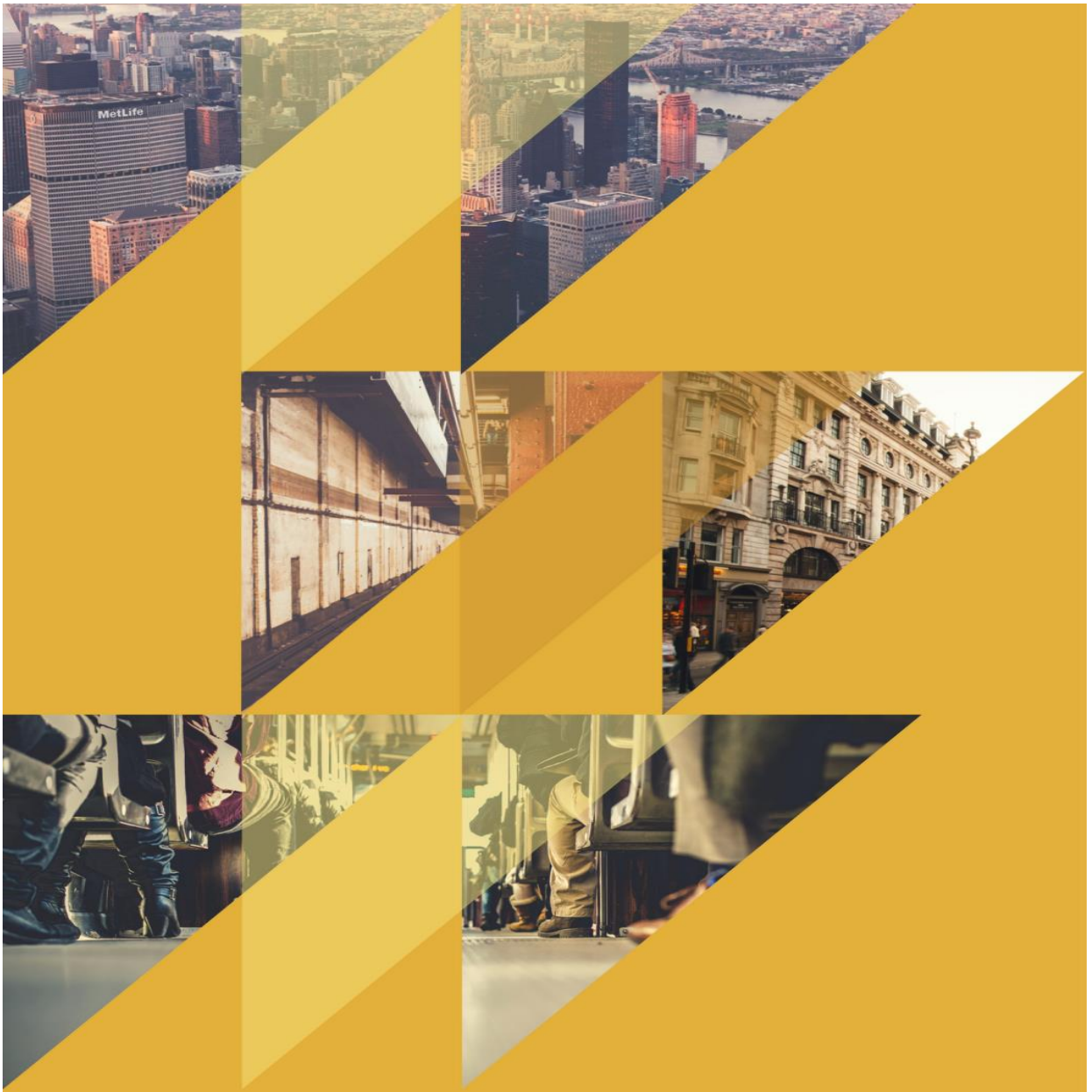


AUDIT SISTEM INFORMASI

Achmad solechan, MSi, MKom.

AUDIT SISTEM INFORMASI

Disusun Oleh:

Achmad Solechan

Kerja sama Penerbit YPAT dengan Universitas STEKOM

Penerbit :
YAYASAN PRIMA AGUS TEKNIK
Redaksi:
Jln Majapahit No 605 Semarang
Tlpn. (024) 6723456
Fax . 024-6710144
Email: penerbit_ypat@stekom.ac.id

Audit Sistem Informasi

Penulis:
Achmad Solechan, SKom., M.Si., M.Kom

ISBN: 978-623-6141-36-6

Editor :
Jarot Dian Susatyono, M.Kom

Penyunting:
Haryo Kusumo, M.Kom.

Desain Sampul dan Tata Letak:
Yuli Fitrianto, ST., M.Kom

Penerbit:
Yayasan Prima Agus Teknik
Redaksi:
Jln Majapahit No 605 Semarang
Tlpn. (024) 6723456
Fax . 024-6710144
Email: penerbit_ypat@stekom.ac.id

Distributor Tunggal:
UNIVERSITAS STEKOM
Jalan Majapahit No. 605 Semarang
Tlpn. (024) 6723456
Fax. 024-6710144
Email: info@stekom.ac.id

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas berkat, rahmat dan karunia-Nya sehingga buku ajar untuk mata kuliah Audit Sistem Informasi ini telah berhasil diselesaikan. Buku ajar ini diperuntukkan sebagai pegangan bagi mahasiswa program studi Sistem Informasi agar mahasiswa dapat memahami dan implementasi secara konsep dan operasional terkait dengan audit sistem informasi.

Bahan ajar ini disusun dengan tujuan menyediakan materi pembelajaran audit sistem informasi untuk mahasiswa sesuai dengan standar kurikulum yang telah ditentukan dan disepakati bersama, dengan materi antara lain tinjauan umum auditing, risiko dalam perkembangan teknologi, sistem pengendalian internal, kode etik audit sistem informasi, standar audit sistem informasi, struktur proses dan mekanisma tata kelola teknologi infomasi, strategi dan teknik tata kelola teknologi informasi, nilai teknologi informasi, tata kelola teknologi informasi, implementasi tata kelola teknologi informasi dan framework IT Balanced Scorecard

Demikian, semoga buku ajar ini dapat bermanfaat bagi anda semua khususnya mahasiswa UNIVERSITAS STEKOM Semarang atau praktisi yang sedang mengembangkan bahan ajar untuk kegiatan perkuliahan.

Semarang, 27 April 2021

Redaksi

DAFTAR ISI

BAB I

Tinjauan Umum Auditing dan Perkembangannya

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- Menjelaskan Pengenalan Audit
- Menjelaskan Perkembangan Audit
- Menjelaskan Audit Internal
- Menjelaskan Fungsi dan Tujuan Audit Internal
- Menjelaskan Independen Audit Internal
- Menjelaskan Laporan Internal Audit
- Menjelaskan Audit Sistem Informasi
- Menjelaskan Tujuan Audit Sistem Informasi
- Menjelaskan *Computer Audit Software* (CAS) atau *Generalized Audit Software* (GAS)
- Menjelaskan Langkah dasar Audit SI

A. Pengenalan Audit

Perkembangan sistem informasi yang digunakan oleh klien berdampak dengan keahlian yang harus dikuasai oleh auditor yang semula pendekatan yang dilakukan dengan cara manual maka dengan perubahan tersebut auditor dituntut untuk menguasai proses sistem informasi yang dipakai klien dan Teknik Audit Berbantuan Komputer (TABK) dengan menyesuaikan proses audit dan prosedur yang digunakan pada saat melaksanakan pekerjaan lapangan misalnya perubahan lingkungan sistem akuntansi yang manual menjadi sistem informasi akuntansi berbasis komputer menyebabkan auditor harus mempelajari karaktristik

lingkungan sistem tersebut. Agar pelaksanaan *auditing* dapat berjalan dengan efektif dan efisien, auditor sudah seharusnya menyesuaikan teknik-teknik auditnya dengan sistem informasi klien.

Untuk memperoleh pemahaman tentang efinisi audit, type-type audit, jenis-jenis auditor, pengetahuan sistem, informasi, berikut akan dibahas secara rinci.

Menurut pendapat Ron Weber (1999), " EDP auditing is the process of collecting and evaluating evidence to determine whether a computer systems safeguards assets, maintains data integrity, achieves organzational goals effectively, and consumes resources effiently". Pengertiannya secara garis besar ialah proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah menetapkan dan menerapkan sistem pengendalian intern yang memadai, semua aktiva dilindungi dengan baik/ tidak disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan system informasi berbasis komputer.

Ada beberapa definisi audit yang diberikan oleh beberapa ahli di bidang akuntansi, antara lain:

Menurut Alvin A.Arens dan James K.Loebbecke : "Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria. Auditing should be done by a competent independent person".

Menurut Mulyadi :"Suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara obyektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan". Dalam melaksanakan audit faktor-faktor berikut harus diperhatikan:

1. Dibutuhkan informasi yang dapat diukur dan sejumlah kriteria (standar) yang dapat digunakan sebagai panduan untuk mengevaluasi informasi tersebut,

2. Penetapan entitas ekonomi dan periode waktu yang diaudit harus jelas untuk menentukan lingkup tanggungjawab auditor,
3. Bahan bukti harus diperoleh dalam jumlah dan kualitas yang cukup untuk memenuhi tujuan audit,

Kemampuan auditor memahami kriteria yang digunakan serta sikap independen dalam mengumpulkan bahan bukti yang diperlukan untuk mendukung kesimpulan yang akan diambilnya.

B. Perkembangan Audit

Pengauditan telah mulai dilakukan sejak abad ke limabelas. Tahun kelahiran pengauditan laporan keuangan secara pasti tidak diketahui, tetapi dari berbagai sumber dapat diketahui bahwa pada sekitar awal abad ke limabelas jasa auditor telah mulai digunakan di Inggris. Meskipun pengauditan telah lahir sejak beberapa abad yang lalu, namun perkembangan yang pesat baru terjadi pada abad ini.

Kelahiran fungsi pengauditan di Amerika Utara berasal dari Inggris. Akuntansi sebagai profesi diperkenalkan di bagian benua ini oleh Inggris pada paruh kedua abad ke sembilan belas. Para akuntan di Amerika Utara mengadopsi bentuk laporan dan prosedur audit sebagaimana yang berlaku di Inggris.Perusahaan-perusahaan publik di Inggris pada waktu itu harus tunduk pada undang-undang yang disebut ***Companies Act***. Menurut undang-undang tersebut semua perusahaan publik harus diaudit. Ketika fungsi audit mulai diekspor ke Amerika Serikat, bentuk laporan model Inggris turut diadopsi pula meskipun peraturan yang berlaku di Amerika Serikat tidak sama dengan yang berlaku di Inggris. Sebagaimana disebutka di atas, di Inggris semua perusahaan publik harus diaudit, sedangkan di Amerika Serikat pada waktu itu tidak wajib diaudit. Keharusan untuk diaudit datang dari badan yang mengatur pasar modal yang disebut ***Securities and Exchange Commission (SEC)***, serta dari pengakuan umum mengenai manfaat pendapat auditor atas laporan keuangan.

Tidak adanya peraturan undang-undang yang mengharuskan audit atas laporan yang diberikan kepada para pemegang saham, menyebabkan audit pada

abad ke semblin belas menjadi beraneka-ragam, kadang-kadang hanya meliputi neraca saja, tapi ada pula yang berupa audit atas semua rekening yang ada pada perusahaan dan dilakukan secara menyeluruh dan mendalam. Auditor biasanya mendapat penugasan dari manajemen atau dari dewan komisaris perusahaan, dan laporan hasil audit biasanya dialamtkan kepada pihak intern perusahaan, bukan kepada para pemegang saham. Pemberian laporan kepada pemegang saham pada waktu itu tidak biasa dilakukan. Para manajer perusahaan hanya mengingikan untuk mendapat jaminan dari auditor bahwa kecurangan dan kekeliruan dalam pencatatan tidak terjadi.

Memasuki abad XX, revolusi industri kira-kira telah berusia 50 tahun dan selama masa itu jumlah perusahaan industri telah berkembang dengan pesat. Jumlah pemegang saham juga semakin bertambah dan mereka sudah mulai menerima laporan auditor. Kebanyakan pemegang saham baru ini tidak memahami makna pekerjaan seorang auditor, dan kesalahpahaman melanda banyak pihak termasuk para pimpinan perusahaan dan bankir. Pada umumnya mereka beranggapan bahwa pendapat auditor adalah jaminan keakuratan laporan keuangan.

Profesi akuntansi di Amerika berkembang pesat setelah berakhirnya Perang Dunia I. Sementara itu kesalahpahaman tentang fungsi pendapat auditor masih terus berlangsung, sehingga pada tahun 1917 ***Federal Reserve Board*** menerbitkan ***Federal Reserve Buletin*** yang memuat cetak ulang suatu dokumen yang disusun oleh ***American Institute of Accountant*** (yang selanjutnya berubah menjadi ***American Institute of Certified Public Accountants*** atau ***AICPA*** pada tahun 1957) yang berisi himbauan tentang perlunya akuntansi yanng seragam, tetapi tulisan tersebut sesungguhnya lebih banyak menguraikan tentang bagaimana mengaudit neraca. Pernyataan teknis ini merupakan pernyataan pertama yang dikeluarkan oleh profesi akuntansi di Amerika Serikat dari sekian banyak pernyataan yang dikeluarkan selama abad ke-20.

Pada awalnya, para akuntan publik menyusun laporan tanpa mengikuti pedoman resmi. Akan tetapi pada 50 tahun terakhir, profesi dengan cepat

mengembangkan redaksi laporan yang umum digunakan melalui ***AICPA***. Redaksi atau susunan kalimat dalam laporan hasil audit tidak lagi merupakan pekerjaan mengarang kalimat dalam laporan, melainkan merupakan proses pengambilan keputusan. Alternatif bentuk tipe laporan yang dapat dipilih auditor tidak banyak, dan sekali auditor memilih jenis pendapat yang diberikan dalam situasi tertentu, auditor tinggal memilih jenis laporan yang dirncang untuk menyatakn pendapat tersebut.

C. Audit Internal

Audit adalah Sebuah proses sitematis untuk secara objektif mendapatkan dan mengevaluasi bukti mengenai pernyataan perihal tindakan dan transaksi bernilai ekonomi, untuk memastikan tingkat kesesuaian antara pernyataan tersebut denngan kriteria yanng telah ditetapkan serta mengkomunikasikan hasil-hasilnya pada para pemakai yang berkepentingan.

Dilihat dari definisi di atas, unsur penting dalam pelaksanaan auditing adalah proses perolehan serta pengevaluasian bukti-bukti dan kriteria-kriteria yang telah ditetapkan. Bukti-bukti yang diperoleh baik dari dalam perusahaan maupun dari luar perusahaan digunakan sebagi bahan evaluasi sehingga hasil audit lebih objektif. Kriteria-kriteria yang ditetapkan digunakan sebagai tolak ukur auditor untuk memberikan pendapatnya yang kemudian dituangkan ke dalam laporan audit. Laporan audit harus dapat memberi informasi kepada para pengguna akan tingkat kesesuaian dari informasi tersebut dengan kriteria-kriteria yang ditetapkan.

Jika dilihat dari pihak yang melakukan pemeriksaan, terdapat dua kelompok auditor yaitu auditor internal dan auditor eksternal. Kedudukan dan tanggung jawab di antara kedua kelompok auditor tersebut sangat berbeda satu sama lain. Seorang auditor internal bekerja pada perusahaan, lembaga pemerintahan, atau perusahaan nirlaba, sedangkan auditor eksternal bekerja pada suatu Kantor Akuntan Publik (KAP). Meskipun pihak yang melakukan internal audit merupakan bagian dari organisasi yang diaudit itu sendiri, tetapi pelaksanaan internal audit harus tetap obyektif dan independen dari aktivitas yang diaudit.

Auditor internal umumnya melapor kepada manajer senior atau dewan direksi, sedangkan auditor eksternal hanya memiliki struktur pelaporan yang terbatas kepada kantor akuntan tempat auditor tersebut bekerja dan pihak ketiga (kreditor dan investor).

Audit internal adalah aktivitas independen, keyakinan obyektif, dan konsultasi yang dirancang untuk menambah nilai dan meningkatkan operasi organisasi. Audit internal ini membantu organisasi mencapai tujuannya dengan melakukan pendekatan sistematis dan disipilin untuk mengevaluasi dan meningkatkan efektifitas manajemen resiko, pengendalian, dan proses tata kelola.

Definisi ini mengandung pengertian bahwa internal audit merupakan suatu aktivitas yang dilakukan untuk membantu manajemen dalam penyediaan informasi, dengan tujuan akhir yaitu menambah nilai perusahaan. Pelaksanaan internal audit dilakukan secara independen dan obyektif yang berarti tidak terpengaruh oleh pihak manapun dan tidak terlibat dalam pelaksanaan kegiatan yang diaudit. Hasil audit yang diperoleh dari pelaksanaan internal audit secara independen dan obyektif tersebut akan dapat diandalkan oleh para pengguna informasi.

Sawyer (2005) mengemukakan definisi audit internal yang menggambarkan lingkup audit internal modern yang luas dan tak terbatas. Audit internal adalah sebuah penilaian yang sistematis dan objektif yang dilakukan auditor internal terhadap operasi dan kontrol yang berbeda-beda dalam organisasi untuk menentukan apakah :

- Informasi keuangan dan operasi telah akurat dan dapat diandalkan,
- Risiko yang dihadapi perusahaan telah diidentifikasi dan diminimalisasi,
- Peraturan eksternal serta kebijakan dan prosedur internal yang biasa diterima telah diikuti,
- Kriteria operasi yang memuaskan telah dipenuhi,
- Sumber daya telah digunakan secara efisien dan ekonomis, dan tujuan organisasi telah dicapai secara efektif --semua dilakukan dengan tujuan

untuk dikonsultasikan dengan manajemen dan membantu anggota organisasi dalam menjalankan tanggung jawabnya secara efektif.

Definisi ini tidak hanya mencakup peranan dan tujuan auditor internal, tetapi juga mengakomodasikan kesempatan dan tanggung jawab. Definisi tersebut juga memadukan persyaratan-persyaratan signifikan yang ada di Standar dan menangkap lingkup yang luas dari auditor internal modern yang lebih menekankan pada penambahan nilai dan semua hal yang berkaitan dengan risiko, tata kelola, dan kontrol.

Perusahaan yang berkembang di Indonesia memiliki kedudukan yang penting dalam perekonomian dan pembangunan bagi masyarakat Indonesia, maka peran internal audit menjadi semakin penting untuk mengawasi perusahaan secara independen.

Definisi lain menurut Sukrisno (2004) mengenai internal audit sebagai berikut: Internal audit adalah pemeriksaan yang dilakukan oleh bagian internal audit perusahaan, baik terhadap laporan keuangan dan catatan akuntansi perusahaan, maupun ketaatan terhadap kebijakan manajemen puncak yang telah ditentukan dan ketaatan terhadap peraturan pemerintah dan ketentuan-ketentuan dari ikatan profesi yang berlaku.

Definisi di atas menunjukkan bahwa internal audit telah mengalami perkembangan. Lingkup internal audit tidak lagi hanya terbatas melakukan pemeriksaan di bidang keuangan saja, tetapi juga melakukan pemeriksaan di bidang lainnya seperti pengendalian, kepatuhan, operasional dan lain-lain.

Bertolak dari definisi-definisi di atas, dalam perkembangannya konsep internal audit telah mengalami perubahan. Peranan internal audit sebelumnya hanya sebatas sebagai pengawas di dalam perusahaan yang kerjanya hanya mencari kesalahan, sedangkan saat ini internal audit dapat memberikan saran dan masukan berupa tindakan perbaikan atas sistem yang telah ada. Oleh karena itu, saat ini internal audit dapat juga dikatakan sebagai konsultan perusahaan dalam mencapai tujuannya di masa yang akan datang. Internal auditor harus selalu

meningkatkan pengetahuan baik di bidang auditing sendiri maupun pengetahuan di bidang bisnis perusahaan agar dapat memberikan saran dan masukan berupa tindakan perbaikan tersebut.

D. Fungsi dan Tujuan Audit Internal

Tujuan Audit internal untuk mengevaluasi kecukupan dan efektivitas sistem pengendalian intern perusahaan serta menetapkan keluasan dari pelaksanaan tanggung jawab yang benar-benar dilakukan.

Perusahaan perkebunan memiliki kedudukan yang penting dalam perekonomian dan pembangunan, maka fungsi internal audit menjadi semakin penting. Secara umum dapat dikatakan bahwa fungsi internal audit bagi manajemen perusahaan adalah untuk menjamin pelaksanaan operasional yang sesuai dengan ketentuan-ketentuan yang berlaku.

Di dalam perusahaan, internal audit merupakan fungsi staff, sehingga tidak memiliki wewenang untuk langsung memberi perintah kepada pegawai, juga tidak dibenarkan untuk melakukan tugas-tugas operasional dalam perusahaan yang sifatnya di luar kegiatan pemeriksaan.

Audit internal terlibat dalam memenuhi kebutuhan manajemen, dan staf audit yang paling efektif meletakkan tujuan manajemen dan organisasi di atas rencana dan aktivitas mereka. Tujuan-tujuan audit disesuaikan dengan tujuan manajemen, sehingga auditor internal itu sendiri berada dalam posisi untuk menghasilkan nilai tertinggi pada hal-hal yang dianggap manajemen paling penting bagi kesuksesan organisasi.

Perumusan fungsi internal audit dalam perusahaan biasanya menyangkut sistem pengendalian manajemen, ketaatan, pengungkapan penyimpangan, efisiensi dan efektivitas, manajemen risiko, dan proses tata kelola (*good corporate governance*).

Fungsi internal audit menjadi semakin penting sejalan dengan semakin kompleksnya operasional perusahaan. Manajemen tidak mungkin dapat mengawasi seluruh kegiatan operasional perusahaan, karena itu manajemen

sangat terbantu oleh fungsi internal audit untuk menjaga efisiensi dan efektivitas kegiatan. Sawyer (2005) menyebutkan fungsi internal audit bagi manajemen sebagai berikut :

- Mengawasi kegiatan-kegiatan yang tidak dapat diawasi sendiri oleh manajemen puncak.
- Mengidentifikasi dan meminimalkan risiko.
- Memvalidasi laporan ke manajemen senior.
- Membantu manajemen pada bidang-bidang teknis.
- Membantu proses pengambilan keputusan.
- Menganalisis masa depan – bukan hanya untuk masa lalu.
- Membantu manajer untuk mengelola perusahaan.

Tujuan pemeriksaan yang dilakukan oleh internal auditor adalah untuk membantu semua pimpinan perusahaan (manajemen) dalam melaksanakan tanggung jawabnya dengan memberikan analisa, penilaian, saran dan komentar mengenai kegiatan yang diperiksanya. Untuk mencapai tujuan tersebut, internal auditor harus melakukan kegiatan-kegiatan berikut :

- Menelaah dan menilai kebaikan, memadai tidaknya dan penerapan dari sistem pengendalian manajemen, pengendalian intern, dan pengendalian operasional lainnya serta mengembangkan pengendalian yang efektif dengan biaya yang tidak terlalu mahal
- Memastikan ketaatan terhadap kebijakan, rencana dan prosedur-prosedur yang telah ditetapkan oleh manajemen
- Memastikan seberapa jauh harta perusahaan dipertanggung jawabkan dan dilindungi dari kemungkinan terjadinya segala bentuk pencurian, kecurangan dan penyalahgunaan
- Memastikan bahwa pengelolaan data yang dikembangkan dalam organisasi dapat dipercaya
- Menilai mutu pekerjaan setiap bagian dalam melaksanakan tugas yang diberikan oleh manajemen.

- Menyarankan perbaikan-perbaikan operasional dalam rangka meningkatkan efisiensi dan efektivitas.

Beberapa hal yang perlu diperhatikan oleh manajemen agar internal audit dapat terlaksana efektif dalam membantu manajemen dengan memberikan analisa, penilaian, dan saran mengenai kegiatan yang diperiksanya adalah :

- Internal audit department harus mempunyai kedudukan independen dalam organisasi perusahaan, yaitu tidak terlibat dalam kegiatan operasional yang diperiksanya.
- Internal audit department harus mempunyai uraian tugas tertulis yang jelas sehingga dapat mengetahui tugas, wewenang dan tanggung jawabnya.
- Internal audit department harus pula memiliki internal audit manual yang berguna untuk :
- Mencegah terjadi penyimpangan pelaksanaan tugas
- Menentukan standar untuk mengukur dan meningkatkan performance
- Memberi keyakinan bahwa hasil akhir internal audit department telah sesuai dengan requirement kepala internal audit

Harus ada dukungan kuat dari top management kepada Internal audit department, dukungan tersebut dapat berupa :

- Penempatan Internal audit department dalam posisi yang independe
- Penempatan audit staf dengan gaji yang menarikpenyediaan waktu yang cukup dari top manajemen untuk membaca, mendengarkan dan mempelajari laporan–laporan Internal audit department dan tanggapan yang cepat dan tegas terhadap saran-saran perbaikan yang diajukan Internal audit department harus memiliki sumber daya yang profesional, capable, bisa bersikap objective dan mempunyai integritas serta loyalitas yang tinggi. Internal audit department harus dapat bekerja sama dengan akuntan publik. Hasil kerja satuan audit intern bisa mempercepat dan mempermudah pelaksanaan pekerjaan akuntan publik.Fungsi audit

internal yaitu melakukan evaluasi dan memberikan kontribusi terhadap peningkatan proses pengelolaan risiko, pengendalian, dan governance, dengan pendekatan yang sistematis, teratur dan menyeluruh. Maksud dari pernyataan tersebut yaitu audit internal membantu organisasi dengan cara mengidentifikasi dan mengevaluasi resiko signifikan dan memberikan kontribusi terhadap peningkatan pengelolaan risiko dan sistem manajemen mutu. Berdasarkan hasil penilaian risiko tersebut, fungsi audit internal mengevaluasi kecukupan dan efektifitas sistem manajemen mutu, yang mencakup governance, kegiatan operasi, dan sistem informasi organisasi.

E. Independen Audit Internal (IAD)

Salah satu hal yang harus diperhatikan agar suatu perusahaan dapat memiliki departemen audit internal yang efektif adalah departemen audit internal tersebut harus mempunyai kedudukan yang independen dalam organisasi perusahaan.

Sukrisno (2004), mengemukakan bahwa independensi internal auditor antara lain tergantung pada: Kedudukan Internal Audit Department (IAD) tersebut dalam organisasi perusahaan, maksudnya kepada siapa IAD bertanggung jawab.

Apakah IAD dilibatkan dalam kegiatan operasional.

Jika ingin independen, departemen audit internal tidak boleh terlibat dalam kegiatan operasional perusahaan. Misalnya tidak boleh ikut serta dalam kegiatan

penjualan dan pemasaran, penyusunan sistem akuntansi, proses pencatatan transaksi, dan penyusunan laporan keuangan perusahaan.

Kedudukan departemen internal audit di dalam perusahaan akan menentukan tingkat kebebasannya dalam menjalankan tugas sebagai auditor. Kedudukan ataupun status departemen audit internal dalam suatu organisasi perusahaan mempunyai pengaruh terhadap luasnya kegiatan serta tingkat independensinya didalam menjalankan tugasnya sebagai pemeriksa. Jadi status organisasi dari departemen audit internal harus cukup untuk dapat menyelesaikan tanggung jawab audit.

Departemen audit internal hanyalah akan seefektif seperti yang diinginkan manajemennya jika ia bebas dari aktivitas-aktivitas yang diauditnya. Hal ini hanya akan dapat tercapai bila departemen audit internal mempunyai kedudukan yang memungkinkan baginya untuk mengembangkan sikap independennya terhadap bagian-bagian lain yang harus diperiksanya. Untuk mencapai keadaan seperti ini, maka auditor internal harus memperoleh dukungan dari pihak manajemen dan dewan komisaris.

Terdapat alternatif kedudukan internal auditor dalam perusahaan yaitu sebagai berikut:

- Internal auditor berada di bawah direktur keuangan.
- Internal auditor berada di bawah direktur utama yang merupakan staf dari direktur utama.
- Internal auditor merupakan staf dewan komisaris.

Kedudukan seorang internal auditor juga tidak memiliki wewenang langsung terhadap tingkatan manajemen di dalam organisasi perusahaan, kecuali pihak yang memang berada di bawahnya dalam satuan kerja internal audit itu sendiri.

Internal audit yang independen tidak dibolehkan untuk terlibat dalam kegiatan operasional perusahaan apalagi kegiatan yang diperiksanya. Sulit bagi seorang auditor untuk memberikan penilaian yang objektif dan independen apabila ternyata ia terlibat dalam kegiatan yang diperiksanya.

Sebagai penilai independen tentang peranan sistem manajemen mutu perusahaan, internal audit hanya menempatkan diri sebagai narasumber dalam pembuatan konsep sistem manajemen mutu. Pihak yang bertanggung jawab penuh dalam perancangan dan implementasi sistem manajemen mutu adalah manajemen dan direksi. Dengan demikian penilaian internal audit terhadap sistem manajemen mutu tetap independen dan objektif, tanpa terlibat langsung dalam perencanaannya.

F. Laporan Internal Audit

Hasil akhir dari pelaksanaan audit internal dituangkan dalam suatu bentuk laporan tertulis melalui proses penyusunan yang baik. Laporan hasil audit internal merupakan suatu alat penting untuk menyampaikan pertanggungjawaban hasil kerja kepada manajemen yaitu sebagai media informasi untuk menilai sejauh mana tugas-tugas yang dibebankan dapat dilaksanakan. Adapun isi atau materi laporan audit internal menurut Boynton (2003) yaitu:

- Suatu laporan tertulis yang ditandatangani harus dikeluarkan setelah pemeriksaan audit selesai. Laporan intern itu bisa dalam bentuk tertulis atau lisan dan dapat disampaikan secara formal ataupun informal.
- Auditor internal harus membahas kesimpulan dan rekomendasi pada tingkatan manajemen yang tepat sebelum mengeluarkan laporan tertulis yang final.
- Laporan haruslah objektif, jelas, ringkas, konstruktif dan tepat waktu.
- Laporan harus menyatakan tujuan, ruang lingkup, dan hasil audit, dan bila tepat, laporan itu juga harus berisi suatu pernyataan pendapat auditor.
- Laporan dapat mencakup rekomendasi untuk perbaikan yang potensial dan mengakui kinerja serta tindakan korektif yang memuaskan.
- Pandangan auditee tentang kesimpulan dan rekomendasi audit dapat disertakan dalam laporan audit.

- Direktur auditing internal atau designee harus mereview dan menyetujui laporan audit final sebelum diterbitkan serta harus memutuskan kepada siapa laporan itu akan dibagikan.

Laporan dari bagian audit internal merupakan suatu alat komunikasi yang di dalamnya terdapat tujuan yang dimulai dari penugasan, luas pemeriksaan, batasan yang dibuat dan juga saran atau rekomendasi kepada pimpinan perusahaan. Tujuan dari laporan audit adalah sebagai berikut:

- Laporan auditor adalah merupakan kesimpulan dari hasil pemeriksaan
- Menyajikan temuan-temuan dari hasil pemeriksaan yang telah dilakukan
- Sebagai dasar untuk kemudian diambil tindakan oleh manajemen terhadap penyimpangan yang terjadi.

Untuk mencapai tujuan tersebut maka laporan yang disampaikan haruslah memiliki unsur-unsur berikut ini:

- Objektif

  Laporan yang disusun harus mengungkapkan fakta dengan teliti berdasarkan data yang dapat diuji kebenarannya. Menyampaikan dengan jelas tentang pokok pemeriksaan yang telah dilakukan sehingga dapat diyakini kebenarannya.
- Clear (jelas) Laporan disusun dengan menggunakan bahasa yang jelas, tidak menimbulkan kesalahpahaman bagi penggunanya. Menerangkan dengan jelas dan lengkap agar dapat dimengerti oleh pihak-pihak yang menggunakannya.
- Ringkas

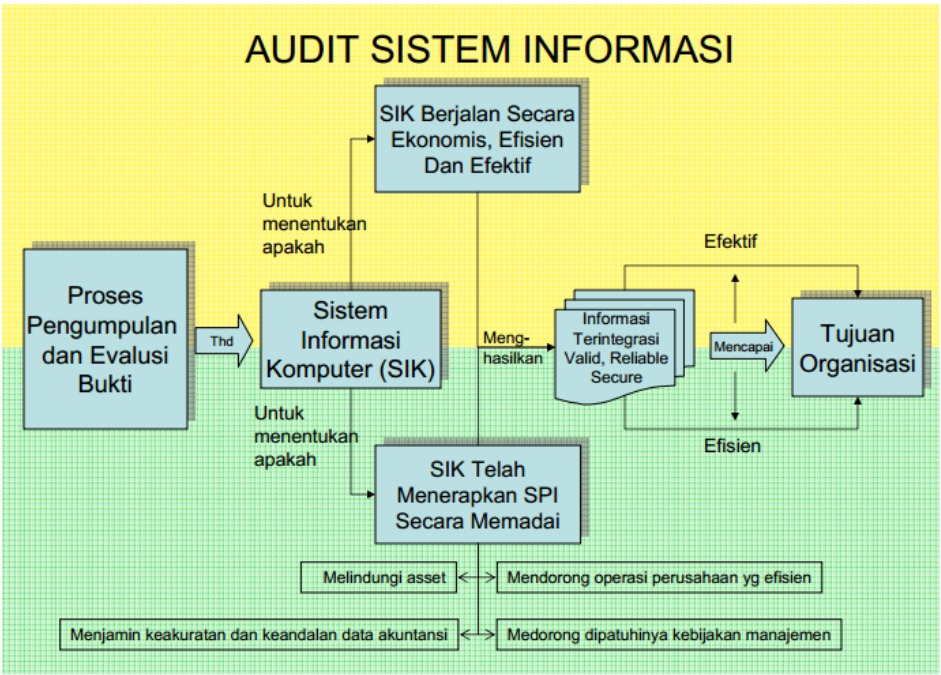
  Struktur laporan yang baik melaporkan dengan ringkas pelaksanaan operasional, pengendalian, dan hasil kerja. Laporan itu harus terhindar dari hal-hal yang tidak relevan, tidak material seperti gagasan, temuan, kalimat dan sebagainya yang tidak menunjang tema pokok laporan, namun tetap menjaga kualitas informasi yang disampaikan

melalui laporan tersebut sehingga dapat memenuhi kebutuhan pemakainya.

- Membangun (konstruktif)
  Laporan yang bersifat membangun adalah laporan yang sedapat mungkin memaparkan rekomendasi tindakan perbaikan yang dapat dilakukan untuk mengupayakan peningkatan operasi.
- Tepat waktu
  Laporan audit hanya dapat bermanfaat dengan maksimal bila laporan tersebut disajikan pada saat dibutuhkan. Sehingga auditor harus mampu menyajikan laporan yang tepat waktu.
  Sebelum disampaikan pada pengguna laporan, peninjauan kembali atas laporan (review) adalah tindakan bijak yang dapat dilakukan audit internal. Hal tersebut bertujuan untuk lebih memastikan kebenaran dan kelengkapannya. Laporan audit akan efektif bila terdapat pelaksanaan tindak lanjut agar proses audit yang berjalan benar-benar memberikan manfaat bagi perusahaan. Untuk itu departemen audit internal bertugas untuk memantau pelaksanaan tindak lanjut, menganalisis kecukupan tindak lanjut disertai identifikasi hambatan pelaksanaanya, dan memberikan laporan atas tindak lanjut tersebut.

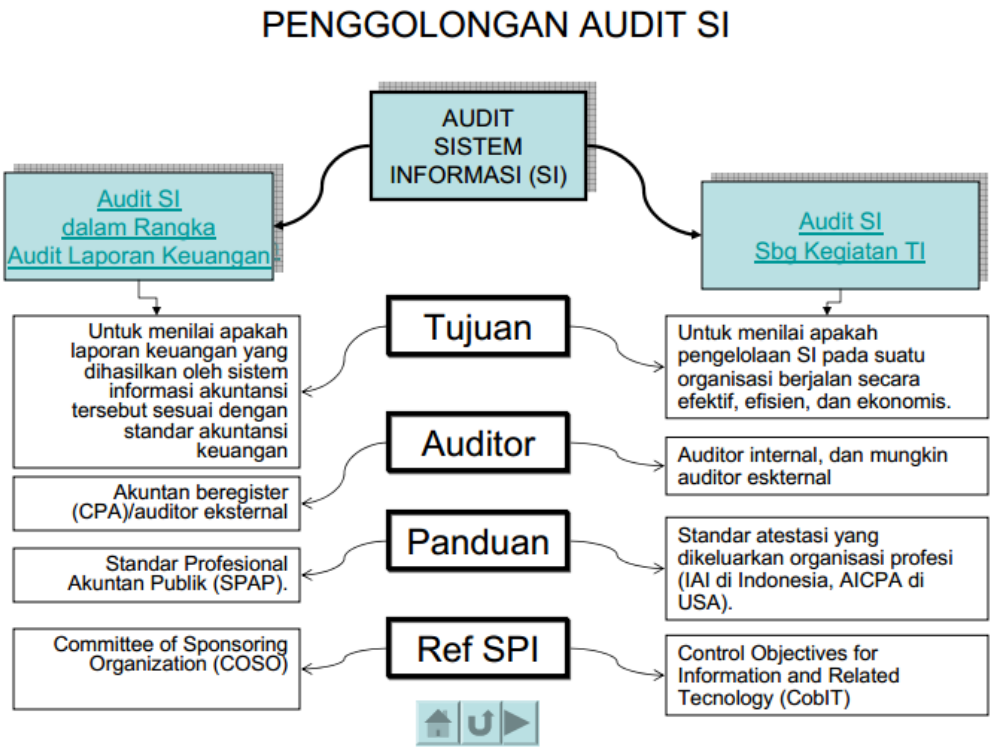
G. Audit Sistem Informasi

Audit sebuah system teknologi informasi untuk saat ini adalah sebuah keharusan. Audit perlu dilakukan agar sebuat system mampu memenuhi syarat IT Governance. Audit system informasi adalah cara untuk melakukan pengujian terhadap system informasi yang ada di dalam organisasi untuk mengetahui apakah system informasi yang dimiliki telah sesuai dengan visi, misi dan tujuan organisasi, menguji performa system informasi dan untuk mendeteksi resiko-resiko dan efek potensial yang mungkin timbul.



Dalam pelaksanaanya, auditor TI mengumpulkan bukti-bukti yang memadai melalui berbagai teknik termasuk survey, wawancara, observasi dan review dokumentasi.

Satu hal yang unik, bukti-bukti audit yang diambil oleh auditor biasanya mencakup pula bukti elektronis. Biasanya, auditor TI menerapkan teknik audit berbantuan computer, disebut juga dengan CAAT (Computer Aided Auditing Technique). Teknik ini digunakan untuk menganalisa data, misalnya saja data transaksi penjualan, pembelian, transaksi aktivitas persediaan, aktivitas nasabah, dan lain-lain.



H. Tujuan Audit Sistem Informasi

Dalam melakukan audit sistem informasi auditor harus memastikan bahwa tujuan-tujuan berikut terpenuhi yaitu :

1. Perlengkapan keamanan melindungi perlengkapan komputer,program, komunikasi dan data dari akses yang tidak sah, modifikasi atau penghancuran.
2. Pengembangan dan perolehan program dilaksnakan sesuai dengan otorisasi khusus dan umum dari pihak manajemen.
3. Modifikasi program dilaksanakan dengan otorisasi dan persetujuan pihak manajemen.

4. Pemrosesan transaksi, file, laporan dan catatan komputer lainnya telah akurat dan lengkap
5. Data sumber yang tidak akurat atau yang tidak memiliki otorisasi yang tepat diidentifikasi dan ditangani sesuai dengan kebijakan manajerial yang telah ditetapkan.
6. File data komputer telah akurat, lengkap dan dijaga kerahasiaannya.

I. Computer Audit Software (CAS) atau Generalized Audit Software (GAS)

CAS : Program komputer yang (berdasarkan spesifikasi dari auditor) menghasilkan program yang melaksanakan fungsi-fungsi audit. CAS idealnya sesuai untuk :

• pemeriksaan file data yang besar
• Mengidentifikasi catatan-catatan yang membutuhkan pemeriksaan audit lebih lanjut.

Fungsi-Fungsi Umum Software Audit Komputer

• Pemformatan ulang
• Manipulasi file
• Perhitungan
• Pemilihan data
• Analisis data
• Pemrosesan file
• Statistik
• Pembuatan laporan

Audit Operasional Atas Suatu SIA Langkah pertama adalah perencanaan audit, yaitu masa pembuatan lingkup dan tujuan audit, tinjauan awal atas sistem dilakukan dan program audit sementara dipersiapkan. Selanjutnya pengumpulan bukti yang mencakup kegiatan-kegiatan:

1. Meninjau kebijakan dokumentasi operasional
2. Melakukan konfirmasi atas prosedur dengan pihak manajemen serta personil operasional
3. Mengamati fungsi-fungsi dan kegiatan operasional
4. Memeriksa rencana dan laporan keuangan serta operasional
5. Menguji akurasi informasi operasional
6. Menguji pengendalian.

J. Langkah dasar Audit SI

Audit dalam konteks teknologi informasi adalah memeriksa apakah sistem komputer berjalan semestinya. Tujuh langkah proses audit:

1. Implementasikan sebuah strategi audit berbasis manajemen risiko serta *control practice* yang dapat disepakati semua pihak.
2. Tetapkan langkah-langkah audit yang rinci.
3. Gunakan fakta/bahan bukti yang cukup, handal, relevan, serta bermanfaat.
4. Buatlah laporan beserta kesimpulannya berdasarkan fakta yang dikumpulkan.
5. Telaah apakah tujuan audit tercapai.
6. Sampaikan laporan kepada pihak yang berkepentingan.
7. Pastikan bahwa organisasi mengimplementasikan managemen risiko serta control practice.

Sebelum menjalankan proses audit, tentu saja proses audit harus direncanakan terlebih dahulu. *Audit planning* (perencanaan audit) harus secara jelas menerangkan tujuan audit, kewenangan auditor, adanya persetujuan managemen tinggi, dan metode audit. Metodologi audit:

1. *Audit subject*. Menentukan apa yang akan diaudit.
2. *Audit objective*. Menentukan tujuan dari audit.

3. *Audit Scope*. Menentukan sistem, fungsi, dan bagian dari organisasi yang secara spesifik/khusus akan diaudit.
4. *Preaudit Planning*. Mengidentifikasi sumber daya dan SDM yang dibutuhkan, menentukan dokumen-dokumen apa yang diperlukan untuk menunjang audit, menentukan lokasi audit.
5. *Audit procedures and steps for data gathering*. Menentukan cara melakukan audit untuk memeriksa dan menguji kendali, menentukan siapa yang akan diwawancara.
6. Evaluasi hasil pengujian dan pemeriksaan. Spesifik pada tiap organisasi.
7. Prosedur komunikasi dengan pihak manajemen. Spesifik pada tiap organisasi.
8. *Audit Report Preparation*. Menentukan bagaimana cara memeriksa hasil audit, yaitu evaluasi kesahihan dari dokumen-dokumen, prosedur, dan kebijakan dari organisasi yang diaudit. Struktur dan isi laporan audit tidak baku, tapi umumnya terdiri atas:
    - Pendahuluan. Tujuan, ruang lingkup, lamanya audit, prosedur audit.
    - Kesimpulan umum dari auditor.
    - Hasil audit. Apa yang ditemukan dalam audit, apakah prosedur dan kontrol layak atau tidak
    - Rekomendasi. Tanggapan dari manajemen (bila perlu).
    - *Exit interview*. *Interview* terakhir antara auditor dengan pihak manajemen untuk membicarakan temuan-temuan dan rekomendasi tindak lanjut. Sekaligus meyakinkan tim manajemen bahwa hasil audit sahih

K. Tahap-tahap Audit Sistem Informasi

Audit Sistem Informasi dapat dilakukan dengan berbagai macam tahap-tahap. Tahap-tahap audit terdiri dari 5 tahap sebagai berikut :

1. Tahap pemeriksaan pendahuluan

Sebelum auditor menentukan sifat dan luas pengujian yang harus dilakukan, auditor harus memahami bisnis auditi (kebijakan, struktur organisasi, dan praktik yang dilakukan). Setelah itu, analisis risiko audit merupakan bagian yang sangat penting. Ini meliputi review atas pengendalian intern. Dalam tahap ini, auditor juga mengidentifikasi aplikasi yang penting dan berusaha untuk memahami pengendalian terhadap transaksi yang diproses oleh aplikasi tersebut. pada tahap ini pula auditor dapat memutuskan apakah audit dapat diteruskan atau mengundurkan diri dari penugasan audit.

2. Tahap Pemeriksaan Rinci.

   Pada tahap ini auditnya berupaya mendapatkan informasi lebih mendalam untuk memahami pengendalian yang diterapkan dalam sistem komputer klien. Auditor harus dapat memperkirakan bahwa hasil audit pada akhimya harus dapat dijadikan sebagai dasar untuk menilai apakah struktur pengendalian intem yang diterapkan dapat dipercaya atau tidak. Kuat atau tidaknya pengendalian tersebut akan menjadi dasar bagi auditor dalam menentukan langkah selanjutnya.

3. Tahap Pengujian Kesesuaian.

   Dalam tahap ini, dilakukan pemeriksaan secara terinci saldo akun dan transaksi. Informasi yang digunakan berada dalam file data yang biasanya harus diambil menggunakan software CAATTs. Pendekatan basis data menggunakan CAATTs dan pengujian substantif untuk memeriksa integritas data. Dengan kata lain, CAATTs digunakan untuk mengambil data untuk mengetahui integritas dan keandalan data itu sendiri.

4. Tahap Pengujian Kebenaran Bukti.

   Tujuan pada tahap pengujian kebenaran bukti adalah untuk mendapatkan bukti yang cukup kompeten,. Pada tahap ini, pengujian yang dilakukan adalah (Davis at.all. 1981):

   a. Mengidentifikasi kesalahan dalam pemrosesan data
   b. Menilai kualitas data
   c. Mengidentifikasi ketidakkonsistenan data
   d. Membandingkan data dengan perhitungan fisik
   e. Konfirmasi data dengan sumber-sumber dari luar perusahaan.

5. Tahap Penilaian Secara Umum atas Hasil Pengujian.

   Pada tahap ini auditor diharapkan telah dapat memberikan penilaian apakah bukti yang diperoleh dapat atau tidak mendukung informasi yang diaudit. Hasil penilaian tersebut akan menjadi dasar bagi auditor untuk menyiapkan pendapatanya dalam laporan auditan.

   Auditor harus mengintegrasikan hasil proses dalam pendekatan audit yang diterapkan audit yang diterapkan. Audit meliputi struktur pengendalian intern yang diterapkan perusahaan, yang mencakup : (1) pengendalian umum, (2) pengendalian aplikasi, yang terdiri dari : (a) pengendalian secara manual, (b) pengendalian terhadap output sistem informasi, dan (c) pengendalian yang sudah diprogram.

L. Berbagai Jenis Audit Lain dan Organisasi Profesi

Penggolongan audit sistem informasi berkaitan dengan organisasi profesi dapat dijelaskan sebagai berikut :

1. Audit Laporan Keuangan

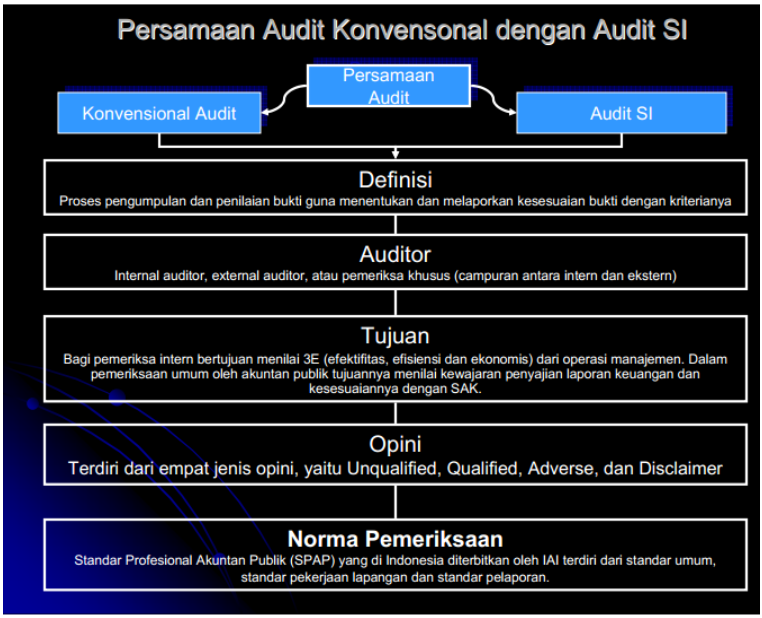
   Audit terhadap sistem informasi akuntansi berbasis teknologi informasi untuk menilai apakah laporan keuangan yang dihasilkan oleh sistem informasi akuntansi tersebut sesuai dengan standar akuntansi keuangan. Kualifikasi auditornya adalah akuntan bergelar CPA (Auditor Eksternal)

   Panduan yang digunakan dalam audit adalah standar profesional akuntan publik (SPAP). Referensi model sistem pengendalian internalnya adalah Commitee of Sponsoring Organization (COSO). Bahan bukti utama audit adalah data akunansi dan internal kontrol.

2. Audit Sistem Informasi sebagai kegiatan tersendiri yang terpisah dari audit keuangan

   Sebagai suatu audit operasional terhadap manajemen sumber daya informasi untuk menilai apakah pengelolaan sistem informasi pada suatu organisasi berjalan secara efektif, efisien dan ekonomis. Audit dilakukan oleh auditor internal (tidak menutup kemungkinan auditor eksternal).

Panduan audit mengacu pada standar atestasi yang dikeluarkan rganisasi profesi (IAI di Indonesia, AICPA di USA, CICA di Kanada) Referensi model sistem pengendalian internalnya adalah Cobit



BAB 2

Risiko dalam Perkembangan Teknologi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- Menjelaskan tentang definisi pengenalan resiko
- Menjelaskan struktur permasalahan algoritma pencarian
- Menjelaskan jenis algoritma pencarian

A. Pengenalan Resiko

Laporan audit standar menjelaskan bahwa audit dirancang untuk memperoleh keyakinan yang memadai-bukan absolute- bahwa laporan keuangan telah bebas dari salah saji yang material. Karena audit tidak menjamin bahwa laporan keuangan telah bebas dari salah saji material, maka terdapat beberapa derajat risiko bahwa laporan keuangan mengandung salah saji yang tidak terdeteksi oleh auditor.

Dengan demikian dalamperencanaan pekerjaannya, auditor harus mempertimbangkan risiko audit tersebut. Menurut SA seksi 312 (PSA No. 25) yang dikutip oleh Soekrisno Agoes (2004), risiko audit adalah risiko yang timbul karena auditor, tanpa disadaritidak memodifikasikan pendapatnya sebagaimana mestinya, atas suatu laporan keuangan yang mengandung salah saji material.

Konsep keseluruhan mengenai risiko audit merupakan kebalikan dari konsep keyakinan yang memadai. Semakin tinggi kepastian yang ingin diperoleh auditor dalammenyatakan pendapat yang benar, semakin

rendah risiko audit yang akan ia terima. Jika 99% kepastian diinginkan, maka risiko audit adalah 1%, sementara.

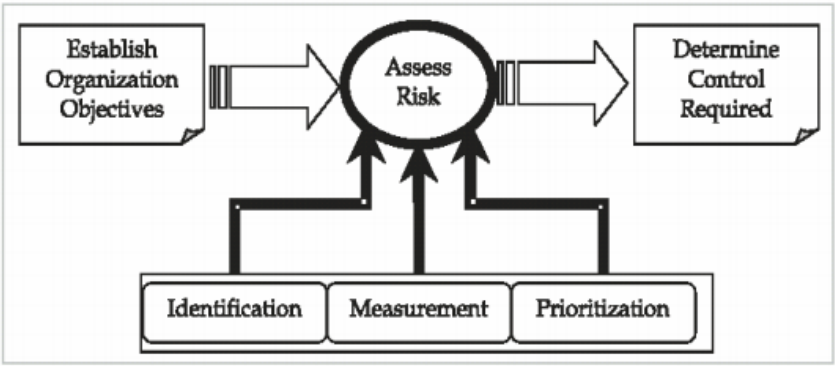
Jika kepastian sebesar 95 % dianggap memuaskan, maka risiko audit adalah 5%. Biasanya pertimbangan professional berkenaan dengan keyakinan yang memadai dan keseluruhan tingkat risiko audit dirancang sebagai satu kebijakan kantor akuntan public, dan risiko audit akan dapat dibandingkan antara satu audit dengan audit lainnya. (Boynton, Jhonson, Kell, 2003). Tantangan akhir dari suatu audit adalah bahwa auditor tidak dapat memeriksa semua bukti yang berkaitan dengan setiap asersi untuk setiap saldo akun dan golongan transaksi. Model risiko audit menjadi pedoman para auditor dalampengumpulan bukti audit, sehingga auditor dapat mencapai tingkat keyakinan yang memadai yang diinginkan.

Perkembangan kegiatan bisnis ternyata mampu mempengaruhi dan membawa perubahan paradigma pelaksanaan audit dari pendekatan dengan pengendalian ke pendekatan audit berdasarkan Risiko (*Risk Based Auditing*). (Pemeriksa No. 93, 2003). Pergeseran fokusaudit dari pengendalian ke risiko telah membuat suatu revolusi yang besar dalampendekatan audit masa kini.

Risk assessment merupakan bagian dari tahapan pertama metodologi Risk Management Based Auditingyang harus dilakukan dalammelaksanakan audit keuangan dengan berbasis pada manajemen risiko. Tahapan tersebut adalah memahamioperasi auditee yang bertujuan untuk mengidentifikasi dan memprioritaskan risiko kegagalan, risiko kekeliruan, dan risiko kecurangan yang dapat mempengaruhi audit laporan keuangan.

Salah satu model Risk Based Auditing yang dapat digunakan adalah model yang diperkenalkan oleh *The Committee of Sponsoring Organizations of the Treadway Commissions* (COSO). Model COSO

menunjukkan hubungan antara risiko organisasi dengan perencanaan audit, yaitu:



Model diatas jelas menunjukkan bahwa penentuan pengendalian yang dibutuhkan oleh organisasi harus melalui tahapan penilaian risiko (risk assessment). Pengendalian yang telah berorientasi kepada risiko akan lebih efektif karena jelasrisiko terkait yang akan di minimalisasi (mitigate). Pengendalian intern yang telah berorientasi kepada risiko akan memberikan tingkat keyakinan yang lebih tinggi kepada auditor atas efektivitas pengendalian tersebut. Semakin efektif pengendalian maka audit juga akan menjadi semakin efisien dan efektif.

Risiko bisnis(business risk) merupakan risiko dimana auditor akan menderita kerugian atau merugikan dalammelakukan praktik profesinya akibat proses pengadilan atau penolakan publik dalamhubungannya dengan audit. (Guy, Dan et al, 2002). Exposure terhadaprisiko bisnis selalu ada tidak peduli apakah auditor melaksanaklan audit sesuai dengan standar audit yang berlaku umum atau tidak. Sebagai contoh, auditor mungkin telah melaksanakan audit dengan benar dan digugat oleh ketidakpuasan pemilik. Dalamkasus ini, auditor mungkin memenangkan tuntutan hukumtetapi reputasi profesinyaakan menjadi rusak.

Risiko bisnis berbeda dengan risikoaudit; akantetapi, auditor mungkin sangat baik memutuskan untuk mengumpulkan lebih banyak bukti yang mengakibatkan meningkatnya risiko bisnis. Berdasarkan standar audit yang berlaku umum (GAAS), auditor tidak dapat memutuskan untuk mengumpulkan lebih sedikit bukti sebagai hasil dari audit klien dengan risiko bisnis minimal.

Pengguna laporan keuangan merupakan unsurutama dalam risiko bisnis. Untuk menentukan tingkat kepastian yang diperlukan, auditor terlebih dahulu harus mengidentifikasi pengguna potensial laporan keuangan. Jumlah pengguna laporan keuangan yang lebih besar akan meningkatkan risiko bisnis dan dapat meningkatkan tingkat kepastian yang diinginkan auditor.

Perkembangan kegiatan bisnis ternyata mampu mempengaruhi dan membawa perubahan paradigma pelaksanaan audit dari pendekatan dengan pengendalian ke pendekatan audit berdasarkan Risiko (Risk Based Auditing).

(Pemeriksa No. 93, 2003). Pergeseran fokusaudit dari pengendalian ke risiko telah membuat suatu revolusi yang besar dalampendekatan audit masa kini.

Sebagai contoh, The Institute ofInternal Auditor (IIA) dalamstandarnya telah menyatakan dengan tegas bahwa fokus utamapelaksanaan pemeriksaan bukan lagi pada pengendalian (control) tetapi pada risiko. Auditor internal diharapkan dapat mengambil kesimpulan apakah sisa Risiko (residual risk) yang diterima oleh manajemen telah memadai. Disamping itu, IIA juga mengharuskan pengendalian internal suatu organisasi harus memiliki suatu perangkat pengelolaan risiko (risk management).

Risk Assessment merupakan bagian dari kegiatan proses manajemen risiko, yaitu mencakup keseluruhan proses dari kegiatan menganalisa risiko dan mengevaluasi risiko. Kegiatan menganalisarisiko berupa kegiatan menggunakan informasi yang tersedia secara sistematis untuk menentukan bagaimana seringnya suatu kejadian mungkin akan terjadi dan dampak atau pengaruh yang akan timbul.

Sedangkan mengevaluasi risiko merupakan suatu proses yang digunakan untuk menentukan prioritas yang diberikan oleh manajemen risiko dengan cara membandingkan tingkatan suatu risiko dengan standar, target ataupun kriteria lainnya yang ditentukan sebelumnya oleh manajemen.

Manajemen risiko diakui sebagai bagian yang tidak terpisahkan dari praktik manajemen yang baik. Manajemen risiko merupakan proses yang berkesinambungan yang terdiri dari langkah-langkah yang jelas secara berurutan, memberikan sumbangan wawasan yang besar terhadap risiko dan dampak yang akan ditimbulkannya, serta memberikan dukungan informasi mengenai risiko bagi para pengambil keputusan.

Risiko audit yang dihadapi auditor hendaknya terus diusahakan dapat diminimalisir untuk menghindari risiko bisnis yang dihadapi oleh pengguna laporan auditor dan juga bertujuan untuk menjaga reputasi dari auditor itu sendiri.

B. Komponen Risiko Audit

Dalam praktik, seorang auditor tidak hanya harus mempertimbangkan risiko audit untuk setiap saldo akun dan golongan transaksi saja, tetapi juga setiap asersi yang relevan dengan saldoakun dan golongan transaksi yang material.

Faktor risiko yang relevan dengan suatu asersi biasanyaberbeda dengan faktor risiko yang relevan dengan asersi lainnya untuk saldo akun atau golongan transaksi yang sama.

SAS NO. 47 (AU 312.20) menyatakan bahwa risiko audit terdiri dari 3 komponen:

1. Risiko bawaan (*Inherent risk*) merupakan kerentanan asersi terhadap salah saji (misstatement) yang material, dengan mengasumsikan bahwa tidak ada pengendalian yang berhubungan. Risiko salah saji (*misstatement*) seperti itu lebihbesar dalambeberapa asersi laporan keuangan dan saldo-saldo ataupengelompokan yang berhubungan daripada yang lainnya. Risiko ini dipertimbangkan pada tahap perencanaan audit. Sebagai contoh, perhitungan yang rumit lebih mungkin disajikan salah jika dibandingkan dengan perhitungan yang sederhana. Akun yang terdiri dari jumlah yang berasal estimasi akuntansi cenderung mengandung risiko lebih besar dibandingkan dengan akun yang sifatnya relatif rutin dan berisi data berupa fakta.
2. Risiko Pengendalian (*Control Risk*) merupakan risiko bahwa suatu salah saji yang material yang akan terjadi dalamasersi tidak dapat dicegah atau dideteksi secara tepat waktu oleh pengendalian perusahaan. Risiko ini merupakan fungsi keefektifan perancangan dan operasi pengendalian internal dalammencapai tujuan entitas yang relevan untuk menyusun laporan keuangan entitas. Beberapa risiko pengendalian akan selalu ada karena keterbatasan yang melekat pada pengendalian internal.
3. Risiko Deteksi (*Detection Risk*) merupakan risiko bahwa auditor tidak dapat mendeteksi salah saji yang material dalamsuatu perusahaan. Risiko ini merupakan fungsi keefektifan prosedur

audit dan aplikasinya oleh auditor. Hal ini sebagian muncul dari ketidakpastian yangada ketika auditor tidak memeriksa semua saldo akun atau kelompok transaksi untuk mengumpulkan bukti tentang asersi lainnya.

C. Hubungan antara Risiko Audit dan Bukti Audit

Auditor dapat menggunakan logika model risiko audit untuk mengambil keputusan tentang sifat, saat, dan luasnyaprosedur audit bagi suatu asersi maupun untuk perikatan para staf pada berbagaiaspek penugasan. Dalam model risiko audit, pertama, auditor menilai risikobahwa salah saji materialakan terjadi pada suatu asersi. Kedua, auditor memperoleh pemahaman tentang struktur pengendalian intern yang relevan dengan asersi tersebutdandapat melaksanakan pengujian tentang efektivitas pengendalian. Setelah mempertimbangkan risiko bawaan dan risiko pengendalian, auditor membuat pertimbangan tentang risiko salah saji yang material dalaminformasi keuangan tentang asersi yang disajikan untuk audit serta menetapkan lingkup prosedur audit yang sesuai.

Apabila risiko bawaan dan risiko pengendalian dapat dikurangi, selanjutnya auditor dapat merancang suatu rencana audit yang memperbolehkan tingkat risiko deteksi yang lebih tinggi. Sebagai contoh auditor mungkin akan menaruh perhatian pada tujuan audit spesifik yang berkaitan dengan asersi penilaian-bahwa penilaian asset tetapyang berkaitan dengan biaya perolehan telah disajikan secara wajar. Hal semacam ini tidak sulit, dan dapat diverifikasi dengan merujuk pada faktur-faktur yang dikeluarkan oleh pemasok. Asumsikan lebih lanjut bahwa auditor telah menetapkan bahwa pengendalian intern entitas atas penilaian dalamsiklus pembelian adalahcukup kuat. Akibatnya, auditor dapat menerima tingkat risiko deteksi yang lebih tinggi serta membatasi

lingkup pelaksanaan pengujian terinci untuk melakukan verifikasi penilaian asset tetap yang berkaitan dengan biaya perolehan. Sebagai kemungkinan lain, apabila auditor menetapkan bahwa risiko pengendalianadalah tinggi untukasersi ini, maka auditor akan menetapkan risiko deteksi pada tingkat yang cukup rendah guna mendapatkan keyakinan yang memadai bahwa laporan keuangan bebas dari salah saji yang material.

Terdapat kemungkinan lain dimana auditor menekankan perhatian pada tujuan audit lain yang berkaitan dengan asersi penilaian, kali ini berkaitan dengan penilaian persediaan pada nilai bersih yangdapat direalisasikan. Dalam hal ini, tingkat subyektivitas yang terlibat dalamasersi ini adalah tinggi. Selanjutnya, diketahui bahwa klien belummenetapkan sistem pengendalian intern yang baik guna me-reviewaspek-aspek nilai bersih yang dapat direlisasikan untuk mendasari catatan akuntansi.Dalamhal ini auditor akan menaksir risiko deteksi pada tingkat yang rendah serta melaksanakan prosedur audit guna mendapatkan keyakinan yang memadai bahwa laporan keuangan bebas dari salah saji material. Auditor dapat menanggapi dengan cara mengaudit harga jual persediaan yang dijual setelah akhir tahun buku (sifat dan saat) untuk barang-barang persediaan yang dijual dalam jumlah besar (luas) guna menilai kelayakan estimasi klien. Auditor juga dapat mengusahakan staf auditor yangmemiliki pengalaman dalam industri ini untuk mangaudit asersi tersebut.

Akhirnya, konsep risiko audit konsisten dengan fakta bahwa audit dirancang untuk memberi keyakinan yang memadai, bukan keyakian yang absolut bahwa laporan keuangan bebas dari salah saji yang material. Audit juga tidak menjamin bahwa laporan keuangan telah bebas dari salah saji yang material. Dengan kata lain terdapat hubungan terbalikantara risiko

audit dan jumlah bukti yang diperlukan untuk mendukung pendapat auditor atas laporan keuangan. Untuk klien tertentu, semakin rendah tingkat risiko audit yang ingin dicapai, semakin besar jumlah bukti yang diperlukan.

D. Materialitas

Materialitas mendasari penerapan standar-standar auditing yang berlaku umum, terutamastandar pekerjaan lapangan dan pelaporan. Oleh karena itu, materialitas memiliki dampak yang mendalampada audit laporan keuangan. Baik ISA 25(6) maupun SAS 47(2) mendiskusikan audit risk dan materiality secara bersama. Ada beberapa persamaan didalam dua dokumen Tersebut dan tidaktampak adanya perbedaan yang signifikan diantara kedua dokumen tersebut.

Kedua standard tersebutmencatat bahwa dua konsep tersebut dipertimbangkan bersama ketika melaksanakan penugasan. Audit risk dan materiality digunakan dalamperencanaan penugasan dan juga dalam mengevaluasi pengumpulan bukti. Kebalikan hubungan tersebut ada diantara audit risk dan materiality. Sebagai contoh, audit risk level rendah konsisten dengan level materiality yang lebih tinggi, dan materiality adalah kenaikan audit risk yang lebih rendah.Kombinasi dari audit risk dan materialitymenentukan nature, timing dan perluasan dari prosedur yang dilakukan.

Baik ISA 25(6) maupun SAS 47(2) menekankan bahwa penetapan level audit risk dan materiality boleh berubah dari tahap perencanaan penugasan ke tahap evaluasi. Perubahan lingkungan atau pengetahuan auditor mungkin menyebabkan audit risk dan materiality yang disusun pada tahap perencanaan diubah.

M. Jenis-jenis Risiko

Risiko dapat dibedakan menjadi beberapa jenis antara lain :

1. Risiko Bisnis

   Risiko bisnis adalah risiko yang dapat disebabkan oleh faktor-faktor internal dan eksternal yang berakibat kemungkinan tidak tercapainya tujuan organisasi. Risiko eksternal misalnya adalah perubahan kondisi perekonomian, tingkat kurs yang berubah mendadak, dan munculnya pesaing baru yang mempunyai potensi yang bersaing tinggi.

2. Risiko Bawaan

   Risiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan, jika tidak ada pengendalian internal. Misalnya kegiatan kampus apabila tidak ada absensi atau daftar kehadiran kuliah akan banyak mahasiswa yang cenderung tidak disiplin hadir mengikuti kuliah. Pada kegiatan perusahaan, seorang kasir mungkin akan tergoda untuk menggunakan uang kas untuk kepentingan pribadi dulu atau pegawai cenderung akan menggunakan barang inventaris kantor, salesman pada suatu dealer mobil cenderung menjual barang sebanyak mungkin karena berkaitan dengan komisi yang akan diperolehnya.

3. Risiko Pengendalian

   Dalam suatu organisasi yang baik seharusnya sudah ada risk assesment dan dirancang pengendalian internal secara optimal terhadap setiap potensi risiko. Risiko pengendalian ialah masih adanya risiko meskipun sudah ada pengendalian. Contoh pada sistem kepegawaian, auditor akan salah menilai jika ternyata dalam daftar hadir pegawai masih terdapat kemungkinan kesalahan / penyalahgunaan yang belum dapat dideteksi oleh prosedur yang ada.

4. Risiko Deteksi

   Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya error yang cukup materialitas atau adanya kemungkinan fraud. Risiko deteksi mungkin dapat terjadi karena ternyata dalam prosedur auditnya tidak dapat mendeteksi terjadinya existing control failure atau sistem pengendalian internal yang ada ternyata tidak berjalan dengan baik

5. Risiko Audit

   Risiko audit sebenarnya adalah kombinasi dari inherent risk, control risk, dan detection risk. Risiko audit adalah risiko bahwa hasil pemeriksaan auditor ternyata belum dapat mencerminkan keadaan yang sesungguhnya.

   Risiko audit (*risk audit*) merupakan risiko kemungkinan auditor eksternal memberikan opini yang salah terhadap fairness laporan keuangan auditee, atau temuan dan rekomendasi yang salah pada laporan hasil pemeriksaan auditor internal.

Sedangkan menurut Jones dan Rama serta Hunton dkk (2004) risiko pada hakekatnya dibagi ke dalam 4 jenis risiko :

1. Execution Risk

   Execution Risk adalah risiko yang berkaitan dengan tidak tercapainya sesuatu yang seharusnya dilaksanakan. Contoh risiko yang bersifat kegagalan dalam melakukan kegiatan yang seharusnya dilaksanakan dengan baik ialah keliru di dalam mengirim barang ke pelanggan

2. Information Risk

   Risiko informasi ialah risiko yang berkaitan dengan kemungkinan kesalahan atau penyalahgunaan data/informasi. Contohnya ialah kesalahan catat / pemasukan / rekam / entri data, kode pelanggan yang

seharusnya 0099 tetapi dicatat 0999. Jika masukan data atau prosesnya salah, informasi yang dihasilkan juga keliru. Dalam sistem informasi berbasis teknologi informasi risiko ini makin tinggi.

3. Asset Protection Risk

   Risiko yang berkaitan dengan saveguarding assets ialah risiko kerusakan, hilang atau asset yang tidak digunakan seperti yang seharusnya, maupun risiko yang dapat timbul terhadap asset perusahaan akibat keputusan yang salah. Misalnya perusahaan mempunyai komputer notebook yang digunakan oleh para stafnya, jika perusahaan tidak bisa mengidentifikasi notebook yang mana, sedang dibawa oleh siapa, dan kapan maka disini timbul risiko terhadap asset. Risiko lain misalnya barang-barang inventaris atau mesin kurang dirawat, asset tidak diberi nomor atau kode identifikasi yang memadai. Demikian juga jika perusahaan mengirim barang kepada pelanggan, padahal penjualan itu tidak layak, maka disini juga timbul risiko terhadap asset.

4. Performance Risk

   Risiko kinerja ini adalah berkaitan dengan kinerja pegawai perusahaan yang tidak dapat dilaksanakan sesuai tujua / standar / ukuran yang ditetapkan. Pada hakekatnya yang bertanggung jawab dan akan mempertanggungjawabkan pengelolaan perusahaan kepada para shareholder dan stakeholder adalah para pengurus perusahaan yang menurut UU PT di Indonesia adalah para anggota Dewan Direksi dan Dewan Komisaris.

5. IT Security Risk

   IT Security Risk berkaitan dengan data integrty dan akses. Data integrity ialah keandalan dan konsistensi data di dalam sistem manajemen data organisasi. Akses ke komputer atau data oleh pihak

berwenang perlu ditanggulangi, karena terkait dengan data integrity, privacy, dan seluruh keamanan sistem.

Pada suatu kasus di kantor mungkin pegawai kurang memperhatikan masalah pengamanan data dan di luar jam kerja petugas cleaning service mungkin saja memakai komputernya untuk bermain internet, ata bahkan mengakses file yang berisi konsep Surat Keputusan Direksi yang amat penting dan rahasia. Risiko makin menjadi terbuka dan peluang ancamannya makin tinggi bila sistem informasinya menggunakan jaringan. Potensi ancaman hacker dan cracker bisa bersifat yang paling berat yaitu mereka membobol dan merusak sistem/data, atau yang paling ringan mereka hanya sekedar masuk dan membaca privacy tanpa merusak atau mengambil apapun.

6. Continuity Risk

   Contonuity risk berkaitan dengan ketersediaan atau stabilitas, backup site, dan recovery pada sistem berbasis teknologi informasi. Backup site adalah cadangan sistem sedangkan backup file adalah cadangan file pada media off line. Recovery adalah sistem pengembalian status terakhir bila suatu proses mengalami gangguan atau terhenti secara tidak normal.

   Misalnya di Amerika dengan adanya asus penabrakan pesawat terbang oleh para teroris ke WTC dan Pentagon pada 11 September. Masalah yang lebih bersifat teknis misalnya ketidaksengajaan operator menghapus dan merusak file, atau petugas membuka email yang ternyata ada virusnya. Sistem backup pada perusahaan kecil misalnya dilakukan dengan membuat copy file data dari hardisk ke disket, sedangkan pada perusahaan besar harus dirancang menggunakan sistem yang lebih baik.

BAB 3

Sistem Pengendalian Internal

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- Menjelaskan tentang pentingnya sistem pengendalian internal
- Menjelaskan tentang fungsi dan komponen pengendalian internal
- Menjelaskan tentang batasan pengendalian internal
- Menjelaskan tentang pihak yang berkepentingan
- Menjelaskan tentang tujuan sistem pengendalian internal
- Menjelaskan tentang prinsip dasar sistem pengendalian internal
- Menjelaskan tentang framework model

A. Pentingnya Sistem Pengendalian Internal

Pengendalian internal adalah Rencana organisasi dan metode bisnis yang dipergunakan untuk menjaga aset, memberikan informasi yang akurat dan andal, mendorong dan memperbaiki efisiensi organisasi serta mendorong kesesuaian dengan kebijakan yang telah ditetapkan.

Penelitian COSO (*committee of sponsoring organizations*) mendefinisikan pengendalian internal sebagai proses yang diimplementasikan oleh dewan komisaris, pihak manajemen dan mereka yang berada dibawah arahannya untuk memberikan jaminan bahwa tujuan pengendalian dapat dicapai yaitu mengenai : efektifitas dan efisiensi operasional organisasi; keandalan pelaporan keuangan; kesesuaian dengan hukum dan peraturan yang berlaku.

Pengendalian internal adalah suatu proses yang dijalankan oleh dewan komisaris, manajemen dan personel lainnya dalam suatu entitas yang dirancang untuk memberikan keyakinan memadai tentang pencapaian tujuan berikut ini :

a. Keandalan pelaporan keuangan
b. Menjaga keyakinan dan catatan organisasi
c. Kepatuhan terhadap hukum dan peraturan
d. Efektivitas dan efisiensi operasi

Dengan diterapkannya sistem komputerisasi, maka sistem pengendalian internal mengalami perubahan. Salah satu sebabnya karena data tidak dapat dilihat lagi pada lembar kertas (jurnal dan buku besar), maka daya saji data sudah tidak dapat dilihat lagi secara visual. Selain itu juga proses komputerisasi dan komunikasi menyebabkan risiko yang dihadapi menjadi semakin besar dan semakin kompleks / rumit. Hal lain misalnya mengenai keamanan perangkat komputer (hardware), program (software), media yang digunakan, proses data, power listrik, temperatur (suhu udara) dan lain-lain. Media penyimpan data, misalnya USB dapat mudah dihapus, terkena virus, dan hal-hal lain yang disengaja dan tidak.

Komputerisasi memang secara mendasar merubah desain sistem informasi khususnya sistem informasi akuntansi, dan struktur pengendalian internalnya. Misalnya bukti jejak audit (audit trail) sebetulnya masih ada, tetapi banyak elemennya yang berubah. Secara manual, jalur audit trail dari laporan yang dihasilkan ke catatan-catatan dan dokumen-dokumen dasar sebagai bukti transaksi cukup jelas dan dapat diikuti atau ditelusuri jejaknya. Dalam siklus akuntansi keuangan sistem akuntansi tradisional, data piutang pada neraca dapat dengan mudah dilacak ke neraca lajur, kemudian buku besar dan faktur penjualan.

Pada sistem komputer, audit trail linkage menjadi lebih sulit dan bahkan seringkali suatu desain komputerisasi dapat memotong jalur yang menunjukkan hubungan antara output dengan darimana inputnya. Dalam sistem informasi akuntansi berbasis komputer desainnya tidak harus dengan jurnal ataupun buku besar. Mungkin saja data mentah pada suatu master file langsung di-generate menjadi laporan akuntansi. Oleh karena itu, dalam mendesain sistem informasi akuntansi dan struktur pengendalian internalnya, desainer harus

mempertimbangkan berbagai aspek agar sistem yang dihasilkan cukup baik, komprehensif, andal dan dapat mengurangi risiko informasi yang dihasilkan.

Dalam audit laporan keuangan yang berubah karena adanya komputerisasi (teknologi informasi) merupakan teknik pemeriksaan, khususnya dalam pengumpulan bahan bukti audit dan penilaiannya (evidence, collection and evaluation). Audit dapat dilakukan dengan pengujian terhadap input / output dari dokumen yang tersedia, pemeriksaan proses melalui berbagai metode tertentu (misalnya : wawancara, kuesioner) atau langsung ke sistem komputernya (pemeriksaaan program dan file/data).

Menurut (IAI, 2002) pengertian sistem pengendalian interal yaitu mengorganisasikan semua metode dan ketentuan yang terkoordinasi yang dianut dalam suatu perusahaan untuk melindungi harta miliknya, mengecek kecermatan dan kehandalan data akuntansi, meningkatnya efisiensi usaha dan mendorong ditaatinya kebijakan manajemen yang telah digariskan. Sedangkan menurut Mulyadi (2001) sistem pengendalian internal meliputi

Suatu organisasi atau entitas bisnis dan perusahaan membutuhkan sistem pengendalian internal karena beberapa alasan :

1. Kewajiban hukum, karena perusahaan memang diwajiban oleh aturan atau peraturan legal untuk menyusun struktur pengendalian internal. Di Amerika sejak tahun 1977 peraturan yang mengatur tentang sistem pengendalian internal diatur dalam FCPA atau Foreign Corrupt Practices Act dan Undang-undang Sarbanes Oxley tahun 2002 dimana perusahaan wajib menerapkan an adequate system of internal control.
2. Struktur pengendalian internal perusahaan ialah kebutuhan atau tanggung jawab direksi (the board) suatu perusahaan.

Konsep klasik pada sistem manual tentang sistem pengendalian internal yaitu :

1. Otorisasi yang memadai atas transaksi dan kegiatan
2. Adanya pemisahan tugas yang memadai
3. Adanya dokumentasi dan pencatatan yang memadai

4. Adanya pengendalian yang memadai atas akses dan penggunaan aktiva perusahaan dan catatan.
5. Adanya pengecekan atas kinerja yang dilakukan secara netral (independen) oleh unit / orang yang terpisah sering disebut dengan verifikasi independen.

Menurut Weber (1999) faktor yang mendorong pentingnya pengendalian dan audit sistem informasi antara lain :

1. Biaya perusahaan yang timbul karena kehilangan data
2. Biaya yang timbul karena kesalahan dalam pengambilan keputusan
3. Biaya yang timbul karena penyalahgunaan komputer
4. Nilai dari hardware, software dan personel
5. Biaya yang besar akibat kerusakan komputer
6. Menjaga kerahasiaan
7. Meningkatkan pengendalian evolusi penggunaan komputer

B. Fungsi dan Komponen Pengendalian Internal

Terdapat tiga fungsi :

1. Pengendalian untuk pencegahan prosedur dan kebijakan yang dibuat untuk mencegah timbulnya suatu masalah misalnya adanya pemisahan tugas, pembagian wewenang dan tanggung jawab, mengendalikan akses fisik atas aset, fasilitas dan informasi.
2. Pengendalian untuk pemeriksaan, prosedur dan kebijakan yang dibuat untuk mengungkapkan adanya masalah atau penyimpangan. Misalnya: pemeriksaan salianan atas perhitungan, mempersiapkan rekonsiliasi bank dan neraca saldo setiap bulan.
3. Pengendalian korektif, prosedur dan kebijakan yang dibuat untuk memecahkan masalah/penyimpangan yang terjadi yang ditemukan pada ditemukan oleh pengendalian pemeriksaan. Misalnya: prosedur yanng dibuat untuk identifikasi penyebab maslah, perbaikan kesalahan dan mengubah sistem agar masalah dimasa datang dapat diminimalisasi.

Menurut Ikantan Akuntan Indonesia (2011) ada lima unsur (komponen) pengendalian yang saling terkait berikut ini:

1. Lingkungan pengendalian

   Menetapkan corak organisasi, mempengaruhi kesadaran pengendalian orang-orangnya. Lingkungan pengendalian merupakan dasar untuk semua komponen pengendalian inter, menyediakan disiplin dan struktur.
2. Penaksiran resiko

   Penaksiran resiko adalah identifikasi entitas dan analisi terhadap resiko yang relevan unutk mencapai tujuannya, membentuk suatu dasar untuk menentukan bagaimana resiko harus dikelola.
3. Aktivitas pengendalian

   Aktivitas pengendalian adalah kebijakan dan prosedur yang membantu menjamin bahwa arahan manajemen dilaksanakan.
4. Informasi dan komunikasi

   Informasi dan komunikasi adalah pengindentifikasian, penangkapan, dan pertukaran informasi dalam suatu bentuk dan waktu yang memungkinkan orang melaksanakan tanggung jawab mereka.
5. Pemantauan

   Pemantauan adalah proses yang menentukan kualitas kinerja pengendalian intern sepanjang waktu.

C. Batasan Pengendalian Internal

Di dalam pengendalian internal menurut COSO (Commitee of Sponsoring Organization) yang dikutip oleh Champlain (2003) terdapat dua aktivitas pengendalian yang ditunjukkan untuk mendorong kehandalan proses informasi yaitu pengendalian umum dan pengendalian aplikasi.

1. Pengendalian Umum

   Pengendalian umum adalah sistem pengendalian internal komputer yang berlaku umum meliputi seluruh kegiatan komputerisasi sebuah organisasi secara menyeluruh. Ruang lingkup yang termasuk dalam pengendalian umum adalah (Gondodiyoto, 2007)

   a. Pengendalian top manajemen dalam lingkup ini termasuk pengendalian manajemen sistem informasi.
   b. Pengendalian manajemen pengembangan sistem termasuk manajemen sistem informasi
   c. Pengendalian manajemen sumber data
   d. Pengendalian manajemen operasi
   e. Pengendalian manajemen keamanan
   f. Pengendalian manajemen jaminan kualitas

2. Pengendalian Khusus atau Aplikasi

   Pengendalian khusus atau aplikasi adalah kontrol internal komputer yang berlaku khusus untuk aplikasi komputerisasi tertentu pada suatu organisasi (Gondodiyoto, 2007). Pengendalian aplikasi terdiri dari 6 pengendalian yaitu :

   a. Pengendalian batasan

      Pengendalian batasan adalah jenis pengendalian yang didesain untuk mengenal identitas dan otentik tidaknya user sistem dan untuk menjaga agar sumberdaya sistem informasi digunakan oleh user dengan cara yang ditetapkan. Yang dimaksud batasan adalah interface atau para pengguna dengan sistem berbasis teknologi informasi. Terdapat beberapa kontrol yang diimplementasikan dalam pengendalian batasan yaitu chryptographic control, acces control, audit trail, dan existance control.

   b. Pengendalian masukan

      Input merupakan salah satu tahap dalam sistem komputerisasi yang paling penting dan mengandung risiko. Pengendalian masukan dirancang dengan tujuan untuk mendapat keyakinan bahwa data transaksi input adalah valid, lengkap, serta bebas dari kesalahan dan penyalahgunaan.

c. Pengendalian Proses

Pengendalian proses adalah pengendalian internal untuk mendeteksi jangan sampai data menjadi error karena adanya kesalahan proses. Tujuan pengendalian pengolahan adalah untuk mencegah agar tidak terjadi kesalahan-kesalahan selama proses pengolahan data.

d. Pengendalian Keluaran

Pengendalian keluaran adalah pengendalian yang dilakukan untuk menjaga input sistem agar akurat, lengkap, dan digunakan sebagaimana mestinya. Pengendalian keluaran ini didesain agar output atau informasi disajikan secara akurat, lengkap, mutakhir, dan didistribusikan kepada orang-orang yang berhak secara cepat waktu dan tepat waktu. Jenis-jenis pengendalian keluaran meliputi pengendalian rekonsiliasi keluaran, penelaahan dan pengujian hasil pengolahan, pengendalian distribusi keluaran dan pengendalian terhadap catatan.

e. Pengendalian Database

Pengendalian database merupakan jenis pengendalian internal yang didesain untuk menjaga akses ke dalam database dan menjaga integritas dari data tersebut.

f. Pengendalian Komunikasi Aplikasi

Pengendalian komunikasi aplikasi merupakan jenis pengendalian internal yang didesain untuk menangani kesalahan selama proses transmisi data dan untuk menjaga keamanan dari data selama pengiriman informasi tersebut.

D. Pihak yang Berkepentingan

Banyak pihak yang terkait atau berkepentingan dengan sistem pengendalian internal yaitu :

1. Manajemen perusahaan

   Pihak manajemen organisasi atau perusahaan berkepentingan terhadap sistem pengendalian internal, karena struktur pengendalian internal suatu perusahaan

pada dasarnya adalah tanggung jawab manajemen puncak (top management). Sistem pengendalian internal membantu direktur dalam hal :

a. Menyediakan data handal untuk pengolahan atau pengurusan perusahaan.
b. Pengamanan asset dan catatan akuntansi entitas atau perusahaan
c. Mendorong peningkatan efisiensi operasional
d. Mendorong ketaatan terhadap kebijakan yang telah ditetapkan
e. Merupakan aturan umum yang harus dijalankan perusahaan,

2. Dewan komisaris, auditor internal, dan sebagainya
3. Para karyawan perusahaan itu sendiri, karena sistem pengendalian internal berfungsi sebagai :
   a. Merupakan aturan umum yang harus dijalankan perusahaan
   b. Merupakan pedoman kerja
   c. Regulatory Body (Badan pengatur / pemerintahan atau ikatan profesi)
   d. Auditor eksternal independen yang bermanfaat :
      1) Untuk mempermudah dalam melakukan studi terhadap siste informasi dari klien yang diaudit
      2) Untuk menetapkan risiko yang dihadapi sebagai auditor
         Sebagai indikator untuk menentukan pendapatnya terhadap keterandalan sistem yang diaudit.

E. Tujuan Sistem Pengendalian Internal

Tujuan dirancangnya pengendalian dari segi pandang manajemen ialah untuk dapat diperolehnya data yang dapat dipercaya, dipatuhinya kebijakan akuntansi yang akan dicapai jika data diolah tepat waktu, penilaian klasifikasi dan pisah batas waktu terjadinya transaksi akuntansi tepat. Tujuan lainnya yaitu pengamanan asset yaitu dengan adanya otorisasi, distribusi output data valid dan diolah serta disimpan secara aman.

Tujuan dirancangnya sistem pengendalian internal pada hakekatnya untuk melindungi harta milik perusahaan, mendorong kecermatan dan kehandalan data dan pelaporan akuntansi, meningkatkan efektivitas dan efisiensi usaha serta

mendorong ditaatinya kebijakan manajemen yang telah digariskan dan aturan-aturan yang ada :

1. Pencatatan, pengolahan data dan penyajian informasi yang dapat dipercaya
   Pimpinan hendaklah memiliki informasi yang benar / tepat dalam rangka melaksanakan kegiatannya. Mengingat bahwa berbagai jenis informasi dipergunakan untuk bahan mengambil keputusan sangat penting artinya, karena itu suatu mekanisme atau sistem yang dapat mendukung penyajian informasi yang akurat sangat diperlukan oleh pimpinan perusahaan.
2. Mengamankan aktiva perusahaan
   Pengamanan atas berbagai harta benda semakin penting dengan adanya komputer. Data atau informasi yang begitu banyak disimpan di dalam media komputer dapat dirusak apabila tidak diperhatikan pengamanannya
3. Meningkatnya efektivitas dan efisiensi operasional
   Pengamanan dalam suatu organisasi merupakan alat untuk mencegah penyimpangan tujuan / rencana organisasi, mencegah penghamburan usaha, menghindarkan pemborosan dalam setiap segi usaha dan mengurangi setiap jenis penggunaan sumber daya yang ada secara tidak efisien.
4. Mendorong pelaksanaan kebijaksanaan dan peraturan yang ada.
   Pimpinan menyusun tata cara dan ketentuan yang dapat dipergunakan untuk mencapai tujuan perusahaan. Sistem pengendalian internal berarti memberikan jaminan yang layak bahwa kesemuanya itu telah dilaksanakan oleh karyawan perusahaan.

F. Prinsip Dasar Sistem Pengendalian Internal

Prinsip umum yang harus diperhatikan dalam menerapkan sistem pengendalian intern yaitu :

1. Sistem pengendalian intern sebagai proses yang integral dan menyatu dengan instansi atau kegiatan secara terus menerus. Sistem Pengendalian Intern akan efektif apabila dibangun ke dalam infrastruktur suatu instansi dengan menjadi bagian dari organisasi yang dikenal dengan istilah ”built-in”. Pengertian

built-in adalah suatu proses yang terintegrasi dengan kegiatan, dan akan menyatu dengan pelaksanaan fungsi manajemen, mulai dari perencanaan sampai evaluasi.

2. Sistem Pengendalian Intern dipengaruhi oleh manusia. Efektivitas sistem pengendalian inten sangat bergantung pada manusia yang melaksanakannya. Manajemen menetapkan tujuan, merancang dan melaksanakan mekanisme pengendalian, memantau serta mengevaluasi pengendalian. Selanjutnya, seluruh pegawai dalam instansi memegang peranan penting untuk melaksanakan sistem pengendalian intern secara efektif.
3. Sistem pengendalian intern memberikan keyakinan yang memadai, bukan keyakiinan yang mutlak. Betapapun baiknya perancangan dan pengoperasian sistem pengendalian intern dalam suatu instansi, tidak dapat memberikan jaminan keyakinan yang mutlak bahwa tujuan instansi dapat tercapai. Hal ini disebabkan kemungkinan pencapaian tujuan tetap dipengaruhi oleh keterbatasan yang melekat dalam seluruh sistem pengendalian intern, seperti kesalahan manusia, pertimbangan yang keliru, dan adanya kolusi.

Sistem Pengendalian Intern diterapkan sesuai dengankebutuhan ukuran, kompleksitas, sifat, tugas dan fungsi Instansi Pemerintah. Bentuk, luasan dan kedalaman pengendalian akan tergantung pada tujuan dan ukuran instansi, serta sesuai dengan kebutuhan dan ciri kegitan serta lingkungan yang melingkupinya, karakter operasi dan lingkungan dimana kegiatan instansi dilaksanakan. Dengan konsep ini, tidak ada pengendalian yang dimiliki suatu instansi yang langsung dapat ditiru dan diterapkan pada instansi lain.

G. Aktivitas dalam Sistem Pengendalian Internal

Merupakan kebijakan dan prosedur, selain dari empatkomponen lain, yang dibuat manajemen untuk memenuhi tujuan dalam laporan keuangan. Aktifitas pengendalian merupakan prosedur pengendalian yang mempunyai tujuan utama yaitu untuk memperoleh jaminan yang memadai bahwa tujuan perusahaan dapat

tercapai. Aktifitas pengendalian terdiri dari kebijakan dan prosedur yang dapat dikategorikan sebagai berikut:

1. Adanya pemisahan tugas yang jelas dan memadai
2. Adanya prosedur otorisasi yang tepat atas transaksi dansegala aktifitas
3. Adanya dokumen dan catatan yang memadai
4. Terdapatnya pengendalian fisik dan dokumen atas aktiva, dokumen dan catatan Pembagian tugas dapat mendukung praktek pengendalianyang sehat jika terdapat uraian tugas yang jelas. Uraian tugas harus diatur dan ditetapkan secara tertulis yang dibuat oleh manajemen dalam bentuk pedoman buku yang berisi peraturan-peraturan mengenai tata kerja yang akan dilakukan di perusahaan.

Terdapat prinsip-prinsip umum yang harus diperhatikan terhadap pembagian tugas dalam suatu organisasi, yaitu:

1. Adanya pemisahan fungsi antara fungsi penyimpanan aktiva dengan fungsi akuntansi
2. Adanya pemisahan fungsi antara fungsi otorisasi transaksi dengan fungsi penyimpanan aktiva
3. Adanya pemisahan fungsi antara fungsi otorisasi transaksi dengan fungsi akuntansi
4. Jika menggunakan sistem komputer, harus ada pemisahanfungsi antara sistem, programmer, operator, pengarsipan, dan kelompok pengendalian data.

Pemisahan fungsi ini bertujuan untuk mencegah terjadinya kekeliruan dan penyelewengan yang dilakukan karyawan dalam melaksanakan tugasnya, dimana adanya saling uji diantara fungsi-fungsi yang terlibatdalam menangani suatu transaksi dari awal sampai akhir dengan tidak melibatkan bagian lain.

Dokumen dan catatan yang memadai sangat diperlukan untuk mendukung adanya aktifitas-aktifitas pengendalian. Adanya formulir merupakan sarana yang diperlukan untuk merekam setiap pemberian otorisasi terlaksananya suatu

transaksi. Formulir merupakan dasar untuk pencatatan ke dalam buku besarperusahaan, oleh karena itu perancangannya harus memenuhi kriteria perancangan formulir yang baik. Ada beberapa kriteria perancangan formulir yang baik, yaitu sebagai berikut:

1. Formulir digunakan pada saat terjadinya atau segera setelah terjadinya transaksi
2. Perancangan formulir harus sederhana dan informatif
3. Formulir dirancang dengan layout yang memungkinkan pengisian data secara optimal dan lengkap

Formulir dinomori secara pranomor tercetak guna pengendalian. Secara umum formulir yang dibuat oleh perusahaan telah memenuhi perancangan formulir yang baik. Tetapi ada sedikit kelemahan yaitu formulir tidak dinomori secara pranomor tercetak, sehingga tidak adanya pengendalian terhadap pertanggungjawaban dan pengawasan setiap formulir yang digunakan.

Pengendalian internal dikembangkan untuk menyediakan pencapaian tujuan bisnis perusahaan dan pencegahan risiko yang tidak diinginkan. Pengendalian internal yang sudah ada pada sistem tradisional dikembangkan atau dirancang ulang. Sistem informasi yang dirancang dengan baik harus mempunyai kontrol yang dibangunm, yang mencakup semua fungsi meliputi:

1. Pengendalian internal akuntansi pada kegiatan akuntansi atau pembukuan, tujuannya adalah melindungi aset atau menjaga keandalan catatan keuangan.
2. Pengendalian operasi yang ditujukan oleh operasional sehari-hari, fungsi dan aktivitas serta menjamin aktivitas yang dilakukan sesuai dengan tujuan.
3. Pengendalian administrasi yang memperhatikan efisiensi operasi dalam area fungsional dan ketaatan terhadap kebijakan manajemen.

BAB 4

Kode Etik Audit Sistem Informasi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- ❖ Menjelaskan tentang kode etik audit
- ❖ Menjelaskan tentang standar audit
- ❖ Menjelaskan tentang standar audit ISACA

A. Kode Etik Audit

Perkembangan teknologi dan sistem informasi banyak membawa perubahan pada berbagai aspek kehidupan, khususnya yang mempengaruhi etika dan sosial masyarakat. Beberapa organisasi telah mengembangkan kode etik sistem informasi. Namun demikian, tetap ada perdebatan berkaitan dengan kode etik yang dapat diterima secara umum dengan kode etik sistem informasi yang dibuat secara spesifik. Sebagai manajer maupun pengguna sistem informasi, kita didorong untuk mengembangkan seperangkat standar etika untuk pengembangan kode etika sistem informasi, yaitu yang berbasiskan pada lima dimensi moral yang telah disampaikan di awal, yaitu:

1. Hak dan kewajiban informasi; Kode etik sistem informasi harus mencakup topik-topik, seperti: privasi e-mail setiap karyawan, pemantauan tempat kerja, perlakuan informasi organisasi, dan kebijakan informasi untuk pengguna.
2. Hak milik dan kewajiban; Kode etik sistem informasi harus mencakup topik-topik, seperti: lisensi penggunaan perangkat lunak, kepemilikan data dan fasilitas organisasi, kepemilikan perangkat lunak yang buat oleh pegawai pada perangkat keras organisasi, masalah *copyrights* perangkat lunak. Pedoman

tertentu untuk hubungan kontraktual dengan pihak ketiga juga harus menjadi bagian dari topik di sini.

3. Akuntabilitas dan pengendalian; Kode etik harus menyebutkan individu yang bertanggung jawab untuk seluruh sistem informasi dan menggaris bawahi bahwa individu-individu inilah yang bertanggung jawab terhadap hak individu, perlindungan terhadap hak kepemilikan, kualitas sistem dan kualitas hidup.
4. Kualitas sistem; Kode etik sistem informasi harus menggambarkan tingkatan yang umum dari kualitas data dan kesalahan sistem yang dapat ditoleransi. Kode etik juga harus dapat mensyaratkan bahwa semua sistem berusaha mengestimasi kualitas data dan kemungkinan kesalahan sistem.
5. Kualitas hidup; Kode etik sistem informasi juga harus dapat menyatakan bahwa tujuan dari sistem adalah meningkatkan kualitas hidup dari pelanggan dan karyawan dengan cara mencapai tingkatan yang tinggi dari kualitas produk, pelayanan pelanggan, dan kepuasan karyawan.

Kode etik pada prinsipnya merupakan sistem dari prinsip-prinsip moral yang diberlakukan dalam suatu kelompok profesi yang ditetapkan secara bersama. Kode etik suatu profesi merupakan ketentuan perilaku yang harus dipatuhi oleh setiap mereka yang menjalankan tugas profesi tersebut, seperti dokter, pengacara, polisi, akuntan, penilai, dan profesi lainnya

B. Standar Audit

Standar audit merupakan ukuran mutu pekerjaan audit yang ditetapkan oleh organisasi profesi audit, yang merupakan persyaratan minimum yang harus dicapai auditor dalam melaksanakan tugas auditnya. Standar audit diperlukan untuk menjaga mutu pekerjaan auditor.

Standar audit yang termuat dalam Standar Profesional Akuntan Publik (Ikatan Akuntan indonesia,2001), Standar Umum, Standar Pekerjaan Lapangan dan Standar Pelaporan.

1. Standar Umum

Audit harus dilaksanakan oleh seseorang atau lebih yang memiliki keahlian dan pelatihan teknis yang cukup sebagai auditor. Dalam melaksanakan audit sampai pada suatu pernyataan pendapat, auditor harus senantiasa bertindak sebagai seorang ahli dalam bidang auditing. Pencapaian keahlian tersebut dimulai dari pendidikan formal ditambah dengan pengalaman-pengalaman dalam praktik audit dan menjalani pelatihan teknis yang cukup. Asisten junioryang baru masuk dalam karir auditing harus memperoleh pengalaman profesionalnya dengan mendapatkan supervisi yang memadai dan review atas pekerjaannya dari atasannya yang lebih berpengalaman. Pelatihan yang dimaksudkan di sini mencakup pula pelatihan kesadaran untuk secara langsung terus menerus mengikuti perkembangan yang terjadi dalam bidang bisnis dan ketentuan baru dalam prinsip akuntansi dan standar auditing yang ditetapkan oleh Ikatan Akuntan Indonesia.

Dalam Semua Hal yang Berhubungan dengan Perikatan, Independensi dan Sikap Mental Harus dipertahankan Oleh Auditor. Standar ini mengharuskan seorang auditor bersikap independen, yanga artinya seorang auditor tidak mudah dipengaruhi karena pekerjaannya untuk kepentingan umum. Kepercayaan masyarakat umum atas independensi sikap auditor independen sangat penting bagi perkembangan profesi akuntan publik. Untuk menjadi independen, seorang auditor harus secara intelektual jujur.

Profesi akuntan publik telah menetapkan dalam kode Etik Akuntan Indonesia, agar anggota profesi menjaga dirinya dari kehilangan persepsi independensi dari masyarakat. Independensi secara intrinsik merupakan masalah mutu pribdai, bukan merupakan suatu aturan yang dirumuskan untuk dapat diuji secara objektif. BAPEPAM juga dapat menetapkan persyaratan independensi bagi auditor yang melaporkan tentang informasi keuangan yang akan diserahkan yang mungkin berbeda dari Ikatan Akuntan Indonesia (IAI).

Dalam Pelaksanaan Audit dan Penyusunan Laporannya Auditor Wajib Menggunakan Kemahiran Profesionalnya dengan Cermat dan Seksama.

Pengguanaan kemahiran profesional dengan cermat dan seksama menekankan tanggungjawab setiap profesional yang bekerja dalam organisasi auditor.

2. Standar Pekerjaan Lapangan
    a. Pekerjaan harus direncanakan sebaik-baiknya dan jika digunakan asisten harus disupervisi dengan semestinya.
    b. Pemahaman memadai atas pengendalian intern harus diperoleh untuk merencanakan audit dan menentukan sifat,saat dan lingkup pengujian yang akan dilakukan.
    c. Bukti audit kompeten yang cukup harus diperoleh melalui inspeksi, pengamatan dan permintaan keterangan dan konfirmasi sebagai dasar memadai untuk menyatakan pendapat atas laporan keuangan yang diaudit.
3. Standar Pelapor
    a. Laporan auditor harus menyataklan apakah laporan keuangan telah disusun sesuai dengan prinsip akuntansi yang berlaku umum di indonesia.
    b. Laporan auditor harus menunjukkan, jika ada ketidakonsistenan penerapan prinsip akuntansi dalam penyusunan laporan keuangan periode berjalan dibandingkan dengan penerpan prinsip akuntansi tersebut dalam periode sebelumnya.
    c. Pengungkapan informatif dalam laporan keuangan harus dipandang memadai, kecuali dinyatakan lain dalam laporan auditor.
    d. Laporan auditor harus memuat suatu pernyataan pendapat mengenai laporan keuangan secara keseluruhan atau suatu asersi bahwa pernyataan demikian tidak dapat diberikan. Jika pendapat secara keseluruhan tidak dapat diberikan, maka alasannya hrus dinyatakan. Dalam hal nama auditor dikaitkan dengan laporan keuangan, maka laporan auditor harus memuat petunjuk yang jelas mengenai sifat pekerjaan audit yang dilaksanakan, jika ada, dan tingkat tanggung jawab yang dipikul oleh auditor. Standar-standar tersebut di atas dalam banyak hal saling

berhubungan dan saling bergantung satu dengan lainnya. Keadaan yang berhubungan erat dengan penentuan dipenuhi atau tidaknya suatu standar, dapat berlaku juga untuk standar yang lain. "Materialitas" dan "risiko audit" melandasi penerapan semua standar auditing, terutama standar pekerjaan lapangan dan standar pelaporan.

Konsep "materialitas" bersifat bawaan dalam pekerjaan auditor independen. Dasar yang lebih kuat harus dicari sebagai landasan pendapat auditor independen atas unsur-unsur yang secara relatif lebih penting dan unsur-unsur yang mempunyai kemungkinan besar salah saji material. Misalnya, dalam perusahaan dengan jumlah debitur yang sedikit, dengan nilai piutang yang besar, secara individual piutang itu adalah lebih penting dan kemungkinan terjadinya salah saji material juga lebih besar jika dibandingkan dengan perusahaan lain yang mempunyai jumlah nilai piutang yang sama tetapi terdiri dari debitur yang banyak dengan nilai piutang yang relatif kecil. Dalam perusahaan manufaktur dan perusahaan dagang, sediaan umumnya mempunyai arti penting, baik bagi posisi keuangan maupun hasil usaha perusahaan, sehingga secara relatif sediaan memerlukan perhatian auditor yang lebih besar dibandingkan dengan sediaan dalam perusahaan jasa. Begitu pula, piutang umumnya memerlukan perhatian yang lebih besar dibandingkan dengan premi asuransi dibayar di muka.

C. Standar Audit ISACA

Standar yang digunakan dalam mengaudit teknologi informasi adalah standar yang diterbitkan oleh ISACA yaitu ISACA IS Auditing Standard. Selain itu ISACA juga menerbitkan IS Auditing Guidance dan IS Auditing Procedure. Standar adalah sesuatu yang harus dipenuhi oleh IS Auditor. Guidelines memberikan penjelasan bagaimana auditor dapat memenuhi standar dalam berbagai penugasan audit, dan prosedur memberikan contoh langkah-langkah yang perlu dilalui auditor dalam penugasan audit tertentu sehingga sesuai dengan standar. Bagaimanapun IS auditor harus bisa menggunakan judgement profesional

ketika menggunakan guidance dan procedure. Berikut adalah standar audit ISACA :

1. Audit Charter

   Standar:

   a. Tujuan, Tanggungjawab, otoritas, dan akuntabilitas fungsi audit SI pada suatu organisasi/perusahaan ataupun penugasan audit harus dengan dibuat tertulis (didokumentasikan) dalam *audit charter* atau *engagement letter***.**
   b. *Audit Charter* atau *Engagement letter* harus disetujui dan ditanda tangani oleh pimpinan organisasi.

   Penjelasan:

   a. Audit SI yang dilakukan oleh fungsi audit itern aktivitasnya bersifat terus berkelanjutan dan tujuan, tanggungjawab,otoritas dan akuntabilitas harus tercantum dalam *Audit charter*. *Audit charter* dapat direview secara periodik (misalnya tiap tahun) untuk disesuaikan dengan perubahan-perubahan yang mungkin terjadi.
   b. Penugasan audit yang dilakukan oleh auditor eksternal independen (pada umumnya audit dilaksanakan oleh satu kali penugasan) perlu dibuat *lettet of engagemen* untuk setiap penugasan audit.
   c. *Audit Charter /Letter of Engagement* harus cukup detail mengatur tujuan, tanggungjawab, batasan dari fungsi/penugasan audit yang dilaksanakan.
   d. Informasi terkait terdapat pada IS auditing Guideline (G5,Audit Charter), COBIT Framwork, Control objective (M4).

2. Organisational Independence

   Standar :

   a. Independensi Profesional

      Dalam segala hal yang berkaitan dengan audit, auditor harus independen dalam sikap dan penampilan.

b. Independensi Organisasi

Fungsi audit SI harus bebas (tidak ada cinflict of interest) dari area yang diperiksa untuk dapat menyelesaikan tugas audit dengan baik.

Penjelasan :

a. Baik pada audit charter atau letter of engagement harus dinyatakan secara jelas mengenai independensi dan akuntabilitas fungsi audit.
b. Auditor harus selalu independen dalam sikap, kenyataan maupun penampilan selama tuguas audit tersebut.
c. Dalam menjalankan tugas auditor harus independen: baik dalam hal sikap, tingkah laku dan tempat dimana dia bertugas. Jika ada hal-hal yang menyebabkan pelemahan independensi tersebut, maka detail penyebab pelemahan independensi atau penyimpangan tersebut harus dikemukakan kepada pihak-pihak yang berkepentingan.
d. Independensi selalu dievaluasi secara periodik(oleh fungsi audit, manajemen dan komite audit).
e. Informasi terkait terdapat pada : IS Auditing Guideline(G17, Effect of Non audit Role on the IS auditor's independence), IS Auditing Guideline (G12, Organi-sational Relationship and Independence), dan COBIT Framwork, Control objective (M4)

3. Profesional Independence

Standar :

a. Auditor SI harus menganut dan berpegang teguh pada kode etik profesi auditor SI(ISACA) dalam menjalankan tugas auditnya.
b. Auditor SI harus menjalankan tugasnya secara seksama (due professional care) dan bekerja sesuai dengan standar professional audit.

Penjelasan:

a. Kode etik auditor SI ISACA terus dikoreksi dari waktu ke waktu sesuai dengan perksmbengan kebutuhan profesi audit SI, dan oleh karenanya auditor SI atau anggota ISACA harus tetap mengikuti perkembangan terkini kode etik profesi tersebut.
b. Standar profesional pemeriksaan SI ISACA direview secara periodik dan secara terus menerus disempurnakan, dan oleh karenanya auditor SI atau anggota ISACA harus tetap mengikuti perkembangan terkini standar profesional audit SI tersebut.
c. Kelalaian atau kesengajaan tidak mematuhi kode etik dan standar profesional tersebut dapat mengakibatkan pemeriksaan pada pemegang CISA atau anggota ISACA dan dapat diberikan hukuman kedisplinan.
d. Informasi terkait terdapat pada : IS Auditing Guideline (G19, Irregularities and Illegal Acts), IS Auditing Guideline (G7, Due Professional Care), IS Auditing Guideline (G12, Organisational Relationship and Independence), dan COBIT Framework (Control objective, M4).

4. Professional Compentence

Standar :

a. Auditor SI harus mampu secara professional, mempunyai pengetahuan dan keahlian teknis untuk melakukan penugasan tuguas audit.
b. Auditor SI harus memelihara kemampuan professionalnya dengan pendidikannya dan pelatihan berkelanjutan.

Penjelasan :

a. Auditor SI harus memberikan keyakinan bahwa mampu atau kompeten secara professional (memiliki pengetahuan, keahlian teknis, dan pengalaman sesuai dengan tuguas audit yang dijalankannya), jika tidak auditor SI yang bersangkutan harus mundur dari penugasan itu.

b. Auditor SI harus mengikuti pendidikan dan pelatihan professional yang diperlukan, khususnya sertifikasi CISA. Auditor SI yang belum memperoleh CISA harus benar-benar mendapatkan pendidikan formal, pelatihan, dan pengalaman dibidang audit SI.
c. Ketika seseorang auditor SI memimppin tim audit, ketua tim auditor SI harus mendapat keyakinan bahwa seluruh anggota telah mempunyai kemampuan professional yang diperlukan untuk dapat melaksanakan tugas audit SI.
d. Informasi terkait terdapat pada :CISA certification and trtaining material, CISA continuing certification and aducation requirement, COBIT Framework, Control objectives (M2, M3, dan M4).

5. Planning

Standar :

a. Auditor SI harus membuat rencana kerja audit SI, mencakup tujuan audit, dan bahwa kegiatan-kegiatan auditnya akan sesuai dengan aturan hukum dan standar professional audit yang ada.
b. Auditor SI harus melakukan teknik pendekatan audit berbasis risiko (risks-based audit) dan mendokumtasikannya dengan baik.
c. Auditor SI harus menyusun rencana kerja audit, mencakup rincian tentang hakekat dan tujuan audit, periode atau waktu yang diperlukan, dan sumber daya yang diperlukan untuk penugasan audit tersebut.
d. Auditor SI harus menyusun rencana kerja audit dan program audit, mencakkup prosedur audit yang diperlukan untuk penyelesaian tugas audit itu.

Penjelasan :

a. Untuk fumgsi internal audit, perencanaan audit harus dikembangkan dan diupdate sebagai aktivitas berkelanjutan, dan menjadi dasar seluruh kegiatan audit sebagaimana dinyatakan pada audit charter. Rencana kerja

audit tersebut harus disetujui oleh komite audit (jika diperusahaan itu ada komite audit).

b. Untuk audit SI yang dilaksanakan oleh auditor eksternal, perencanaan audit disusun untuk setiap penugasan audit (dengan letter of engagement).
c. Auditor SI harus memahami bidang dan kegatan yang diperiksa. Tingkat pemahaman tersebut menentukan pengorganisasian, lingkungan, penaksiran, risiko dan sasaran audit.
d. Auditor SI harus melakukan risk assessment, sehingga diperoleh keyakinan memadai bahwa hal-hal yang bersifat material telah dicakup dalam audit pemeriksaan. Setelah kemudian baru dikembangkan strategi audit, konsep atau level materialitas, dan sumber dayanya.
e. Rencana kerja / program audit dapat diperbaharui dengan adanya issues baru, temuan, kesalahan asumsi, atau penaksiran risiko baru yang dikatahui setelah prosedur audit dijalankan.
f. Informasi terkait terdapat pada : IS Auditing Guideline (G6, Materiality Concept for Auditing Information System), IS Auditing Guideline (G15, Planning), IS Auditing Guideline (G13, Use of risk Assesment in Audit planning), IS Auditing Guideline (G16, Effect of Third Parties on an organisation's IT Controls), dan COBIT Frsmework, Control Objectives.

6. Performance of Audit Work

   Standar :

   a. Supervisi: Staf audit SI harus disupervisi untuk memperoleh keyakinan memadai bahwa tujuan audit telah dicapai sesuai dengan standar profesional audit.
   b. Bukti-audit: dalam pelaksanaan tugasnya auditor SI harus memperoleh bukti yang cukup, reliabel, dan relevan untuk pencapaian tujuan audit. Temuan hasil audit harus didasarkan pada ketersediaan bukti yang cukup, dianalisis dan di-interprestasikan/ dievaluasi dengan baik/tepat.

c. Dokumentasi: Proses audit harus didokumentasikan, menjelaskan pelaksanaan kegiatan audit, dan bukti yang mendukung kesimpulan/ temuan audit.

Penjelasan :

a. Peran dan tanggung jawab team audit SI harus dibangun sejak awal audit, dan harus mengatur hal-hal minimal yang perlu dilakukan terkait dengan decision, execution, dan review roles.
b. Pelaksanaan tugas harus diatur dan didokumentasikan mengikuti prosedur audit tertulis yang ada. Dokumentasi minimal harus membuat: tujuan dan lingkup pekerjaan, program audit, langkah-langkah audit, pengumpulan bukti audit, kesimpulan/ temuan dan reomendasi.
c. Dokumentasi audit harus memungkinkan pihak lain yang independen untuk melakukan penugasan dan mmenghasilkan kesimpulan yang sama.
d. Dokumentasi audit harus menunjukkan secara detail siapa yang melakukan *audit task* dan perannya. Sebagai pedoman umum ialah bahwa tiap task, keputusan, langkah, dan hasil audit dilaksanakan oleh anggota, atau tim, dan direview oleh anggota lain, atau ketua tim, yang ditunjuk sesuai dengan tingkat pentingnya hal itu.
e. Audit SI harus menggunakan bukti-bukti audit yang terpercaya dan sesuai dengan tingkat pentingnya tujuan pemeriksaan bidang itu (mengusahakan perolehan dan evaluasi bukti audit selngkap dan secermat mungkin dengan pertimbangan waktu dan biaya yang sesuai tingkat penting bidang itu.
f. Bukti audit harus lengkap, reliabel, relevan, dan bermanfaat untuk menghasilkan kesimpulan hasil audit. Bukti audit tambahan harus diperoleh jika menurut hemat auditor SI tersebut bukti yang ada belum dapat mendukung kesimpulannya.
g. Informasi terkait terdapat pada : COBIT Framework, Control Objectives.

7. Reporting

   Standar:

   a. Auditor SI harus membuat laporan hasil audit dalam format yang tepat segera setelah selesai melakukan tugas auditnya. Laporan hasil audit harus memuat organisasi, pihak yang dituju, dan batasan-batasan sirkulasi (jika ada).
   b. Laporan audit harus menyebutkan ruang lingkup, tujuan, periode dan waktu pelaksanaan pemeriksaan.
   c. Laporan audit harus berisi temuan, kesimpulan dan rekomendasi, serta pengungkapan mengenai penyedian, kualifikasi atau pembatasan cakupan audit yang dialami oleh auditor SI dalam melaksanakan tugasnya.
   d. Temuan hasil audit yang dilaporkan harus didukung bukti audit yang cukup, lengkap dan kompeten untuk mendukung laporan hasil pemeriksaan itu.
   e. Laporan hasil audit harus ditandatangani, dibubuhi tanggal pelaporan, dan didistribusikan sesuai ketentuan pada *audit charter letter of engagement*.

   Penjelasan:

   a. Bentuk dan isi dari laporan audit berbeda bergantung jenis penugasannya:
   b. Audit (langsung atau atestasi)
   c. Review (langsung atau atestasi)
   d. *Agreed upon procedures* (prosedur yang disepakati)
      a. Jika auditor SI diminta untuk memberikan opininya terhadap lingkungan pengendalian dalam penugasan tersebut, dan bukti audit menujukkan adanya kelemahan material atau signifikan pada struktur pengendalian intern, maka auditor SI tidak dapat mengambil kesimpulan bahwa sistem pengendalian inter yang ada efektif.

Laporan auditor SI harus memberikan gambaran tentang kelemahan tersebut dan dampaknya terhadap tujuan pengendalian.

b. Auditor SI harus mendiskusikan konsep laporan hasil audit dengan manajemen bidang yang diperiksa sebelum finalisasi dan diterbitkannya laporan tersebut, dan bila diperlukan memuat tanggapan atau penjelasan pihak auditan mengenai temuan yang dilaporkan sebagai hasil audit.
c. Jika auditor SI menemukan perbedaan/ penyimpangan yang material pada lingkunagan pengendalian, auditor SI harus mendiskusikannya dengan komite audit atau pihak yang berwenang diperusahaan itu, dan mengungkapkan adanya perbedaan/penyimpangan yang telah dikomunikasikan/didiskusikan.
d. Jika auditor Si menyampaikan beberapa laporan, maka pada laporan akhir hasil audit akhir harus disebutkan atau menjadi referansi bagi seluruh laporan.
e. Auditor SI harus mempertimbangkan atau menilai apakah komunikasi auditor dengan manajemen (bidang yang diperiksa) berbeda pandangan tentang signifikasi/material tidaknya kelemahan struktur pengendalian intern, jika demikaian maka auditor SI harus menyampaikannya kepada komite audit dan atau pejabat berwenang mengenai kelemahan yang sudah didiskusikan dengan pihak manajemen tersebut.
f. Auditor SI harus minta dan mengevaluasi laporan sebelumnya tentang temuan, kesimpulan dan rekomendasi, utuk menentukan apakah sudah dilaksanakan tindakan yang diperlukan sesuai rekomendasi dan waktu yang ditentukan.
g. Informasi terkait terdapat pada: IS *auditing Guideline* (G20, *Reporting*) COBIT *Framework*, (*Control Objectives*, M4.7 dan M4.8).

8. Follow-up Activities

   Standar:

   Setelah laporan hasil audit yang mengemukakan temuan dan rekomendasi, auditor SI harus mengevalusai informasi yang relevan untuk memperoleh keyakinan apakah tindak lanjut yang diperlukan (atas rekomendasi) telah dilaksanakan oleh pihak manajemen sesuai jadwal yang diusulkan (tepat waktu).

   Penjelasan:

   a. Jika telah ada tindak-lanjut atau rencana tindak-lanjut oleh manajemen, hal iyu harus dicantumkan pada laporan hasil audit sebagai sudah dilakukannya tanggapan manajemen terhadap rekomendasi pada laporan audit sebelumnya.
   b. Hakekat, *timing*, dan tingkat tindak-lanjut harus menjadi temuan positif laporan audit, jika tidak (temuan negatif), harusc dijelaskan dampak/ akibatnya. Tanggapan (*reponse*) atau tindak-lanjut menjadi pertimbangan penting bagi *profesional judgement* auditor SI berkaitan dengan risiko dan biaya auditan.
   c. Fungsi audit intern mengembangkan mekanisme pemantauan untuk mengetahui apakah rekomendasi benar-benar telah ditindaklanjuti manajemen, atau pimpinan perusahaan berani mengambil resiko dengan tidak menindak-lanjuti rekomendasi. Tanggungjawab tindak-lanjut atau hal-hal yang terkait dengan itu perlu dicantumkan dalam *audit charter*.
   d. Bergantung pada ruang lingkup dan bentuk penugasan, auditor SI eksternal dapat mempercayakan tindak-lanjut atas rekomendasi yang telah disetujui kepada fungsi audit intern
   e. Jika manajemen memberikan informasi mengenai tindak lanjut rekomendasi, dan aditor SI ragu mengenai hal itu, maka auditor SI dapat melakukan test seperlunya, atau melakukan prosedur yang

diperlukan untuk memastikan posisi atau kondisi tindaklanjut rekomendasi.

f. Belum dilaksanakannya tindak lanjut rekomendasi perlu dilaporkan dan atau dipresentasikan kepada komite audit atau kepada pimpinan perusahaan.
g. Sebagai bagian dari pelaksanaan pemeriksaan, auditor SI harus mengevaluasi apakah temuan yang belum dilakukan tindaklanjut masih relevan.

9. Irregularities and Illegal Acts

Standar:

a. Dalam perencanaan dan pelaksanaan audit untuk mengurai resiko audit, auditor SI harus mempertimbangkan resiko ketidakteraturan dan *illegal acts*.
b. Auditor SI harus bersikap profesional skeptisdalam pelaksanaan audit, paham kemungkinan *misstatements* yang material dapat saja terjadi karena adanya *irrigularities* dan *illegal acts*, diluar evaluasi yang telah dilakukan.
c. Auditor SI harus memahami organisasi dan lingkungannya, termasuk sistem pengendalian internal bidang yang diperiksa.
d. Auditor SI harus memili bukti audit yang lengkap dan kompeten untuk menentukan a;pakah manajemen atau pihak lainnya dalam organisasi mengetahui aktual , curiga atau yang diduga keras terdapat ketidakteraturan dan atau tindakan-tindakan yang ilegal.
e. Dalam menjalankan prosedur audit untuk memahami organisasi dan lingkungannya, auditor SI harus dapat mempertimbangkan kemungkinan hubungan tak terduga atau tidak biasanya terjadinya risiko *misstatements* akibat ketidakteraturan dan atau tindakan-tindakan illegal.

f. Auditor SI harus merancang dan menjalankan prosedur untuk menguji (tes) kecukupan pengendalian intern dan resiko manajemen mengesampingkan pengendalian intern.

g. Jika auditor SI mengidentifikasi adanya *misstatements*, auditor SI harus menilai apakah *misstatements* tejadi akibat *irregularities* dan *illegal acts*, jika iya, auditor SI ahrus memikirkan kemungkinan dampaknya kebidang lain, khusunya berkaitan dengan *representations of management*.

h. Audit Si harus memperoleh representasi tertulis dari manajemen , dilakukan sedikitnya setiap tahun atau lebih sering lagi bergantung pada penugasan audit yang antara lain:

   - Pengakuan tanggungjawab manajemen untuk merancang dan mengimplementasikan kontrol internal untuk mencegah dan mendeteksi *irregularities* dan *illegal acts*.
   - Mengungkapkan kepada auditor mengenai penilian resiko jika terdapat kemungkinan *misstatements* yang mterial sebagai akibat *irregularities* dan *illegal acts*.
   - Mengungkapkan kepada auditor tentang pengetahuannya terhadap *irregularaties* dan *illegal acts*, dampaknya kepada organisasi dan kaitannya dengan manajemen maupun karyawan yang mempunyai peran penting dalam sistem pengendalian intern.
   - Mengungkapkan kepada auditor jika mengetahui atau menduga adanya *irrigularities* dan *illegal acts* atau disampaikan oleh karyawan , pihak regulator atau yang lain.

i. Jika auditor SI mengidentifikasi adanya *irregularaties* dan *illegal acts* atau memperoleh informasi mengenai hal itu, auditor harus mengkomunikasikan ini kepada level manajemen yang tepat sesegera mungkin.

j. Jika auditor SI mengidentifikasi *irregularities* dan *illegal acts* yang melibatkan manajemen atau personil yang berperan dalam internal control. Auditor intern harus mengkomunikasikan hal itu kepada pihak yang bertanggungjawab dalam tatakelola perusahaan.

Penjelasan:

a) Auditor SI harus memperoleh keyakinan memadai bahwa tidak ada *misstatements* yang material akibat *irregularities* dan *illegal acts*. Auditor tidak bisa memeberikan keyakinan penuh karena beberapa faktor, misalnya penggunaan *judgement*, tingkat pengujian, dan keterbatasan yang melekat pada iternal control
b) Resiko tidak terdeteksinya *misstatements* akibat *illegal acts* lebih tinggi daripada resiko tidak terdeteksinya *misstatements* akibat *irregularities/ error*, karena *illegal acts* menyangkut skema yang lebih rumit.
c) Pengalaman dan pemahaman auditor terhadap organisasi sangat membantu pelaksanaan pemeriksaan. Dalam melakukan penyelidikan dan prosedur-prosedur audit, auditor diharapkan tidak mengesampinggkan pengalaman sebelumnya harus tetap bersikap skeptis profesional. Auditor sebaiknya tidak cepat puas dengan bukti yang ada karena terlalu berasumsi atas kejujuran dan integritas manajemen melainkan harus selalu memeriksa dan mendiskusikan kemungkinan adanya *irregularities* dan *illegal acts* sepanjang pelaksanaan penugasan auditnya.

10. IT Goverance

Standar:

a. Auditor Si harus melakukan peninjauan dan penilian apakah fungsi SI sudah selaras dengan visi, misi, tata-nilai, dan strategis serta tujauan organisasi.

b. Auditor SI melakukan peninjauan apakah fungsi SI memiliki pernyataan yang jelas mengenai kinerja tyang diharapkan oleh organisasi (efektif dan efesien) dan dinilai apakah hl-hal tersebut sudah tercapai.
c. Auditor Si harus meninjau dan menilai efektivitas sumberdaya SI dan kinerja proses manajemennya.
d. Auditor Si harus meninjau dan menilai kepatuhan terhadap legal, lingkungan dan kualitas informasi, dan keamanan.
e. Dalam pemeriksaan dan evaluasi fungsi SI, auditor sebaiknya menggunakan pendekatan audit berbasis resiko (risk-based audit approach).
f. Audit SI harus meninjau dan menilai lingkungan pengendalian auditan.
g. Auditor SI harus meninjau dan menilai resiko yang mungkin terjadi dalam lingkungan sistem berbasi teknologi informasi.

Penjelasan:

a) Auditor sistem informasi harus meninjaubdan menilai resiko pada lingkungan kerja SI yang mendukung proses-proses bisnis. Pelaksanaan audit SI harus mendukung organisasi tersebut dengan identifikasi dean evaluasi kemungkinan resiko, menyempurnakan *risks management* dan *control system.*
b) Tatakelola teknologi informasi harus melekat pada setiap kegiatan fungsi SI.

11. Use of risk assessment in Audit Planning

    Standar:

    a. Audit SI harus menggunakan teknik penilian resiko yang cocok dalam pengembaangan rencana kerja audit SI, dan dalam menentukan prioritas alokasi sumberdaya audit efektif.
    b. Ketika merencanakan peninjauan individual, auditor SI harus mengidentifikasi dan menilai resiko yang relevan dari area yang diperiksanya.

    Penjelasan:

    a. Penilaian resiko adalah teknik yang digunakan untuk memeriksa *auditable unit* mana dari *audit universe* (keseluruhan unut/area yang dapat diaudit) dan memilih area/ bidang yang didahulukan diaudit dikarenakan beresiko paling tinggi.
    b. Suatu *audit unit* adalah sebagai segmen atau area/ bidang yang mempunyai karakteristik tersendiri dalam organisasi dan sistemnya.
    c. Penentuan dari keseluruhan audit SI harus didasarkan kepada pengetahuan dari perencanaan strategis teknologi informasi organisasi dan operasionalnya yang diperoleh dari diskusi dengan manajemen yang bertanggungjawab.
    d. *Risks assessment exercise* digunakan untuk pengembangan perencanaan audit SI, didokumentasikan sedikitnya dalam basis tahunan.
    e. penggunaan penilian resiko dalam pemilihan obyek audit memungkinkan auditor SI untuk mengkuantifikasi jumlah sumberdaya audit SI yang harus dimiliki untuk dapat menyelesaikan tugas audit.
    f. Sebagai kelanjutan setelah selesainya pemeriksaan, auditor SI harus memastikan bahwa manajemen resiko perusahaan telah diperbaruhi

sesuai dengan temuan dan rekomendasi untuk kebaikan dimasa mendatang.

12. Audit Materiality

Standar:

a. Auditor SI harus memoertimbangkan konsep materialitas dengan hubungannya dengan resiko audit.
b. Dalam merencanakan audit, auditor SI mempertimbangkan kelemahan-kelemahan potensial atau tidak adanya kontrol internal dan apakah hal itu dapat mempunyai akibat yang signifikan pada SI.
c. Auditor SI mempertimbangkan dampak kumulatif dari kelemahan atau ketiadaan pengendalian intern.
d. Laporan auditor SI harus mengungkapkan adanya pengendalian internm yang tidak efektif atau tidak adanya pengendalian intern (terhadap resiko tertentu) dan dampaknya.

Penjelasan:

a. Resiko audit adalah resiko bahwa auditor SI menarik kesimpulan yang tidak tepat berdasrkan temuan audit. Auditor Si harus memahami tiga komponen resikon audit, yaitu: resiko bawaan, resiko pengendalian, dan resiko deteksi.
b. Dalam merencanakan dan melaksanakan pemeriksaan, auditor Si harus berusaha untuk mengurai resiko audit sampai pada tingkat serendah mungkin yang dapat diterima untuk dapat mencapai tujuan audit.
c. Kelemahan pengendalian intern dianggap "materialitas" jika ketiadaan kontrol internal dapat berakibat kegagalan untuk memperoleh keyakinan memadai bahwa tujuan penegndalian intern akan tercapai.

13. Using the Work of Other Experts

Standar:

a. Auditor SI harus, jika memungkinkan menggunakan hasil kerja auditor atau tenaga ahli lain.
b. Auditor SI harus menilai kualifikasi profesional, kompetensi, pengalaman yang relevan, sumberdaya, independdensi, dan proses *quality control* dari ahli lain tersebut, sebelum menerima penugasan audit.
c. Auditor SI harus meninjjau, menilai dan evaluasi hasil kerja tenaga ahli lain tersebut sebagi bagian dari audit dan menentukan tingkat penggunaan atau mengesampingkan hasil kerja tenaga ahli lain tersebut.
d. Auditor SI harus menetukan dan menyimpulkan apakah hasil kerja tenaga ahli lain tersebut cukup memadai dan lengkap untuk mendukung auditor SI menarik kesimpulan sesuai tujuan audit (dan kesimpulan tersebut harus secara jelas didokumentasikan).

Penjelasan:

a. Auditor SI harus mempertimbangkan penggunaan hasil kerja tenaga ahli lain jika ada kemungkinan kendala dalam audit atau hal itu bermanfaat baginya (misalnya keahlian tenaga ahli lain tersebut, sifat kegiatan yang diperiksa, keterbatasan sumberdaya audit, atau keterbatasan waktu).
b. Tenaga ahli lain yang dimaksud misalnya auditor SI eksternal, konsultan, atau tenaga ahli dalam pekerjaan ini, baik yang telah ditetapkan oleh manajemen senior maupun oleh tim audit.
c. Tenaga ahli dapat berasl dari dalam atau luar organisasi.

14. Audit Evidence

Standar:

a. Auditor SI harus memilih bukti audit yang cukup dan layak (lengkap dan kompeten) untuk dapat menarik kesimpulan hasil audit.
b. Auditor SI harus mengevaluasi kompetensi dan kecukupan bukti audit.

Penjelasan:

a. Appropriate audit evidence

   Kepantasan bukti audit ditentukan oleh:

   - Prosedur yang dilaksanakan auditor untuk memperoleh bukti audit tersebut dan hasil yang diperoleh.
   - Bukti berbentuk dokumen-dokumen (*softcopy* dan *hardcopy*) , catatan atau bukti penguat lain yang diperlukan dalam pemeriksaan, termasuk temuan dan hasil pelaksanaan audit.
   - Dalam perolehan bukti audit dari suatu *test of controls*, auditor SI harus mengingat kecukupan bukti audit diperlukan untuk mendukung penilian terhadap risiko pengendalian.

b. Reliable evidence

   Secara umum bukti audit yang didapat dipercaya adalah:

   - Bukti tertulis, dibanding bukti tidak tertulis.
   - Diperoleh dari sumber independen.
   - Diperoleh langsung oleh auditor, dibanding yang disediakan oleh auditan.
   - Sertifikasi atau dikelola oleh pihak yang independen.

c. Sufficient evidence

   Bukti audit dikatakan cukup jika:

- Dapat mendukung pengambilan kesimpulan sesuai tujuan audit, khusunya yang bersifat materialitas/ signifikan.
- Bukti audit harus objektif dalam arti dapat digunakan pihak ketiga yang independen dan akan menghasilkan kesimpulan yang sama.
- Pada situasi bila auditor SI tidak dapat memperoleh cukup bukti audit, maka hal ini harus diungkapkan secara konsisten dengan laporan audit.

d. Proteksi dan Retensi

- Bukti audit harus aman dari akses yang tidak berwenang maupun kemungkinan dilakukan modifikasi.
- Bukti audit harus disimpan (retensi) paling tidak sampai selesainya penugasan audit, maupun sesuai dengan ketentuan hukum, aturan dan kebijakan yang ada.

BAB 5

Standar Audit Sistem Informasi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- Menjelaskan tentang standar audit
- Menjelaskan tentang kebutuhan audit fisik
- Menjelaskan tentang IT Governance
- Menjelaskan tentang ERP System Review

A. Standar Audit

Sifat khusus dari sistem informasi (IS) audit dan keterampilan yang diperlukan untuk melaksanakan audit tersebut memerlukan standar yang berlaku khusus untuk IS audit. Salah satu tujuan dari ISACA ® adalah untuk memajukan standar global yang berlaku untuk memenuhi visinya. Pengembangan dan penyebaran Standar Audit IS adalah batu penjuru dari kontribusi ISACA profesional untuk komunitas audit. Itu kerangka untuk Standar Audit IS menyediakan berbagai tingkat bimbingan:

1. Standar menetapkan persyaratan wajib untuk IS audit dan pelaporan. Mereka menginformasikan:
    - IS auditor dari tingkat minimum kinerja yang dapat diterima yang diperlukan untuk memenuhi tanggung jawab profesional yang ditetapkan dalam ISACA Kode Etik Profesional.
    - Manajemen dan pihak berkepentingan lainnya dari harapan profesi tentang pekerjaan praktisi.
    - Pemegang Auditor Sistem Informasi Certified ™ (CISA ®) penetapan persyaratan.Kegagalan untuk mematuhi standar dapat mengakibatkan investigasi perilaku pemegang CISA

oleh Dewan Direksi atau ISACA ISACA sesuai komite dan, akhirnya, tindakan disipliner.

2. Pedoman memberikan panduan dalam menerapkan IS Standar Audit. Auditor IS harus mempertimbangkan mereka dalam menentukan bagaimana mencapai pelaksanaan standar, menggunakan penilaian profesional dalam aplikasi mereka dan bersiaplah untuk membenarkan keberangkatan apapun. Itu tujuan dari Pedoman Audit IS adalah untuk memberikan informasi lebih lanjut tentang cara untuk mematuhi Standar Audit IS.

   Prosedur memberikan contoh-contoh prosedur IS auditor mungkin mengikuti dalam pengauditan. Dokumen prosedur memberikan informasi tentang bagaimana untuk memenuhi standar saat melakukan pekerjaan IS audit, tetapi tidak menetapkan persyaratan. Tujuan dari IS Prosedur audit adalah untuk memberikan informasi lebih lanjut tentang cara untuk mematuhi Standar Audit IS.

B. Kebutuhan Audit Fisik

Ketika merencanakan IS audit , IS Auditor harus memperhitungkan jenis bukti audit yang akan dikumpulkan, yang digunakan sebagai bukti audit untuk memenuhi pemeriksaan tujuan, dan berbagai tingkat atas keandalan. Di antara hal yang harus dipertimbangkan adalah kemerdekaan dan kualifikasi penyedia audit bukti. Sebagai contoh nyata mengaudit bukti dari ketiga yang independen pihak dapat lebih diandalkan dibandingkan audit bukti dari organisasi yang diaudit. Bukti audit fisik umumnya lebih handal daripada representasi dari seorang individuS. Berbagai jenis audit bukti yang IS Auditor harus pertimbangkan untuk menggunakan meliputi :

- Proses diamati dan keberadaan item fisik.

  Proses yang diamati dan Keberadaan barang fisik dapat mencakup pengamatan kegiatan , properti dan sistem informasi fungsi, seperti :

  - ✓ Inventarisasi media di luar kantor lokasi penyimpanan.
  - ✓ Sebuah sistem komputer keamanan kamar di operasi.

- Bukti audit Dokumenter.

  Bukti audit dokumenter direkam pada kertas atau media lainnya , dapat meliputi :

  - ✓ Hasil ekstraksi data.
  - ✓ Rekaman transaksi.
  - ✓ Daftar Program.
  - ✓ Faktur.
  - ✓ Aktivitas dan kontrol log.
  - ✓ Dokumentasi pengembangan sistem.

- Representasi.

  Representasi dari mereka yang diaudit dapat menjadi bukti audit, seperti :

  - ✓ Kebijakan dan prosedur tertulis.
  - ✓ Flowchart Sistem.
  - ✓ Pernyataan tertulis atau lisan.

- Analisis

  Hasil analisis informasi melalui perbandingan , simulasi , perhitungan dan penalaran juga dapat digunakan sebagai bukti audit. Contoh termasuk:

  - ✓ Benchmarking IS kinerja terhadap organisasi lain atau masa lalu periode.
  - ✓ Perbandingan tingkat kesalahan antara aplikasi , transaksi dan pengguna.

  Auditor harus mempertimbangkan waktu selama informasi ada atau tersedia dalam menentukan sifat, waktu, dan luasnya pengujian substantif, dan jika berlaku, kepatuhan pengujian. Untuk Misalnya, bukti audit diproses oleh Electronic Data Interchange (EDI), Dokumen Image Processing (DIP), dan sistem dinamis seperti spreadsheet, mungkin tidak dapat diambil setelah ditetapkan. Jangka waktu jika perubahan pada file yang tidak dikendalikan atau file tidak didukung.

Auditor harus merencanakan untuk menggunakan bukti audit terbaik dicapai konsisten dengan pentingnya audit obyektif dan waktu dan usaha yang terlibat dalam memperoleh bukti audit. Dimana bukti audit yang diperoleh dibentuk representasi lisan sangat penting untuk opini audit atau kesimpulan. IS Auditor harus mempertimbangkan memperoleh konfirmasi dokumenter dari representasi , baik di atas kertas atau di media lainnya.

C. IT Governance

Informasi dan teknologi (IT) governance adalah disiplin subset dari tata kelola perusahaan , berfokus pada informasi dan teknologi (IT) dan kinerja dan risiko manajemen. Kepentingan dalam pengelolaan TI adalah karena kebutuhan yang sedang berlangsung dalam organisasi untuk memfokuskan upaya penciptaan nilai pada tujuan strategis organisasi dan untuk mengelola kinerja mereka yang bertanggung jawab untuk menciptakan nilai ini dalam kepentingan terbaik dari semua pemangku kepentingan. Hal ini telah berkembang dari The Principles of Scientific Management, Total Quality Management dan ISO 9001 sistem manajemen mutu.

Secara historis, eksekutif tingkat papan ditangguhkan keputusan TI kunci untuk manajemen TI dan pemimpin bisnis perusahaan . tujuan jangka pendek dari mereka yang bertanggung jawab untuk mengelola IT dapat bertentangan dengan kepentingan terbaik dari para pemangku kepentingan lainnya kecuali pengawasan yang tepat didirikan.

IT governance secara sistematis melibatkan semua orang : anggota dewan, manajemen eksekutif, staf, pelanggan, masyarakat, investor dan regulator. Kerangka IT Governance digunakan untuk mengidentifikasi, membangun dan menghubungkan mekanisme untuk mengawasi penggunaan informasi dan teknologi yang terkait untuk menciptakan nilai dan mengelola risiko yang terkait dengan penggunaan informasi dan teknologi.

IT governance sering bingung dengan manajemen TI, kepatuhan dan kontrol IT. Masalahnya meningkat dengan istilah-istilah seperti "Pemerintahan, risiko dan kepatuhan (GRC)" yang menetapkan hubungan antara pemerintahan dan kepatuhan . Fokus utama dari tata kelola TI adalah pengelolaan sumber daya TI atas nama berbagai pemangku kepentingan yang peringkatnya didirikan oleh badan organisasi. Sebuah cara sederhana untuk menjelaskan tata kelola TI adalah : apa yang ingin dicapai dari leveraging sumber daya TI. Sementara manajemen IT adalah tentang "Perencanaan, pengorganisasian, memimpin dan mengendalikan penggunaan sumber daya TI "(yaitu, bagaimana), tata kelola TI adalah tentang menciptakan nilai bagi para pemangku kepentingan berdasarkan arah yang diberikan oleh orang-orang yang memerintah. ISO 38500 telah membantu memperjelas tata kelola TI dengan menggambarkan model untuk digunakan oleh direksi perusahaan.

Sementara direksi bertanggung jawab untuk pelayanan ini tidak biasa yang akan mendelegasikan tanggung jawab ini kepada manajemen (bisnis dan TI) yang diharapkan untuk mengembangkan kemampuan yang diperlukan untuk memberikan kinerja yang diharapkan. Sementara mengelola risiko dan memastikan kepatuhan merupakan komponen penting dari pemerintahan yang baik, fokus utama adalah pada memberikan nilai dan mengelola kinerja (yaitu "Pemerintahan, Nilai pengiriman dan Kinerja manajemen" (GVP).

BAB 6

Prosedur Audit Sistem Informasi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- Menjelaskan tentang audit sistem informasi
- Menjelaskan tentang jenis-jenis audit sistem informasi
- Menjelaskan tentang tujuan audit sistem informasi
- Menjelaskan tentang prosedur pengukuran risiko
- Menjelaskan tentang risk control system
- Menjelaskan tentang risk based audit
- Menjelaskan tentang Computer Assisted Audit Techniques (CAAT)Tools untuk menguji pengendalian

A. Audit Sistem Informasi

Audit Sistem Informasi (*Informatin System Audit*) atau EDP Audit (*Electronic Data Processing Audit*) atau *computer audit* adalah proses pengumpulan data dan pengevaluasian bukti-bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah menetapkan dan menerapkan sistem pengendalian internal yang memadai, semua aktiva dilindungi dengan baik atau disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efesiensi penyelenggaraan sistem informasi berbasis komputer (Ron Weber 1999:10).

B. Jenis-jenis Audit Sistem Informasi

1. Audit Laporan Keuangan (*Financial Statement Audit*)

Adalah audit yang dilakukan untuk mengetahui tingkat kewajaran laporan keuangan yang disajikan oleh perusahaan (apakah sesuai dengan standar akuntansi keuangan serta tidak menyalahi uji materialitas). Apabila sistem akuntansi organisasi yang diaudit merupakan sistem akuntansi berbasis komputer, maka dilakukan audit terhadap sistem informasi akuntansi apakah proses/mekanisme sistem dan program komputer telah sesuai, pengendalian umum sistem memadai dan data telah substantif.

2. Audit Operasional (*Operational Audit*)

Audit terhadap aplikasi komputer terbagi menjadi tiga jenis, antara lain:

a. ***Post implementation Audit* (Audit setelah implementasi)**
Auditor memeriksa apakah sistem-sistem aplikasi komputer yang telah diimplementasikan pada suatu organisasi/perusahaan telah sesuai dengan kebutuhan penggunanya (efektif) dan telah dijalankan dengan sumber daya optimal (efisien). Auditor mengevaluasi apakah sistem aplikasi tertentu dapat terus dilanjutkan karena sudah berjalan baik dan sesuai dengan kebutuhan usernya atau perlu dimodifikasi dan bahkan perlu dihentikan. Pelaksanaan audit ini dilakukan oleh auditor dengan menerapkan pengalamannya dalam pengembangan sistem aplikasi, sehingga auditor dapat mengevaluasi apakah sistem yang sudah diimplementasikan perlu dimutakhirkan atau diperbaiki atau bahkan dihentikan apabila sudah tidak sesuai kebutuhan atau mengandung kesalahan.

b. *Concurrent audit* (audit secara bersama)
Auditor menjadi anggota dalam tim pengembangan sistem (system development team). Mereka membantu tim untuk meningkatkan

kualitas pengembangan sistem yang dibangun oleh para sistem analis, designer dan programmer dan akan diimplementasikan. Dalam hal ini auditor mewakili pimpinan proyek dan manajemen sebagai quality assurance.

c. *Concurrent Audits* (audit secara bersama-sama)

Auditor mengevaluasi kinerja unit fngsional atau fungsi sistem informasi (pusat/instalasi komputer) apakah telah dikelola dengan baik, apakah kontrol dalam pengembangan sistem secara keseluruhan sudah dilakukan dengan baik, apakah sistem komputer telah dikelola dan dioperasikan dengan baik.

Dalam mengaudit sistem komputerisasi yang ada, audit ini dilakukan dengan mengevaluasi pengendalian umum dari sistem-sistem komputerisasi yang sudah diimplementasikan pada perusahaan tersebut secara keseluruhan.

Saat melakuan pengujian-pengujian digunakan bukti untuk menarik kesimpulan dan memberikan rekomendasi kepada manajemen tentang hal-hal yang berhubungan dengan efektifitas, efisiensi, dan ekonomisnya sistem.

C. Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Ron Weber (1999:11-13) secara garis besar terbagi menjadi empat tahap, yaitu:

1. Pengamanan Aset

   Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, file data harus dijaga oleh suatu sistem pengendalian intern yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset merupakan suatu hal yang sangat penting yang harus dipenuhi oleh perusahaan.

2. Menjaga integritas data

   Integritas data (*data integrity*) adalah salah satu konsep dasar sistem inforamasi. Data memeiliki atribut-atribut tertentu seperti: kelengkapan, keberanaran, dan keakuratan. Jika integritas data tidak terpalihara, maka suatu perusahaan tidak akan lagi memilki hasil atau laporan yang beanr bahkan perusahaan dapat menderita kerugian.

3. Efektifitas Sistem

   Efektifitas sistem informasi perusahaan melikiki peranan pentigndalam proses pemgambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan user.

4. Efisiensi Sistem

   Efisiensi menjadi hal yang sangat penting ketika suatu komputer tidak lagi memilki kapasitas yang memadai atau harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan user dengan sumber daya informasi yang minimal.

5. Ekonomis

   Ekonomis mencerminkan kalkulasi untuk rugi ekonomi (*cost/benefit*) yang lebih bersifat kuantifikasi nilai moneter (uang). Efisiensi berarti sumber daya minimum untuk mencapai hasil maksimal. Sedangkan ekonomis lebih bersifat pertimbangan ekonomi.

D. Prosedur Pengukuran Risiko

Sejak dilahirkan oleh *Institute of internal audit*, definisi fungsi internal audit telah dirancang untuk memenuhi ruang lingkup pengendalian intern, manajemen risiko dan governance. Demikian pula fungsi internal audit di sektor perbankan di Indonesia yang lazim disebut dengan Satuan Kerja Audit Intern Bank (SKAI). Penerapan manajemen risiko di sektor Perbankan di Indonesia terutama dipicu dengan berlakuknya Peraturan Bank Indonesia (PBI) No.5/8/PBI/2003 tanggal 19 Mei 2003 yang kemudian disempurnakan dengan PBINo.11/25/PBI/2009 tanggal

1 Juli 2009 tentang Penerapan Manajemen Risiko bagi Bank Umum. Terkait dengan peranan SKAI dalam manajemen risiko, dalam peraturan tersebut (pasal 15) SKAI wajib melakukan penilaian terhadap sistem pengendalian intern dalam penerapan manajemen risiko, yang meliputi:

1. Penilaian kesesuaian sistem pengendalian intern dengan jenis dan tingkat risiko yang melekat pada kegiatan usaha bank;
2. Penilaian penetapan wewenang dan tanggung jawab untuk pemantauan kepatuhan kebijakan, prosedur dan limit;
3. Penilaian penetapan jalur pelaporan dan pemisahan fungsi yag jelas dari satuan kerja operasional kepada satuan kerja yang melaksanakan fungsi pengendalian;
4. Penilaian struktur organisasi yang menggambarkan secara jelas kegiatan usaha bank;
5. Penilaian pelaporan keuangan dan kegiatan operasional yang akurat dan tepat waktu;
6. Penilaian kecukupan prosedur untuk memastikan kepatuhan bank terhadap ketentuan dan perundang-undangan yang berlaku;
7. Kaji ulang yang efektif, independen dan obyektif terhadap prosedur penilaian kegiatan operasional bank;
8. Penilaian pengujian dan kaji ulang yang memadai terhadap sistem informasi manajemen;
9. Penilaian dokumentasi secara lengkap dan memadai terhadap prosedur operasional, cakupan dan temuan audit, serta tanggapan pengurus bank berdasarkan hasil audit;
10. Verifikasi dan kajiulang secara berkala dan berkesinambungan terhadap penanganan kelemahan-kelemahan bank yang bersifat material dan tindakan pengurus bank untuk memperbaiki penyimpangan-penyimpangan yang terjadi.

E. Risk Control System

Ruang lingkup peranan SKAI dalam penerapan manajemen risiko di bank umum seperti disebutkan di atas secara umum mensyaratkan bahwa SKAI wajib melakukan penilaian terhadap sistem pengendalian intern yang terkait dengan penerapan manajemen risiko atau umumnya disebut *Risk Control System.*

Dalam metodologi *risk assessment,* umumnya risiko yang diukur adalah *residual risk* atau risiko yang tersisa. *Residual risk* ini merupakan hasil dari risiko yang melekat (*inherent risk*) dari usaha yang dilaksanakan bank setelah diperhitungkan mitigasinya dengan*risk control system* yang ada/diterapkan. Sebagai contoh risiko operasional karena penyalahgunaan wewenang *user* dalam penggunaan teknologi informasi untuk mendukung operasional bak. Semakin tinggi limit kewenangan *user* (jumlah transaksi, menu transaksi, akses user dan lain-lain), maka risiko melekat akibat penyalahgunaan tersebut juga semakin tinggi. *Risk control system* yang diterapkan oleh bank harus dapat dinilai oleh SKAI sejauh mana dapat memitigasi risiko melekat tersebut, sehingga dengan demikian *residual risk* yang tersisa merupakan *acceptable risk* yang dapat diterima oleh manajemen bank sebagai cerminan *risk appetite*-nya.

Dalam Peraturan Bank Indonesia tersebut di atas (pasal 2) disinilah inti penerapan manajemen risiko bank yang sekurang-kurangnya meliputi:

1. Pengawasan aktif dewan komisaris dan direksi;
2. Kecukupan kebijakan, prosedur dan penetapan limit;
3. Kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko serta sistem informasi manajemen risiko;
4. Sistem pengendalia intern yang menyuluruh.

Empat komponen tersebut dibangun sebagai *risk control system,* yang harus diukur oleh satuan kerja manajemen risiko di bank serta di evaluasi dan dinilai kecukupan, efektivitas serta efisiensinya oleh SKAI.

F. Risk Based Audit

Lebih lanjut, SKAI didorong untuk mengoptimalkan peranannya didalam penerapan manajemen risiko di bank dengan cara melakukan penajaman dan memfokuskan kegiatannya untuk mendukung mekanisme pemantauan risiko oleh manajemen. Atas dasar itulah, SKAI menerapkan metodologi *risk based audit*. Namun demikian, apa sebenarnya *risk based audit* tersebut? Pelaksanaan audit berdasarkan pengukuran risiko, maksudnya?

Beberapa SKAI bank berada di dalam kondisi 'bermimpi' bahwa *risk based audit* merupakan teori audit yang didasarkan pada atau dimulai dengan suatu prosedur penilaian risiko. Namun didalam penerapannya pelaksanaan audit tidak berbeda dari yang 'dulu-dulu'. Hal ini karena paradigma SKAI di dalam menerapkan *risk based audit* masih tidak jelas dan rancu dengan metodologi pengukuran risko atau malah ikut-ikutan melakukan pengukuran terhadap risiko. Penerapan suatu *Risk based audit* memang membutuhkan tahapan awal penilaian terhadap risiko. Penilaian ini umumnya di bank meliputi penilaian terhadap*inherent risk* dan *risk control system* yang telah difasilitasi oleh satuan kerja manajemen risiko di bank. SKAI harus melakukan validasi terhadap penilaian *inherent risk* dan melakukan pengujian-pengujian terhadap *risk control system* yang ada, untuk melaporkan *residual risk*yang masih tersisa sebagai bahan manajemen di dalam proses pengambilan keputusan.

Untuk mendukung optimalisasi, efektivitas dan efisiensi sumberdaya audit yang dimiliki, SKAI akan melakukan pengujian-pengujian terhadap *risk control system* melalui pendekatan-pendekatan (*audit approach)* yang beragam. Semakin tinggi risiko hasil penilaian *inherent risk* atau kurang memadainya *risk control system* yang ada, maka SKAI semakin mengalokasikan sumberdaya auditnya (tenaga audit, waktu audit, prosedur audit dan lainnya).

Sebagai contoh gambaran adalah sebagai berikut. Berdasarkan pengukuran, risiko hukum atas aktivitas perkreditan suatu bank dalam tingkatan menengah cenderung naik. Hal tersebut karena:

1. Secara *inherent,* banyaknya permasalahan kelehaman pengikatan pinjaman dan pengikatan agunan/jaminan kredit secara hukum.Kondisi frekuensi (*likelyhood)* ini oleh SKAI harus ditindaklajuti dengan meningkatkan sampling audit pada saat penyusunan program audit.
2. Terdapat kelehaman beberapa prosedur operasional sebagai *Risk control system,* antara lain lemahnya review dan supervisi dari atasan, keterbatasan jumlah staf untuk prosedur tambahan, dan prosedur operasional yang kurang jelas/detail. Kondisi ini menuntut SKAI untuk melakukan pengujian-pengujian melalui suatu pendekatan audit dengan prosedur audit yang lebih komprehensif. Mulai dari melakukan review terhadap kecukupan kebijakan/sistem dan prosedur, pengujian pemahaman pelaksana, tingginya tingkat *human error*, konfirmasi kepada pihak debitur, pemeriksaan secara on the spot terhadap agunan, dan seterusnya yang menunjukkan kompleksnya prosedur audit untuk menguji kelemahan *risk control system* yang mengakibatkan tingginya*residual risk* di atas *risk appetite* manajemen bank.

G. Computer Assisted Audit Techniques (CAAT)Tools untuk menguji pengendalian

Test Data method, digunakan untuk menguji integritas aplikasi dengan memproses input data yang disiapkan khusus untuk menguji aplikasi yang sedang direview, hasil dari tes dibandingkan dengan ekspektasi output yang diharapkan untuk mendapat evaluasi yang objektif atas logika aplikasi dan keefektifan pengendalian. Tahapannya

1. Creating test data, auditor menyiapkan data transaksi yang valid maupun tidak untuk menguji input error, logical process dan irregularity.
2. Base Case System Evaluation (BCSE), dilakukan dengan memproses seluruh jenis transaksi secara berulang sampai didapatkan hasil; yang konsisten dan valid.
3. Tracing, teknik menguji aplikasi dengan mengikuti alur logika aplikasi.

Keunggulan :
(1) menyediakan auditor bukti eksplisit mengenai fungsi aplikasi (2) tidak mengganggu operasi perusahaan (3) tidak banyak membutuhkan keahlian komputer yang tinggi dari pihak auditor
Kelemahan : (1) auditor mendapatkan aplikasi untuk diuji dari personel perusahaan, sehingga ada kemungkinan diberikan versi yang berbeda dari yang digunakan (2) hanya menyediakan informasi integritas aplikasi di satu waktu tersebut (3) biaya tinggi.

The Integrated Test Facility, teknik otomasi untuk menguji logika aplikasi dan pengendalian saat operasi normal sedang berjalan
Keuntungan : (1) mendukung dilakukannya waskat atas pengendalian; (2) dapat menguji aplikasi secara ekonomis tanpa mengganggu operasional.
Kelemahan : ada potensi merusak data perusahaan.
Parallel simulation, dilakukan dengan menulis program yang mensimulasikan fitur kunci atau proses aplikasi yang sedang direview. Tahapannya :

1. Auditor harus memahami aplikasi yang akan direview
2. Auditor mengidentifikasi proses dan pengendalian dalam aplikasi yang penting untuk disimulasi
3. Auditor membuat simulasi menggunakan 4GL atau GAS
4. Auditor menjalankan program simulasi menggunakan data-data yang telah dipilih untuk menghasilkan output
5. Auditor mengevaluasi dan merekonsiliasi hasil simulasi dengan hasil apabila menggunakan aplikasi aslinya.

H. Control Effectiveness

Control Effectiveness adalah pengendalian secara efektif dimana audit internal adalah suatu fungsi penilaian yang idenpenden dalam suatu organisasi untuk menguji dan mengevaluasi kegiatan organisasi yang dilaksanakan. Tujuan audit internal adalah membantu para anggota organisasi / perusahaan agar dapat

melaksanakan tanggungjawabnya secara efektif. Untuk itu auditor internal akan melakukan analisis, penilaian dan mengajukan saran-saran. Tujuan Audit mencakup pula pengembangan pengawasan yang efektif dengan biaya yang wajar. Selain itu juga audit internal merupakan suatu aktivitas indenpenden, keyakinan objectif dan konsultasi yang dirancang untuk memberikan nilai tambah dan meningkatkan operasi organisasi. Audit pun harus membantu organisasi/perusahaan mencapai tujuannya dengan menerapkan sistematis dan berdisplin untuk mengevaluasi dan meningkatkan efektivitas manajemen resiko, pengendalian dan proses pengaturan dan pengelolaan organisasi.

BAB 7

Struktur, Proses dan Mekanisme Tata Kelola Teknologi Informasi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- Menjelaskan tentang Struktur Tata Kelola Teknologi Informasi
- Menjelaskan tentang Proses Tata Kelola Teknologi Informasi
- Menjelaskan tentang Mekanisme Tata Kelola Teknologi Informasi

Pada pengelolaan teknologi informasi bagi organisasi terdapat beberapa elemen penting yang harus diperhatikan. Secara tidak langsung beberapa elemen ini saling berkaitan dalam rangka menjadikan tata kelola teknologi yang relevan dan sesuai serta terstruktur sehingga tidak terjadi kesalah pahaman antara manajemen eksekutif sampai dengan bagian operasional terkait hal apa saja serta peranan yang harus dilakukan oleh masing- masing aktor pada organisasi.

Pada dasarnya Tata Kelola Teknologi Informasi adalah suatu kekhawatiran tentang dua hal, yaitu : bahwa TI memberikan nilai bisnis dan bahwa risiko TI telah diantisipasi. Yang pertama didorong oleh keselarasan (struktur) strategis TI dengan bisnis, sedangkan kedua didorong oleh pengaplikasian akuntabilitas ke dalam perusahaan. Kedua kebutuhan pengukuran misalnya penggunaan Balance Scorecard.

A. Struktur Tata Kelola Teknologi Informasi

Keputusan untuk menerapkan Kerangka Kerja TI terkadang dapat disebabkan oleh isu tertentu atau suatu masalah kritis. Untuk dapat menempatkan struktur, proses dan mekanisme Tata Kelola teknologi Informasi sehingga dapat dipahami satu dengan lainnya. Berikut ini kerangka kerja berdasarkan Peterson's Framework (Peterson, 2002) Struktur melibatkan keberadaan bertanggung jawab seperti eksekutif TI dan keragaman TI serta proses merujuk strategis TI sampai dengan pengambilan keputusan dan monitoring.

1. Roles and Responsibilities

   Pendefinisian tugas dan tanggung jawab yang jelas dan tidak ambigu dari berbagai pihak yang terlibat merupakan prasyarat penting untuk penggunaan kerangka kerja tata kelola TI yang efektif. Hal ini merupakan peran dari direksi dan manajemen eksekutif untuk merumuskan tugas serta tanggung jawab dan memastikan bahwa semuanya jelas dipahami pada seluruh lini pada organisasi.

2. IT Strategy Committee and IT Steering Committiees

   Seperti yang telah disebutkan bahwa Tata Kelola Teknologi Informasi harus menjadi bagian integral dari tata kelola perusahaan dan merupakan perhatian dari direksi serta manajemen eksekutif yang bertanggung jawab untuk mengatur dan megelola perusahaan. Berikut ini tabel penjelas antara kedua bentuk tersebut :

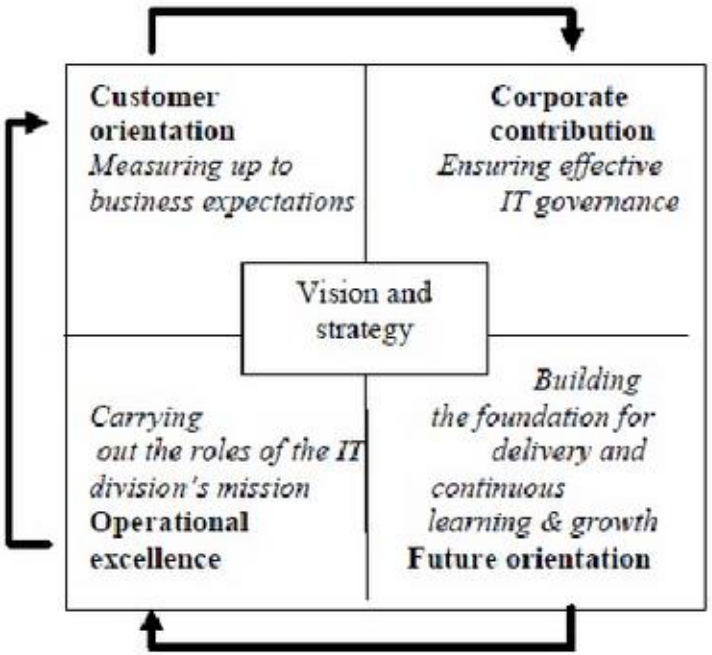
	IT Strategy Committee	*IT Steering Committiees*
Wewenang	• Menyarankan Direksi dan Manajemen strategi TI • Didelegasikan oleh direksi untuk memberikan masukan terkait strategi • Fokus pada tujuan saat ini dan isu strategis TI masa depan	• Membantu eksekutif di pelaksanaan strategi TI • Mengawasi manajemen layanan TI • Berfokus pada implementasi
Keanggotaan	• Direksi dan bukan anggota direksi	• CIO serta konsultan yang berkaitan dengan TI padaperusahaan

3. IT Organisation Structure

   Efektifitas Tata Kelola Teknologi Informasi juga ditentukan oleh bagaimana TI diatur dalam sebuah organisasi dimana pengambilan keputusan TI berada pada oraganisasi tersebut sehingga semua lini dari organisasi dapat mengambil manfaat dari pengambilan keputusan melalui TI. Pemanfaatan TI juga harus disusun secara jelas dan teratur dalam organisasi.

4. Balanced Scoreracrds

   Evaluasi dari suatu organisasi tidak harus terbatas pada keuangan tradisional melainkan evaluasi harus dilengkapi dengan langkah–langkah mengenai kepuasan pelanggan, internal proses dan kemampuan untuk berinovasi. Hasil yang dicapai dalam bidang–bidang perspektif tambahan harus menjamin masa depan hasil keuangan dan mendorong organisasi menuju tujuan strategisnya dan menjaga keempat perepktif dalam keseimbangan. Pembangunan IT Development Balanced Scorecard dan IT Operational Balanced Scorecard didefinisikan sebagai enabler untuk Strategic Balanced Scorecard yag digunakan untuk enabler dari Business Balance Scorecard.



Strategic Balanced Scorecard yang digunakan untuk enabler Business Balance Scorecard.

5. Proses Tata Kelola Teknologi Informasi

Strategic Information Systems Planning Menurut (EARL J.M. 1993) Strategoc Information Systems Planning (SISP) memiliki empat komponen utama, yaitu : menyelaraskan TI dengan tujuan bisnis, memanfaatkan TI guna keunggulan kompetitif, mengarahkan efisiensi dan efektifitas pengelolaan sumber daya TI, dan mengembangkan kebijakan teknologi dan arsitektur.

COBIT and ITIL Control Objectived for Information and related Technology (COBIT) menyediakan 34 proses TI yang sesuai dengan tingkatan organisasi yang bertujuan sebagai pengendali dan pedoman manajemen termasuk model kematangan (maturity models) dan penilaian (scorecard) dibentuk indikator

tujuan utama dan indikator kinerja utama. Tujuan COBIT juga dapat membantu untuk mendukung IT Governance dalam suatu organisasi. Kontrol Tujuan dari "Membantu dan menyarankan pengguna IT".

Jadi, COBIT memberitahu apa yang harus dilakukan dan ITIL menjelaskan secara rinci bagaimana itu harus dilakukan Service Level Agreements (SLA) SLA mendukung kebutuhan proses Service Level Management (SLM) to menjalankan peran penting. Fungsi SLA adalah mendefinisikan apa tingkat layanan yang diterima oleh pengguna dan yang dicapai oleh penyedia layanan, mendefinisikan apa yang dapat diterima bersama dan disepakati dalam hal ini merupakan indikator kualitas dari layanan yang diberikan.

Information Economics Metode ekonomi informasi yang dikembangkan oleh Benson dan Parker dapat digunakan sebagai penyelaras dimana bisnis dan TI dapat menghasilkan proyek–proyek TI dengan cara ini dapat diprioritaskan dan proyek mana yang dapat dipilih. Ekonomi informasi berawal dari Return On Investment (ROI) dimana akan dihitung suatu pengembalian modal dari investasi yang dilakukan meliput berapa lama, berapa jumlahnya dan dampak yang akan didapati.

6. Mekanisme Tata Kelola Teknologi Informasi

Banyak penelitian menyebutkan bahwa ini merupakan bagian yang paling penting dalam kerangka kerja Tata Kelola TI, untuk mencapai keselarasan bisnis dan TI secara berkelanjutan. Terdapat beberapa hal yang perlu diperhatikan dalam praktik implementasi Tata Kelola TI :

a. Mengadopsi pendekatan *enterprise* yang lebih luas
   - Bisnis dan TI harus bekerja bersama-sama untuk mendefinisikan dan mengendalikan kebutuhan bisnis
   - TI perlu untuk mengembangkan sebuah model pengendalian yang dapat digunakan oleh semua divisi di organisasi
   - Pendekatan komite direkomendasikan dalam mengatur, menyetujui dan mengawasi kebijakan

- Pandangan/pemahaman mengenai tata kelola TI harus sama. Terpadu di seluruh organisasi berdasarkan "bahasa yang sama"
- Harus ada pemahaman (dan persetujuan) yang jelas oleh stakeholder atas apa saja yang ada di dalam ruang lingkup tata kelola TI

b. Komitmen TOP *Level Management*
   - Tata Kelola TI perlu sebuah mandat dan arahan dari dewan direksi/Eksekutif Level *management*
   - Pastikan manajemen bertanggungjawab dalam bisnis dan TI yang telah ditetapkan

c. Model Tata Kelola dan Pengendalian yang disepakati bersama
   - Meskipun akan menjadi tantangan serta dorongan, kerangka kerja yang disepakati bersama untuk mendefinisikan proses-proses TI dan pengendalian, harus didefinisikan, agar tata kelola berjalan dengan baik
   - Proses tata Kelola TI perlu untuk diintegrasikan dengan praktik tata kelola perusahaan, sehingga Tata Kelola TI tidak hanya menjadi milik proses-proses TI saja
   - Kerangka kerja perlu untuk didukung dengan komunikasi yang efektif dan kesadaran, sehingga tujuan dapat dimengerti
   - Pemberian insentif/*reward*harus dipertimbangkan guna memotivasi ketaatan pada kerangka kerja
   - Pengembangan TI organisasi yang terdesentralisasi
   - Hindari administrasi yang bertele-tele

d. Rasa percaya dibutuhkan untuk mendapatkan fungsi TI sepenuhnya (internal/external)
   - Agar Tata Kelola TI dapat bekerja pada suplier dan penyedia layanan TI lainnya, serta tahu bagaimana caranya agar dapat selaras dengan permintaan konsumen, rasa percaya harus dikembangkan dengan cara apapun.

- Contohnya, melalui *awareness program*, workshop, direktur TI bertindak sebagai jembatan antara bisnis dan TI

e. Sistem pengukuran yang akan menjamin tujuan selalu dipantau
   - Menciptakan *scorecard*TI, yang akan mendukung dan memperkuat pencapaian tujuan tata kelola TI
   - Menciptakan langkah awal pengukuran yang dapat meningkatkan kesadaran dan inisiasi terhadap program Tata kelola TI
   - Kegunaan pengukuran harus dalam ranah bisnis dan disetujui oleh stakeholder

f. Fokus pada biaya
   - Pastikan akan ada kesempatan untuk melakukan *financial savings*, sebagai konsekuensi dari implementasi Tata Kelola TI yang semakin baik.

Agar dapat menempatkan struktur tata kelola TI, proses dan mekanisme terkait dalam hubungan yang komprehensif di antara mereka. Analisis utama menekankan penggunaan tiga pilar kerangka kerja tata kelola TI yang didasarkan pada hasil kerja ITGI, yaitu standar industri, praktik terbaik pelanggan, dan kepemimpinan. Kerangka kerja ini mengungkapkan pentingnya jaminan bahwa TI akan mendukung sasaran bisnis, mengoptimumkan investasi bisnis di bidang TI dan mengelola risiko dan peluang dari TI.

Karena TI harus selaras dengan strategi bisnis maka TI harus dikelola dalam komitmen dan akurasi yang sama, dan diatur oleh komite TI pada dewan direksi dan komite strategi TI, yang terdiri atas dewan direksi dan non direksi.Komite tersebut harus menjamin bahwa TI merupakan agenda regular dari dewan direksi.

Dalam lingkungan kematangan tata kelola TI , SLA dan dukungan pada proses Service Level Manajemen (SLM) diperlukan untuk peran yang penting.

Fungsi SLA adalah :

1. Mendefinisikan level layanan yang diterima oleh pengguna dan mampu diberikan oleh penyedia layanan;
2. Mendefinisikan hal-hal yang dapat diterima dan kesepakatan terkait dengan indikator-indikator kualitas layanan.

Untuk mengimplementasikan kerangka kerja tata kelola TI, organisasi perlu melakukan diagnosis atas dirinya sendiri mengenai hal apa yang perlu dilakukan untuk mengefektifkan tata kelola TI dan untuk mengidentifikasi peluang peningkatannya.

Untuk meningkatkan levelnya, organisasi sekurang-kurangnya harus mengenal pentingnya mengetahui isu tata kelola TI serta solusinya, didukung dengan kerangka kerja dan struktur yang telah ditetapkan. COBIT melihat bahwa menerapkan mekanisme *governance* secara efektif tidaklah mudah, namun harus melalui berbagai tahap *maturity* (kematangan) tertentu. Model *m aturity* untuk mengontrol proses IT, sehingga manajemen dapat mengetahui dimana posisi organisasi sekarang, dan diposisi dimana organisasi ingin berada.

Paling tidak posisi *maturity* sebuah organisasi terkait dengan keberadaan dan kinerja proses *IT Governance* dapat dikategorikan menjadi enam tingkatan, yaitu:

a. 0 = *Non existent* (tidak ada), merupakan posisi kematangan terendah, yang merupakan suatu kondisi dimana organisasi merasa tidak membutuhkan adanya mekanisme proses *IT Governance* yang baku, sehingga tidak ada sama sekali pengawasan terhadap *IT Governance* yang dilakukan oleh organisasi.

b. *1 = Initial* (inisialisasi), sudah ada beberapa inisiatif mekanisme perencanaan, tata kelola, dan pengawasan sejumlah *IT Governance* yang dilakukan, namun sifatnya masih *ad hoc*, *sporadis*, tidak kosisten, belum formal, dan reaktif.
c. *2 = Repeatable* (dapat diulang), kondisi dimana organisasi telah memiliki kebiasaan yang terpola untuk merencanakan dan mengelola *IT Governance* dan dilakukan secara berulang-ulang secara reaktif, namun belum melibatkan prosedur dan dokumen formal.
d. *3 = Defined* (ditetapkan), pada tahapan ini organisasi telah memiliki mekanisme dan prosedur yang jelas mengenai tata cara dan manajemen *IT Governance*, dan telah terkomunikasikan dan tersosialisasikan dengan baik di seluruh jajaran manajemen.
e. 4 = *Managed* (diatur), merupakan kondisi dimana manajemen organisasi telah menerapkan sejumlah indikator pengukuran kinerja kuantitatif untuk memonitor efektivitas pelaksanaan manajemen *IT Governance*.
f. 5 = *Optimised* (dioptimalisasi), level tertinggi ini diberikan kepada organisasi yang telah berhasil menerapkan prisip-prinsip *governance* secara utuh dan mengacu *best practice*, dimana secara utuh telah diterapkan prinsip-prinsip *governance*, seperti *transparency*, *accountability*, *responsibility*, dan *fairness*.

Dengan adanya *maturity level model*, maka organisasi dapat mengetahui posisi kematangannya saat ini, dan secara terus menerus serta berkesinambungan harus bersaha untuk meningkatkan levelnya sampai tingkat tertinggi agar aspek governance terhadap teknologi informasi dapat berjalan secara efektif.

BAB 8

Strategi dan Teknik Tata Kelola Teknologi Informasi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- Menjelaskan tentang Faktor Penentu Tata Kelola Teknologi Informasi
- Menjelaskan tentang Strategi IT Governance untuk Bisnis

A. Faktor Penentu Tata Kelola Teknologi Informasi

Tata kelola TI yang bersifat sentralisasi diasosiasikan dengan organisasi berskala kecil dengan strategi busnis yang berorientasi pada biaya dan di cirikan oleh struktur data dan kelola bisnis, stabilitas lingkungan, profuk/layanan bisni dengan intensif informasi intensif yang rendah serta pengalaman bisnis dan kompetensi pengelolaan teknologi informasi yang masih rendah

Tata kelola TI yang bersifat terdesentralisasi diasosiasikan dengan organisasi besar dengan strategi bisnis yang berfokus pada inovasi, dicirikan oleh struktur tat kelola bisnis terdesentralisasi, lingkungan yang cenderung berubah, produk dan proses bisnis dengan intensif informasi yang tinggi serta pengalaman bisnis dan kompetensi pengelolaan TI yang tinggi. Ciri fleksibilitas menurut (D'Aveni,1999; El Sawy,dkk1999)

- Penekanan waktu dan biaya dalam iklus hidup produk dan desain.
- Mempercepat kemajuan teknologi
- Kesetiaan konsumen yang brubah-ubah
- Produk layanan yang dikhususkan, bersifat intensif terhadap pengetahuan
- Masuknya kompetitor baru yang tidak terduga,reposisi pejabat

- ❖ Pendefisian kembali batasan-batasan industri dan organisasi
- ❖ Volatilitas pasar global

B. Strategi IT Governance untuk Bisnis

Penanganan IT pada organisasi selalu menjadi masalah bagi para top eksekutif karena sifat teknis dari IT. Keputusan-keputusan kunci tentang IT hanya diserahkan kepada profesional TI. Sementara tata kelola IT (*IT governance*) menyiratkan suatu sistem di mana semua stakeholder, termasuk dewan direksi, pelanggan internal, dan bidang terkait seperti keuangan dan sumber daya manusia diperlukan masukannya dalam proses perencanaan dan pengambilan keputusan tentang IT agar tercipta *IT business alignment* dalam organisasi. Perencanaan yang baik merupakan fokus utama penerapan *IT business alignment* pada *IT governance*. *IT business alignment* harus sejalan dan sesuai dengan harapan organisasi dan dibutuhkan untuk mendukung pencapaian visi dan misi yang telah ditetapkan. *IT business aligment* mengarah dan menyoroti peran IT dalam pengembangan strategi bisnis dengan mempertimbangkan penyelarasan sumber daya infrastruktur dan pengintegrasian fungsional IT dan bisnis. Untuk itu diperlukan *strategic alignment* dan langkah-langkah serius dalam menerapkannya untuk mendukung dan menunjang kelangsungan organisasi.

Pencapaian strategic alignment internal terjadi ketika pengarah dari network konsisten dan sejajar dengan keinginan pelanggan dan pendapatan. Namun demikian, penerapan IT pada organisasi masih banyak yang belum efektif, dilakukan secara tradisional, belum alignment dengan bisnis, dan pengambilan keputusan kunci dibidang IT dilakukan dan diberikan hanya kepada para profesional IT saja. Hal ini disebabkan karena para direksi mempunyai keterbatasan pengetahuan dan pengalaman teknik dibidang IT. Sementara IT governance organisasi yang tidak efektif dapat menyebabkan [1]: kerugian bisnis, penurunan reputasi, melemahkan kemampuan daya saing, ketidak tepatan jadwal proyek, pemborosan biaya, mutu produksi yang tidak sesuai dengan harapan, mempengaruhi efisiensi organisasi, serta tidak terpenuhinya inovasi dan

keuntungan yang dijanjikan. Pada bagian lain, Tiwana et al. [2] menemukan bahwa integrasi pengetahuan berpengaruh secara positif terhadap fleksibilitas dalam proyek TI organisasi. Karena itu, pengetahuan tentang strategic alignment IT business para direksi, eksekutif dan stakeholder organisasi yang menerapkan IT perlu dikembangkan. Artikel ini bermaksud membahas dan memberikan informasi tentang strategic alignment IT business sebagai salah satu komponen IT governance organisasi.

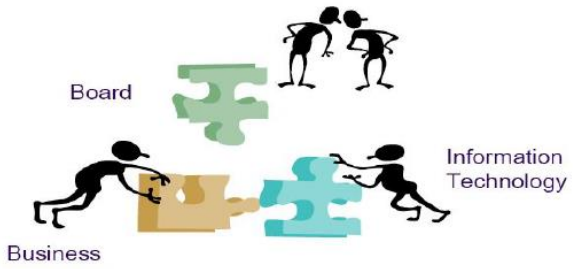
IT Governance mencakup pembuatan keputusan, akuntabilitas pelaksanaan kegiatan penggunaan IT, siapa pengambil keputusan, mengolah proses pembuatan keputusan, dan pengimplementasian keputusan-keputusan yang berkaitan dengan IT dalam organisasi. IT Governance menyediakan struktur, menghubungkan proses IT, sumber daya IT, dan informasi bagi strategi serta tujuan suatu organisasi. Untuk dapat memiliki IT governance yang efektif, organisasi harus mengimplmentasikan IT governance focus area [3] secara holistik.

No.	Fokus Area / Bidang	Keterangan
1.	Strategic Alignment	Berfokus pada memastikan hubungan bisnis dan rencana IT, mendefinisikan, memelihara dan memvalidasi nilai proposisi IT, dan menyelaraskan operasi IT dengan operasi perusahaan (kesesuaian operasi IT dengan operasi perusahaan).
2.	Value Delivery	Melaksanakan proposisi nilai sepanjang siklus pengiriman, memastikan bahwa IT memberikan manfaat sesuai dengan yang dijanjikan terhadap strategi, berkonsentrasi pada mengoptimalkan biaya dan membuktikan nilai intrinsik IT.
3.	Resource Management	Fokus terhadap investasi optimal, pengelolaan yang baik, sumber *ciritical* IT: aplikasi, informasi, infrastruktur dan pengguna/sumber daya manusia. Isu critical yang berhubungan dengan optimasi pengetahuan dan infrastruktur.
4.	Risk Management	Membutuhkan kesadaran risiko oleh pejabat perusahaan senior, pemahaman yang jelas tentang risk appetite perusahaan, pengertian kepatuhan persyaratan, transparansi tentang risiko yang signifikan terhadap perusahaan, dan menanamkan tanggung jawab manajemen resiko dalam organisasi.
5.	Performace measurement	Track dan memantau pelaksanaan strategi, penyelesaian proyek, penggunaan sumber daya, proses kinerja dan pelayanan, misalnya menggunakan balance scorecard yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan yang terukur di luar akuntansi konvensional.

Tampak pada Tabel IT Governance Focus Area [3], strategic alignment merupakan unsur pertama dalam IT governance yang berfokus dalam memastikan hubungan bisnis dan perencanaan IT, mendefinisikan, memelihara dan mengukur validasi nilai proporsi IT, dan menyelaraskan (alignment) operasi IT dengan

operasi perusahaan. Strategic alignment merupakan fokus utama, berperan strategis dan dominan dalam memenuhi harapan penerapan IT terhadap pencapaian visi, misi dan keberlangsungan suatu organisasi. Namun demikian, IT governance biasanya bekerja secara berbeda antara praktek dengan teorinya. Bekerja atau tidaknya IT governance sebagian besar karena hubungan antara manusia, bukan karena struktur atau proses. Oleh karena itu, Reich dan Benbasat [4] menjelaskan bahwa selain memiliki pengetahuan bisnis, para eksekutif hendaknya juga memiliki kemampuan IT dan saling memahami perspektif lain, berkontribusi untuk proses input masing-masing, dan menghormati kontribusi dan tantangan yang dibuat oleh satu sama lainnya.

IT bisnis alignment telah diidentifikasi sebagai sumber daya organisasi yang penting, memfasilitasi fleksibilitas IT dan fleksibilitas bisnis. Karena itu strategic alignment of IT business menekankan otoritas pada IT governance yang baik, dan memastikan IT memberikan kontribusi secara efektif terhadap pencapaian tujuan strategis organisasi. Organisasi harus membangun keselarasan dalam proses IT governance, disusun dengan baik, menjadi tujuan kelembagaan, dan dapat diartikulasikan. Tujuannya adalah menyediakan kerangka tujuan strategi IT, melakukan pengukuran dan penilaian tahunan, dan menguji keselarasannya. Perencanaa n strategis IT dan strategic alignment yang efektif dapat dicapai jika IT governance organisasi dilaksanakan, dikembangkan/dibangun secara modern dengan memperhatikan aspek eksternal, melibatkan pihak eksternal, para stakeholder, direksi, komisaris, dan pihak yang tidak berlatar belakang IT. Tetapi Chan et al. menjelaskan bahwa rekan IT yang kompeten lebih mungkin untuk dipercaya dan berkonsultasi dalam proses pengambilan keputusan, sehingga mereka lebih sadar akan perkembangan bisnis baru dan mengoperasikannya dalam persyaratan bisnis yang muncul. Dengan demikian strategic alignment dapat disusun secara komprehensif, mencakup seluruh proses bisnis, alignment dengan semua komponen dalam organisasi. Strategic aligment tidak boleh diarahkan kepada satu capaian tertentu, tetapi dipengaruhi dan ditengahi oleh faktor yang lain, seperti kelurusan antara strategy IT dan business strategy.

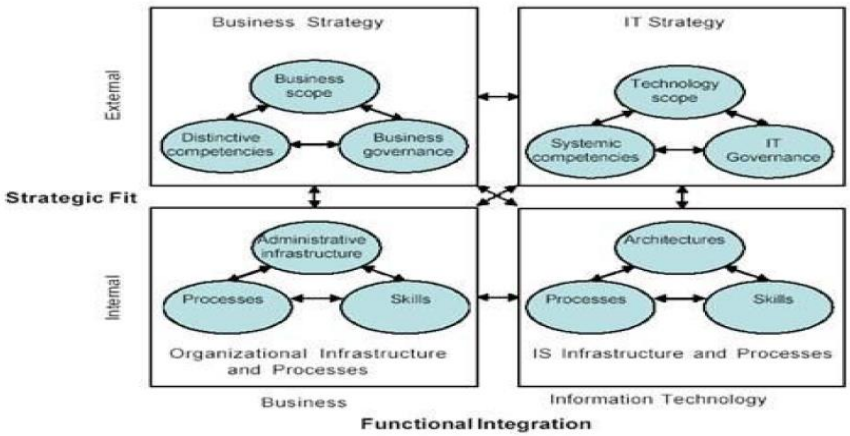


Gambar 1. Kondisi dan Usaha Strategic Aligment of IT Governance

Gambar 1. Kondisi dan usaha strategic aligment of IT governance mengilustrasikan kondisi IT organisasi yang tidak memiliki IT governance dan strategic alignment yang baik. IT governance organisasi yang tidak baik/tidak efektif dapat menyebabkan: kerugian bisnis, penurunan reputasi, melemahkan kemampuan daya saing, ketidak tepatan jadwal proyek, pemborosan biaya, mutu produksi yang tidak sesuai dengan harapan, mempengaruhi efisiensi organisasi, serta tidak terpenuhinya inovasi dan keuntungan yang dijanjikan. Strategic alignment IT business yang baik dimulai dari sistem perencanaan dan pengendalian, dan mengacu pada konsistensi aktivitas internal dalam menerapkan dan membedakan komponen strategi IT business aligment. Strategic alignment IT business bertujuan untuk mengatasi jurang kesenjangan yang besar antara tujuan organisasi dan pemahaman penyedia/ pengelola layanan TI. Strategic alignment IT business juga dapat berperan dalam hal penetapan strategis yang tepat, penyelarasan, dan keselarasan organsasi dan sumber daya manusia. Peran strategic aligment ini ditegaskan oleh McKinsey yang menyatakan bahwa investor membayar premi yang besar untuk investasi di perusahaan-perusahaan dengan standar tata kelola yang tinggi.

Alignment ditafsirkan sebagai keterkaitan yang direncanakan dan koheren terus-menerus antara semua komponen perusahaan, personalia, dan sistem IT sehingga memberikan kontribusi terhadap performance perusahaan. Strategic alignment diinterpretasikan sebagai proses yang berkesinambungan dari

keterkaitan sadar dan koheren dari semua komponen dan personil bisnis dan TI dalam rangka memberikan kontribusi terhadap kinerja organisasi dari waktu ke waktu. Strategic alignment berfokus pada kegiatan manajemen untuk meningkatkan performance kohesif dibidang IT dan bagian fungsional organisasi lainnya, misalnya: keuangan, pemasaran, sumber daya manusia, dan manufaktur. Sehubungan dengan hal ini, Tallon dan Kraemer [14] telah menemukan bahwa alignment tertinggi terdapat pada produksi, operasi, dan hubungan pelanggan, dan yang terendah terdapat pada dalam penjualan dan pemasaran. Pendapat yang lainnya menyatakan bahwa rancangan dan strategic alignment IT business adalah domain dari enterprise architecture. Para peneliti telah menunjukkan bahwa keselarasan strategis berkorelasi dengan kinerja perusahaan. Sementara Marquest P et al. dan Ekstedt et al. menyatakan bahwa empat perspektif IT business aligment strategic yang berbeda berhubungan satu sama lain (lintas domain) ketika kesesuaikan strategis dan integrasi fungsional dalam model SAM dinilai secara bersamaan. Keempat perspektif strategis tersebut adalah: (a) perspektif strategi eksekusi, (b) perspektif potensi teknologi, (c) perspektif potensi kompetitif, dan (d) perspektif tingkat pelayanan. Perspektif ini diklasifikasikan dalam dua kategori yang meliputi: (i) strategi bisnis sebagai driver yang mencakup perspektif pelaksanaan strategi dan teknologi perspektif potensial, dan (ii) strategi IT sebagai enabler yang mencakup perspektif potensial kompetitif dan tingkat pelayanan perspektif. IT business strategic alignment memiliki fokus dalam memastikan hubungan antara bisnis dan rencana TI, menentukan, merawat dan memastikan IT value proposition; dan pada aligning IT op-eration. Pendapat tentang strategic alignment ini diperkenalkan oleh Henderson dan Venkatraman yang dijadikan landasan filosofi berfikir seperti pada Gambar 2.



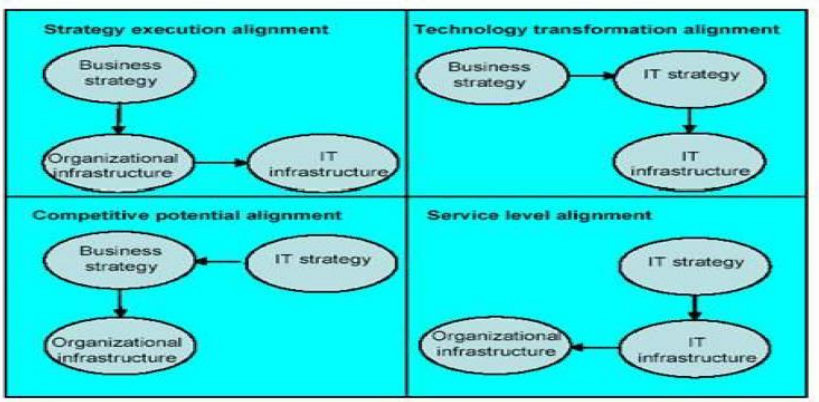
Strategic Fit dan Functional Integration

Tampak pada gambar 2, strategic alignment dibagi menjadi empat elemen: (a) business strategy, (b) IT strategy, (c) organizational infrastructure and process, (d) IS infrastructure and process. Elemen tersebut terdiri dari dua bagian, yaitu: bagian eksternal (business strategy dan IT strategy), dan bagian internal (organizational infrastructure and process, dan IS infrastructure and process). Keduanya harus diselaraskan dengan menggunakan: (a) strategic fit: bagaimana strategi IT harus dibahasakan dalam domain external (how the firm is positioned in the IT marketplace) dan domain internal (how IT infrastructure should be configered), dan (b) functional integration: bagaimana arah TI akan mempengaruhi arah bisnis (business domain).

Berdasarkan model yang dikenalkan oleh Henderson et al., selanjutnya Marques et al. dan Ekstedt et al. membuat strategic aligment model dan menetapkan empat bagian yang harus bersinergi untuk mencapai alignment: (i) business strategy, (ii) IT strategy, (iii) organizational infrastructure, dan (iv) theier interdependencies. Berdasarkan beberapa pendapat dan hasil penelitian tersebut, dapat disimpulkan bahwa IT business strategic alignment yang tepat, kredibilitas dan relevan dibangun dengan memperhatikan prioritas IT, anggaran, isu-isu bisnis

yang paling hangat dan menjadi perhatian organisasi dan pelanggan. Hal ini dapat diperoleh melalui diskusi dengan dengan stakeholder dan pelanggan bisnis untuk memahami apa yang penting baginya. Kebutuhan stakeholder tersebut selanjutnya diterjemahkan kedalam IT business strategic alignment yang mudah dipahami oleh para CEO dan pelanggan untuk memastikan bahwa IT dapat memberikan perannya secara optimal untuk memenuhi dan menjawab kebutuhan tersebut.

Salah satu contoh model alignment yang baik dikembangkan oleh Luftman. Penilaian keselarasan strategis Luftman's menyajikan sebuah pendekatan untuk menentukan alignment bisnis perusahaan IT berdasarkan enam variabel, yaitu: (i) keterampilan, (ii) teknologi ruang lingkup, (iii) kemitraan, (iv) tata kelola, (v) pengukuran kompetensi nilai, dan (iv) komunikasi. Model tambahan adalah model yang diajukan oleh Laagland et al. Model ini menetapkan bahwa arsitektur bisnis dan arsitektur IT harus terintegrasi untuk mendapatkan hasil yang total efektif dalam organisasi. Pada bagian lain Henderson dan Venkatraman dalam teorinya mengatakan ada empat model alignment IT business tersebut dapat dicapai Gambar 3.

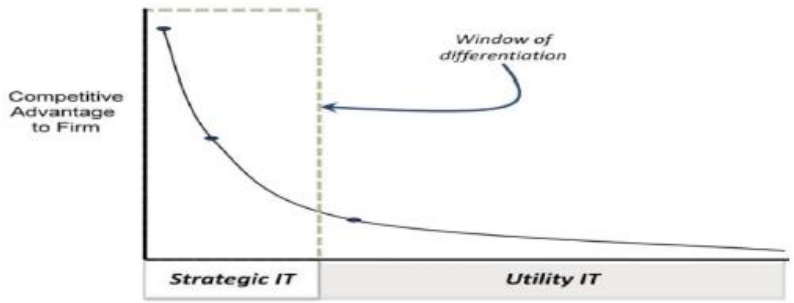


Gambar 3 Model Alignment IT Business

Berdasarkan Gambar 3, model alignment IT business dapat dicapai dengan cara: (1) Strategic execution alignment yaitu bersifat hirarkis dan paling umum,

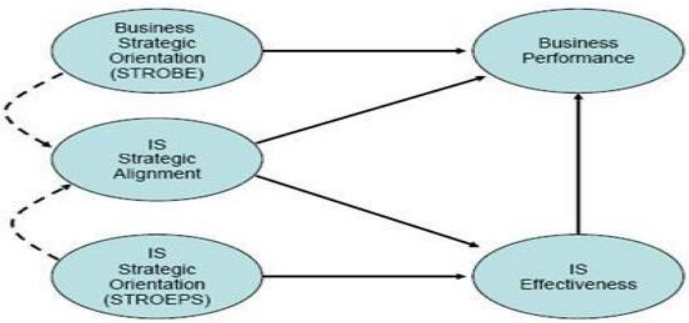
dimana strategi bisnis menentukan desain organisasi dan juga desain infrastruktur IT. Strategi ini merupakan yang paling banyak manfaatnya dalam penerapan strategic alignment. (2) Technoloy transparmation alignment yaitu dimulai dari strategi bisnis, tetapi fokus pada implementasi strategi IT yang tepat, kemudian pada infrastruktur dan proses. Strategi ini memfokuskan pada penerapan strategic agar hasil yang dicapai bisa maksimal. (3) Competitive potential alignment yaitu Paradigma ini memungkinkan adaptasi atau munculnya suatu strategi bisnis karena munculnya kapabilitas baru dari IT yang dapat mempengaruhi strategic alignment. (4) Service level prespektive yaitu cara pandang ini lebih berpikir pada bagaimana cara membuat unit/organisasi IT yang menyediakan layanan prima. Sehingga proses ini berjalan dengan baik pula sesuai dengan kebutuhan dan jenis oraganisasi yang di bentuk.

Terciptanya strategic alignment yang baik melalui penerapan salah satu model alignment tersebut di atas dapat meningkatkan peran IT dalam menciptakan peluang dan keunggulan kompetitif perusahaan. Hal ini diperkuat oleh kurva Chappell David seperti pada gambar 4, yang menggambarkan perbedaan peran strategic IT (bagian dari strategic alignment) dan utility IT dalam mendukung dan menciptakan peluang baru dan meningkatkan kemampuan kompetitif.



Gambar 4 Kurva peran strategic IT dan utility IT
dalam menciptakan peluang dan keunggulan kompetitif

Berdasarkan gambar 4, tampak bahwa strategic IT dapat mendukung penciptaan peluang baru dan meningkatkan keunggulan kompetitif lebih tinggi dibandingkan dengan utility IT tanpa strategic. Dengan demikian strategic alignment IT business sangat dibutuhkan oleh organisasi untuk mengoptimalkan peran IT dalam mencapai tujusan organisasi, menciptakan peluang dan meningkatkan kemampuan kompetitif. Sementara itu, agar *strategic aligment* yang sudah ditetapkan dapat berjalan sesuai dengan yang telah ditentukan diperlukan *assessment* (pemantauan) secara tertatur yang ditetapkan dalam bentuk *assessing strategic alignment.* Untuk maksud tersebut, terdapat beberapa teori yang berkaitan dengan pengaruh pencapaian bisnis dan kelelarasan IT bisnis. Hasil penelitian Smit Martin et al., telah meringkas teori utama dan mengembangkannya menjadi model riset untuk menilai hubungan antara penguasaan IT (pengambilan keputusan tentang IT), *alignment* antara kebutuhan *business* dan jasa IT/sistem informasi, kualitas informasi, dan kinerja *business process* pada suatu organisasi. Model *assessing strategic alignment* dibuat untuk menggambarkan efektivitas IT dan pencapaian bisnis.



Gambar 5 Kerangka keselarasan efektivitas
strategi sistem informasi terhadap capaian bisnis

Tampak pada gambar 5, strategic alignment digambarkan sebagai keselarasan antara orientasi bisnis unit yang strategis, orientasi sistem yang strategis, dan mengkalkulasi tigkat kelurusan strategis sistem yang digunakan perusahaan untuk mendukung orientasi strategis. Sehubungan dengan hal ini, Chan et al. dan Melville et al. telah melakukan pengujian dampak strategic alignment.

Hasilnya menyatakan bahwa dampak strategic aligment tidak boleh diarahkan kepada satu capaian tertentu, tetapi dipengaruhi dan ditengahi oleh faktor yang lain, seperti kelurusan antara strategy IT dan business strategy Model Chan et al. menilai capaian bisnis dan alignment sistem informasi yang strategis dengan menggunakan lima keselarasan yaitu: (i) orientsi strategis dari business enterprise, yaitu realized business strategy, (ii) performance bisnis, (iii) efektivitas IT atau sistem informasi, yaitu kontribusi IT terhadap bisnis dan nilai saat ini yang ditaksir dengan menentukan kepuasan bisnis, sistem informasi, pengelolaan, jasa, informasi produk, termasuk pengembangan kompetensi end user, (iv) orientasi strategis dari portopolio saat ini dari aplikasi sistem informasi, yaitu strategi sistem informasi yang direalisir, yang diperkirakan dengan menentukan sistem informasi yang mendukung bisnis internal, dan (v) strategic alignment sistem informasi, yaitu menghitung skor business strategic orientation dan information systems/IT strtagiec orientation.

BAB 9

Nilai Teknologi Informasi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- ❖ Menjelaskan tentang Pendekatan Audit Sistem Informasi
- ❖ Menjelaskan tentang Pemahaman Konsep Audit Sistem Informasi
- ❖ Menjelaskan tentang Tahapan Audit Sistem Informasi

A. Pendekatan Audit Sistem Informasi

Audit Sistem Informasi merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi harta milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien (Weber,1999). Mengacu pada pendapat Weber, R. (1999), audit dan sistem pengendalian menjadi semakin penting dalam sistem informasi berbasis komputerisasi, dengan alasan sebagai berikut :

(1) Besarnya biaya dan kerugian apabila data di dalam komputer hilang. (2) Biaya yang harus dibayar bila sampai mutu keputusan buruk akibat pengolahan data yang salah (informasi untuk bahan pengambilan keputusan salah). (3) Potensi kerugian kalau terjadi kesalahan/penyalahgunaan komputer. (4) Nilai (investasi) yang tinggi dalam pengadaan maupun perawatan mesin (hardware dan software). (5) Nilai atau biaya yang tinggi yang dikeluarkan untuk pendidikan personil. (6) Biaya yang tinggi bila terjadi computer errors. (7) Perlunya dijaga privacy, mengingat di komputer tersedia data rahasia. (8) Agar perkembangan dan pertumbuhan komputerisasi dapat terkendali (controlled evolution of computer used).

Audit Sistem Informasi sendiri merupakan gabungan dari berbagai macam ilmu, antara lain : Tradisional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer dan *Behavioral Science*.

Seorang Auditor Sistem Informasi, apabila telah memperoleh sertifikasi, maka akan mendapat gelar Certified Information System Auditor (CISA). Audit Sistem Informasi digolongkan menjadi tiga jenis, yaitu :

1. ***Auditing around the computer***. Auditor hanya membandingkan input dan output, tanpa menilai atau mengetahui proses komputer yang digunakan. Pendekatan ini merupakan pendekatan yang mula-mula ditempuh auditor. Asumsi yang digunakan dalam pendekatan ini adalah apabila contoh output dari suatu sistem adalah benar berdasarkan input, maka pemrosesannya tentu dapat diandalkan. Berdasarkan kualitas pemrosesan dan sistem aplikasi, pemrosesan sistem aplikasi tidak diperiksa secara langsung. Selain itu, auditor memandang komputer sebagai black box. Auditor menggunakan metode ini hanya untuk mendapatkan biaya murah.

   Keadaan dapat dipulihkan kembali jika sistem aplikasi mempunyai tiga karakteristik sebagai berikut :

   a. Sistem harus sederhana dan berorientasi pada sistem batch, Pada umumnya, sistem batch komputer merupakan suatu pengembangan langsung dari sistem manual. Sistem batch harus mempunyai kriteria sebagai berikut :
      1) Resiko yang ada harus rendah. Resiko ini tidak dapat dikelompokkan dengan subjek kesalahan material akibat ketidakberesan dan ketidakefisienan dalam beroperasi.
      2) Logika sistem harus tepat sasaran. Tidak ada rutinitas (kegiatan) yang dikembangkan untuk mengizinkan komputer untuk memproses data.
      3) Transaksi inout dilakukan dengan sistem batch dan kontrol diperlihara dengan metode tradisional.

4) Proses utama terdiri dari penyelesaian input data dan memperbaharui file master secara terus-menerus.
5) Adanya jejak audit (audit trail) yang jelas. Laporan terperinci dipersiapkan pada kunci pokok dalam sistem.
6) Jadwal pekerjaan relatif sangat stabil dan sistem jarang dimodifikasi.
7) Seringkali keefisienan biaya dalam metode Auditing Around the Computer pada saat aplikasi yang digunakan untuk keseragaman kemasan dalam program software.

b. Auditor harus menggunakan metode Auditing Around the Computer pada pengguna lebih tinggi daripada sistem kontrol komputer untuk menjaga perawatan keintegrasian data dan mencapai tujuan keefektifan dan keefisienan sistem. Biasanya metode Auditing Around the Computer adalah pendekatan yang sederhana yang berhubungan dengan audit dan dapat dipraktekan oleh auditor yang mempunyai pengetahuan teknik yang sedikit tentang komputer. Kelemahan yang ada pada pendekatan ini antara lain :
   1) Umumnya database mencakup jumlah data yang banyak dan sukar ditelusuri secara manual.
   2) Tidak memberikan ruang lingkup yang luas bagi auditor untuk menghayati dan mendalami keberadaan komputer
   3) Cara ini mengabaikan pengendalian sistem dalam pengolahan komputer itu sendiri sehingga rawan terhadap adanya kelemahan dan kesalahan yang terdapat di dalam komputer itu sendiri.
   4) Kemampuan komputer sebagai fasilitas penunjang pelaksaan audit menjadi sia-sia.
   5) Tidak dapat mencakup keseluruhan maksud dan tujuan penyelenggaraan audit.

c. Auditing with the computer. Dalam melaksanakan pemeriksaan auditor menggunakan bantuan komputer. Misalnya untuk melakukan analisa data dan mengecek kebenaran perhitungan, menggunakan bantuan audit software. Pendekatan ini merupakan cara audit yang sangat bermanfaat, khususnya dalam pengujian substantif atas file dan record perusahaan. Audit software yang digunakan merupakan program komputer yang membantu auditor untuk melakukan pengujian dan evaluasi kehandalan data, file dan record perusahaan . Bentuk yang lebih maju dalam metode ini adalah Generalized Audit Software yaitu program audit yang berlaku umum untuk klien. Keunggulan metode ini adalah :

   a. Merupakan program komputer yang diproses untuk membantu pengujian pengendalian sistem komputer klien itu sendiri.
   b. Dapat melaksanakan tugas audit yang terpisah dari catatan klien, yaitu dengan mengambil copy data atau file untuk dilakukan pengujian dengan komputer lain.

   Kelemahan metode ini adalah dibutuhkan upaya dan biaya yang relatif besar untuk pengembangannya.

d. Auditing through the computer. Auditor melakukan pengetesan data untuk diproses dan hasil proses tersebut kemudian dianalisa untuk membuktikan keandalan dan keakuratan program komputer tersebut. Dengan kata lain metode ini adalah pendekatan audit yang berorientasi pada komputer dengan membuka black box dan secara langsung berfokus pada operasi pemrosesan dalam sistem komputer. Dengan asumsi bahwa apabila pemrosesan mempunyai pengendalian yang memadai, maka kesalahan dan penyalahgunaan tidak akan terlewat untuk dideteksi, sebagai akibat dari keluaran yang dapat diterima. Keunggulan dari metode ini adalah :

   1) Dapat meningkatkan kekuatan terhadap pengujian sistem aplikasi secara efektif, dimana ruang lingkup dan kemampuan dari pengujian yang dilakukan dapat diperluas sehingga tingkat kepercayaan

terhadap keandalan dari pengumpulan dan pengevaluasian bukti dapat ditingkatkan.

2) Dengan memeriksa secara langsung, logika pemrosesan dari sistem aplikasi, dapat diperkirakan kemampuan sistem dalam menangani perubahan dan kemungkinan kehilangan yang terjadi pada masa yang akan datang.

Kelemahan dari metode ini adalah :

1) Biaya yang dibutuhkan relatif tinggi yang disebabkan jumlah jam kerja yang banyak untuk dapat lebih memahami struktur kontrol internal dari pelaksanaan sistem aplikasi.
2) Butuh banyak keahlian teknis yang lebih mendalam untuk memahami cara kerja sistem.

B. Pemahaman Konsep Audit Sistem Informasi

Penerapan komputerisasi dalam suatu organisasi untuk mengelola sumber daya dan dana, pencatatan, pengawasan dan pelaporan kegiatan serta laporan keuangan, akan membawa akibat terhadap prosedur dan teknik audit yang dilakukan oleh internal auditor maupun eksternal auditor.

Audit manual menekankan pentingnya evaluasi bukti pendukung yang dihasilkan oleh suatu system yaitu untuk mendukung pendapat auditor. Sedangkan audit komputer lebih menekankan pada keandalan pengendlian di lingkungan Pengolahan Data Elektronik. Pada kondisi inilah Auditor Sistem Informasi (Information System Auditor = IS Auditor) diperlukan untuk membantu eksternal auditor dan internal auditor dalam melaksanakan pemeriksaan.

IS Auditor akan melaksanakan evaluasi dan testing terhadap pengendalian dan prosedur yang berlaku serta menerapkan dan mengembangkan teknik-teknik audit komputer termasuk pengembangan audit software.

Seorang auditor di bidang Sistem Informasi harus mengetahui dan memahami konsep teknologi informasi seperti :

1. Sistem Informasi dan Organisasi dari Sistem Informasi Manajemen.
2. Konsep computer.
3. Pengetahuan di bidang komputer (hardware dan software).
4. Sistem dan jaringan telekomunikasi
5. Kemampuan untuk mengidentifikasi resiko baru dan pengendalian yang diperlukan dalam lingkungan bisnis yang berbasis computer.
6. Pengetahuan tentang bagaimana menggunakan komputer untuk mengaudit komputer.
7. Untuk memperoleh tenaga IS Auditor dapat dilakukan dengan beberapa cara :
   a. Mendidik personil yang memiliki latar belakang akunting/auditing untuk memahami konsep dasar prinsip data processing, struktur sistem komputer, prosedur dan pengendalian sistem aplikasi komputer manajemen data, pengendalian operasi komputer serta pengendalian terhadap pengembangan suatu sistem.
   b. Mendidik personil yang memiliki latar belakang EDP untuk memahami masalah auditing, khususnya yang berkaitan dengan masalah kontrol atau pengendalian internal.

C. Tahapan Audit Sistem Informasi

Lima Untuk melaksanakan audit sistem informasi, ada beberapa tahapan yang perlu dilakukan. Tahapan-tahapan tersebut ialah :

1. Planning the Audit

   Perencanaan merupakan tahap pertama dari kegiatan audit. Bagi eksternal auditor hal ini artinya adalah melakukan investigasi terhadap klien untuk mengetahui :
   a. Apakah pekerjaan mengaudit dapat diterima.
   b. Staff yang akan ditempatkan untuk melaksanakan audit.
   c. Membuat perjanjian perjanjian audit.
   d. Menghasilkan informasi latar belakang klien.
   e. Mengerti tentang masalah hukum klien.

f. Melakukan analisa terhadap prosedur yang ada untuk mengerti tentang bisnis klien
g. Mengidentifikasi resiko audit.

2. Test of Control

   Auditor melakukan Test of Control ketika menilai bahwa resiko terhadap control (pengedalian) berada pada level kurang dari maksimum, mereka mengandalkan control sebagai dasar untuk mengurangi biaya testing. Sampai pada tahap ini auditor tidak mengetahui apakah identifikasi control telah berjalan dengan efektif, test of control memerlukan evaluasi yang lebih spesifik terhadap materi control.

3. Test of Transaction

   Auditor melakukan test (pengujian) terhadap transaksi untuk mengevaluasi Apakah kesalahan atau proses yang tidak biasa terjadi pada transaksi yang mengakibatkan kesalahan pencatatan yang material pada laporan keuangan. Pengujian terhadap transaksi ini termasuk menelusuri jurnal dari sumber dokumen, memeriksa file berharga dan mengecek keakuratan perhitungan. Pemakaian komputer sangat membantu pekerjaan ini dan auditor harus menggunakan software audit umum untuk mengecek apakah bunga yang dibayar kepada bank telah sesuai perhitungannya.

4. Test of Balances or Overall Result

   Untuk mengetahui pendekatan yang digunakan pada tahap ini, yang harus diperhatikan adalah tujuan pengamanan harta dan data integrity. Beberapa jenis substantive test terhadap saldo yang digunakan adalah konfirmasi piutang, perhitungan fisik persediaan dan perhitungan ulang penyusutan aktiva tetap.

5. Completion of The Audit

   Pada tahap ini, auditor harus merumuskan pendapat tentang kehilangan material dan keabsahan pernyataan laporan muncul dan memuat sebuah laporan. Jenis-jenis pendapat auditor yaitu :

a. *Disclaimer of Opinion* (Tidak Memberikan Pendapat)
   Setelah melakukan audit, auditor tidak dapat memberikan opini
b. *Adverse Opnion* (Pendapat Tidak Wajar)
   Auditor menyimpulkan bahwa kehilangan material telah muncul atau laporan keuangan telah dinyatakan salah secara material.
c. Q*ualified Opinion* (Wajar Dengan Pengecualian)
   Auditor menyimpulkan bahwa kehilangan telah muncul / kesalahan laporan secara\material.
d. *Unqualified Opinion* (Wajar Tanpa Pengecualian)
   Auditor percaya bahwa tidak ada kehilangan material / laporan yang salah.

BAB 10

Tata Kelola Teknologi Informasi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- Menjelaskan tentang Pentingnya Tata Kelola Teknologi Informasi
- Menjelaskan tentang Pengertian Tata Kelola Teknologi Informasi
- Menjelaskan tentang Tanggung Jawab Tata Kelola Teknologi Informasi
- Menjelaskan tentang Kerangka Kerja Tata Kelola Teknologi Informasi
- Menjelaskan tentang Manfaat Tata Kelola Teknologi Informasi
- Menjelaskan tentang Model Tata Kelola Teknologi Informasi

A. Pentingnya Tata Kelola Teknologi Informasi

Di lingkungan yang sudah memanfaatkan teknologi informasi, tata kelola TI menjadi hal penting yang harus diperhatikan. Hal ini dikarenakan ekspektasi dan realitas seringkali tidak sesuai. Pihak shareholder perusahaan selalu berharap agar perusahaan dapat :

1. Memberikan solusi teknologi informasi dengan kualitas yang bagus, tepat waktu dan sesuai dengan anggaran
2. Menguasai dan menggunakan teknologi informasi untuk mendatangkan keuntungan
3. Menerapkan teknologi informasi untuk meningkatkan efisiensi dan produktivitas sambil menangani risiko teknologi informasi.

Tata kelola teknologi informasi yang dilakukan secara tidak efektif akan menjadi awal terjadinya pengalaman buruk yang dihadapi perusahaan, yang memicu munculnya fenomena investasi teknologi informasi yang tidak diharapkan, seperti :

1. Kerugian bisnis, berkurangnya reputasi, dan melemahnya posisi kompetensi.
2. Tenggang waktu yang terlampaui, biaya lebih tinggi dari yang diperkirakan, dan kualitas lebih rendah dari yang diantisipasi.
3. Efisiensi dan proses inti perusahaan terpengaruh secara negatif oleh rendahnya kualitas penggunaan teknologi informasi

Kegagalan dari inisiatif teknologi informasi untuk melahirkan inovasi atau memberikan keuntungan yang dijanjikan.

B. Pengertian Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi adalah struktur kebijakan dan prosedur atau kumpulan proses yang bertujuan untuk memastikan kesesuaian penerapan teknologi informasi dengan dukungannya terhadap pencapaian tujuan institusi, dengan cara mengoptimalkan keuntungan dan kesempatan yang ditawarkan teknologi informasi, mengendalikan penggunaan terhadap sumber daya teknologi informasi dan mengelola risiko-risiko terkait teknologi informasi.

Menurut *IT Governance Institute* (ITGI) Tata kelola TI merupakan tanggung jawab dari pimpinan puncak Dan eksekutif manajemen dari suatu perusahaan. Dijelaskan pula bahwa Tata kelola TI merupakan bagian dari pengelolaan perusahaan secara keseluruhan yang terdiri dari kepemimpinan dan struktur organisasi dari proses yang ada adalah untuk memastikan kelanjutan TI organisasi dan pengembangan strategi dan tujuan organisasi.

Tata kelola TI yang bersifat sentralisasi diasosiasikan dengan organisasi berskala kecil dengan strategi busnis yang berorientasi pada biaya dan di cirikan oleh struktur data dan kelola bisnis, stabilitas lingkungan, profuk/layanan bisni dengan intensif informasi intensif yang rendah serta pengalaman bisnis dan kompetensi pengelolaan teknologi informasi yang masih rendah

Tata kelola TI yang bersifat terdesentralisasi diasosiasikan dengan organisasi besar dengan strategi bisnis yang berfokus pada inovasi, dicirikan oleh struktur tat kelola bisnis terdesentralisasi, lingkungan yang cenderung berubah, produk dan proses bisnis dengan intensif informasi yang tinggi serta pengalaman bisnis dan kompetensi pengelolaan TI yang tinggi. Ciri fleksibilitas menurut (D'Aveni,1999; El Sawy,dkk1999)

- Penekanan waktu dan biaya dalam iklus hidup produk dan desain.
- Mempercepat kemajuan teknologi
- Kesetiaan konsumen yang brubah-ubah
- Produk layanan yang dikhususkan, bersifat intensif terhadap pengetahuan
- Masuknya kompetitor baru yang tidak terduga,reposisi pejabat
- Pendefisian kembali batasan-batasan industri dan organisasi
- Volatilitas pasar global

Berdasarkan definisi tata kelola teknologi informasi dari *IT Governance Institute* (ITGI) dikemukakan bahwa tata kelola teknologi informasi adalah tanggung jawab dari dewan direksi dan manajemen eksekutif, oleh karenanya tata kelola teknologi informasi harus merupakan bagian yang tidak terpisahkan dari tata kelola perusahaan. Tata kelola perusahaan merupakan suatu sistem yang mengarahkan dan mengendalikan entitas-entitas pada suatu perusahaan. Ketergantungan bisnis akan suatu teknologi informasi telah membuatnya tidak dapat menyelesaikan isu tata kelola perusahaan tanpa adanya pertimbangan terhadap teknologi informasi. Sebagai gantinya teknologi informasi dapat mempengaruhi peluang strategi dan menghasilkan kritik atas perencanaan strategis yang telah dibuat. Dalam hal tersebut tata kelola teknologi informasi memungkinkan perusahaan untuk mengambil keuntungan maksimal atas informasi, dan juga merupakan penggerak tata kelola perusahaan. Hubungan antara tata kelola teknologi informasi dengan tata kelola perusahaan dapat dilihat pada gambar 6 dibawah ini:

Gambar 6
Hubungan Tata Kelola TI dan Tata Kelola Perusahaan

C. Tanggung Jawab Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi bukan bidang yang terpisah dari pengelolaan perusahaan, melainkan merupakan komponen pengelolaan perusahaan secara keseluruhan, dengan tanggung jawab utama sebagai berikut :

1. Memastikan kepentingan stakeholder diikutsertakan dalam penyusunan strategi perusahaan
2. Memberikan arahan kepada proses-proses yang menerapkan strategi perusahaan.
3. Memastikan proses-proses tersebut menghasilkan keluaran yang terukur
4. Memastikan adanya informasi mengenai hasil yang diperoleh dan mengukurnya
5. Memastikan keluaran yang dihasilkan sesuai dengan yang diharapkan.

D. Kerangka Kerja Tata Kelola Teknologi Informasi

Peran dan fungsi utama dalam Tata Kelola TI mencakup dua hal utama, yaitu : pengaturan (govern) dan pengelolaan (manage). Pengaturan (govern) mencakup hal – hal apa yang mendasari tata kelola tersebut yang ditentukan melalui pendefinisian strategi dan kontrol. Contoh kerangka kerja yang masuk dalam

cakupan ini adalah COBIT. Adapun bagaimana tata kelola tersebut dilaksanankan merupakan cakupan dari pengelolaan (manage) yang ditentukan melalui rencana taktis dan eksekusi. Lebih jauh lagi, strategi dan kontrol yang masuk dalam cakupan pengaturan dipenuhi dengan penentuan kebijakan dan standar TI. Kebijakan tersebut merupakan pernyataan level tertinggi dan dapat digunakan sebagai acuan umum jika standar tidak tersedia. Standar sendiri ditentukan mengacu pada kebijakan dan menyediakan kriteria yang dapat digunakan untuk mengukur keakurasian dan efektivitas prosedur (mekanisme dilakukan sesuai dengan aturan yang ditetapkan).

E. Manfaat Tata Kelola Teknologi Informasi

Manfaat tata kelola teknologi informasi antara lain :

1. Untuk mengatur penggunaan teknologi informasi
2. Memastikan kinerja teknologi informasi sesuai dengan tujuan / fokus utama area tata kelola teknologi informasi.

F. Model Tata Kelola Teknologi Informasi

Beberapa model tata kelola teknologi informasi antara lain :

1. The Information Technology Infrastructure Library (ITIL)
   ITIL dikembangkan oleh The Office of Government Commerce (OGC) suatu badan dibawah pemerintah Inggris, dengan bekerja sama dengan The IT Service Management Forum (ITSMF) dan British Standard Institute (BSI). ITIL merupakan suatu framework pengelolaan layanan teknologi informasi (IT Service Management – ITSM) yang sudah diadopsi sebagai standar industri pengembangan perangkat lunak di dunia. ITSM memfokuskan diri pada 3 tujuan utama yaitu :
   a. Menyelaraskan layanan teknologi informasi dengan kebutuhan sekarang dan akan datang dari bisnis dan pelanggannya.
   b. Memperbaiki kualitas layanan-layanan teknologi informasi

c. Mengurangi biaya jangka panjang dari pengelolaan layanan-layanan tersebut.

Standar ITIL berfokus kepada pelayanan customer dan sama sekali tidak menyertakan proses penyelarasan startegi perusahaan terhadap strategi IT yang dikembangkan.

2. ISO / IEC 17789

   ISO / IEC 17789 dikembangkan oleh The International Organization for Standardization (ISO) dan The International Electrotechnical Comission (IEC) 17789 bertujuan memperkuat 3 elemen dasar keamanan informasi yaitu :

   a. Confidentialy – memastikan bahwa informasi hanya dapat diakses oleh yang berhak
   b. Integrity – menjaga akurasi dan selesainya informasi dan metode pemrosesan
   c. Availability – memastikan bahwa user yang terautorisasi mendapatkan akses kepada informasi dan aset yang terhubung dengannya ketika memerlukannya.

3. COSO

   COSO merupakan kependekan dari Commitee of Sponsoring Organization of The Treadway Comission, sebuah organisasi di Amerika yang berdedikasi dalam meningkatkan kualitas pelaporan finansial mencakup etika bisnis, kontrol internal dan corporate governance.

   COSO terdiri dari 3 dimensi yaitu :

   a. Komponen kontrol COSO. COSO mengidentifikasi 5 komponen kontrol yang diintegrasikan dan dijalankan dalam semua unit bisnis dan akan membantu mencapai sasaran kontrol internal, meliputi : monitoring, information and communication, control activities, risk asessment dan control environment.

b. Sasaran kontrol internal. Sasaran kontrol internal dikategorikan menjadi beberapa area sebagai berikut :
   1) Operations – efisiensi dan efektivitas operasi dalam mencapai sasaran bisnis yang juga meliputi tujuan kinerja dan keuntungan
   2) Financial reporting – persiapan pelaporan anggaran finansial yang dapat dipercaya
   3) Compliance – pemenuhan hukum dan aturan yang dapat dipercaya

c. Unit / Aktivitas terhadap organisasi. Dimensi ini mengidentifikasi unit / aktivitas pada organisasi yang menghubungkan kontrol internal. Kontrol internal menyangkut keseluruhan organisasi dan semua bagian-bagiannya. Kontrol internal seharusnya diimplementasikan terhadap unit-unit dan aktivitas organisasi.

4. COBIT (Control Objective for Information and Related Technology)

   COBIT framework dikembangkan oleh IT Governance Institute, sebuah organisasi yang melakukan studi tentang model pengelolaan IT yang berbasis di Amerika Serikat. COBIT Framework terdiri atas 4 domain utama :

   a. Domain perencanaan dan Pengorganisasian (*Planning and Organization*), domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi teknologi informasi dengan strategi perusahaan. Terdapat 11 proses tata kelola teknologi informasi yang harus diperhatikan oleh perusahaan, masing-masing adalah :

      PO1. Menyusun Rencana Strategis Teknologi Informasi
      PO2. Mendefinisikan Arsitektur Informasi Korporat
      PO3. Menentukan Arah Perkembangan Teknologi
      PO4. Merancang Struktur Organisasi Teknologi Informasi
      PO5. Mempertimbangkan Investasi Teknologi Informasi
      PO6. Mengkomunikasikan Arah dan Sasaran Manajemen
      PO7. Mengembangkan Sumber Daya Manusia

PO8. Menjamin Pemenuhan Standar Eksternal
PO9. Mengkaji Resiko
PO10. Mengelola Proyek Teknologi Informasi
PO11. Memelihara Kualitas

b. Domain Pengadaan dan Penerapan (*Acquisition and Implementation*), domain ini menitikberatkan pada proses pemilihan, pengadaan dan penerapan teknologi informasi yang digunakan.
Terdapat 6 (enam) proses tata kelola teknologi informasi yang harus diperhatikan oleh perusahaan, masing-masing adalah sebagai berikut:
DS1. Mengidentifikasikan Solusi bagi Perusahaan
DS2. Mengadakan dan Memelihara Perangkat Lunak Aplikasi
DS3. Membangun dan Mengembangkan Infrastruktur Teknologi
DS4. Menyusun Prosedur Kerja dan Pemeliharaan
DS5. Mengakreditasi Sistem
DS6. Mengelola Perubahan

c. Domain Pemanfaatan dan Pemeliharaan (*Delivery and Support*), domain ini menitikberatkan pada proses pelayanan teknologi informasi dan dukungan teknisnya.
Terdapat 13 (tiga belas) proses tata kelola teknologi informasi yang harus diperhatikan oleh perusahaan, masing-masing adalah sebagai berikut:
DS1. Menentukan Standar Kepuasan
DS2. Memonitor Keterlibatan Pihak Ketiga
DS3. Menjaga Kinerja dan Kapasitas
DS4. Menjamin Pelayanan yang Berkesinambungan
DS5. Mengelola Sistem Keamanan
DS6. Mengidentifikasikan dan Mengalokasikan Biaya
DS7. Mendidik dan Melatih Pengguna
DS8. Membantu Pelanggan Sistem
DS9. Memantau Konfigurasi

DS10. Mengatasi Keluhan dan Masalah
DS11. Mengelola Data
DS12. Mengelola Fasilitas
DS13. Mengelola Operasi

d. Domain Pengawasan dan Penilaian (*Monitoring and Evaluation*), domain ini menitikberatkan pada proses pengawasan pengelolaan teknologi informasi pada organisasi.
   Terdapat 4 (empat) proses tata kelola teknologi informasi yang harus diperhatikan oleh perusahaan, masing-masing adalah sebagai berikut:
   M1. Memantau Keseluruhan Proses
   M2. Mengkaji Ketersediaan Kontrol Internal
   M3. Menyediakan Penjamin Independen
   M4. Mempersiapkan Tim Audit Independen

COBIT mempunyai model kematangan (maturity model) untuk mengontrol proses-proses teknologi informasi dengan menggunakan metode penilaian (scoring) sehingga suatu organisasi dapat menilai proses-proses teknologi informasi yang dimilikinya dari skala non exist (skor 0) sampai dengan optimised (skor 5). COBIT juga mempunyai ukuran-ukuran lainnya sebagai berikut :

1. Critical Success Factors (CSF) adalah hal-hal atau kegiatan penting yang dapat digunakan manajemen untuk dapat mengontrol proses-proses teknologi informasi di organisasinya.
2. Key Goal Indicators (KGI) adalah ukuran-ukuran yang akan memberikan gambaran kepada manajemen apakah proses-proses teknologi informasi yang ada telah memenuhi kebutuhan proses bisnis yang ada. KGI biasanya berbentuk kriteria informasi :
   a. Ketersediaan informasi yang diperlukan dalam mendukung kebutuhan bisnis
   b. Tidak adanya risiko integritas dan kerahasiaan data

c. Efisiensi biaya dari proses dan operasi yang dilakukan
d. Konfirmasi reliabilitas, efektivitas dan compliance

3. Key Performance Indicators (KPI) adalah ukuran-ukuran untuk menentukan kinerja proses-proses teknologi informasi dilakukan untuk mewujudkan tujuan yang telah ditentukan. KPI biasanya berupa indikator kapabilitas, pelaksanaan dan kemampuan sumber daya teknologi informasi.

BAB 11

Implementasi Tata Kelola Teknologi Informasi

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

- ❖ Menjelaskan tentang Implementasi IT Governance
- ❖ Menjelaskan tentang Perbandingan Implementasi IT Governance

A. Implementasi IT Governance

Persaingan bisnis yang semakin ketat menimbulkan kebutuhan akan penyusunan strategi bisnis yang handal. Menyusun suatu strategi yang membuat organisasi tersebut tidak hanya dapat bertahan, namun memiliki keunggulan yang kompetitif. Tujuan dari strategi bisnis adalah membuat keselarasan bekerja dari top level manajemen hingga ke bagian bawah yaitu pelaksana. Semua komponen dari organisasi dapat menjalankan tugas sesuai dengan tujuan organisasi yang telah dirumuskan dalam strategi bisnis. Seiring dengan perkembangan zaman, dunia bisnis saat ini tidak dapat dipisahkan lagi dari teknologi informasi (TI).

TI tidak lagi dipandang hanya sebagai pendukung, akan tetapi TI telah dianggap bagian strategi bisnis, termasuk antara lain: Menjadi garis depan layanan bagi konsumen atau masyarakat; Pengintegrasian proses-proses bisnis organisasi; Kunci penghematan biaya operasional organisasi; dan lain sebagainya. Bahkan dampak berkembang-pesatnya TI, berpotensi mentrasformasikan bisnis atau melahirkan sektor industri baru. Meskipun demikian, besarnya investasi di bidang TI seringkali tidak diimbangi dengan manfaat yang dapat diperoleh. Banyak sekali

proyek-proyek TI justru menghambur-hamburkan uang tanpa menghasilkan value-added yang dicita-citakan.

Definisi umum dari Tata Kelola TI adalah pertanggung-jawaban eksekutif dan direksi yang melibatkan kepemimpinan, struktur organisasi, dan proses - dalam memastikan bahwa TI menjadi pendukung dan bagian dari realisasi strategi serta pencapaian tujuan organisasi. Terdapat lima bidang utama dalam Tata Kelola TI, yaitu:

1. *Stategic Aligment* : Keharmonisan antara TI dengan bisnis.
2. *Value Delivery*: Memastikan pemanfaatan penerapan TI.
3. *Risk Management*: Pengelolaan resiko penerapan TI dan pemanfaatan TI untuk mengendalikan resiko bisnis.
4. *Resource Management*: Pengelolaan kemampuan organisasi untuk menerapkan TI.
5. *Performance Measurement*: Pemantauan kinerja layanan TI.

Bidang-bidang Tata Kelola TI di atas dilaksanakan secara berkesinambungan dengan melibatkan review dan evaluasi secara periodik. Selanjutnya bagaimana caranya untuk memulai implementasi Tata Kelola TI. Berikut ini proses-proses yang dapat dilakukan untuk menjadikan organisasi meraih Good IT Governance. IT Governance yang tidak efektif akan menjadi awal terjadinya pengalaman buruk yang dihadapi perusahaan seperti (1) Kerugian bisnis, berkurangnya reputasi dan melemahnya posisi kompetisi; (2) Tenggang waktu yang terlampaui, biaya lebih tinggi dari yang diperkirakan, dan kualitas lebih rendah dari yang telah diantisipasi; (3) Efisiensi dan proses inti perusahaan terpengaruh secara negatif oleh rendahnya kualitas penggunaan TI; (4) Kegagalan inisiatif TI untuk melahirkan inovasi atau memberikan keuntungan yang dijanjikan; (5) Penggunaan standar IT Governance mempunyai keuntungan-keuntungan sebagai berikut.

Pertama, The Wheel Exists, penggunaan standar yang sudah ada dan *mature* akan sangat efisien. Perusahaan tidak perlu mengembangkan sendiri *framework* dengan mengandalkan pengalamannya sendiri yang tentunya sangat terbatas.

Kedua, *Structured*, standar-standar yang baik menyediakan suatu *framework* yang sangat terstruktur, yang dapat dengan mudah dipahami dan diikuti oleh manajemen. Lebih lanjut lagi, *framework* yang terstruktur dengan baik akan memberikan setiap orang pandangan yang relatif sama. *Ketiga*, *Best Practices*, standar-standar tersebut telah dikembangkan dalam jangka waktu yang relatif lama dan melibatkan ratusan orang dan organisasi di seluruh dunia. Pengalaman yang direfleksikan dalam model-model pengelolaan yang ada tidak dapat dibandingkan dengan suatu usaha dari satu perusahaan tertentu. *Keempat*, *Knowledge Sharing*, dengan mengikuti standar yang umum, manajemen akan dapat berbagi ide dan pengalaman antar organisasi melalui *user groups*, *website*, majalah, buku, dan media informasi lainnya. *Kelima*, *Auditable*, tanpa standar baku, akan sangat sulit bagi auditor, terutama auditor dari pihak ketiga untuk melakukan kontrol secara efektif. Dengan adanya standar, maka baik manajemen maupun auditor mempunyai dasar yang sama dalam melakukan pengelolaan TI dan pengukurannya.

Ada berbagai standar model *IT Governance* yang banyak digunakan saat ini, antara lain :

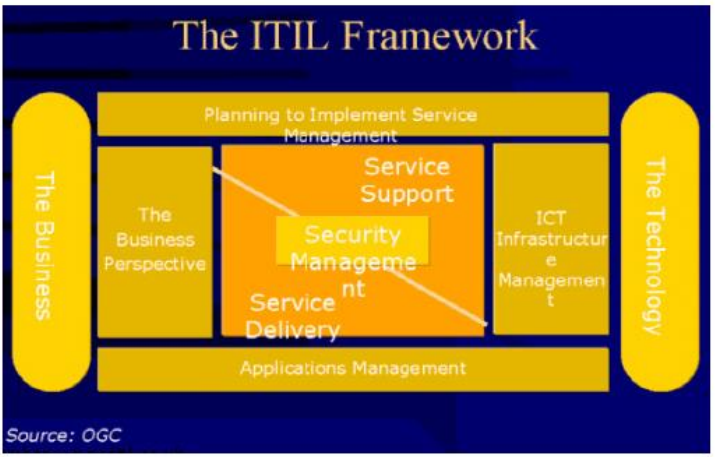
1. ITIL (The IT Infrastructure Library)

   ITIL dikembangkan oleh *The Office of Government Commerce* (OGC), yaitu suatu badan di bawah pemerintah Inggris, yang bekerja sama dengan *The IT Service Management Forum* (ITSMF), suatu organisasi independen mengenai manajemen pelayanan TI dan *British Standard Institute* (BSI), suatu badan penetapan standar pemerintah Inggris. ITIL merupakan suatu *framework* pengelolaan layanan TI (*IT Service Management – ITSM*), yang sudah diadopsi sebagai standar industri pengembangan industri perangkat lunak di dunia. ITIL dikembangkan pertama kali pada pada akhir tahun 1980.

   IT Infrastructure Library (ITIL) adalah serangkaian dokumen yang digunakan untuk membantu implementasi dari sebuah kerangka kerja untuk pengelolaan layanan teknologi informasi (ITSM, *IT Service*

Management). Kerangka kerja ini mendefinisikan bagaimana pengelolaan layanan yang terintegrasi, berbasiskan proses, dan praktik-praktik terbaik yang diterapkan di dalam organisasi. Awalnya diharapkan untuk memperbaiki pengelolaan layanan TI di pemerintahan Inggris. Namun, karena merupakan sebuah kerangka kerja, maka penerapannya tetap relevan untuk segala jenis bisnis atau organisasi yang memiliki ketergantungan pada infrastruktur TI.

epartemen internal dan berisi sebuah infrastruktur TI. Infrastruktur TI ini adalah sebuah bentuk untuk mendeskripsikan perangkat keras, perangkat lunak, prosedur, komunikasi yang berhubungan dengan komputer, dokumentasi dan keahlian yang diperlukan untuk mendukung layanan TI. Komponen-komponen ini beserta penggunaanya harus dikelola sehingga muncul istilah pengelolaan infrastruktur TI. Secara keseluruhan, layanan TI dan pengelolaan infrastruktur TI dinyatakan sebagai pengelolaan layanan TI. Fokus utama dalam pengelolaan layanan TI (ISTM) pada umumnya dibagi ke dalam 2 area, yaitu dukungan layanan dan penghantaran layanan. Secara bersamaan, kedua area ini merupakan disiplin yang menyediakan dan mengelola layanan TI yang efektif. Framework ITIL untuk menjembatani antara scope bisnis dengan scope teknologi dengan membagi 7 set fokus sebagaimana digambarkan dalam Gambar 7 berikut ini.



Gambar 7
Tujuh Set yang Menjadi Fokus dalam ITIL

Penjelasan dari 7 set yang menjadi fokus dalam ITIL adalah sebagai berikut. Pertama, dukungan layanan; menggambarkan komponen-komponen yang berkaitan dengan penyediaan stabilitas dan fleksibilitas untuk layanan TI. Topik ini berhubungan dengan identifikasi dan merekam konfigurasi TI seperti barang, kejadian, masalah, dan perubahan. Topik ini melingkupi meja layanan, pengelolaan kejadian, pengelolaan masalah, pengelolaan perubahan, pengelolaan rilis, dan pengelolaan konfigurasi. Kedua, penghantaran layanan; mendeskripsikan proses yang dibutuhkan untuk menghantarkan layanan TI yang berkualitas dan efektif secara biaya, yang melingkupi pengelolaan ketersediaan, pengelolaan kapasitas, pengelolaan keberlangsungan layanan TI, pengelolaan tingkat layanan, dan pengelolaan keuangan untuk layanan TI. Ketiga, pengelolaan keamanan; melingkupi keamanan dari penyedia layanan dan mengidentifikasi bagaimana pengelolaan keamanan berhubungan dengan petugas keamanan TI. Keempat, perspektif bisnis; melingkupi isu-isu yang berkaitan dengan TI yang

harus dihadapi oleh para manajer bisnis. Kelima, pengelolaan infrastruktur ICT; melingkupi pengelolaan layanan jaringan, pengelolaan operasi, pengelolaan pemroses lokal, instalasi komputer dan penerimaan, dan pengelolaan system. Keenam, pengelolaan aplikasi; melingkupi dukungan siklus hidup PL, pengujian dari layanan TI dan perubahan bisnis dengan penekanan pada kebutuhan yang jelas, definisi dan implementasi dari solusi untuk memenuhi kebutuhan bisnis pengguna. Ketujuh, perencanaan untuk mengimplementasikan pengelolaan layanan; melingkupi cara bagaimana memulai ITIL dalam organisasi dan membantu organisasi dalam mengidentifikasi kekuatan dan kelemahannya.

ITSM memfokuskan diri pada 3 tujuan utama, yaitu (1) Menyelaraskan layanan TI dengan kebutuhan sekarang dan akan datang dari bisnis dan pelanggannya; (2) Memperbaiki kualitas layanan-layanan TI; dan (3) Mengurangi biaya jangka panjang dari pengelolaan layanan-layanan tersebut. Standar ITIL berfokus kepada pelayanan customer dan sama sekali tidak menyertakan proses penyelarasan strategi perusahaan terhadap strategi yang dikembangkan.

2. ISO/IEC 17799 (The International Organization for Standardization/The International Electrotechnical Commission),

   ISO/IEC 17799 dikembangkan oleh The International Organization for Standardization (ISO) dan The International Electrotechnical Commission (IEC), dengan titel ”Information Technology - Code of Practice for Information Security bulan desember 2000.

   ISO/IEC 1799 bertujuan memperkuat 3 elemen dasar keamanan informasi, yaitu (1) *Confidentiality*, memastikan bahwa informasi hanya dapat diakses oleh yang berhak; (2) *Integrity*, menjaga akurasi dan selesainya informasi dan metode pemrosesan; serta (3) *Availability*, memastikan bahwa *user* yang terotorisasi mendapatkan akses kepada informasi dan aset yang terhubung dengannya ketika memerlukannya.

ISO/IEC 17799 terdiri dari 10 domain, yaitu (1) *Security policy*, memberikan panduan dan masukan pengelolaan dalam meningkatkan keamanan informasi; (2) *Organizational security*, memfasilitasi pengelolaan keamanan informasi dalam organisasi; (3) *Asset classification and control*, melakukan inventarisasi aset dan melindungi aset tersebut dengan efektif; (4) *Personnel security*, meminimalisasi resiko *human error*, pencurian, pemalsuan atau penggunaan peralatan yang tidak selayaknya; (5) *Physical and environmental security*, menghindarkan *violation*, *deterioration* atau *disruption* dari data yang dimiliki; (6) *Communications and operations management*, memastikan penggunaan yang baik dan selayaknya dari alat-alat pemroses informasi; (7) *Access control*, mengontrol akses informasi; (8) *Systems development and maintenance*, memastikan bahwa keamanan telah terintegrasi dalam sistem informasi yang ada; (9) *Business continuity management*, meminimalkan dampak dari terhentinya proses bisnis dan melindungi proses-proses perusahaan yang mendasar dari kegagalan dan kerusakan yang besar; serta (10) *Compliance*, menghindarkan terjadinya tindakan pelanggaran atas hukum, kesepakatan atau kontrak, dan kebutuhan keamanan.

3. COSO (Committee of Sponsoring Organization of the Treadway Commission),

   COSO merupakan kependekan dari Committee of Sponsoring Organization of the Treadway Commission, sebuah organisasi di Amerika yang berdedikasi dalam meningkatkan kualitas pelaporan finansial mencakup etika bisnis, kontrol internal dan corporate governance. Komite ini didirikan pada tahun 1985 untuk mempelajari faktor-faktor yang menunjukkan ketidaksesuaian dalam laporan finansial.

   Pada awal tahun 90-an, PricewaterhouseCouper bersama komite ini melakukan extensive study mengenai kontrol internal, yang menghasilkan COSO Framework yang digunakan untuk mengevaluasi

efektifitas kontrol internal suatu perusahaan. Sejak itu, komunitas finansial global, termasuk badan-badan regulator seperti public accounting dan internal audit professions, telah mengadopsi COSO. Hal ini juga bernilai untuk perusahaan manapun yang ingin memastikan sistem kontrol internalnya dengan menggunakan standar internasional.

Keuntungan implementasi COSO *framework* akan didapat oleh (1) CEO/CFO perusahaan Australia yang menerapkan SEC dan mereka yang memerlukan standar Sarbanes-Oxley test section 302 dan 404; (2) CEO/CFO perusahaan Australia yang menjadi bagian SEC dan mungkin memerlukan layanan kantor pusat untuk beberapa tes; (3) Manajer kunci (biasanya dalan keuangan) dan auditor internal yang bekerja untuk organisasi di atasnya dan memerlukan bantuan informasi dari CEO/CFO, agar mereka dapat menerapkan standar Sarbanes-Oxley; dan (4) Manajer senior yang memerlukan kepastian organisasi, apakah telah memiliki sistem kontrol internal untuk menyediakan kemampuan memasarkan dan meningkatkan harga saham.

Kerangka kerja COSO terdiri atas 3 dimensi. Pertama, komponen kontrol COSO. COSO mengidentifikasi 5 komponen kontrol yang diintegrasikan dan dijalankan dalam semua unit bisnis, dan akan membantu mencapai sasaran kontrol internal, yakni monitoring, information and communications, control activities, risk assessment, dan control environment. Kedua, sasaran kontrol internal. Sasaran kontrol internal dikategorikan menjadi beberapa area, yakni (1) Operations, efisisensi dan efektifitas operasi dalam mencapai sasaran bisnis yang juga meliputi tujuan performansi dan keuntungan; (2) Financial reporting, persiapan pelaporan anggaran finansial yang dapat dipercaya; dan (3) Compliance, pemenuhan hukum dan aturan yang dapat dipercaya. Ketiga, unit/aktifitas terhadap organisasi. Dimensi ini mengidentifikasikan unit/aktifitas pada organisasi yang menghubungkan kontrol internal. Kontrol internal menyangkut keseluruhan organisasi dan semua bagian-bagiannya.

Kontrol internal seharusnya diimplementasikan terhadap unit-unit dan aktifitas organisasi.

4. COBIT (Control Objectives for Information and related Technology).

   COBIT Framework dikembangkan oleh IT Governance Institute, sebuah organisasi yang melakukan studi tentang model pengelolaan TI yang berbasis di Amerika Serikat. COBIT berorientasi pada bisnis dan di-design dan dikerjakan tidak hanya oleh user dan auditor, tetapi juga sebuah panduan kemprehensif bagi pihak manajemen maupun pemilik bisnis proses tersebut. COBIT memberikan sebuah Maturity process untuk mengendalikan proses TI sehingga pihak manajemen dapat memetakan di mana posisi perusahaan tersebut, keadaan perusahaan sesuai tidaknya dengan class industry ataupun terhadap standar internasional, faktor kritikal sukses organisasi yang mendefinisikan prioritas manajemen TI yang harus didahulukan dan diimplementasikan atau dikendalikan, dan menetapkan key goal indicator dan key performance indicator untuk menjadi landasan tolak ukur bagi mengukur keberhasilan TI dalam mencapai tujuan dan kesesuaianya dengan kebijakan organisasi.

   COBIT Framework terdiri atas 4 domain utama, yakni (1) Plan and organize. Domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi TI dengan strategi perusahaan; (2) Acquire and implement. Domain ini menitikberatkan pada proses pemilihan, pengadaan, dan penerapan teknologi informasi yang digunakan; (3) Deliver and support. Domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya; (4) Monitor and evaluate. Domain ini menitikberatkan pada proses pengawasan dan mengevaluasi pengelolaan TI pada organisasi.

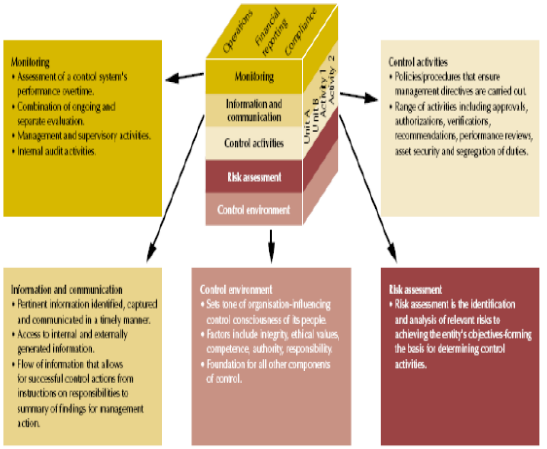
   COBIT mempunyai model kematangan (maturity model) untuk mengontrol proses-proses TI, dengan menggunakan metode penilaian (scoring) sehingga suatu organisasi dapat menilai proses-proses TI yang

dimilikinya dari skala non-existent sampai dengan optimized (dari 0 sampai 5). Maturity model ini akan memetakan (1) Current status dari organisasi, untuk melihat posisi organisasi saat ini; (2) Current status dari kebanyakan industri saat ini, sebagai perbandingan; (3) Current status dari standar internasional, sebagai perbandingan tambahan; dan (4) Strategi organisasi dalam rangka perbaikan, level yang ingin dicapai oleh organisasi.

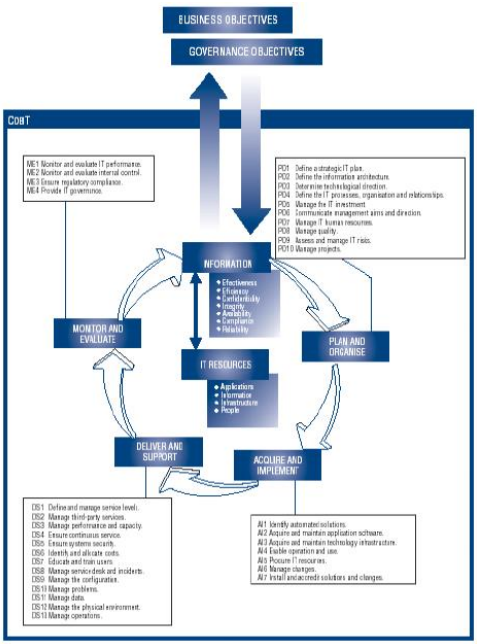
Selain itu, COBIT juga mempunyai ukuran-ukuran lainnya sebagai berikut. Pertama, Critical Success Factors (CSF), yaitu mendefinisian hal-hal atau kegiatan penting yang dapat digunakan manajemen untuk dapat mengontrol proses-proses TI di organisasinya. Kedua, Key Goal Indicators (KGI), yaitu mendefinisikan ukuran-ukuran yang akan memberikan gambaran kepada manajemen apakah proses-proses TI yang ada telah memenuhi kebutuhan proses bisnis yang ada. KGI biasanya berbentuk kriteria informasi (1) Ketersediaan informasi yang diperlukan dalam mendukung kebutuhan bisnis; (2) Tidak adanya resiko integritas dan kerahasiaan data; (3) Efisiensi biaya dari proses dan operasi yang dilakukan; (4) Konfirmasi reliabilitas, efektifitas, dan *compliance*. *Ketiga*, *Key Performance Indicators* (KPI) yaitu mendefinisikan ukuran-ukuran untuk menentukan kinerja proses-proses TI dilakukan untuk mewujudkan tujuan yang telah ditentukan. KPI biasanya berupa indikator-indikator kapabilitas, pelaksanaan, dan kemampuan sumber daya TI.

B. Perbandingan Implementasi IT Governance

ITIL sangat fokus kepada proses desain dan implementasi TI, serta pelayanan pelanggan (*customer service*), hal ini diperlihatkan bahwa hampir seluruh proses pada domain AI dan DS COBIT dilakukan.



Gambar 8 Framework ITIL



Gambar 9 Framework COBIT

COBIT 4.1 dengan COBIT 5 mempunyai beberapa perbedaan, terutama dalam pembagian domain dan aktivitas proses kerjanya. Pada kerangka kerja COBIT 5, terdapat pemisahaan yang tegas antara tata-kelola dengan manajemen. Tata kelola pada sebagian besar perusahaan merupakan tanggung jawab dari dewan direksi yang dipimpin oleh pemilik, sedangkan pengaturan merupakan tanggung jawab semua manajer eksekutif yang dipimpin oleh direktur operasional dalam menjalankan operasional kerja.

Metode analisis data pada penelitian ini dilakukan dengan beberapa tahap, yaitu:

1. Penentuan Domain

   Pada tahap ini domain yang akan dievaluasi berdasarkan kebutuhan layanan Teknologi Informasi dari fakultas dengan mengadopsi standar domain yang terdapat dalam kerangka kerja COBIT yaitu *Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS)* dan *Monitor and Evaluate (ME)*.

2. Penentuan Proses Kontrol

   Pada tahap ini dibuat daftar skala prioritas terhadap proses kontrol yang terdapat dalam masing-masing domain yang telah ditentukan pada tahap sebelumnya. Untuk mendapatkan skala prioritas proses kontrol dibuat kuisioner yang disebarkan kepada narasumber yang ditelah ditentukan.

3. Penentuan Indikator Kerja

   Indikator kinerja mendefinisikan bagaimana proses fungsi Teknologi Informasi dapat dilaksanakan dengan baik untuk mencapai suatu tujuan. Penentuan indikator berdasarkan *control objective* dari masing-masing proses kontrol dalam kerangka kerja COBIT.

   Pada penelitian ini menggunakan 11 *control objective* dari 4 domain antara lain:

   a. Domain Plan and Organise (PO)

      1) PO1 Pendefinisian Rencana Strategis Teknologi Informasi

2) PO4 Pendefinisian Proses Teknologi Informasi, Organisasi dan keterhubungannya
3) PO7 Manajemen Sumber Daya Manusia (SDM)

b. Domain Acquire and Implement (AI)
1) AI1 Mengidentifikasi Solusi Otomatis
2) AI3 Pemeliharaan Infrastruktur Teknologi Informasi
3) AI6 Mengelola Perubahan

c. Domain Deliver and Support (DS)
1) DS1 Menetapkan dan Mengelola Tingkat Layanan
2) DS11 Mengelola Data

d. Domain Monitor and Evaluate (ME)
1) ME1 Mengawasi dan Mengevaluasi Kinerja Teknologi Informasi
2) ME2 Mengawasi dan Mengevauasi Kontrol Internal
3) ME4 Menyediakan Tata Kelola Teknologi Informasi

4. Pemetaan Tingkat Kematangan

Pada tahap ini dilakukan pemetaan tingkat kematangan tata kelola Teknologi Informasi dengan menggunakan alat ukur model kematangan yang diadopsi dari standar COBIT menggunakan *Maturity Level*. Data diperoleh dari kuisioner.

BAB 12

Framework IT Balanced Scorecard

Setelah mempelajari Bab ini, Anda diharapkan mempunyai pengetahuan untuk :

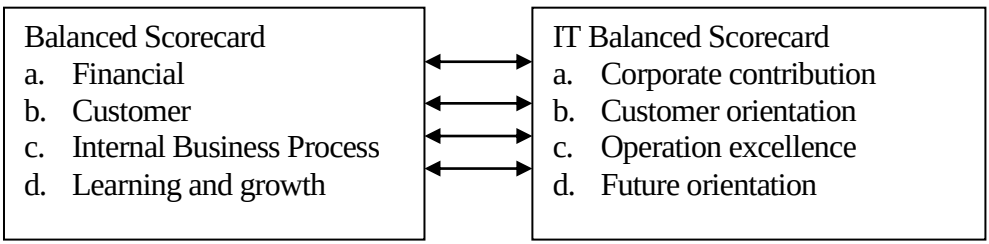
- Menjelaskan tentang Balanced Scorecard
- Menjelaskan tentang Faktor-faktor Penghambat *Balanced Scorecard*
- Menjelaskan tentang Keunggulan *Balanced Scorecard*
- Menjelaskan tentang Faktor-faktor yang Memacu Implementasi *Balanced Scorecard*
- Menjelaskan tentang Perspektif IT Balanced Scorecard

A. Balanced Scorecard

Balanced scorecard terdiri dari 2 kata yaitu *balanced* (berimbang) dan *scorecard* yaitu kartu skor. Kartu skor adalah kartu yang digunakan untuk mencatat skor hasil kinerja seseorang. Kartu skor juga dapat digunakan untuk merencanakan skor yang hendak diwujudkan oleh personil di masa depan. Melalui kartu skor, skor yang hendak diwujudkan oleh personil di masa depan dibandingkan dengan hasil kinerja sesungguhnya. Hasil perbandingan ini digunakan untuk melakukan evaluasi atas kinerja personil yang bersangkutan. Dengan demikian *balanced scorecard* merupakan alat kontemporer manajemen yang digunakan untuk mendongkrak kemampuan organisasi dalam melipatgandakan kinerja keuangan. Oleh karena itu, organisasi pada dasarnya adalah institusi pencipta kekayaan, penggunaan *balanced scorecard* dalam pengelolaan menjanjikan peningkatan signifikan kemampuan organisasi dalam menciptakan kekayaan.

Balanced scorecard merupakan sistem manajemen strategis yang menterjemahkan visi dan strategi suatu organisasi kedalam tujuan dan ukuran operasional. *Balanced scorecard* adalah konsep perencanaan dan implementasi manajemen strategik yang komprehensif yang ditemukan oleh Kaplan dan Norton (1995) terdiri dari empat perspektif yaitu (1) pelanggan, (2) keuangan, (3) internal dan (4) pembelajaran dan pertumbuhan.

Kemudian pada tahun 1997, Van Grembergen dan Van Bruggen mengadopsi balanced scorecard untuk dipergunakan pada Departemen Teknologi Informasi, sehingga terjadi perubahan perspektif pada model tradisional dan model *IT Balanced Scorecard* yang dapat dilihat pada gambar berikut : (Jogiyanto, 2011)



Gambar 10
Perubahan Perspektif *Balanced Scorecard* Tradisional menjadi
IT Balanced Scorecard (Sumber : Jogiyanto, 2011)

B. Faktor-faktor Penghambat *Balanced Scorecard*

Faktor-faktor penghambat *Balanced Scorecard* yaitu : (Vincent Gaspersz, 2002)

1. Tidak banyak orang dalam organisasi yang memahami strategi organisasi mereka.
   a. Hambatan Orang (*People Barrier*)
      Banyak orang dalam organisasi memiliki tujuan yang tidak terkait dengan strategi organisasi.

b. Hambatan Sumber Daya (*Resource Barrier*)
   Waktu, energi, dan uang tidak dialokasikan pada hal-hal yang penting (kritis) dalam organisasi.
c. Hambatan Manajemen (*Management Barrier*)
   Manajemen menghabiskan terlalu sedikit waktu untuk strategi organisasi dan terlalu banyak waktu untuk pembuatan keputusan taktis jangka pendek.

C. Keunggulan Balanced Scorecard

Balanced scorecard memiliki keunggulan yang menjadikan sistem manajemen strategik sekarang berbeda dengan sistem manajemen strategik dalam manajamen tradisional. Keunggulan *balanced scorecard* dalam sistem perencanaan strategik mampu menghasilkan rencana strategik yang memiliki karakteristik antara lain : (Norton dan Kaplan, 2000)

1. Komprehensif
   Balanced scorecard memperluas perspektif yang dicakup dalam perencanaan strategik dari yang sebelumnya hanya terbatas pada perspektif keuangan, meluas ke tiga perspektif yang lain yaitu customer, proses bisnis internal serta pembelajaran dan pertumbuhan.
2. Koheren
   Balanced scorecard mewajibkan personal untuk membangun hubungan sebab akibat diantara berbagai sasaran strategik yang dihasilkan dalam perencanaan strategik. Setiap sasaran strategik yang ditetapkan dalam persepsktif non keuangan harus mempunyai hubungan kausal dengan sasaran keuangan, baik secara langsung maupun tidak langsung.
3. Seimbang
   Keseimbangan sasaran strategik yang dihasilkan oleh sistem perencanaan strategik penting untuk menghasilkan kinerja keuangan berjangka panjang.

4. Terukur

   Balanced scorecard mengukur sasaran-sasaran strategik yang sulit untuk diukur. Dalam pendekatan *balanced scorecard* sasaran ketiga perspektif non keuangan ditentukan ukurannya agar dapat dikelola, sehingga dapat diwujudkan.

D. Faktor-faktor yang Memacu Implementasi *Balanced Scorecard*

Sistem pengukuran yang ditetapkan perusahaan mempunyai dampak yang besar terhadap perilaku manusia di dalam maupun di luar organisasi. Untuk berhasil dan tumbuh dalam persaingan, perusahaan harus menggunakan sistem pengukuran dan manajemen yang diturunkan dari strategi dan kapasitas yang dimiliki perusahaan. Banyak perusahaan yang mencanangkan strategi tentang hubungan dengan pelanggan, komitmen utama dan kapasitas perusahaan, ketika proses memotivasi dan mengukur kinerja masih dilaksanakan dengan menggunakan berbagai ukuran finansial. *Balanced Scorecard* mempertahankan ukuran finansial sebagai suatu ukuran yang lebih luas dan terpadu, yang mengaitkan pelanggan yang ada saat ini, proses internal, kinerja pekerja dan sistem dengan keberhasilan finansial jangka panjang.

Balanced Scorecard menterjemahkan misi dan strategi ke dalam berbagai tujuan dan ukuran yang tersusun ke dalam empat perspektif : finansial, konsumen, proses bisnis internal serta pembelajaran dan pertumbuhan. Keempat perspektif tersebut memberi keseimbangan antara tujuan jangka pendek dan jangka panjang antara hasil yang diinginkan dengan faktor pendorong tercapainya hasil dan antara ukuran obyektif yang keras dengan ukuran subyektif yang lebih lunak.

E. Perspektif IT Balanced Scorecard

Terdapat beberapa perspektif dalam mengevaluasi kinerja IT yaitu :

1. Perspektif Kontribusi Organisasi (*Corporate Contribution*)

   Perspektif kontribusi organisasi (*corporate contribution*) adalah perspektif yang mengevaluasi kinerja IT berdasarkan pandangan dari manajemen eksekutif, para direktur dan shareholder. Evaluasi IT dapat dipisahkan menjadi dua macam :

   - Jangka pendek berupa evaluasi secara finansial
   - Jangka panjang yang berorientasi pada proyek dan fungsi IT itu sendiri.

   Proyek-proyek IT seharusnya dapat memberikan nilai tambah bagi organisasi. Nilai tambah disini bukan hanya melibatkan resiko dalam pencapaiannya. Penggunaan tolak ukur keuangan sebagai satu-satunya pengukur kinerja organisasi memiliki beberapa kelemahan, antara lain :

   - Pemakaian kinerja keuangan sebagai satu-satunya penentu kinerja organisasi bisa mendorong manajer untuk mengambil tindakan jangka pendek dengan mengorbankan kepentingan jangka panjang. misalkan, untuk menaikkan profit seorang manajer bisa saja mengorbankan komitmennya terhadap pengembangan dan pelatihan bagi karyawan, termasuk investasi-investasi dalam sistem dan teknologi untuk kepentingan organisasi di masa mendatang. Hal ini akan mengakibatkan kinerja keuangan akan meningkat untuk jangka pendek tapi dalam jangka panjang justru akan merugikan.
   - Diabaikannya aspek pengukuran non-finansial termasuk intangible asset dan intagible benefit, pada umumnya akan memberikan pandangan yang keliru bagi manajer mengenai situasi dan kondisi organisasi di masa sekarang apalagi di masa mendatang.
   - Kinerja keuangan pada dasarnya hanya bertumpu pada kinerja masa lalu dan kurang mampu sepenuhnya untuk menuntun organisasi ke arah tujuan organisasi di masa mendatang.

2. Perspektif Orientasi Pengguna (*User Orientaiton*)

   Perspektif orientasi pengguna (*user orientation*) adalah perspektif yang mengevaluasi kinerja IT berdasarkan cara pandang pengguna bisnis (pelanggan kita) dan lebih jauh lagi adalah pelanggan dari unit bisnis yang ada. Dalam perspektif ini organisasi melakukan identifikasi pelanggan dan segmen pasar yang akan dimasuki. Dan dengan perspektif orientasi pengguna ini maka organisasi dapat menyelaraskan berbagai ukuran pelanggan penting yaitu : kepuasan, loyalitas, retensi, akuisisi dan profitabilitas, dengan pelanggan sendiri dan segmen pasar sasaran. Selain itu perspektif ini juga memungkinkan organisasi melakukan identifikasi dan pengukuran dimana secara eksplisit menetapkan proposisi nilai (faktor pendorong) yang akan organisasi berikan kepada pelanggan dan pasar sasaran. Jadi jika pengguna tidak merasa puas maka akan banyak keluhan atau bahkan akan menurunkan kinerja pengguna di masa yang akan datang, walaupun kinerja mereka saat ini terlihat baik. Secara umum, perspektif ini memiliki dua kelompok pengukuran, yaitu :

   a. Kelompok pengukuran pelanggan utama

      Merupakan ukuran generik yang digunakan hampir semua organisasi, yang terdiri dari ukuran: pangsa pasar, retensi pelanggan, akuisisi pelanggan, kepuasan pelanggan dan profitabilitas pelanggan.

      1) Pangsa pasar

         Mencerminkan bagian yang dikuasai oleh organisasi atas keseluruhan pasar yang ada, yang meliputi antara lain : jumlah pelanggan, jumlah penjualan, dan volume unit penjualan.

      2) Retensi pelanggan

         Mengukur tingkat dimana organisasi dapat mempertahankan hubungan yang baik dengan penggunanya.

      3) Akuisisi pelanggan

         Mengukur tingkat dimana suatu unit bisnis mampu menarik pelanggan baru atau memenangkan bisnis baru.

4) Kepuasan pelanggan

Menaksir tingkat kepuasaan pelanggan terkait dengan kriteria kinerja spesifik dalam value proposiiton.

5) Profitabilitas pelanggan

Berhasil dalam empat ukuran pelanggan utama sebelumnya bukanlah jaminan bahwa sebuah organisasi memiliki pelanggan yang menguntungkan. Karena kepuasan pelanggan dan pangsa pasar yang besar hanyalah sebuah alat untuk mencapai pengembalian finansial yang tinggi, organisasi berharap untuk dapat mengukur tidak hanya besaran bisnis yang dilakukan dengan pelanggan tetapi juga profitabilitas dari bisnis ini, terutama dalam segmen pelanggan sasaran. Organisasi tidak hanya menginginkan pelanggan yang lebih dari sekedar terpuaskan dan senang tetapi juga pelanggan yang memberikan keuntungan. Sebuah ukuran finansial seperti profitabilitas pelanggan dapat membantu organisasi untuk tetap berfokus pada pelanggan, dan di lain pihak dapat mengungkapkan pelanggan sasaran tertentu yang tidak memberian keuntungan.

b. Kelompok pendorong kinerja

Kelompok pengukuran yang merupakan faktor pendorong kinerja (pembeda) hasil pelanggan. Kelompok pengukuran ini menawarkan proposisi nilai pelanggan yang diberikan organisasi. Proposisi nilai ini menyatakan atribut yang diberikan organisasi kepada produk dan jasanya untuk menciptakan loyalitas dan kepuasan pelanggan dalam pasar sasaran.

1) Product/service attributes

Atribut produk atau jasa mencakup fungsionalitas produk atau jasa tersebut, harga dan mutu. Pengguna memiliki preferensi yang berbeda-beda atas produk yang ditawarkan.

2) Customer relationship

Menyangkut perasaan pelanggan terhadap proses pembelian produk yang ditawarkan organisasi. Perasaan konsumen ini sangat dipengaruhi oleh responsivitas dan komitmen organisasi terhadap pelanggan berkaitan dengan masalah waktu penyampaian. Waktu merupakan komponen yang penting dalam persaingan organisasi. Pelanggan biasanya menganggap penyelesaian order yang cepat dan tepat waktu sebagai faktor yang penting bagi kepuasan mereka.

3) Image and reputaiton

Menggambarkan faktor-faktor intangible yang menarik seorang konsumen untuk berhubungan dengan organisasi. Membangun image dan reputasi dapat dilakukan melalui iklan dan menjaga kualitas seperti yang dijanjikan.

3. Perspektif keunggulan operasional (*operational excellence*)

Perspektif ini adalah perspektif yang menilai kinerja IT berdasarkan cara pandang manajemen IT itu sendiri dan lebih jauh lagi adalah pihak yang berkaitan dengan audit dan pihak yang menetapkan aturan-aturan yang digunakan.

Keunggulan operational suatu organisasi dapat dilihat pada operasi bisnis internal yang terjadi, yang dapat dibagi ke dalam :

a. Inovasi

Dalam proses ini, unit bisnis menggali pemahaman tentang kebutuhan laten dari pelanggan dan menciptakan produk dan jasa yang mereka butuhkan. Proses inovasi dilakukan dan setelah melalui serangkaian tes dan telah memenuhi syarat-syarat pemasaran dan dapat dikomersilkan maka produk atau jasa tersebut diperkenalkan kepada pelanggan. Akitvitas ini merupakan akitvitas penitng yang berlangsung untuk jangka panjang sehingga menentukan kesuksesan organisasi dimasa sekarang dan dimasa mendatang.

b. Operasional

Proses ini merupakan proses dalam pembuatan dan penyampaian produk atau jasa. Dalam proses ini pengukuran yang terkait dapat dikelompokkan pada waktu, kualitas dan biaya.

c. Pelayanan purna jual

Proses ini dimulai pada saat produk atau jasa sudah terjual atau digunakan. Organisasi dapat mengukur apakah upayanya dalam proses ini telah sesuai dengan harapan pelanggan. Pengukuran pada proses ini dapat menggunakan tolak ukur yang bersifat kualitas, biaya dan waktu.

4. Perspektif orientasi dimasa depan (*future orientation*)

Perspektif ini adalah perspektif yang menilai kinerja IT berdasarkan cara pandang dari departemen itu sendiri, yaitu : pelaksanaan, para praktisi dan profesional yang ada. Pada perspektif terakhir ini akan menyiapkan infrastruktur organisasi yang memungkinkan tujuan-tujuan dalam tiga perspektif lainnya dapat dicapai. Kemampuan organisasi untuk dapat menghasilkan produk atau jasa di masa mendatang dengan kemampuan layanan yang memuaskan harus dipersiapkan mulai dari saat ini. Pihak manajemen harus dapat memperkirakan tren di masa mendatang dan membuat langkah - langkah persiapan dalam mengantisipasinya. Dalam perspektif ini terdapat tiga kategori yang dapat diperhatikan secara khusus dalam penanganan di masa depan yaitu :

a. Kapabilitas pekerja

Salah satu perubahan yang dramatis dalam pemikiran manajer selama tahun – tahun terakhir ini adalah peran pegawai dalam organisasi. Perencanaan dan pelaksanaan pelatihan kembali (reskilling) pegawai yang dapat menjamin kecerdasan dan kreativitasnya dapat dimobilisasi untuk mencapai tujuan organisasi. Tiga pengukuran utama yang berlaku umum adalah :

1) Kepuasan pekerja : menyatakan bahwa moral pekerja dan kepuasan kerja secara keseluruhan saat ini dipandang sangat penting oleh sebagian besar organisasi. Pekerja yang puas merupakan pra-kondisi bagi meningkatnya produkitvitas, daya tanggap dan layanan pelanggan di masa kini maupun masa mendatang.
2) Resensi pekerja : menyatakan lama tidaknya para pekerja yang diminati organisasi dapat bertahan bekerja. Hal ini berdasarkan teori bahwa pada dasarnya suatu organisasi membuat investasi jangka panjang dalam diri para pekerja sehingga seitap kali ada pekerja yang berhenti dan bukan atas keinginan organisasi maka itu merupakan suatu kerugian modal intelektual bagi organisasi tersebut.
3) Produktivitas pekerja : merupakan suatu ukuran hasil atau dampak keseluruhan usaha peningkatan moral dan keahlian pekerja, inovasi, proses internal dan kepuasan pelanggan. Tujuannya adalah membandingkan keluaran yang dihasilkan oleh para pekerja dengan jumlah pekerja yang dikerahkan untuk menghasilkan keluaran tersebut.

Selain tiga pengukuran inti tersebut di atas, maka terdapat pula faktor pendorong yang penting, yaitu :

1) Kompetensi staf

   Dengan adanya transformasi organisasi maka para pekerja harus mengambil tanggung jawab baru agar tujuan pelanggan dan keunggulan operasional dapat tercapai. Oleh karena itu maka dibutuhkannya pelatihan ulang dapat dipandang dalam dua dimensi yaitu : tingkat pelatihan yang dibutuhkan dan persentase tenaga kerja yang membutuhkan pelatihan ulang. Bila tingkat pelatihan ulang pekerja rendah, latihan dan pendidikan normal sudah mencukupi bagi organisasi untuk mempertahankan kapabilitas kerja. Dalam hal ini pelatihan ulang bukan merupakan prioritas untuk mendapat

tempat dalam IT Balanced Scorecard. Hal yang berbeda berlaku untuk situasi sebaliknya, dimana pekerja membutuhkan latihan khusus.

b. Infrastruktur Teknologi

Mencerminkan kekuatan tepat guna dan sasaran dari teknologi yang digunakan organisasi dalam pencapaian tujuan-tujuannya. Faktor-faktor yang dapat dimasukkan dalam kategori ini antara lain: penggunaan teknologi strategis, penggunaan database strategis, pengalaman yang dimiliki (experience capture), proprietary aplikasi dan paten atau hak cipta.

c. Ilmu untuk bertindak

Faktor pendorong ini biasanya diakibatkan oleh situasi dan kondisi tertentu yang tercipta dalam pelaksanaan proses-proses bisnis maupun dalam pencapaian tujuan strategis organisasi. Faktor-faktor yang termasuk dalam kategori ini antara lain : siklus keputusan penting, fokus strategi, pemberdayaan staf, personal aligment, moral pekerja dan kerjasama tim.

d. Kapabilitas sistem informasi

Selain motivasi dan keahlian pekerja, jika ingin para pekerja dapat bekerja secara lebih efektif dalam lingkungan yang kompetitif saat ini dan di masa mendatang, maka diperlukan data dan informasi yang lebih banyak, yang menyangkut pelanggan, keadaan pasar, proses internal dan konsekuensi finansial keputusan organisasi.

e. Motivasi, pemberdayaan dan keselarasan

Kapabilitas di atas tidak akan memberikan kontribusi bagi keberhasilan organisasi jika para pekerja tidak termotivasi bertindak untuk kepentingan terbaik organisasi, atau jika mereka tidak diberikan kebebasan membuat keputusan dan mengambil tindakan. Sebuah ukuran motivasi pekerja yang sederhana dan banyak digunakan adalah banyaknya saran yang diberikan per pekerja.

Ukuran ini mengukur partisipasi pekerja dalam meningkatkan kinerja organisasi. Ukuran seperti ini dapat diperkuat lagi dengan sebuah ukuran pelengkap yaitu jumlah saran yang dilaksanakan, yang menilai mutu saran yang mereka dihargai dan benar-benar diperhatikan.

Sedangkan faktor pendorong kinerja keselarasan perorangan dan organisasi berfokus pada pemahaman dan penyelarasan tujuan setiap departemen dan atau pekerja dengan tujuan organisasi yang telah dinyatakan dalam IT Balanced Scorecard.

DAFTAR PUSTAKA

Boynton, Johnson, Kell, 2003. "*Modern Auditing"*. Seventh Edition. John Wiley & Sons, Inc.

Champlain, Jack, J. 2003. *Auditing Information System*. Second Edition. New York : John Wiley and Son.

Dan M. Guy, C. Wayne Alderman, Alan J. Winters, 2002. *"Auditing"*. Fifth Edition. Alih Bahasa Erlangga Jakarta. Jones dan Rama serta Hunton dkk (2004)

Gaspersz, Vincent, 2002, "Sistem Manajemen Kinerja Terintegrasi: Balanced Scorecard Dengan Six Sigma", PT. Gramedia Pustaka Utama, Jakarta.

Gondodiyoto, Sanyoto. 2007. *Audit Sistem Informasi dan Pendekatan COBIT*. Edisi Revisi. Jakarta : Mitra Wacana Media.

Ikantan Akuntan Indonesia, 2002. *Standar Akuntansi Keuangan*. Jakarta : Penerbit Salemba Empat.

Ikantan Akuntan Indonesia, 2011. *Standar Profesional Akuntan Publik*. Jakarta : Penerbit Salemba Empat.

Ikatan Akuntansi Indonesia. (2001). Standar Profesional akuntan publik. Jakarta: Salemba Empat Patria.

Jogiyanto, W. A. 2011. Sistem Tata Kelola Teknologi Informasi. Yogyakarta: Penerbit Andi.

Kaplan, Robert S. dan David P. Norton, (2000), "*Balanced Scorecard*: Menerapkan strategi menjadi aksi", Erlangga, Jakarta.

Mulyadi, 2002, Auditing Buku 1, Salemba Empat, Jakarta.

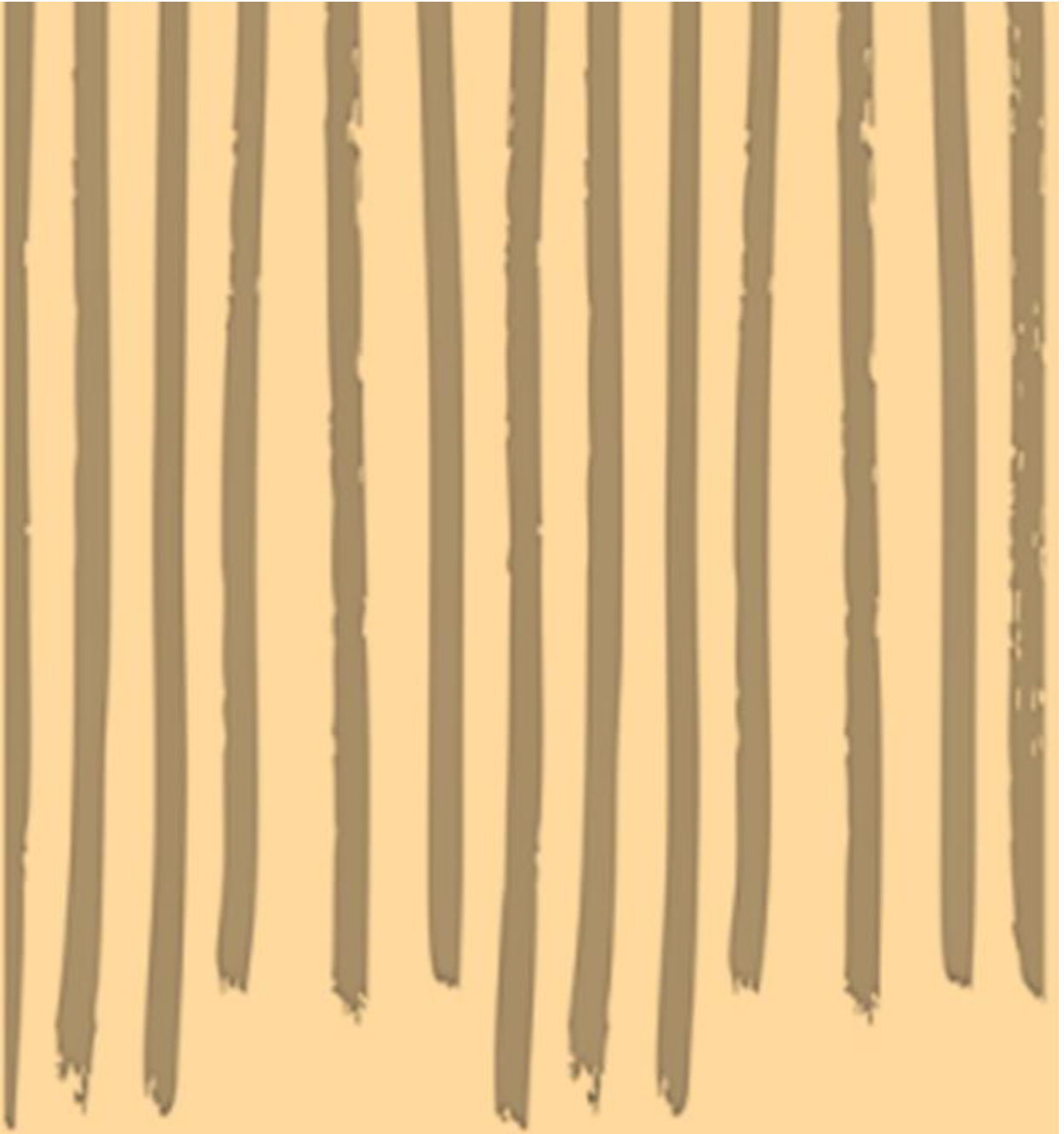
Mulyadi. 2001. *Sistem Akuntansi*. Edisi ke-3. Jakarta . Salemba Empat

Sawyer et al. 2005, Sawyer's Internal Auditing, Buku 1 s.d 3, edisi ke lima,. Salemba empat. Jakarta. Indonesia.

Soekrisno Agoes, 2004. "*Auditing (Pemeriksaan Akuntan) Oleh KAP"*. Edisi Tiga. LPFEUI Jakarta.

Surendro, Kridanto. 2009. Implementasi Tata Kelola Teknologi Informasi. Bandung : Penerbit Informatika.

Weber, Ron. 1999. *Information system Control Audit* New Jersey: Prentice Hall.




YPAT


9 786236 141366