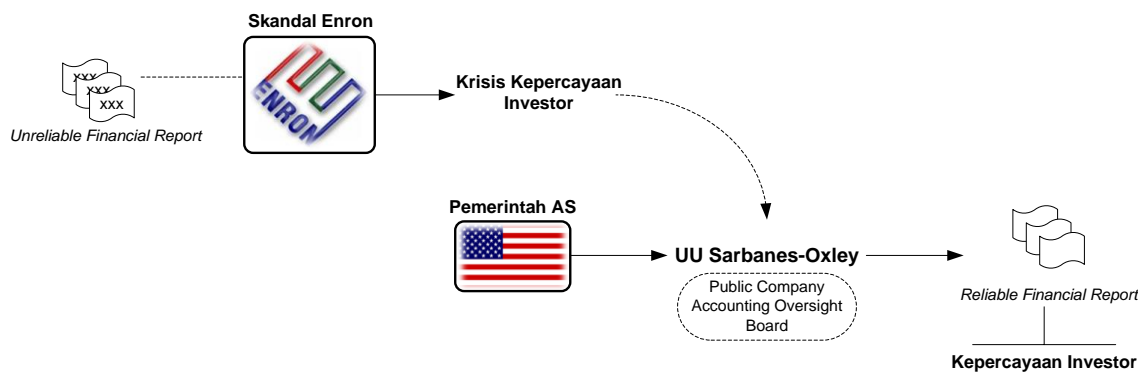


BAB II DASAR TEORI

2.1 SOX (Sarbanes-Oxley Act)



Gambar II-1 Gambaran Peran dan Definisi SOX

Sarbanes-Oxley Act (Pub. L. No. 107-204, 116 Stat 745) adalah sebuah landasan hukum yang disahkan pada 23 Januari 2002 oleh kongres Amerika Serikat. Undang-undang ini dikenal sebagai *Public Company Accounting Reform and Investor Protection Act of 2002* atau undang-undang perlindungan investor dan pengaturan akuntansi perusahaan publik yang seringkali disebut SOX atau Sarbox. Pada Gambar II-1 terlihat bahwa SOX lahir sebagai bentuk tindakan penanggulangan pemerintah Amerika Serikat terhadap sejumlah skandal yang menimbulkan krisis kepercayaan para investor.

Pada tahun 2002 terjadi skandal laporan keuangan serta proses pelaporannya pada perusahaan-perusahaan besar, seperti Enron, Tyco International, WorldCom dan perusahaan akuntan publik, Arthur Andersen. Skandal tersebut berupa kesalahan dalam proses penyingkapan⁴ sehingga laporan audit transaksi keuangan perusahaan tidak dapat diandalkan (*unreliable financial report*). Kejahatan yang terkait berupa penyalahgunaan dana dan aset yang tersirat sebagai salah saji (ketidakakuratan penyajian) materialitas⁵

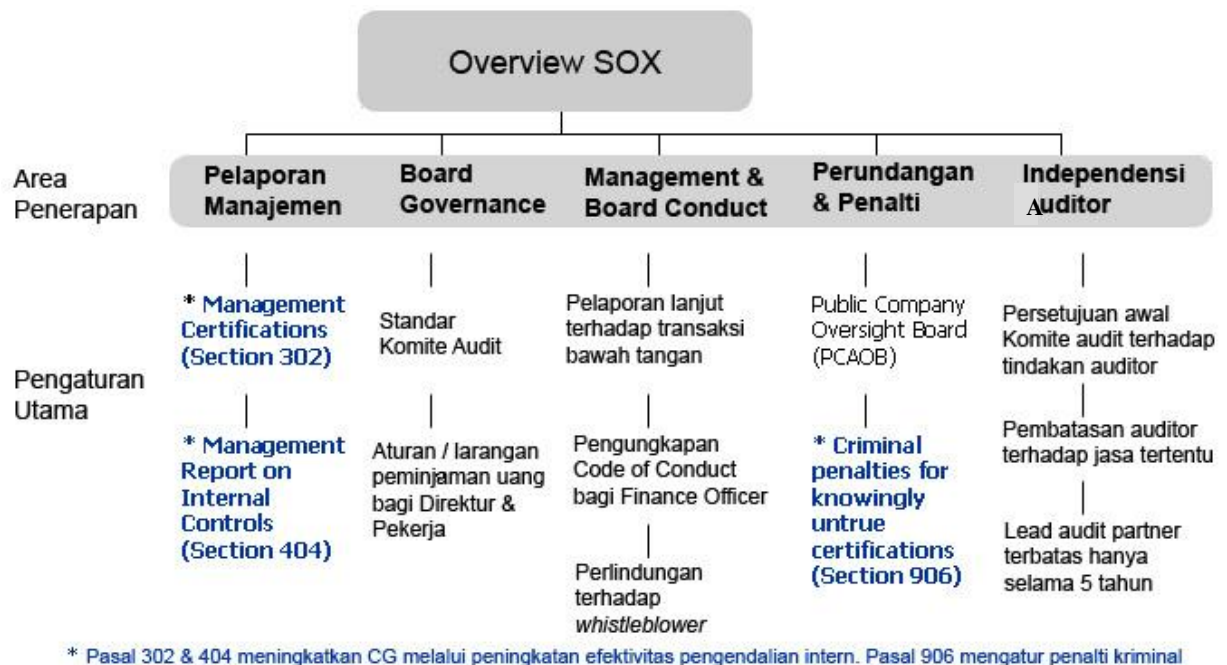
⁴ Meliputi penyingkapan terhadap politik dan proses bisnis perusahaan yang dilakukan oleh pihak eksekutif perusahaan

⁵ Materialitas adalah materi atau elemen penilaian yang besar dan melemahkan sehingga dapat berpengaruh langsung terhadap pengambilan keputusan calon investor

keuntungan, pengeluaran, nilai aset dan liabilitas perusahaan, atau keterangan pelaksanaan kerjasama perusahaan dengan perusahaan lain. Bentuk kejahatan lain adalah tidak terdapat pernyataan yang jelas terhadap pembagian wewenang dalam pelaksanaan proses audit, sehingga pengusutan sulit dilakukan. Hal-hal tersebut menyebabkan turunnya kepercayaan pasar terhadap praktek audit akuntan publik dan terhadap keabsahan laporan keuangan perusahaan publik.

Sebagai usaha dalam mengembalikan kepercayaan pihak investor dalam pasar modal, SOX mengatur kebijakan dalam perusahaan publik yang meliputi [GON07] :

- Pengembangan tatakelola perusahaan yang baik
- Pembaruan akuntansi
- Penyusunan tata cara penyingkapan informasi keuangan yang transparan
- Pengungkapan hasil kerja yang dicapai manajemen
- Penegakan kode etik pejabat di bidang keuangan
- Pembatasan kompensasi bagi pihak eksekutif
- Pemberlakuan komite audit independen
- Penegasan tanggung jawab para anggota dewan komisaris, direksi, dan komite audit.



Gambar II-2 Overview Sarbanes-Oxley Act

SOX mengakibatkan dibentuknya PCAOB (*Public Company Accounting Oversight Board*) yang independen dan penuh waktu bekerja di bawah SEC (*Security and Exchange Commission*) mengawasi firma akuntan publik dan mengeluarkan standar yang berhubungan dengan akuntansi dan proses audit. PCAOB juga berperan sebagai penegak hukum terhadap *corporate fraud* dan memberikan perlindungan terhadap *whistleblower*⁶.

SOX terdiri atas 11 judul utama dengan 69 pasal. Terdapat dua pasal pada SOX yang menjadi acuan utama dalam proses audit dan pengendalian internal pelaporan keuangan. Pasal-pasal tersebut adalah :

- **Pasal 302** *Corporate responsibility for financial reports* – Pasal ini menunjukkan perlunya *CEO (Chief Executive Officer)* dan *CFO (Chief Financial Officer)* atau sederajat, secara personal melakukan pengesahan terhadap sah atau tidaknya laporan keuangan perusahaan dan memastikan tidak ada salah saji materialitas dan bertanggung jawab penuh terhadap pelaksanaan pengendalian intern laporan keuangan tersebut [SOX02].
- **Pasal 404** *Management assesment of internal controls* – Pasal ini meliputi proses pengesahan (*attestation*) serta penilaian (*assesment*) dari kendali pelaporan keuangan mencakup pengaturan dan penegakan struktur serta prosedur pelaksanaan kontrol yang tepat bagi setiap perusahaan [SOX02].

Berhubungan dengan kegiatan audit, praktisi profesional TI, terutama pada posisi eksekutif, perlu untuk menguasai konsep pengendalian intern secara teoretis dan dapat mempraktekkannya dengan baik. *CIO (Chief Information Officer)* harus dapat memahami keseluruhan rencana *compliance* SOX perusahaan, menyusun rencana *compliance* TI perusahaan, dan menjamin keintegrasian di antara keduanya. Melihat hal tersebut, maka pasal yang paling bersesuaian dengan kepentingan praktisi professional TI adalah pasal 404 yang mencakup pengendalian intern.

⁶ *Whistleblower* : istilah yang diberikan kepada pegawai atau seseorang yang mengadukan penyimpangan.

2.1.1 SOX Pasal 404

Undang-undang SOX pasal 404 terdiri atas 2 sub-pasal utama, Penilaian Pihak Manajemen terhadap Pengendalian Intern (*Management Assessment of Internal Control*) dan Penyingkapan Permasalahan pada Waktu Berlangsung (*Real-Time Issuer Disclosure*).

Management Assessment of Internal Control

Laporan pengendalian intern harus berisi dua poin utama. Pertama, laporan wajib menyatakan pertanggungjawaban pihak manajemen terhadap rancangan serta pengelolaan struktur pengendalian intern dan prosedur yang digunakan. Laporan juga harus dilengkapi dengan hasil penilaian auditor intern terhadap efektivitas pengendalian intern pelaporan keuangan secara berkala, minimal sekali pertahun.

Kedua, laporan berisi keterangan lanjutan dari poin pertama, menyatakan bahwa pihak akuntan publik yang mengeluarkan laporan audit menguji dan menyertakan hasil dari pengujiannya terhadap penilaian yang dilakukan oleh pihak manajemen perusahaan sesuai standar atau perjanjian yang berlaku antar komite audit eksternal.

Real-Time Issuer Disclosure

Sebagai bentuk perlindungan kepada investor, laporan audit harus mudah dipahami. Penyampaiannya lugas dan menggunakan presentasi grafis, seperti *charts*. Selain itu, informasi yang disampaikan harus berupa informasi terkini dan dapat dipertanggungjawabkan oleh semua pihak yang menerbitkan laporan tersebut.

2.1.2 Dampak SOX 404

SOX 404 menyebabkan perusahaan memiliki kewajiban hukum melaporkan pengendalian intern terhadap proses pelaporan keuangan. SEC menetapkan empat elemen utama yang harus tercakup dalam laporan keuangan perusahaan publik adalah :

- Pernyataan pertanggungjawaban pihak manajemen perusahaan (CEO dan CFO) terhadap penyusunan dan pengelolaan struktur pengendalian intern yang tepat bagi sistem pelaporan keuangan perusahaan.

- Pengidentifikasian *framework* yang digunakan oleh pihak manajemen dalam melakukan evaluasi pengendalian intern terhadap pelaporan keuangan.
- Penilaian terhadap efektivitas pengendalian intern pelaporan keuangan yang dilakukan oleh manajemen melalui pihak auditor internal perusahaan.
- Atestasi auditor eksternal terhadap poin di atas.

Karena dampak implementasi SOX 404 cukup besar dan signifikan, maka pihak manajemen perlu untuk mengetahui lebih dalam mengenai konsep pengendalian intern agar dapat menerapkan *framework* yang tepat untuk pengendalian intern perusahaannya.

2.2 Pengendalian Intern

Pengendalian intern (*internal control*) awalnya berasal dari ranah akuntansi yang bersifat kontrol dan ditujukan untuk menghindari *clerical error* dan kesalahan pencatatan [GON07].

Terdapat dua jenis pengendalian berdasarkan *Statement of Auditing Standards* (SAS)⁷ No. 1/1973, yaitu administratif dan akuntansi. Pengendalian administratif meliputi rencana organisasi dan prosedur yang menyangkut efisiensi usaha dan ketaatan terhadap kebijaksanaan/peraturan pimpinan perusahaan. Hal tersebut mencakup analisis statistik, *time & motion study*⁸, laporan kegiatan, program latihan pegawai dan pengawasan mutu, serta kebijakan akuntansi.

Sementara pengendalian akuntansi meliputi rencana organisasi, prosedur, serta catatan yang menjamin pengamanan terhadap harta dan dapat diandalkannya laporan keuangan perusahaan.

⁷ SAS adalah pedoman yang ditujukan kepada auditor eksternal terhadap standard yang diterima secara umum dalam auditing sehubungan dengan tindakan pengauditan dan pengeluaran laporan. SAS umumnya dikeluarkan oleh badan pengatur akuntan di daerahnya, untuk Indonesia berarti IAI (Ikatan Auditor Indonesia)

⁸ *Time & motion study* adalah pengukuran terhadap tingkat efektivitas yang dilakukan melalui pergerakan atau perpindahan suatu aktivitas yang mengkonsumsi waktu dan sumber daya menggunakan teknik-teknik seperti *work sampling*, *work-unit activity*, *time standards*, dsb.

COSO kemudian mendefinisikan pengendalian intern sebagai sebuah proses, yang dipengaruhi oleh badan direksi yang dirancang untuk menegaskan *assurance* yang memadai untuk mencapai (1) efektivitas dan efisiensi pada operasional. (2) reliabilitas pelaporan keuangan (3) kepatuhan terhadap hukum dan peraturan yang berlaku.

Berdasarkan perkembangan peran pengendalian intern, Michael P. Cangemi menambahkan pendefinisian pengendalian intern sebagai penegasan *assurance* terhadap : (1) pengamanan aset (2) akurasi dan reliabilitas informasi produk/jasa (3) peningkatan efisiensi (4) kepatuhan terhadap peraturan perusahaan (5) kepatuhan terhadap undang-undang dan hukum (6) pengelolaan dampak negatif serta resiko yang mungkin muncul sehubungan dengan penipuan, kejahatan dan aktivitas yang mencurigakan lain [GON07].

Secara menyeluruh, ITGI kemudian mendefinisikan pengendalian intern sebagai peraturan, prosedur, penerapan aturan, serta struktur organisasi yang dirancang untuk memperoleh keyakinan yang *reasonable* terhadap terwujudnya objektivitas bisnis dan pencegahan maupun pengkoreksian terhadap kejadian yang tidak diharapkan [ITG05]. Definisi ini yang akan digunakan selanjutnya.

Tujuan umum dari pengendalian intern adalah [HAL07] :

1. Mengamankan aktiva perusahaan
2. Memastikan akurasi dan keandalan berbagai catatan dan informasi akuntansi
3. Menyebarkan efisiensi dalam operasi perusahaan
4. Mengukur ketaatan dengan berbagai kebijakan dan prosedur yang ditetapkan oleh pihak manajemen.

Sejak disahkannya SOX, terdapat perubahan dramatis dalam peranan pengendalian intern, audit internal, serta auditing eksternal pada perusahaan publik. Pasal 404 memberi dampak yang paling besar karena berhubungan langsung dengan efektivitas sistem pengendalian intern pelaporan keuangan itu sendiri.

2.2.1 Pengendalian Intern Terhadap Pelaporan Keuangan

SOX 404 menyebabkan pihak eksekutif perusahaan publik dan pihak auditor independen bertanggung jawab dalam menciptakan, mengevaluasi, dan memonitor

efektivitas pengendalian intern terhadap pelaporan keuangan (*internal control over financial report*). Bagi perusahaan maju dan berkembang saat ini, peran TI sangat krusial untuk mencapai hal tersebut. Dengan diterapkannya *ERP (Enterprise Resource Planning)* yang terintegrasi atau dengan menerapkan kumpulan aplikasi perangkat lunak dalam kegiatan operasional dan manajemen keuangan perusahaan, TI merupakan fondasi utama pengendalian intern terhadap pelaporan keuangan yang efektif.

Pengendalian intern terhadap pelaporan keuangan adalah sebuah proses yang dirancang dan dikelola oleh pihak manajemen perusahaan, menyediakan *assurance* yang tepat terhadap reliabilitas pelaporan keuangan [PWC04]. Pengendalian intern terhadap pelaporan keuangan membantu mendeteksi terjadinya penipuan dan mencegah *financial statements* yang tidak akurat.

Laporan keuangan terdiri atas dua bagian utama :

- **Laporan pihak manajemen.** Terdapat pencantuman tanggung jawab pihak manajemen untuk mempertahankan pelaporan keuangan yang memadai dan memberikan pengujian terhadap efektifitas laporan keuangan tersebut. Apabila terdapat satu buah *material weakness* (materialitas), maka proses pelaporan keuangan tidak dapat disebut efektif dan laporan keuangan tidak dapat diterbitkan.
- **Laporan pihak auditor.** Pihak auditor independen melakukan evaluasi dan melaporkan ketepatan laporan hasil pengujian yang dilakukan oleh pihak manajemen. Kegiatan audit terhadap pelaporan keuangan perusahaan kembali dilakukan dengan hasil akhir opini auditor independen⁹ terhadap laporan keuangan perusahaan dan efektifitasnya.

Kedua jenis laporan ini (pihak manajemen dan pihak auditor) juga berlaku untuk penerapan audit pengendalian intern perusahaan.

⁹ Opini yang dikeluarkan oleh auditor independen adalah : *unqualified* (dikeluarkan jika hasilnya wajar tanpa pengecualian, atau hanya membutuhkan paragraf penjelas), *qualified* (dikeluarkan jika hasilnya wajar namun memiliki pengecualian), *adverse* (dikeluarkan jika hasilnya tidak wajar dan memiliki materialitas), dan *disclaimer* (dikeluarkan jika pihak auditor tidak dapat mengeluarkan opini)

2.2.2 Konsep Penerapan Pengendalian Intern

Sesuai yang tertera pada referensi [PWC04], pada sistem manual, penerapan klasik pengendalian intern dapat dijabarkan sebagai :

- Penerapan sistem otorisasi transaksi.
- Pemisahan/pembagian tugas, wewenang dan tanggung jawab dalam perusahaan (antara operasional, tugas penyimpanan harta kekayaan, penyimpanan uang dan pembukuan).
- Pendokumentasian dan pencatatan yang memadai.
- Pengendalian akses dan penggunaan aktiva perusahaan dan catatan.
- Pengecekan terhadap kinerja yang dilakukan secara netral (independen oleh unit/orang terpisah), sering disebut dengan istilah verifikasi independen.

Aktivitas pengendalian merupakan kebijakan dan prosedur yang ditetapkan manajemen untuk memenuhi tujuan pelaporan keuangan, khususnya pada sistem yang dijalankan secara manual. Dengan digunakannya TI, segala hal manual secara otomatis akan terlaksana pada sistem.

2.2.2.1 Penggolongan Pengendalian Intern

Ditinjau dari sifatnya, sistem pengendalian intern dapat dibedakan dalam berbagai sudut pandang pengelompokan sebagai berikut :

A. Pengelompokan sesuai dengan peranannya, pendekatan ini umumnya dikenal sebagai model pengendalian PDC :

- *Preventive controls* :

Pengendalian intern yang dirancang dengan tujuan untuk mengurangi kemungkinan atau mencegah agar tidak terjadi kesalahan maupun penyalahgunaan. Tipe kendali ini merupakan lini terdepan dari pertahanan dalam struktur pengendalian.

- *Detection controls* :

Alat, teknik ataupun prosedur ini dirancang untuk mengidentifikasi dan mengekspos peristiwa yang tidak diinginkan yang lolos dari pengendalian

preventif. Ketika pengendalian detektif mengidentifikasi adanya penyimpangan maka peringatan akan muncul untuk menarik perhatian ke masalah terkait.

- *Corrective controls* :

Pengendalian ini sifatnya korektif. Jika terdapat data yang tidak valid tetapi tidak terdeteksi oleh *detection controls* atau data yang tidak valid yang terdeteksi oleh program validasi, terdapat prosedur yang jelas dalam melakukan pembetulan terhadap kesalahan tersebut. Untuk setiap kesalahan yang dideteksi akan terdapat lebih dari satu tindakan perbaikan yang mungkin dapat dilakukan.

B. Pengelompokan berdasarkan letak kendali :

- *General controls* :

Pengendalian yang berlaku untuk seluruh kegiatan komputerisasi pada suatu organisasi. Pengendalian umum juga sering dikenal sebagai pengendalian dari segi manajemen. Pengendalian umum dapat juga diartikan sebagai pengendalian yang tidak terkait langsung dengan aplikasi tertentu.

- *Application controls* :

Pengendalian yang dirancang khusus untuk aplikasi tertentu. Pengendalian ini memandang dari perspektif teknis. Pengendalian aplikasi sering disebut juga pengendalian transaksi karena dirancang berkaitan dengan aplikasi tertentu.

2.2.3 Framework Pengendalian Intern

Dalam implementasinya, pengendalian intern menggunakan *framework* tertentu sebagai referensi. *COSO Framework* memiliki model yang bersifat generik dan kebanyakan rancangan *framework* lain mengacu kepadanya. *Framework* yang ditawarkan oleh COSO bersifat fleksibel dan dapat diterapkan dalam perusahaan apapun. *COSO Framework* merupakan model untuk pengendalian intern yang dapat diterima secara umum pada tingkat internasional.

2.2.3.1 Definisi COSO *Framework*

COSO mendefinisikan pengendalian intern sebagai proses manajemen dasar, yaitu perancangan, pelaksanaan, dan pengawasan. Tindakan pengendalian bukan sesuatu yang ditambahkan dalam proses, melainkan bagian integral dari proses.

2.2.3.2 Komponen COSO *Framework*

COSO terdiri atas lima komponen yang saling berhubungan sebagai berikut :

1. *Control Environment* (lingkungan pengendalian)

Komponen ini merupakan fondasi bagi komponen yang lain dengan perannya untuk membangun iklim yang kondusif bagi para karyawan mengenai kesadaran pentingnya kontrol. Terdiri atas tujuh bagian utama, yaitu :

- a. Integritas dan nilai etos
- b. Komitmen terhadap kompetensi
- c. *Boards of Director* atau komite audit
- d. Filosofi manajemen dan gaya operasional
- e. Struktur organisasi

2. *Risk Assessment* (Penilaian Resiko)

COSO mengarahkan untuk melakukan identifikasi terhadap resiko dari tiap aktivitas. Pada tahap *risk assessment*, juga terdapat *cost-benefit consideration* yang memperhitungkan *cost* dan *benefits* yang akan dihasilkan dari suatu penerapan kendali. Terdiri atas empat bagian utama, yaitu :

- a. *Entity-Wide Objectives*
- b. *Activity-Level Objectives*
- c. Identifikasi resiko
- d. Manajemen perubahan

3. *Control Activities* (Aktivitas Pengendalian)

Merupakan kebijakan dan prosedur yang dirancang untuk memastikan dilaksanakannya kebijakan manajemen dan bahwa resiko sudah diantisipasi dan penanganannya dilakukan dengan sesuai.

Aktivitas pengendalian terdiri atas tujuh bagian utama, yaitu :

- a. *Review Top Level*
- b. Manajemen aktivitas
- c. Pemrosesan informasi
- d. Kendali fisik
- e. Indikator performansi
- f. Pembagian wewenang
- g. Pengendalian terhadap Sistem informasi :

Data center, pengembangan dan perawatan aplikasi, perangkat lunak sistem, pengamanan akses, pengendalian aplikasi

4. *Information & Communication* (Informasi & Komunikasi)

Komponen ini menjelaskan bahwa sistem informasi sangat penting bagi keberhasilan atau peningkatan mutu operasional organisasi. Informasi, baik yang diperoleh secara eksternal maupun dari pengolahan internal merupakan potensi strategis (*potential strategic*) perusahaan. Terdiri atas dua bagian utama, yaitu : informasi dan komunikasi.

5. *Monitoring* (Pemantauan)

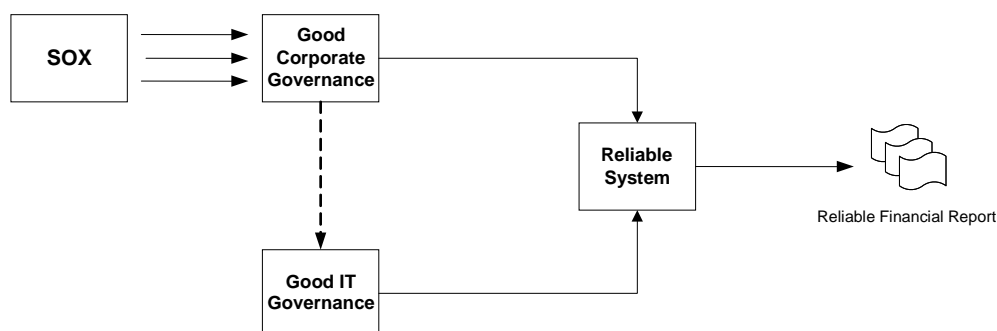
Pemantauan / *monitoring* dijabarkan dalam COSO untuk memastikan kehandalan sistem dan pengendalian internnya dari waktu ke waktu. Terdiri dari tiga bagian utama, yaitu :

- a. *Ongoing monitoring*
- b. Evaluasi terpisah (*separate evaluation*)
- c. Pelaporan terhadap defisiensi

2.3 Tata Kelola TI (*IT Governance*)

Tata kelola TI didefinisikan sebagai sistem yang mengatur dan mengendalikan seluruh TI perusahaan yang strukturnya akan menetapkan pendistribusian hak dan tanggung jawab antara pihak-pihak yang terlibat dan berisikan peraturan serta prosedur pembuatan keputusan dalam TI perusahaan [BRA03].

2.3.1 Peranan Tata Kelola TI



Gambar II-3 Diagram Keterhubungan

Perusahaan memerlukan laporan keuangan yang baik dan dengan peran TI saat ini, pada Gambar II-3 terlihat bahwa laporan keuangan yang *reliable* (terpercaya, handal, akurat, terkendali, transparan) bisa didapatkan melalui sistem TI yang *reliable*. Sistem *reliable* dapat didapatkan dari perpaduan tata kelola perusahaan dan tata kelola TI perusahaan yang baik.

Pihak manajemen menyadari bahwa teknologi sistem dapat memberikan dampak yang signifikan terhadap tingkat kesuksesan perusahaan. Hal tersebut mempengaruhi pandangan manajemen terhadap peran dan fungsi operasional TI sebagai sebuah *competitive advantage* perusahaan. Agar sebuah perusahaan dapat menjadi perusahaan yang sukses, maka informasi perusahaan harus terkelola dengan baik, sehingga investasi teknologi yang dilakukan dapat memberikan dampak positif bagi perusahaan. Terkait dengan hal tersebut, yang perlu diperhatikan adalah :

- Sejalannya strategi TI perusahaan dengan strategi perusahaan dan mendukung *objective* perusahaan dengan memberikan yang diperlukan oleh bisnis.
- Terpetakannya proses TI perusahaan menjadi model yang dapat diterima dan dipahami oleh manajemen perusahaan.
- Adaptif serta tanggapnya TI perusahaan menghadapi perubahan yang terjadi dalam perusahaan serta peluang baik bagi perusahaan.
- Terkelolanya manajemen resiko terkait dengan TI perusahaan.

- Terjalinnnya komunikasi yang efektif antara bisnis, TI, dan pihak relasi bisnis perusahaan.
- Terukur dan terujinya performansi TI perusahaan, sesuai dengan titik kendali yang dirancang.

Untuk mencapai hal tersebut, maka dibutuhkan sebuah *control framework* yang spesifik ditujukan untuk diterapkan pada manajemen TI perusahaan, sebagai pedoman tata kelola TI terutama dalam menghasilkan laporan keuangan yang *reliable*.

2.3.2 COBIT (*Control Objective for IT and Related Technology*)

COBIT adalah sebuah *framework* dan seperangkat *tools* pendukung yang digunakan oleh manajer untuk menjembatani perbedaan-perbedaan yang terdapat pada kebutuhan kendali, permasalahan-permasalahan teknis, pengelolaan resiko bisnis, dan mengkomunikasikan level kendali tersebut kepada *stakeholder*.

2.3.2.1 Karakteristik COBIT

- ***Business-focused* (terpusat pada bisnis)**

Framework COBIT didasarkan pada keterhubungan antara tiga hal utama yaitu *business requirements*, *IT resources*, dan *IT process*.

- ***Process-oriented* (berorientasi proses)**

COBIT mendefinisikan kegiatan TI dalam empat domain model proses yang generik, yaitu *Plan and Organise (PO)*, *Acquire and Implement (AI)*, *Deliver and Support (DS)*, dan *Monitor and Evaluate (ME)*. Hal ini akan dijabarkan pada Bab 2.3.2.2 Domain pada COBIT. Domain merupakan hasil pemetaan fase pengembangan teknologi informasi, yaitu perencanaan (*planning*), pembangunan (*develop*), operasional (*run*), dan pengawasan (*monitor*).

- ***Control-based* (berdasarkan kendali)**

Kendali dijabarkan sebagai kebijakan, prosedur, atau struktur organisasi yang dirancang untuk menjamin tercapainya tujuan perusahaan dan membangun batasan serta rencana preventif terhadap kejadian-kejadian yang tidak diinginkan.

IT control objective adalah sebuah pernyataan yang menggambarkan tujuan atau hasil yang ingin dicapai dengan mengimplementasikan prosedur kendali pada aktivitas TI tertentu [ITG06].

- ***Measurement-Driven***

Pengukuran yang digunakan COBIT terhadap kinerja tata kelola TI :

- Pemodelan *maturity* digunakan sebagai *benchmark* dan identifikasi kapabilitas atau tindakan yang harus diambil untuk dapat meningkatkan performansi. Pemodelan *maturity* untuk pengendalian intern disertakan pada Lampiran B.
- Metrik dan tujuan performansi menunjukkan kesesuaian proses TI dalam mencapai tujuan bisnis dan TI perusahaan. Metrik digunakan juga untuk mengukur performansi proses internal sesuai prinsip '*balanced scorecard*'¹⁰
- Gol aktivitas (*activity goal*) untuk pengukuran terhadap performansi yang efektif terhadap proses.

2.3.2.2 Domain pada COBIT

Terdapat empat domain utama dalam *framework* COBIT :

1. *Plan and Organize (PO)*

Domain ini meliputi strategi dan identifikasi peran TI untuk berkontribusi dalam mencapai objektivitas bisnis perusahaan. Dalam merealisasikan visi strategis perusahaan diperlukan perencanaan, komunikasi dan pengelolaan yang tepat, terutama pada sektor infrastruktur teknologi perusahaan.

2. *Acquire and Implement (AI)*

Untuk memenuhi strategi TI, solusi-solusi TI perlu untuk diidentifikasi, dikembangkan atau diperoleh, diimplementasikan, dan diintegrasikan dalam proses bisnis. Sebagai tambahan, perubahan serta pengelolaan selanjutnya

¹⁰ *Balanced scorecard* adalah sebuah pendekatan yang digunakan untuk mengukur performansi suatu perusahaan melalui empat cara pandang yang seimbang : dari segi financial, pelanggan, proses bisnis internal, dan pegawai (pertumbuhan dan proses pembelajaran). Pendekatan ini diperkenalkan pertama kali pada tahun 1992 oleh Robert Kaplan dan David Norton. [WEB01]

juga dibahas dalam domain ini agar menjamin solusi-solusi TI tersebut tetap sesuai dengan objektivitas perusahaan.

3. *Deliver and Support (DS)*

Domain ini fokus terhadap pengimplementasian sesungguhnya terhadap pelayanan yang diberikan, termasuk *service delivery*, *security & continuity management*, *service support* untuk pengguna, manajemen data dan fasilitas operasional.

4. *Monitor and Evaluate (ME)*

Seluruh proses TI perlu untuk diperiksa dan diberi penilaian terhadap kualitas dan kepatuhannya terhadap kebutuhan kendali perusahaan dari waktu ke waktu. Domain ini akan mencakup manajemen, pengawasan terhadap pengendalian intern, kepatuhan terhadap pengaturan dan penyediaan tata kelola yang sesuai.

2.3.3 Area Fokus Tata Kelola TI

Menurut analisis yang dilakukan terhadap tata kelola TI, dapat dijelaskan bahwa terdapat lima kelompok besar area fokus tata kelola TI sebuah perusahaan. Berikut adalah penjabarannya serta fokus yang disorot terhadap pengendalian intern dan pemetaannya dengan model teoretis. Dalam membentuk pemetaan, digunakan titik kendali dengan derajat kepentingan (*importance level*) yang berbeda-beda dan yang memiliki tingkat keterhubungan primer maupun sekunder dengan fokus tata kelola TI.

Primer berarti antara fokus area tata kelola TI dengan titik kendali COBIT terkait dengan erat dalam penerapannya dan saling tergantung secara keseluruhan, sehingga seluruh aspek dalam titik kendali tersebut akan terkait langsung dengan area fokus. Pada keterhubungan sekunder, berarti tidak segala aspek titik kendali tersebut terkait dengan area fokus. Pada pemetaan yang tidak mengandung keterhubungan primer maupun sekunder tidak berarti tidak ada keterhubungan sama sekali di antara area fokus dan titik kendali tersebut, tetapi keterhubungan tersebut sangat kecil dan tidak mencakup seluruh bagian.

Tabel II-1 Pemetaan Fokus Area Tata Kelola TI

	IMPORTANCE	Focus Area				
		Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement
Plan and Organize						
PO1 Define a Strategic IT Plan	H	P		S	S	
PO2 Define the Information Architecture	L	P	S	P	S	
PO3 Determine Technological Direction	M	S	S	P	S	
PO4 Define IT Processes, Organisation & Relationship	L	S		P	P	
PO5 Manage the IT Investment	M	S	P	S		S
PO6 Communicate Management Aims and Direction	M	P			P	
PO7 Manage IT Human Resource	L	P		P	S	S
PO8 Manage Quality	M	P	S		S	
PO9 Assess and Manage IT Risks	H	P			P	
PO10 Manage Projects	H	P	S	S	S	S
Acquire and Implement						
AI2 Acquire and Maintain Application Software	M	P	P	S	S	
AI3 Acquire and Maintain Technology Infrastructure	M	P	P		S	
AI4 Enable Operation and Use	L			P		
AI5 Procure IT Resource	L	S	P	S	S	
AI6 Manage Changes	M		S	P		
AI7 Install and Accredite Solutions and Changes	H		P	S		
AI1 Identify Automated Solutions	M	S	P	S	S	S
Deliver and Support						
DS1 Define and Manage Service Levels	M	P	P	P		P
DS2 Manage Third-Party Services	L		P	S	P	S
DS3 Manage Performance and Capacity	L	S	S	P	S	S
DS4 Ensure Continuous Service	M	S	P	S	P	S
DS5 Ensure System Security	H				P	
DS6 Identify and Allocate Users	L		S	P		S
DS7 Educate and Train Users	L	S	P		S	
DS8 Manage Service Desk and Incidents	L	S	P			S
DS9 Manage the Configurations	M		P		S	
DS10 Manage Problems	M		P		S	
DS11 Manage Data	H		P	P	P	
DS12 Manage the Physical Environment	L			S	P	
DS13 Manage Operations	L			P		
Monitor and Evaluate						
ME1 Monitor and Evaluate IT Performance	H					P
ME2 Monitor and Evaluate Internal Control	M		P		P	
ME3 Ensure Regulatory Compliance	H	P			P	
ME4 Provide IT Governance	H	P	P	P	P	P

Area fokus yang pertama adalah arah strategis (*strategic alignment*) perusahaan. Area ini menjelaskan tentang perlunya arah strategis yang mengatur serta mengarahkan gol dan objektif utama perusahaan dalam setiap aspek tata kelola perusahaan. Arah strategis ini diatur dan dijalankan oleh pihak eksekutif perusahaan dalam menjalankan kegiatan operasionalnya dan membangun tata kelola untuk tiap-tiap bagian perusahaan. Termasuk tata kelola TI yang sejalan dan selalu mendukung arah strategis tata kelola perusahaan.

Mendukung hal ini, yang penting untuk dilaksanakan adalah membangun rancangan arah strategis tata kelola TI, termasuk pengaturan terhadap pelaksanaan proyek, komunikasi yang baik terhadap perancangan pihak manajemen, serta penanggulangan resiko. Dalam membangun perencanaan tata kelola TI tersebut, perlu dilaksanakan penilaian serta pengelolaan yang dilakukan secara kontinyu terhadap resiko-resiko atau kelemahan-kelemahan TI yang telah terdeteksi dan memerlukan tindakan kendali preventif maupun korektif. Kendali ini kemudian harus dipastikan pemenuhannya dengan melakukan proses audit.

Area fokus kedua adalah *value delivery*. Pada area ini yang menjadi tujuan utama adalah bagaimana *value* tata kelola TI dapat tersampaikan dengan baik melalui pengaturan *resource* dalam tata kelola TI. Pengaturan tersebut akan meliputi antara lain, keuangan dan penggunaan dana investasi TI perusahaan untuk tata kelola TI, manajemen terhadap proyek TI, manajemen terhadap perubahan (*change management*), otomasi terhadap solusi, pengaturan kesepakatan dengan pihak ketiga, manajemen pelatihan bagi *user*, dan sebagainya. Pada dasarnya, pengaturan yang berhubungan dengan fokus area *value delivery*, akan berpengaruh langsung terhadap tingkat kualitas dari penerapan atau penggunaan sistem TI secara keseluruhan bagi user.

Area fokus ketiga adalah *resource management* atau pengelolaan sumber daya yang digunakan dalam tata kelola TI. Telah dijabarkan sebelumnya bahwa sumber daya dalam TI meliputi sumber daya manusia (*user, developer, support technicians*), aplikasi atau perangkat lunak yang digunakan, infrastruktur teknologi, seperti jaringan, perangkat keras yang digunakan serta perlengkapannya, dan yang terakhir adalah perangkat

informasi atau data yang diolah itu sendiri. Keempat unsur utama dalam tata kelola TI ini memerlukan efisiensi tinggi dalam kegiatan operasional hariannya agar tepat guna dan memiliki manfaat bagi semua pihak yang membutuhkannya.

Dalam penerapannya, hal-hal yang perlu untuk diperhatikan antara lain adalah pendefinisian arsitektur utama informasi terkait serta penentuan arah teknologi yang akan dikembangkan,

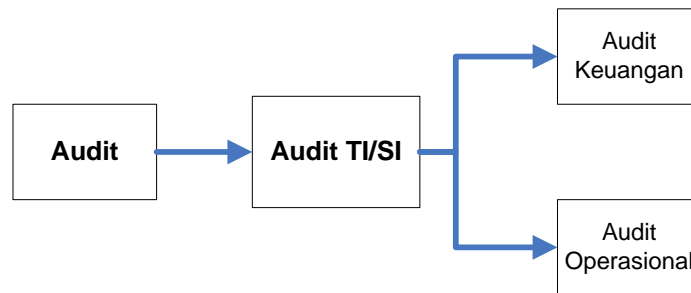
Area fokus keempat adalah *risk management* atau pengelolaan resiko terhadap tata kelola TI perusahaan. Hal yang menjadi perhatian utama adalah kegiatan yang perlu dilakukan oleh pihak manajemen perusahaan agar dapat melakukan pengukuran dan penilaian terhadap resiko serta manajemen penanganan resiko tersebut. Hal ini dilakukan sebagai bentuk penjaminan terhadap pengamanan sistem termasuk di dalamnya pengelolaan terhadap data perusahaan, serta pengaturan terhadap pelanggaran peraturan perusahaan yang mungkin terjadi sebagai salah satu bentuk resiko yang harus dihadapi perusahaan.

Selain itu, untuk dapat melakukan pengelolaan terhadap resiko diperlukan pendefinisian proses-proses, organisasi, serta keterhubungan antar proses yang terdefinisi dengan jelas di dalam tata kelola TI perusahaan, baik untuk personel maupun pihak ketiga. Manajemen terhadap resiko juga dilakukan dengan memastikan bahwa servis akan berkelanjutan dan berjalan pada lingkungan (*physical environment*) yang sesuai. Manajemen resiko TI juga menjadi salah satu titik penting pada implementasi pengendalian intern tata kelola TI.

Area terakhir atau kelima dari tata kelola TI adalah *Performance Measurement* yang mengatur bagaimana performansi dari TI perusahaan dapat terukur. Area fokus ini terutama berhubungan dengan proses monitoring dan evaluasi dari performansi tata kelola TI itu sendiri, sehingga akan dibutuhkan pendefinisian serta pengelolaan dari tingkatan pelaksanaan servis tiap sistem sebagai *threshold*.

2.4 IS Auditing (Audit TI/SI)

Audit pada dasarnya adalah sebuah proses yang sistematis dan objektif dalam mengevaluasi kegiatan ekonomi serta memperoleh bukti-bukti yang relevan, guna memberikan asersi dan menilai sejauh apakah tindakan ekonomi yang dijalankan sesuai dengan kriteria yang berlaku dan melaporkannya kepada pihak yang berkepentingan.



Gambar II-4 Penjabaran Audit

Terdiri dari dua dimensi utama, yaitu Audit keuangan dan Audit operasional terhadap manajemen sumber daya informasi, Audit TI dapat diartikan secara harafiah menjadi dua. Yang pertama, audit keuangan bertujuan untuk memastikan tidak adanya salah saji material pada laporan keuangan dengan menggunakan sistem audit berbasis komputer. Sementara pemahaman kedua (yang digunakan dalam Tugas Akhir ini) mengaudit efektivitas, efisiensi, serta tepat guna tidaknya unit fungsional sistem serta kinerja manajemen TI pada suatu perusahaan. Sehingga definisi yang digunakan adalah : Audit sistem informasi (teknologi informasi) merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi asset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta dapat menggunakan sumber daya yang dimiliki secara efisien [WEB02].

Sesuai dengan yang dipaparkan dalam 2.2.2.1, Audit TI dapat dikelompokkan berdasarkan letak kendalinya, yaitu :

- Pengendalian Umum (*general control*). Aplikasi ini bertujuan sebagai pengendali umum yang menjamin integritas data yang terdapat dalam sistem komputer dan

sekaligus meyakinkan integritas program atau aplikasi yang digunakan untuk melakukan pemrosesan data.

- Pengendalian Aplikasi (*application control*). Aplikasi ini ditujukan untuk memastikan bahwa data di-input secara benar ke dalam aplikasi, diproses secara benar, dan terdapat pengendalian yang memadai atas output yang dihasilkan.

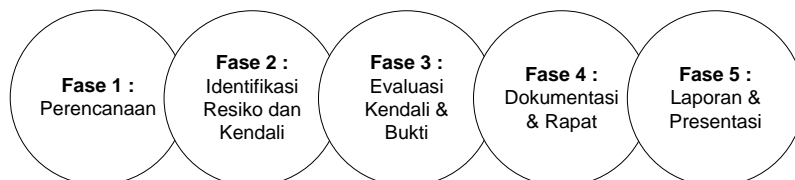
Aspek yang diperiksa pada audit sistem TI adalah :

- Audit secara keseluruhan yang menyangkut *availability system, reliability, confidentiality, integrity, dan security*.
- Audit proses, meliputi modifikasi pada program, audit atas sumber data, audit file data, audit storage, serta alur data dan informasi dalam perusahaan.

2.4.1 Tahapan Audit TI

Pada dasarnya, tahapan-tahapan dalam audit TI tidak berbeda dengan audit pada umumnya. Perbedaannya dengan audit biasa, seringkali auditor TI menerapkan teknik audit berbantuan computer, yang disebut juga (*Computer Aided Auditing Technique*). Teknik ini digunakan untuk menganalisis data.

Secara garis besar terdapat 5 tahapan utama dalam metodologi audit TI, yaitu :



Gambar II-5 Tahapan Audit TI

Fase 1 – Fase Perencanaan

Tahap perencanaan mutlak dilakukan sebagai tahap pendahuluan untuk mengenal objek yang akan diperiksa dan mendapatkan program audit yang dirancang dengan tepat bagi perusahaan terkait. Informasi yang dikumpulkan oleh tim auditor pada **Fase 1** meliputi definisi perusahaan, gambaran proses bisnis perusahaan, proses sistem dalam perusahaan, meliputi alur data dan aset serta proses audit yang dilakukan oleh perusahaan selama ini. Tim auditor mendefinisikan kebutuhan audit perusahaan tersebut guna merancang pedoman

audit yang sesuai bagi perusahaan yang juga meliputi scope audit, rentang waktu pelaksanaan, dan prakarsa pelaksana termasuk tahapan pelaksanaan dan penanggung jawab pelaksana.

Fase 2 – Mengidentifikasi resiko dan kendali

Pada fase ini, setelah memahami proses TI perusahaan, tim audit melakukan identifikasi terhadap resiko-resiko yang mungkin dihadapi serta bentuk kendali yang diterapkan oleh sistem untuk menanggulangi atau mencegah resiko tersebut. Identifikasi ini didapatkan melalui observasi langsung terhadap keseluruhan tata kelola TI perusahaan termasuk sistem yang digunakan serta dokumentasi terkait. Pada umumnya di perusahaan besar, pedoman telah ditetapkan oleh kebijakan perusahaan pusat berupa poin-poin titik kendali yang dibangun berdasarkan *framework* tertentu yang digunakan oleh perusahaan seperti misalnya COBIT. Berdasarkan titik kendali tersebut, pihak auditor mengidentifikasi kendali nyata yang diterapkan pada sistem TI perusahaan.

Fase 3 – Mengevaluasi kendali dan mengumpulkan bukti.

Berdasarkan pengidentifikasian kendali yang dilakukan pada **Fase 2**, pada fase ini pihak auditor melakukan evaluasi terhadap kendali tersebut. Bukti yang dikumpulkan pada audit TI mencakup juga bukti elektronik. Dalam pelaksanaannya, auditor TI mengumpulkan bukti-bukti yang memadai melalui berbagai teknik termasuk survei, wawancara (*interview*), observasi dan review dokumentasi (termasuk *source code* apabila dibutuhkan).

Fase 4 – Mendokumentasikan temuan dan mendiskusikan dengan auditee

Auditor bertanggung jawab terhadap pendokumentasian temuan-temuan dalam proses audit. Apabila ada faktor-faktor kendali yang kurang tepat atau temuan-temuan lain, pihak auditor berkewajiban untuk membuka diskusi dengan pihak auditee. Dalam diskusi ini, auditor menyampaikan hasil temuannya dan apabila ada sesuatu yang kurang, auditor mengusulkan suatu bentuk solusi kepada auditee dan auditee melaksanakan tindak lanjut dari solusi tersebut. Pada tahap

paska-audit, pihak auditor memiliki kewajiban untuk menuntaskan pemeriksaan terhadap tindak lanjut auditee menyikapi kekurangan tersebut.

Fase 5 – Laporan akhir & mempresentasikan hasil yang diperoleh.

Sesuai dengan standar auditing ISACA, selain melakukan pekerjaan lapangan, auditor juga harus menyusun laporan yang mencakup tujuan pemeriksaan, sifat dan kedalaman pemeriksaan yang dilakukan. Laporan ini juga harus menyebutkan organisasi yang diperiksa, pihak pengguna laporan yang dituju dan batasan-batasan distribusi laporan. Laporan juga harus memasukkan temuan, kesimpulan, dan rekomendasi sebagaimana layaknya laporan audit pada umumnya.

2.4.2 Standar Audit TI

Standar yang digunakan dalam mengaudit TI adalah standar yang diterbitkan oleh ISACA yaitu *ISACA IS Auditing Standard* yang menjadi referensi [ISA07]. Selain itu ISACA juga menerbitkan *IS Auditing Guidance* dan *IS Auditing Procedures*. *Standard* didefinisikan sebagai hal mandat yang harus dipatuhi oleh IS Auditor, *Guidelines* memberikan penjelasan bagaimana auditor dapat memenuhi standar dalam berbagai penugasan audit, dan *Procedures* memberikan contoh langkah-langkah yang perlu dilalui oleh auditor dalam penugasan audit tertentu sehingga sesuai dengan standar. Namun, selain hal tersebut, IS Auditor harus bisa menggunakan penilaian profesional ketika menggunakan *guidance* dan *procedure*.

ISACA IS Auditing Standard terdiri atas standar-standar, yang menjabarkan mulai dari *audit charter* hingga etos kerja, kegiatan audit, pelaporan, aktivitas lanjutan pasca audit (*follow-up*), hingga Tata kelola TI. *ISACA IS Auditing Guidelines* terdiri atas 32 *guidance* dalam audit TI yang meliputi petunjuk pelaksanaan audit area-area tertentu yang penting. *ISACA IS Auditing Procedures* terdiri atas sembilan prosedur yang menunjukkan langkah-langkah yang dilakukan auditor dalam penugasan audit yang spesifik seperti prosedur *assessment*, pengujian terhadap sistem deteksi (*detection system*) dan sebagainya.