT control processes, which are: 1) Plan and Organize; 2) Acquire and Implement; 3) Deliver and Support; and 4) Monitor and Evaluate.*
According to Brand and Boonen (2008, p28), IT Process in Domain Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate based on COBIT:

Gambar 2.5  *Four Boards IT Control Process Domain*

Sumber: *Accounting Information System* (2008, p251)
According to Gelinas and Dull (2008, p252), the definitions of each COBIT domains are:

1. **Plan and Organize Domain**

   Within the Plan and Organize domain are processes to develop the strategy and tactics for realizing an organization’s IT strategy. The overriding goal of these processes is to identify ways that IT can best contribute to the achievement of the organization’s objectives. After a strategic vision is set, management must communicate the vision to affected parties (inside and outside the organization) and
put in place the IT organization and technology infrastructure that enables that vision. These processes must identify and address external threats and internal and external IT requirements, and identify and take advantage of opportunities for strategic implementation of emerging information technology.

2. Acquire and Implement Domain

Processes within the Acquire and Implement domain are designed to identify, develop or acquire, and implement IT solutions, and integrate them into the business process. Once installed, procedures must also be in place to maintain and manage changes to existing systems. Failure to successfully execute these processes can lead to significant risks throughout the organization. For example, if we do not correctly determine the requirements for a new information system and see that those requirements are satisfied by the new system, the new system could cause us to violate accounting standards or perform calculations incorrectly that lead to incorrect financial reporting. Or we may not complete the development on time, putting us at a competitive disadvantage if our competition implements such a system first and within budget. Finally, should we had to develop proper controls for the new system, we could experience several risk, including erroneous financial reporting, fraud, and loss of resources.

3. Deliver and Support Domain

The Deliver and Support domain includes processes to deliver required IT services efficiently and effectively; ensure security and continuity of services; set up support services, including training; and ensure integrity of application data. Management wants to know that IT services are delivered in line with business priorities and in a cost-effective manner. Application programs and data must be available as needed,
and the integrity and confidentiality of data must be maintained. Computing resources that are lost, destroyed, or unavailability for use can lead to lost revenues as well as increased costs to correct problems that may have occurred. Finally, unauthorized use of the computing resources can lead to fraud and sanctions or violations of laws and regulations, such as those related to privacy.

4. Monitor and Evaluate Domain

Within the Monitor and Evaluate domain is a process to assess IT services for quality and to ensure compliance with control requirements. Monitoring may be performed as a self-assessment activity within IT, by an entity’s internal/IT audit group, or by an external organization such as a public accounting firm. Without the feedback provided by the monitoring process, the system of internal control is not complete.

Di dalam kerangka COBIT ada 4 domain yaitu Plan and Organize, Acquire and Implement, Deliver and Support dan Monitor and Evaluate. Plan and Organize adalah proses yang digunakan untuk mengembangkan strategi dan taktik untuk mewujudkan strategi organisasi TI. Tujuan utama dari proses ini adalah untuk mengidentifikasikan cara-cara yang terbaik agar TI dapat berkontribusi pada pencapaian tujuan organisasi. Acquire and Implement adalah proses yang dirancang untuk mengidentifikasi, mengembangkan atau memperoleh dan menerapkan solusi TI serta mengintergrasikannya ke dalam proses bisnis. Deliver and Support adalah proses yang diperlukan untuk memberikan layanan TI secara efektif dan efisien, menjamin keamanan dan kelangsungan layanan, mengatur dukungan layanan termasuk pelatihan dan
menjamin integritas data aplikasi. *Monitor and Evaluate* adalah suatu proses untuk menilai kualitas layanan TI dan memastikan kepatuhan dengan persyaratan kontrol.

**Proses Empat Domain COBIT**

![COBIT Processes Defined Within the Four Domains](image)

*Gambar 2.6  COBIT Processes Defined Within the Four Domains*

*Sumber: ITGI-COBIT 4.1th edition (2007, p26)*
2.5 Sistem Informasi Akuntansi

2.5.1 Jenis-Jenis Transaksi SIA

According to Jones and Rama (2006, p4), types of transaction in Accounting System Information are divided into three parts:

a. An acquisition (purchasing) cycle

“The process of purchasing and paying for goods or services.”

b. A conversion cycle

“The process of transforming acquired into goods and services.”

c. A revenue cycle

“The process of providing goods or services to customers and collecting cash”

Dari kutipan di atas dapat disimpulkan bahwa jenis-jenis transaksi Sistem Informasi Akuntansi ada 3, yaitu siklus akuisisi, siklus konversi, dan siklus pendapatan.

2.5.2 Penjualan dan Penerimaan Kas

According to Elder et.al (2010, p443) accounts and classes of transactions in the sales and collection cycle, which are: a) Sales (cash and sales on account); b) Cash receipts; c) Sales returns and allowances; d) Write off of uncollectible accounts; e)Estimate of bad debt expense.

Yang terdapat dalam akun dan kelas transaksi siklus penjualan adalah penjualan tunai dan kredit, penerimaan kas, retur dan potongan penjualan, penghapusan piutang tak tertagih dan perkiraan beban hutang.
2.5.2.1 Penjualan

Menurut Bodnar dalam Puspitawati dan Anggadini (2011, p166), penjualan adalah suatu usaha yang terpadu untuk mengembangkan rencana-rencana strategis yang diarahkan pada usaha pemuasan kebutuhan dan keinginan pembeeli, guna mendapatkan penjualan yang menghasilkan laba. Penjualan merupakan sumber hidup suatu perusahaan, karena dari penjualan dapat diperoleh laba serta suatu usaha memikat konsumen yang diusahakan untuk mengetahui daya tarik mereka sehingga dapat mengetahui hasil produk yang dihasilkan. Selain itu, aktivitas penjualan kredit biasanya dilakukan dengan cara pelanggan / customer melakukan order pemesanan penjualan terlebih dahulu.

Untuk lebih jelasnya prosedur penjualan kredit terdiri dari aktivitas:

a) Permintaan informasi persediaan barang/jasa; b) Penerimaan pesanan penjualan (order penjualan); c) Pengecekan persediaan dan harga; d) Persetujuan kredit; e) Pengambilan barang/persediaan; f) Pembuatan faktur penjualan; g) Pengiriman barang; h) Pencatatan transaksi; i) Penagihan.

According to Elder et.al (2010, p455) sales are accurately recorded. The accurate recording of sales transaction concern:

a. Shipping the amount of goods ordered

b. Accurately billing for the amount of goods shipped

c. Accurately recording the amount billed in the accounting records

Pencatatan yang akurat dari transaksi penjualan ada 3, antara lain: pengiriman jumlah barang yang dipesan, penagihan untuk jumlah barang yang dikirim secara akurat dan pencatatan jumlah tagihan dalam catatan akuntansi.
2.5.2.2 Penerimaan Kas

According to Weygant et al (2011, p348), types of receivable, which are:

1. **Account Receivable**

   *Are amounts owed by customers on account. They result from the sale of goods and services. Companies generally expect to collect these receivables within 30 to 60 days. Accounts receivable are the most significant type of claim held by a company.*

2. **Notes Receivable**

   *Are claims for which formal instruments of credit are issued as proof of the debt. A note receivable normally extends for time periods of 60-90 days or longer and requires the debtor to pay interest. Notes and accounts receivable that result from sales transactions are often called trade receivables.*

3. **Other Receivables**

   *Include non-trade receivables. Examples are interest receivable, loans to company officers, advances to employees, and income taxes refundable. These do not generally result from the operations of the business. Therefore companies generally classify and report them as separate items in the statement of financial position.*

Dapat disimpulkan bahwa ada 3 jenis piutang dalam Akuntansi adalah piutang, wesel tagih dan piutang lainnya.