



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

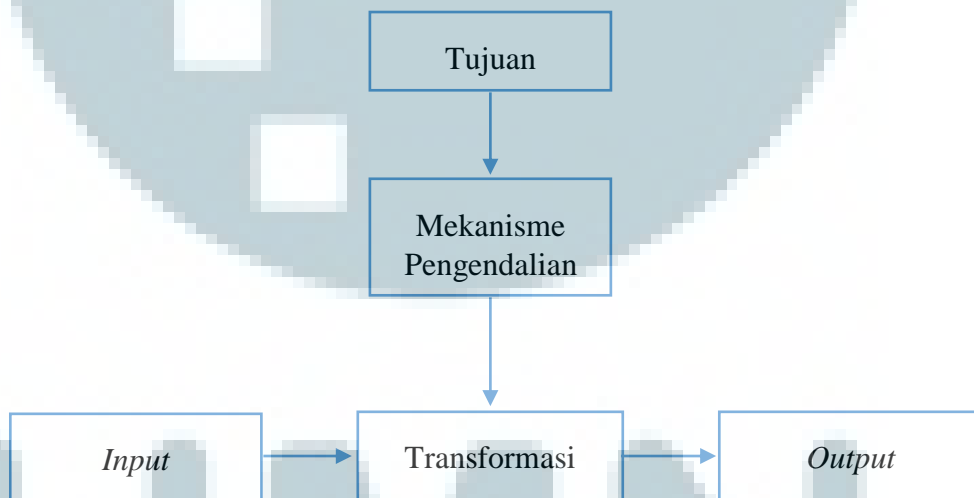
This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB II

LANDASAN TEORI

2.1 Pengertian Sistem

Sistem adalah suatu kumpulan yang kompleks dan saling berinteraksi apabila mereka menjadi satu kesatuan (Bennet, 2010). Menurut O'Brien dan Marakas (2009) berpendapat bahwa sistem diartikan sebagai sekumpulan komponen yang saling terkait dengan batasan jelas dan bekerjasama untuk mencapai tujuan dengan menerima input serta menghasilkan output dalam proses transformasi yang terorganisir.



Gambar 2.1 Komponen Sistem

Dari definisi di atas dapat disimpulkan bahwa sistem adalah sekumpulan komponen yang kompleks yang saling terkait dan berinteraksi untuk mencapai tujuan dengan menerima *input* dan menghasilkan *output* dengan batasan yang jelas.

Menurut Jogiyanto (2005) suatu sistem memiliki sifat-sifat tertentu, yaitu:

1. Komponen sistem

Suatu sistem terdiri dari sejumlah komponen yang saling berinteraksi, saling bekerja sama membentuk satu kesatuan.

2. Batas sistem

Batas sistem merupakan daerah yang membatasi antara suatu sistem dengan sistem yang lain atau dengan lingkungan luarnya.

3. Lingkungan luar sistem.

Lingkungan luar dari sistem adalah apapun di luar batas sistem yang mempengaruhi sistem.

4. Penghubung sistem

Penghubung (*interface*) merupakan media penghubung antara satu subsistem dengan subsiste lainnya.

5. Masukan sistem

Masukan sistem adalah energi yang dimasukkan ke dalam sistem. Masukan dapat berupa masukan perawatan (*maintenance input*) dan masukan sinyal (*signal input*).

6. Keluaran sistem

Keluaran sistem adalah hasil energi yang diolah dan diklasifikasikan menjadi keluaran yang berguna dan sisa pembuangan.

7. Pengolah sistem

Suatu sistem dapat mempunyai suatu bagian pengolah yang akan mengubah masukan menjadi keluaran.

8. Sasaran sistem

Sasaran sistem menentukan masukan yang dibutuhkan dan keluaran yang dihasilkan sistem. Suatu sistem dapat dikatakan berhasil jika dapat mencapai sasaran atau tujuannya.

2.2 Pengertian Informasi

Menurut Laudon (2010), informasi adalah data yang telah dibuat ke dalam bentuk yang memiliki arti berguna bagi manusia sedangkan menurut Whitten (2004) informasi adalah data yang telah diproses menjadi sebuah bentuk yang lebih berarti bagi seseorang.

Menurut Bodnar (2000) [1] informasi adalah data yang diolah sehingga dapat dijadikan dasar untuk mengambil keputusan yang tepat.

Dari pengertian di atas penulis dapat mengambil kesimpulan bahwa informasi adalah data yang sudah diproses menjadi suatu bentuk yang lebih berarti yang dapat digunakan sebagai dasar pengambilan keputusan.

2.3 Pengertian Sistem Informasi

Menurut Laudon (2010) sistem informasi merupakan komponen yang saling bekerjasama untuk mengumpulkan, mengolah, menyimpan, dan menyebarkan informasi untuk mendukung pengambilan keputusan, koordinasi, pengendalian, analisis masalah, dan visualisasi dalam sebuah organisasi.

Menurut O'Brien dan Marakas (2009) pengertian sistem informasi adalah kombinasi teratur dari orang-orang, perangkat keras, perangkat lunak, jaringan

komunikasi dan basis data yang mengumpulkan, mengubah, dan menyebarkan informasi dalam sebuah organisasi.

Sedangkan menurut Stair dan Reynolds (2010) mendefinisikan sistem informasi sebagai seperangkat elemen atau komponen yang saling terkait yang dikumpulkan (*input*), dimanupulasi (*process*), disimpan, disebarkan (*output*) untuk mencapai tujuan.

Dari pengertian di atas dapat disimpulkan bahwa sistem informasi adalah kombinasi teratur dari elemen-elemen yang saling terkait untuk mengumpulkan, mengolah, dan menyebarkan informasi untuk mencapai tujuan tertentu.

2.4 Audit

Setiap didirikannya perusahaan salah satu tujuannya pasti adalah memperoleh laba di samping dengan tujuan lainnya. Untuk mencapai tujuan dari perusahaan maka perusahaan harus memiliki strategi bisnis serta setiap proses bisnis atau tahapan bisnis yang akan dilaksanakan harus direncanakan, dianalisa, dan diteliti secara seksama terlebih dahulu oleh pada eksekutif manajemen. Seiring berjalannya waktu maka kebutuhan perusahaan juga akan bertambah, dengan berkembangnya perusahaan maka permasalahan yang akan dihadapkan oleh perusahaan tersebut juga akan semakin besar dan rumit. Tugas dan tanggung jawab dari manajemen akan semakin besar oleh karena itu manajemen memerlukan alat bantu untuk dapat mengendalikan kegiatan-

kegiatan yang ada. Audit merupakan salah satu alat bantu para manajemen untuk sebagai fungsi pengawasan dan pengendalian.

2.4.1 Pengertian Audit

Menurut Arens, et al (2010) audit adalah akumulasi dan evaluasi dari bukti mengenai informasi yang ada untuk menentukan dan melaporkan tingkatan dari korespondensi atau kesesuaian antara informasi dengan kriteria yang ada. Proses audit harus dilakukan oleh seorang yang kompeten dan independen.

Menurut Mulyadi (2004) audit adalah suatu proses sistematis untuk memperoleh dan mengevaluasi bukti secara objektif mengenai pertanyaan-pertanyaan tentang kegiatan dan kejadian ekonomi yang bertujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang sudah ditetapkan, serta penyampaian hasil-hasilnya kepada pemangku kepentingan.

Dari pengertian di atas maka dapat diperoleh pengertian audit adalah proses dari mengumpulkan dan mengevaluasi bukti-bukti yang ada pada perusahaan yang dilaksanakan oleh seorang yang kompeten dan independen serta bertujuan untuk menilai dan melaporkan hasil tingkatan kesesuaian antara bukti yang ada dengan kriteria yang sudah ditetapkan.

2.4.2 Tujuan Audit

Tujuan perusahaan melakukan audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai

pemenuhan terhadap standar yang terdefinisi (ISACA, 2006). Selain itu dengan dilakukannya audit perusahaan dapat mengetahui kelemahan atau hal-hal yang dapat menimbulkan risiko pada perusahaan, hasil dari audit ini adalah rekomendasi terhadap kondisi yang ada pada perusahaan pada saat itu agar bagaimana dapat meningkatkan kualitas dari perusahaannya serta tindakan apa saja yang dapat dilakukan perusahaan untuk mengatasi ataupun mencegah risiko yang ada.

2.5 Audit Sistem Informasi

2.5.1 Pengertian Audit Sistem Informasi

Menurut Weber (1999) audit sistem informasi adalah proses dari pengumpulan dan pengevaluasian bukti untuk menentukan apakah sistem informasi dapat melindungi aset, dan apakah teknologi informasi yang ada dapat memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efisien.

Menurut Gondodiyoto (2003) audit sistem informasi merupakan suatu cara evaluasi suatu sistem untuk mengetahui bagaimana tingkat kesesuaian antara aplikasi sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah suatu sistem informasi telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis, memiliki mekanisme pengamanan aset yang memadai, serta menjamin integritas data yang memadai.

Dari pengertian di atas dapat disimpulkan bahwa audit sistem informasi adalah proses pengumpulan bukti dan evaluasi untuk mengetahui tingkat kesesuaian sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah sistem informasi telah didesain dan diimplementasikan secara efektif, efisien dan ekonomis, serta dapat menjaga dan memelihara aset perusahaan.

2.5.2 Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Weber (1999) terbagi menjadi empat, yaitu:

1. Meningkatkan keamanan aset perusahaan

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

2. Meningkatkan integritas data

Integritas data adalah suatu konsep dasar sistem informasi dimana keaslian suatu data sangatlah penting untuk dapat diolah agar menjadi suatu informasi yang valid. Data memiliki atribut seperti kelengkapan, kebenaran, dan keakuratan.

3. Meningkatkan efektifitas sistem

Suatu sistem dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan pengguna dan juga sesuai dengan tujuan dan strategi perusahaan.

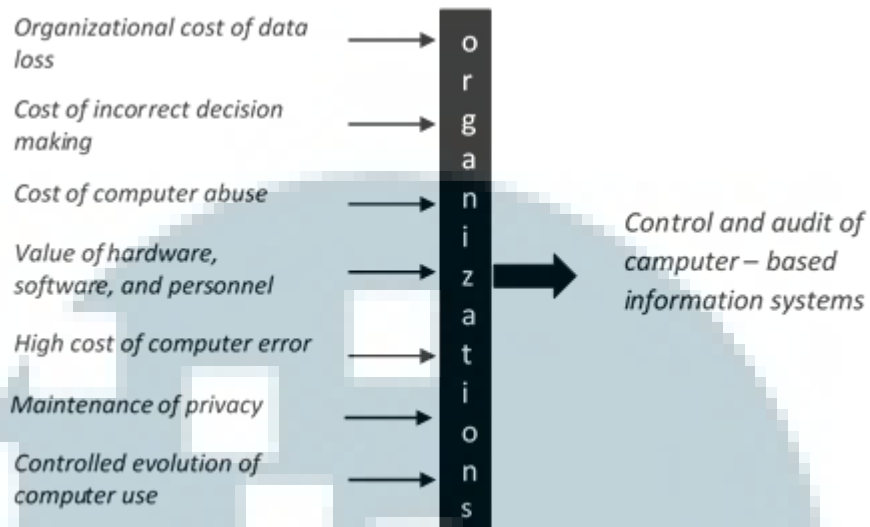
4. Meningkatkan efisiensi sistem

Efisiensi menjadi hal yang sangat penting ketika suatu komputer tidak memiliki kapasitas yang memadai, saat hal itu terjadi maka perusahaan tidak dapat menjalankan proses bisnisnya sesuai dengan tujuan dan strategi yang sudah ditetapkan.

Selain empat tujuan utama di atas, Weber (1999) menjelaskan bahwa ada beberapa faktor yang menjadikan kontrol dan audit sistem informasi pada perusahaan sangatlah penting, antara lain untuk:

1. Memastikan agar komputer dikelola dengan teratur dan sesuai arahan.
2. Mendeteksi risiko kehilangan data.
3. Mendeteksi risiko kesalahan pengambilan keputusan, akibat dari kesalahan informasi yang diproses oleh sistem.
4. Menjaga aset perusahaan seperti nilai *hardware*, *software*, dan personil perusahaan.
5. Mendeteksi risiko kesalahan komputer.
6. Mendeteksi risiko penyalahgunaan komputer (*fraud*).
7. Menjaga kerahasiaan.
8. Meningkatkan pengendalian evolusi penggunaan komputer.

Dalam penjelasannya Weber (1999) menggambarkan *the need for controls and audit of computers* seperti pada gambar 2.2.



Gambar 2.2 Control & audit for CBIS (Weber, 1999)

2.5.3 Jenis Audit Sistem Informasi

Arens, et al (2010) mengelompokkan audit ke dalam tiga jenis, yaitu:

1. *Operational Audits* (Audit Operasional)

Audit operasional mengevaluasi efisiensi dan efektivitas dari prosedur dan kebijakan serta metode operasi suatu organisasi. Hasil dari audit operasional ini adalah rekomendasi dari auditor yang ditujukan pada manajemen agar dapat meningkatkan kegiatan operasionalnya.

2. *Compliance Audits* (Audit Kepatuhan)

Audit kepatuhan bertujuan untuk menentukan apakah klien telah mengikuti prosedur atau aturan yang telah ditetapkan, seperti pelaksanaan ketentuan upah minimum, pelaksanaan undang –

undang perpajakan, dan pelaksanaan prosedur yang telah ditetapkan oleh pimpinan perusahaan.

3. *Financial Statement Audits* (Audit Laporan Keuangan)

Audit laporan keuangan bertujuan untuk menentukan apakah laporan keuangan secara keseluruhan informasi yang diuji telah disajikan sesuai dengan kriteria yang telah ditentukan. Pada umumnya yang telah ditetapkan tersebut adalah prinsip akuntansi yang berlaku umum yaitu Standar Akuntansi Keuangan (SAK).

Namun bila ditinjau dari jenis pemeriksaannya menurut Agoes (2012^[i2]) audit dapat dibedakan menjadi empat, yaitu:

1. *Management Audits* (Operasional Audit)

Pemeriksaan terhadap kegiatan operasi suatu perusahaan atas semua kebijakan termasuk kebijakan akuntansi dan operasional yang telah ditetapkan oleh manajemen. Hal ini dilakukan untuk mengetahui apakah kegiatan operasi tersebut sudah dilakukan secara efektif, efisien, dan ekonomis.

2. *Internal Audits* (Audit Internal)

Menurut definisi yang ada pada Standar Profesi Audit Internal (SPAI) tahun 2004, audit internal adalah suatu aktivitas penilaian independen di dalam suatu organisasi untuk penelitian kegiatan pembukuan, finansial, dan kegiatan lainnya, sebagai dasar untuk membantu pimpinan perusahaan. Pemeriksaannya memiliki

pengendalian manajerial yang berfungsi dengan jalan mengukur dan menilai efektivitas sarana pengendalian.

3. *Compliance Audit* (Pemeriksaan Akuntansi)

Pemeriksaan ini dilakukan untuk mengetahui apakah perusahaan sudah mentaati semua peraturan dan kebijakan yang berlaku, baik yang ditetapkan langsung oleh pihak perusahaan ataupun pemerintah. Pemeriksaan bisa dilakukan oleh KAP ataupun bagian internal audit perusahaan.

4. *Computer Audits*

Pemeriksaan yang dilakukan oleh Kantor Akuntan Publik (KAP) terhadap perusahaan yang dalam pemrosesan data dan informasi akuntansinya dengan menggunakan *Electronic Data Processing (EDP) System*.

2.5.4 Metode Audit Sistem Informasi

Dalam melakukan audit atau pemeriksaan sistem informasi dalam perusahaan, seorang Auditor dapat menggunakan beberapa cara:

1. *Audit around the computer* (Audit di sekitar komputer)

Pada metode ini auditor tidak perlu menguji pengendalian sistem informasi berbasis komputer klien secara langsung, yaitu pada *program file* atau data yang ada pada komputer. Auditor hanya perlu memeriksa kesesuaian *input* dan *output* dari sistem aplikasi

yang digunakan. Langkah-langkah yang dilakukan auditor dalam menggunakan metode ini adalah:

- a. Meninjau dan menguji pengendalian masukan (*input controls*).
- b. Menghitung hasil yang diperkirakan (*expected*) dari proses transaksi yang diperiksa.
- c. Membandingkan dengan hasil sesungguhnya yang dihitung secara manual, hal ini dilakukan untuk mendapatkan keyakinan bahwa proses yang dilakukan program komputer sudah berjalan benar.

Kondisi yang cocok untuk menggunakan metode ini, antara lain:

- a. Kurangnya pengetahuan auditor mengenai aspek teknis komputer atau keterbatasan lainnya.
- b. Dokumen sumber tersedia dalam bentuk kertas.
- c. Sistem komputer yang diterapkan masih sederhana

Keunggulan metode ini adalah pelaksanaan audit jadi lebih sederhana, dan auditor yang kurang memiliki pengetahuan dan kemampuan dalam bidang komputer dapat dilatih dengan mudah untuk melaksanakan audit.

2. *Audit through the computer* (Audit melalui komputer)

Dalam metode ini auditor melakukan pemeriksaan langsung terhadap program dan *file* komputer pada audit sistem informasi

berbasis komputer. Auditor dapat melakukan pemeriksaannya dengan cara cek logika dari program ataupun melakukan *desk checking* pada logika program atau *source code* dari program. Selain itu auditor dapat meminta penjelasan dari teknisi komputer mengenai spesifikasi sistem atau program yang diperiksanya. Pada metode ini fokus utama auditor langsung pada operasi pemrosesan di dalam sistem komputer.

Kondisi yang cocok untuk metode ini, antara lain:

- a. Sistem aplikasi komputer memproses *input* yang cukup besar dan juga menghasilkan *output* yang cukup besar sehingga memperluas cakupan yang dapat diaudit untuk meneliti kebenarannya.
- b. Bagian penting dari struktur pengendalian internal perusahaan terdapat di dalam komputerisasi yang digunakan.
- c. Sistem logika komputer sangat kompleks dan memiliki banyak fasilitas pendukung.

Kelebihan daripada metode ini adalah auditor memperoleh kemampuan yang besar dan efektif dalam melakukan pengujian terhadap sistem komputer, merasa lebih yakin terhadap kebenaran hasil kerjanya, dan dapat menilai kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan.

3. *Audit with the computer* (Audit dengan komputer)

Dalam metode ini auditor menggunakan *software* dalam melakukan pemeriksaannya, selain itu ada beberapa cara yang dapat digunakan oleh auditor untuk melaksanakan prosedur audit:

- a. Melakukan pengujian dengan sistem komputer klien itu sendiri sebagai bagian dari pengujian pengendalian.
- b. Menggunakan komputer sebagai alat bantu kegiatan audit, seperti untuk administrasi dan surat-menyurat, pembuatan tabel/jadwal, dan berbagai kegiatan *office automation* lainnya.

Software audit yang digunakan dapat dikelompokkan menjadi dua yaitu perangkat lunak audit khusus (SAS, *Specialized Audit Software*) dan perangkat lunak audit umum (GAS, *Generalized Audit Software*).

2.5.5 Tahapan Audit Sistem Informasi

Tahapan audit sistem informasi dibagi menjadi empat tahapan (Hermawan, 2011) yaitu:

1. Tahap perencanaan audit

Dilakukan untuk mengetahui tentang *auditee* (organisasi yang akan diaudit) dan mempelajari tentang proses bisnis perusahaan yang akan diaudit.

2. Tahap persiapan audit

Auditor merencanakan dan memantau pelaksanaan audit sistem informasi secara terperinci dan mempersiapkan alur dan dokumen kerja audit sistem informasi yang akan dipakai.

3. Tahap pelaksanaan audit

Melakukan pengumpulan dan evaluasi bukti dari data yang ditemukan dan juga melakukan uji kepatutan (*compliance test*) yaitu dengan menyesuaikan keadaan sebenarnya dengan standar pengelolaan proses TI yang didefinisikan dalam kerangka kerja ISO 27002. Selanjutnya auditor melakukan penyusunan temuan serta rekomendasi guna diberikan kepada *auditee*.

4. Tahap pelaporan audit

Pada tahap ini auditor membuat *draft* pelaporan yang objektif dan komprehensif yang nantinya akan ditunjukkan ke *auditee*.

Menurut CISA *Study Guide* (2012), terdapat sepuluh tahap melakukan audit:

1. Persetujuan *audit charter* atau surat perjanjian
2. Perencanaan ulang audit
3. Penilaian risiko
4. Menentukan apa saja yang memungkinkan untuk diaudit
5. Melakukan audit
6. Pengumpulan bukti
7. Melakukan pengujian audit
8. Analisis hasil audit

9. Laporan dari hasil audit

10. Menindaklanjuti kegiatan yang sudah diaudit

Sedangkan menurut Hunton (2004) dalam penjelasannya menyebutkan untuk melakukan audit TI terdapat beberapa tahap yaitu perencanaan, penilaian risiko, pengembangan program audit, mengumpulkan bukti, pembentukan kesimpulan, mempersiapkan pendapat audit, dan tindak lanjut (*following up*).

1. Perencanaan / *Planning*

Tahap awal dari melakukan audit TI adalah perencanaan audit yang mencakup risiko-risiko apa saja yang dapat terjadi, bagaimana menjalin hubungan dengan klien, bagaimana cara untuk membiasakan diri dengan lingkungan sekitar dan menentukan siapa saja *staff-staff* audit. Tahapan perencanaan menurut ISACA *standard* 050.010 (2012) adalah:

1. Menentukan batasan dan tujuan audit.
2. Menentukan penilaian awal yang relevan.
3. Mengumpulkan pengetahuan tentang organisasi, proses bisnis, keuangan, risiko bawaan dan isu-isu lingkungan yang berhubungan erat dengan industri atau klien.
4. Mengidentifikasi pihak *eksternal* (*outsourcing*).
5. Membangun program audit yang berisi prosedur-prosedur audit yang akan dilakukan selama proses audit.

6. Membuat rencana audit yang akan dilakukan selama audit.

7. Mengumpulkan dokumen proses audit meliputi rencana audit, program audit dan dokumentasi penting lainnya untuk memberikan pengertian mengenai bisnis klien.

2. Penilaian risiko / *what can we go wrong?*

Untuk melakukan audit terdapat salah satu pendekatan *risk-based audit* yaitu metode audit internal untuk meyakinkan kecukupan bahwa risiko pada sebuah perusahaan dikelola sesuai dengan batasan risiko yang ditetapkan oleh perusahaan. Dalam metode tersebut penilaian risiko ada pada seputar pertanyaan “*what can we go wrong?*”/ kesalahan apa yang dapat terjadi? auditor akan menjadikan hal tersebut menjadi fokus pertama dalam menentukan risiko apa saja yang dapat terjadi saat melakukan audit.

3. Pengembangan program audit / *the audit program*

Dalam audit TI, prosedur – prosedur audit harus disesuaikan dengan *hardware*, *software*, jaringan, dan topologi yang digunakan serta lingkungan sistem. Program audit umumnya meliputi komponen- komponen:

1. Lingkup audit
2. Tujuan audit
3. Prosedur audit

4. Detail administrasi (perencanaan dan pelaporan)

4. Mengumpulkan bukti / *gathering evidence*

Untuk membuat kesimpulan dari temuan audit harus disertakan dengan analisis dan pendapat yang didasari oleh teori yang tepat dari bukti-bukti yang ada. Kunci dasar audit adalah menemukan bukti untuk memperoleh opini audit yang akan dibentuk. Berdasarkan ISACA *guideline* tipe bukti yang dikumpulkan auditor sistem informasi meliputi:

1. Proses observasi dan keberadaan dari komponen fisik seperti operasi-operasi komputer dan prosedur *backup*.
2. Bukti dokumentasi seperti *program change logs, access logs system, authorization table*.
3. Representasi seperti *flowchart, DFD*, dan prosedur tertulis.
4. Analisis seperti prosedur *Computer Assisted Audit Tools (CAATs)* yang berjalan

5. Pembentukan kesimpulan / *forming conclusions*

Evaluasi dari bukti-bukti yang telah dikumpulkan dan mengambil kesimpulan apakah tujuan audit tercapai dan proses audit berjalan sesuai dengan prosedur perusahaan atau tidak. Auditor juga mengidentifikasi kondisi-kondisi tertentu yang ditemukan dari hasil auditnya.

6. Mempersiapkan pendapat audit / *the audit opinion*

Dalam pembuatan laporan audit sistem informasi, ada panduan umum yang diatur oleh ISACA *guideline*:

1. Nama dari organisasi yang diaudit.
2. Judul, tanda tangan, dan tanggal.
3. Penjelasan mengenai tujuan audit dan apakah tujuan audit tercapai.
4. Ruang lingkup audit meliputi area audit, periode pelaksanaan audit, lingkungan aplikasi atau proses yang diaudit.
5. Penjelasan mengenai batasan ruang lingkup auditor.
6. Standar dan kriteria dimana auditor melakukan pekerjaan audit.
7. Penjelasan terperinci dari hasil temuan audit.
8. Kesimpulan dari area-area audit yang dievaluasi.
9. Rekomendasi atau saran untuk perbaikan atau peningkatan.
10. Hal-hal yang terjadi setelah pekerjaan audit selesai.

7. Tindak lanjut / *following up*

Setelah auditor mengkomunikasikan hasil audit kepada klien dan menyampaikan opini auditnya, auditor akan membuat ketetapan untuk *follow up activities* dengan klien mengenai apakah

masalah-masalah yang ada sudah diperbaiki dan saran dari auditor apakah sudah dilakukan.

2.6 Teknik Pengumpulan Data

Dalam audit sistem informasi seorang auditor harus mengumpulkan sebanyak-banyaknya bukti atau sumber data yang ada pada perusahaan sebagai acuan dalam melakukan penilaiannya. Menurut Loftland (2000) sumber data utama dalam penelitian kualitatif ialah kata-kata dan tindakan, selebihnya adalah data tambahan seperti dokumen dan lain-lain. Adapun jenis data tersebut dibagi menjadi dua, yaitu:

1. Data primer

Data dan informasi yang diperoleh secara langsung dari narasumber atau orang-orang yang berkaitan langsung dengan penelitian.

2. Data sekunder

Data berupa dokumen-dokumen seperti laporan dan arsip lain yang berhubungan dengan penelitian. Seperti profil perusahaan, struktur organisasi, peraturan-perturan organisasi, dan lain sebagainya.

Dalam pengumpulan sumber data atau informasi penelitian, menurut Bungin (2001) teknik pengumpulan data adalah bagian instrumen pengumpulan data yang menentukan berhasil atau tidaknya suatu penelitian. Kesalahan penggunaan teknik pengumpulan data jika tidak digunakan dengan semestinya akan berakibat fatal terhadap hasil dari penelitian yang dilakukan.

Adapun beberapa teknik pengumpulan data sebagai berikut:

1. *Interview* (Wawancara)

Percakapan langsung dengan dua pihak yaitu pewawancara yaitu pihak yang mengajukan pertanyaan dan responden sebagai pemberi jawaban atas pertanyaan.

2. Observasi Dokumentasi

Pengamatan terhadap data tertulis yang ada dan dapat digunakan sebagai pendukung pencapaian tujuan penelitian.

2.7.1 *Capability Process Model*

Pada COBIT 5.0 didukung oleh pendekatan penilaian kapabilitas proses berdasarkan ISO/IEC 15504. ISO 15504-2 menjelaskan pengukuran untuk penilaian kemampuan proses dari kerangka kerja COBIT didefinisikan ke dalam enam *level* poin dari skala 0-5, yang dimana mempresentasikan peningkatan kemampuan proses yang diimplementasikan.

1. *Level 0 (Incomplete)*

Proses tidak melaksanakan atau gagal untuk mencapai tujuan proses.

Pada tingkat ini, ada sedikit atau tidak sama sekali bukti dari setiap pencapaian tujuan proses.

2. *Level 1 (Performed)*

Proses diimplementasikan untuk mencapai tujuan bisnisnya.

3. *Level 2 (Managed)*

Proses yang diimplementasikan dikelola dan hasilnya ditetapkan serta dikontrol.

4. *Level 3 (Established)*

Proses didokumentasikan dan dikomunikasikan.

5. *Level 4 (Predictable)*

Proses dimonitor, diukur, dan diprediksi untuk mencapai hasil.

6. *Level 5 (Optimizing)*

Proses yang telah diprediksi kemudian ditingkatkan untuk memenuhi tujuan bisnis yang relevan dengan tujuan yang akan datang.

Pengukuran kemampuan proses berdasarkan dari kumpulan atribut proses, yang dimana masing-masing atribut mendefinisikan aspek tertentu dari kemampuan proses. Tingkatan pencapaian dari atribut proses meliputi empat tingkatan poin (*level rating point*) yang sudah ditetapkan oleh COBIT Process Assessment Model (PAM).

Tabel 2.1 *Level Rating Point*

<i>Level</i>	<i>Rating</i>
<i>N – Not achieved</i>	<i>0 – 15% achievement</i>
<i>P – Partially achieved</i>	<i>16-50% achievement</i>
<i>L – Largely achieved</i>	<i>51-85% achievement</i>
<i>F – Fully achieved</i>	<i>86-100% achievement</i>

Jika setiap proses menghasilkan persentase di atas 85% maka proses tersebut layak untuk melanjutkan penilaian di *level* selanjutnya.

2.7 Pengertian IT Governance

Tata kelola TI (*IT Governance*) menurut *IT Governance Institute* (ITGI) adalah bagian dari perusahaan yang mengelola secara keseluruhan yang terdiri dari kepemimpinan dan struktur organisasi dari proses yang ada untuk memastikan kelanjutan teknologi informasi organisasi dan pengembangan tujuan dan strategi organisasi. *IT Governance* merupakan tanggung jawab dari pimpinan utama dan manajemen eksekutif dari suatu perusahaan.

Dengan kata lain dapat dikatakan bahwa *IT Governance* adalah suatu struktur organisasi dan proses yang saling berhubungan untuk mengelola dan mengendalikan perusahaan untuk mencapai tujuan dan strategi perusahaan dengan menambahkan nilai tambah dari pemanfaatan teknologi informasi di dalamnya.

2.8 COBIT 5.0

2.7.2 Definisi COBIT 5.0

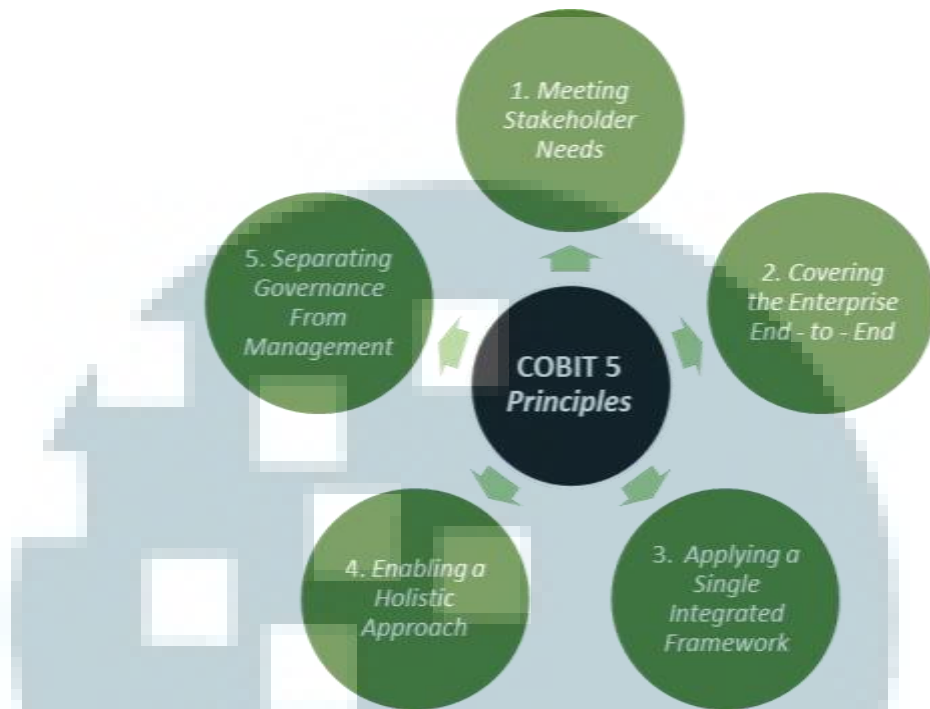
COBIT 5.0 merupakan sebuah kerangka kerja menyeluruh yang dapat membantu perusahaan dalam mencapai tujuannya dalam bidang tata kelola dan manajemen teknologi informasi perusahaan. Menurut Gondodiyoto (2007) menjabarkan bahwa COBIT adalah sekumpulan dokumentasi *best practice* untuk tata kelola TI yang dapat membantu auditor, pengguna sistem, dan manajemen dalam menyematani risiko organisasi dengan kebutuhan pengendalian, serta masalah-masalah TI.

2.7.3 Sejarah Singkat COBIT

COBIT (*Control Objective for Information and Related Technology*) merupakan kerangka kerja Audit Teknologi Informasi yang dibuat oleh ISACA (*Information System Audit and Control Association*) pada tahun 1996. Selanjutnya pada tahun 1998 ISACA menerbitkan COBIT edisi kedua, COBIT 3.0 pada tahun 2000, kemudian COBIT 4.0 pada tahun 2005, COBIT 4.1 pada tahun 2007, dan pada tahun 2012 ISACA merilis COBIT 5.0 yang dilengkapi dengan *balance scorecard* dan digunakan sebagai audit TI, dimana sebanding dengan standar industri lainnya seperti ITIL, CMM, BS779, ISO9000.

2.7.4 Prinsip COBIT 5.0

COBIT 5.0 bersifat umum dan berguna untuk segala jenis ukuran perusahaan, baik dalam bidang komersial, sektor non profit atau pada sektor pemerintahan atau publik. COBIT 5.0 didasarkan pada lima prinsip utama untuk tata kelola dan manajemen TI perusahaan. Dari kelima prinsip ini memungkinkan perusahaan untuk membangun sebuah struktur atau kerangka tata kelola dan manajemen yang efektif, yang dimana dapat mengoptimalkan investasi dan penggunaan TI untuk mendapatkan keuntungan bagi para *stakeholder* serta untuk menambahkan nilai tambah perusahaan.

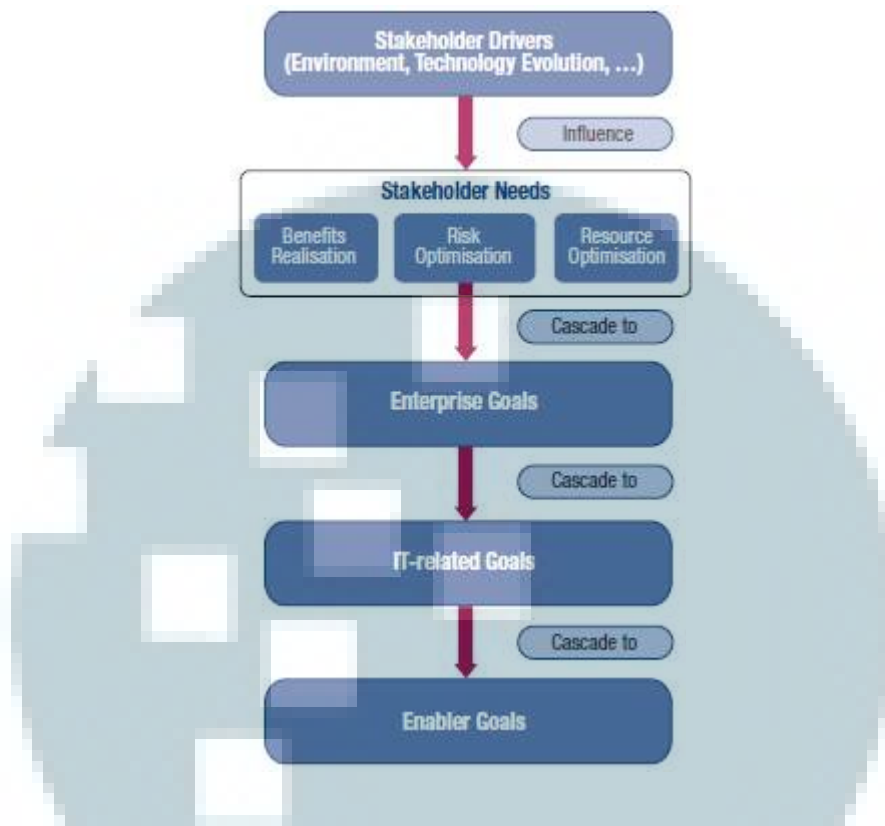


Gambar 2.3 Lima Prinsip COBIT 5.0

Berdasarkan gambar 2.3, dijelaskan bahwa:

1. *Meeting stakeholder needs* (Memenuhi kebutuhan *Stakeholder*)

Perusahaan menciptakan nilai untuk para *stakeholdernya* dengan menjaga keseimbangan antara realisasi keuntungan, optimalisasi risiko, dan penggunaan sumber daya sesuai dengan tujuan perusahaan. Setiap perusahaan memiliki tujuan yang berbeda, COBIT 5.0 dapat dikostumisasi sesuai dengan tujuan dan kebutuhan perusahaan sesuai dengan konteks perusahaan itu sendiri. Agar dapat sesuai dengan tujuan perusahaan COBIT 5.0 dikostumisasi melalui pengaliran tujuan (*goal cascade*).



Gambar 2.4 Goals Cascade Overview

Berikut adalah penjelasan dari gambar 2.4, yaitu:

- a. Penggerak *stakeholder* (perubahan strategi, lingkungan bisnis, teknologi baru, dan peraturan baru) mempengaruhi kebutuhan *stakeholder*.
- b. Kebutuhan *stakeholder* diturunkan menjadi tujuan perusahaan.
- c. Tujuan perusahaan diturunkan menjadi tujuan yang berhubungan dengan TI.
- d. Tujuan TI diturunkan menjadi tujuan pemicu (*enabler goal*).

2. *Covering the enterprise end-to-end* (Mencakup seluruh perusahaan)

COBIT 5.0 tidak hanya berfokus pada fungsi TI tetapi juga pada seluruh informasi dan teknologi yang berkaitan dengan fungsi IT sebagai suatu aset yang perlu ditangani oleh perusahaan.

3. *Applying single integrated framework* (Menerapkan suatu kerangka tunggal yang terintegrasi)

COBIT 5.0 merupakan standar yang relevan, lengkap menjangkau semua aspek perusahaan, dan terbaru yang memungkinkan perusahaan untuk menggunakan COBIT 5.0 sebagai kerangka kerja untuk tata kelola dan manajemen TI secara menyeluruh dan terintegrasi.

4. *Enabling holistic approach* (Menggunakan pendekatan yang menyeluruh)

COBIT 5.0 mendefinisikan serangkaian *enabler* (pemicu) untuk mendukung implementasi sistem yang komprehensif mengenai tata kelola dan manajemen TI perusahaan. COBIT 5.0 membagi pemicu menjadi tujuh kategori, yaitu

- a. *Principles, policies, and frameworks*
- b. *Processes*
- c. *Organisational structures*
- d. *Culture, ethics, and behaviour*
- e. *Information*

f. *Services, infrastructure, and applications*

g. *People, skill, and competencies*

Setiap pemicu saling berhubungan yang harus selalu dipertimbangkan oleh perusahaan.

5. *Separating governance from management* (Pemisah tata kelola dari manajemen)

Pada COBIT 5.0 ini dibuat suatu perbedaan yang jelas antara tata kelola dan manajemen. Perbedaan antara tata kelola dan manajemen menurut COBIT 5.0 adalah :

a. Tata kelola

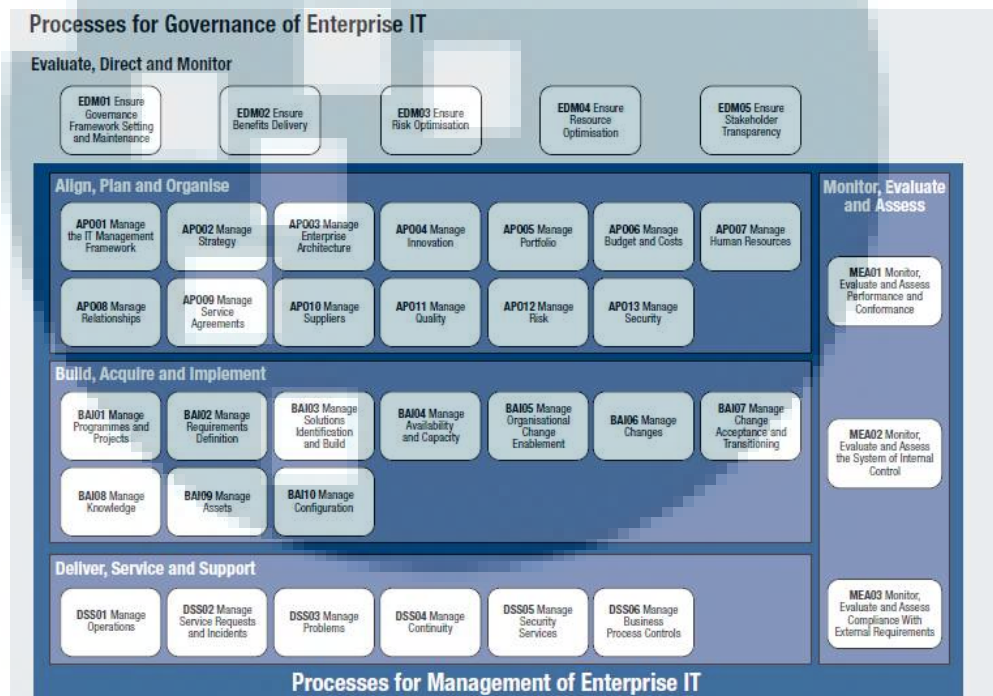
Menjamin kebutuhan *stakeholder* selalu dievaluasi untuk menentukan tujuan perusahaan yang seimbang dan disepakati untuk dicapai, menentukan arah melalui penentuan prioritas dan pengambilan keputusan, dan memantau pemenuhan unjuk kerja terhadap tujuan dan arah yang disepakati.

b. Manajemen

Merencanakan, membangun, menjalankan, dan memantau aktivitas dalam rangka penyelarasan dengan arah perusahaan yang telah ditentukan oleh badan pengelola (tata kelola), untuk mencapai tujuan perusahaan.

2.7.5 Komponen *Control Objectives*

Kerangka kerja COBIT 5.0 memiliki 37 proses yang menentukan dan menjelaskan secara detail mengenai proses tata kelola dan manajemen. Proses-proses tersebut biasa ditemukan dalam perusahaan yang berhubungan dengan aktivitas TI dan mudah dipahami dalam operasional TI dan oleh manajer bisnis dari perusahaan.



Gambar 2.5 Model Refrensi Proses

Dalam COBIT referensi model proses tersebut dikelompokkan kembali menjadi lima domain, yaitu:

1. *Evaluate, Direct, and Monitor*

Memastikan bahwa tujuan dari perusahaan dapat dicapai dengan cara mengevaluasi kebutuhan dan kondisi dari *stakeholder*, melakukan

arahan terhadap tujuan dan strategi perusahaan, serta melakukan *monitoring* terhadap setiap kinerja yang dilakukan oleh perusahaan.

Tabel 2.2 *Evaluate, Direct, and Maintenance*

EDM	EDM Deskripsi
EDM01	Memastikan pengaturan kerangka tata kelola dan pemeliharaan
EDM02	Memastikan manfaat pengiriman
EDM03	Memastikan optimisasi risiko
EDM04	Memastikan optimisasi sumber daya
EDM05	Memastikan transparansi <i>stakeholder</i>

2. *Align, Plan, and Organize*

Domain ini berfungsi agar perusahaan dapat menggunakan teknologi seoptimal mungkin dari mulai penyelarasan, perencanaan, dan pengaturan.

Tabel 2.3 *Align, Plan, and Organize*

APO	APO Deskripsi
APO01	Mengelola kerangka kerja manajemen TI
APO02	Mengelola Strategi
APO03	Mengelola arsitektur perusahaan
APO04	Mengelola inovasi
APO05	Mengelola portofolio
APO06	Mengelola anggaran dan biaya
APO07	Mengelola sumber daya manusia
APO08	Mengelola hubungan
APO09	Mengelola perjanjian bisnis
APO010	Mengelola <i>supplier</i>
APO011	Mengelola kualitas
APO012	Mengelola risiko
APO013	Mengelola keamanan

3. *Build, Acquire, and Implement*

Digunakan untuk melakukan pengendalian dan pemeliharaan terhadap sistem apakah sudah berjalan sesuai dengan tujuan yang ada.

Tabel 2.4 *Build, Acquire, and Implement*

BAI	BAI Deskripsi
BAI01	Mengelola program dan proyek
BAI02	Mengelola definisi kebutuhan
BAI03	Mengelola dan membangun solusi identifikasi
BAI04	Mengelola ketersediaan dan kapasitas
BAI05	Mengelola perubahan organisasi pemberdayaan
BAI06	Mengelola perubahan
BAI07	Mengelola penerimaan perubahan dan transisi
BAI08	Mengelola pengetahuan
BAI09	Mengelola asset
BAI010	Mengelola konfigurasi

4. *Deliver, Service, and Support*

Fokus dari pada domain ini adalah segala yang berhubungan dengan pelayanan TI dan dukungan teknisnya pada proses bisnis dari suatu perusahaan.

Tabel 2.5 *Deliver, Service, and Support*

DSS	DSS Deskripsi
DSS01	Mengelola operasi
DSS02	Mengelola permintaan layanan dan insiden
DSS03	Mengelola masalah
DSS04	Mengelola kontinuitas
DSS05	Mengelola layanan keamanan
DSS06	Mengelola kontrol proses bisnis

5. *Monitor, Evaluate, and Assess*

Digunakan agar perusahaan dapat memantau proses yang sedang berjalan dalam perusahaan agar *output* dari sistem yang dipakai dapai sesuai dengan tujuan awal dan berjalan secara efektif dan efisien.

Tabel 2.6 *Monitor, Evaluate, and Assess*

MEA	MEA Deskripsi
MEA01	Memantau, mengevaluasi, dan menilai kinerja dan kesesuaian
MEA02	Memantau, mengevaluasi, dan menilai sistem pengendalian internal
MEA03	Memantau, mengevaluasi, dan menilai kepatuhan terhadap persyaratan eksternal

UMMN