MODUL

AUDIT SISTEM INFORMASI Dan Tata Kelola

Disusun oleh :

Eva Zuraidah M.Kom

2019

Pertemuan 1

1.1. Definisi Kontrol

Kontrol adalah sebuah sistem untuk mencegah, mendeteksi atau memperbaiki situasi yang tidak teratur.

Terdapat tiga aspek penting yang berkaitan dengan definisi kontrol di atas, yaitu :

a. Kontrol adalah sebuah sistem, dengan kata lain kontrol terdiri atas sekumpulan komponen-komponen yang saling berhubungan dan bekerja sama untuk mencapai tujuan yang sama.
b. Fokus dari kontrol adalah situasi yang tidak teratur, dimana keadaan ini bisa terjadi jika ada masukan yang tidak semestinya masuk ke dalam sistem.
c. Kontrol digunakan untuk mencegah, mendeteksi dan memperbaiki situasi yang tidak teratur, sebagai contoh :
    1) Preventive control : instruksi yang diletakkan pada dokumen untuk mencegah kesalahan pemasukan data
    2) Detective control : Kontrol yang diletakkan pada program yang berfungsi mendeteksi kesalahan pemasukan data
    3) Corrective control : program yang dibuat khusus untuk memperbaiki kesalahan pada data yang mungkin timbul akibat gangguan pada jaringan, komputer ataupun kesalahan user.

Secara umum, fungsi dari kontrol adalah untuk menekan kerugian yang mungkin timbul akibat kejadian yang tidak diharapkan yang mungkin terjadi pada sebuah sistem. Tugas auditor adalah untuk menetapkan apakah kontrol sudah berjalan sesuai dengan yang diharapkan untuk mencegah terjadinya situasi yang tidak diharapkan. Auditor harus dapat memastikan bahwa setidaknya ada satu buah kontrol yang dapat menangani resiko bila resiko tersebut benar-benar terjadi.

Para auditor sistem informasi secara khusus berkonsentrasi pada evaluasi kehandalan atau efektifitas pengendalian / kontrol sistem.

1.1.1. Control Audit Sistem Informasi

Control Audit Sistem Informasi terdiri dari :

a. Kontrol lingkungan (Environmental controls)

   Pengendalian lingkungan meliputi hal-hal seperti kebijakan keamanan IS, standar, dan pedoman; struktur pelaporan dalam lingkungan pemrosesan IS (termasuk operasi komputer dan pemrograman); kondisi keuangan organisasi dan vendor jasa

b. Kontrol keamanan fisik (Physical security controls)

   Kontrol keamanan fisik berkaitan dengan perlindungan terhadap perangkat keras komputer, komponen, dan fasilitas di mana mereka berada.

c. Kontrol keamanan logis (Logical security controls)

   Kontrol keamanan logis adalah yang telah dikerahkan dalam sistem operasi dan aplikasi untuk membantu mencegah akses tidak sah dan penghancuran yang disengaja atau disengaja terhadap program dan data.

d. Kontrol operasi IS (IS operating controls)

   Kontrol operasi sistem informasi, yang dirancang untuk membantu memastikan bahwa sistem informasi beroperasi secara efisien dan efektif. Kontrol ini termasuk penyelesaian tepat waktu dan akurat pekerjaan produksi, distribusi media output, kinerja cadangan dan prosedur pemulihan, kinerja prosedur pemeliharaan.

1.1.2. Faktor – Faktor Kontrol dan Audit

Faktor-faktor yang mendorong pentingnya kontrol dan audit sistem informasi (Weber, 1999, p.6) adalah antara lain untuk :

a. Mendeteksi agar komputer tidak dikelola secara kurang terarah

b. Mendeteksi resiko kehilangan data.

c. Mendeteksi resiko pengambilan keputusan yang salah akibat informasi hasil proses sistem komputerisasi salah/lambat/tidak lengkap.

d. Menjaga aset perusahaan karena nilai hardware, software dan personil yang lazimnya tinggi.

e. Mendeteksi resiko error komputer.

f. Mendeteksi resiko penyalahgunaan komputer (fraud).

g. Menjaga kerahasiaan

h. Meningkatkan pengendalian evalusi penggunaan komputer

1.2. Definisi Audit Sistem Informasi.

Pengertian Audit adalah aktivitas pengumpulan dan pemeriksaan bukti terkait suatu informasi untuk menentukan dan membuat laporan tentang tingkat kesesuaian antara informasi dengan kriteria yang ditetapkan.

Suatu proses sistematis mendapatkan dan mengevaluasi bukti-bukti secara objektif sehubungan dengan asersi atas tindakandan peristiwa ekonomi untuk memastikan tingkat kesesuaian antara asersi-asersi tersebut danmenetapkan kriteria serta mengkomunikasikan hasilnya kepada pihak - pihak yang berkepentingan. (Messi eret al 2006)

Audit pada dasarnya adalah proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti bukti tindakan ekonomi, guna memberikan asersi/ pernyataan dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kretaria yang berlaku dan mengkomunikasikan hasilnya kepada pihak yang terkait. (Wardani ,2014)

Audit adalah : Suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara objektif 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. (Mulyadi ,2014:9)

Pada awal konsep / bidang kontrol internal mungkin hanya merupakan mekanisme yang sangat tinggi dari segi pandang manajemen perusahaan yaitu sebagai sistem yang dapat ,menjamin dipatuhinya kebijakan perusahaan oleh para pegawai, melindungi *aset* perusahaan, dan menghindari terjadinya kesalahan / kekeliruan dan penyalahgunaan.

Audit sistem informasi adalah proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien (Weber dalam Yaner, Tanuwijaya, & Sutomo, 2018: 2).

Pengertian sistem Sistem adalah kumpulan dari elemen-elemen berupa data, jaringan data, jaringan kerja dari prosedur-prosedur yang saling berhubungan, sumber daya manusia, teknologi baik hardware maupun software yang saling berinteraksi sebagai satu kesatuan untuk mencapai tujuan/sasaran tertentu yang sama. (Maniah dan Dini Hamidin, 2017)

Pengertian Audit Sistem Informasi Beberapa ahli mengemukakan bahwa pengertian audit sistem informasi adalah sebagai berikut:

a. Audit sistem informasi adalah kegiatan yang dilakukan dengan tujuan untuk menilai apakah pengendalian sistem informasi telah dapat memberikan keyakinan yang memadai atas pengamanan aset, integritas data, efektivitas, dan efisiensi.(I Putu Agus Swastika dan Lanang Agung Raditya Putra 2016),

b. Audit sistem informasi adalah proses pengumpulan dan evaluasi buktibukti untuk menentukan apakah sistem komputer yang digunakan telah pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien. (Tata Sutabri ,2012)
c. Audit sistem informasi adalah pemeriksaan atau audit yang dilaksanakan dalam rangka IT Governance, merupakan audit operasional secara khusus terhadap pengelolaan sumber daya informasi. (Sanyoto Gondodiyoto, 2007)

Secara umum audit teknologi informasi dimaksudkan untuk mengevaluasi tingkat kesesuaian antara teknologi informasi dengan prosedur bisnis (business processes) perusahaan, untuk mengetahui apakah suatu teknologi informasi telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis. Sehingga, memiliki mekanisme pengamanan aset, serta menjamin integritas data yang memadai (Gondodiyoto, 2017).

Audit Teknologi Informasi adalah mengevaluasi dan mengumpulkan bukti dari adanya sebuah sistem komputer untuk menjaga integritas data serta melindungi sistem komputer yang digunakan. Integritas data yang dijaga merupakan aset perusahaan dalam mencapai tujuan perusahaan secara efektif dan menggunakan sumber daya yang ada. Audit Teknologi Informasi mencakup berbagai macam ilmu yang menjadi suatu kesatuan, diantaranya Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntasi, Ilmu Komputer, dan Behavioral Science (Isa, 2012a).

1.2.1. **Langkah – langkah audit sistem informasi**.

Proses audit sistem informasi adalah proses yang berkaitan langsung dengan kompleksitas. Terkadang auditor harus menyelesaikan tugasnya dalam sistem yang sangat banyak dan kompleks. Karena kompleksitas merupakan akar permasalahan dari

setiap problem yang dihadapai oleh para profesional, maka para ilmuwan telah berusaha untuk membuat panduan untuk mengurangi kompleksitas tersebut, yaitu :

a. Memecah sebuah sistem yang besar menjadi beberapa subsistem untuk dievaluasi secara terpisah
b. Menentukan kehandalan setiap subsistem dan pengaruh setiap subsistem terhadap kehandalan sistem secara keseluruhan

1.2.**2.** *Tahapan Audit*

Dalam melakukan kegiatan audit, penelit memakai tahapan audit sebagai berikut :

1. Planning, mendapatkan pemahaman yang lengkap mengenai bisnis perusahaan yang sedang dilakukan audit. Pada proses ini auditor menentukan ruang lingkup dan tujuan pengendalian, tingkat materialitas, dan outsourcing. Pada tahap ini auditor menetapkan mengapa, bagaimana, kapan dan oleh siapa audit akan dilaksanakan. Untuk mematangkan tahap perencanaan, sebuah program audit awal dipersiapkan untuk menunjukkan sifat, keluasan, dan waktu prosedur-prosedur yang dibutuhkan untuk mencapai tujuan audit dan untuk meminimalkan risiko-risiko audit.
2. Prepare Audit Program, audit program disesuaikan dengan hardware dan software yang dimiliki perusahaan, topologi dan arsitektur jaringan, dan lingkungan serta pertimbangan khusus mengenai industri tersebut. Komponen- komponen dari audit program tersebut adalah: ruang lingkup audit, sasaran audit, prosedur audit, dan rincian administratif (perencanaan dan pelaporan).
3. Gather Evidence, bertujuan untuk mendapatkan bukti-bukti memadai, handal, relevan, dan berguna untuk mencapai sasaran audit secara efektif. Jenis bukti yang sering ditemukan auditor pada kerja lapangan yaitu:

observasi proses-proses dan keberadaan dari item fisik seperi pengoperasian komputer atau prosedur backup data, bukti dalam bentuk dokumen (seperti program change logs, sistem access logs, dan tabel otoritas), gambaran dari perusahaan seperi flowcharts, narratives, dan kebijakan dan prosedur yang tertulis), serta analisa seperti prosedur CAATs yang dijalankan pada data perusahaan.

4. Form Conclusion, mengevaluasi bukti- bukti dan membuat suatu kesimpulan tentang hasil pemeriksaan yang pada akhirnya akan mengarah pada opini audit. Auditor juga akan melaporkan kelemahan dan kelebihan dari sistem.
5. Deliver Audit Opinion, informasi umum yang harus ada dalam sebuah laporan audit yaitu:
    a. Nama dari organisasi/perusahaan yang diaudit
    b. Judul, tanda tangan, dan tanggal
    c. Pernyataan sasaran audit dan apakah audit tersebut telah memenuhi sasaran

        Ruang lingkup audit, termasuk didalamnya area audit fungsional, periode audit yang tercakup, dan sistem informasi, aplikasi, atau lingkungan proses yang diaudit

    d. Pernyataan bahwa telah terjadi pembatasan ruang lingkup dimana auditor tidak dapat melaksanakan pekerjaan audit dengan memadai untuk mencapai sasaran-sasaran audit tertentu
    e. Pengguna laporan audit yang dikehendaki, termasuk beberapa pembatasan dalam pendistribusian laporan audit
    f. Standar-standar dan kriteria yang menjadi dasar auditor untuk

melaksanakan pekerjaan audit tersebut

g. Penjelasan rinci mengenai temuan- temuan penting
h. Kesimpulan dari area audit yang dievaluasi, termasuk di dalamnya syarat dan kualifikasi penting
i. Saran-saran yang tepat untuk tindakan perbaikan dan peningkatan
j. Peristiwa-peristiwa penting yang terjadi setelah masa fieldwork audit yang bersangkutan berakhir

6. Follow Up, melakukan tindak lanjut dengan membuat suatu ketentuan untuk melakukan tindak lanjut bersama dengan perusahaan pada kondisi-kondisi yang dilaporkan atau defisiensi audit yang tidak ter-cover selama kegiatan audit. Tindak lanjut ini dapat dilakukan dengan menelepon pihak menejemen.

1.2.3. Tahapan Audit Sistem Informasi

Berikut ini terdapat beberapa tahapan audit sistem informasi, terdiri atas:

a. Perencanaan Audit (Planning The Audit)

   Perencanaan merupakan fase pertama dari kegiatan audit, bagi auditor eksternal hal ini artinya adalah melakukan investigasi terhadap klien untuk mengetahui apakah pekerjaan mengaudit dapat diterima, menempatkan staff audit, menghasilkan perjanjian audit, menghasilkan informasi latar belakang klien, mengerti tentang masalah hukum klien dan melakukan analisa tentang prosedur yang ada untuk mengerti tentang bisnis klien dan mengidentifikasikan resiko audit.

b. Pengujian Pengendalian (Test Of Controls)

   Auditor melakukan kontrol test ketika mereka menilai bahwa kontrol resiko berada pada level kurang dari maksimum, mereka mengandalkan kontrol sebagai dasar untuk mengurangi biaya testing. Sampai pada fase ini auditor tidak

mengetahui apakah identifikasi kontrol telah berjalan dengan efektif, oleh karena itu diperlukan evaluasi yang spesifik.

c. Pengujian Transaksi (Test Of Transaction)

   Auditor menggunakan test terhadap transaksi untuk mengevaluasi apakah kesalahan atau proses yang tidak biasa terjadi pada transaksi yang mengakibatkan kesalahan pencatatan material pada laporan keuangan. Tes transaksi ini termasuk menelusuri jurnal dari sumber dokumen, memeriksa file dan mengecek keakuratan.

d. Pengujian Keseimbangan atau Keseluruhan Hasil (Tests Of Balances or Overal Result)

   Untuk mengetahui pendekatan yang digunakan pada fase ini, yang harus diperhatikan adalah pengamatan harta dan kesatuan data. Beberapa jenis subtantif tes yang digunakan adalah konfirmasi piutang, perhitungan fisik persediaan dan perhitungan ulang aktiva tetap.

e. Penyelesaian / Pengakhiran Audit (Completion Of The Audit)

   Pada fase akhir audit, eksternal audit akan menjalankan beberapa test tambahan terhadap bukti yang ada agar dapat dijadikan laporan.

Lingkup Audit Sistem Informasi pada umumnya difokuskan kepada seluruh sumber daya sistem informasi yang ada, yaitu Aplikasi, Informasi, Infrastruktur dan Personil.

1.2.4. 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 informasi. Data memiliki atribut-atribut tertentu seperti: kelengkapan, kebenaran dan keakuratan. Jika integritas data tidak terpelihara maka suatu perusahaan tidak akan lagi memiliki hasil atau laporan yang benar bahkan perusahaan dapat menderita kerugian.

3. Efektifitas Sistem

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

6. Ketersediaan.

   Berhubungan dengan ketersediaan dukukan/layanan teknologi informasi TI.TI hendaknya dapat dapat mendukung secara kontinyu terhadap proses bisnis.Semakin sering terjadi gangguan maka berarti tingkat ketersediann sistem rendah.

7. Kerahasian.

   Fokusnya pada proteksi terhadap informasi dan supaya terlindung dari akses dari pihak-pihak yang tidak berwenang.

8. Kehandalan.

   Kesesuaian dan keakuratan bagi manajemen dalam pengelolaan organisasi, pelaporan dan pertanggunjawaban.

9. Menjaga Intergritas Data

   Integritas data adalah salah satu konsep dasar sistem informasi, data memiliki atribut atribut yaitu : kelengkapan, kebenaran, dan keakuratan.

1.2.5. KEUNTUNGAN AUDIT

1. Menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi
2. Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
3. Mengukur tingkat efektifitas dari sistem
4. Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidak sesuaian di masa datang
5. Menyediakan informasi untuk proses peningkatan

6. Meningkatkan saling memahami antar departemen dan antar individu
7. Melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen.

1.2.6. Tinjauan Penting dalam Audit SI / TI

Adapun elemen utama dari aktivitas peninjauan yang dilakukan dalam Audit SI/TI dapat dikalfikasikan kedalam tinjaunan penting sebagai berikut:

a. Tinjauan terkait dengan fisik dan lingkungan yakni: hal hal yang terkait dengan kemanan fisik, suplai sumber daya , temperatur, kontrol kelembaban dan faktor lingkungan lain.
b. Tinjauan administrasi sistem yaitu mencakup tinjaun keamanan sistem operasi, sistem manajemen database, seluruh prosedure administrasi sistem dan pelaksanannya.
c. Tinjauan perangkat lunak . Perangkat lunak yang dimaksud merupakan aplikasi bisnis yang dapat berupa sistem berbasis web untuk pemrosesan permintaan pelanggan hingga Enterprise Reasource Planining (ERP) yang kini menjadi inti dari proses bisnis diperusahaan
d. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan sistem, batasan tingkat keamanan, tinjauan terhadap firewall, daftar kontrol akses router, prort scaning serta pendeteksian akan gangguan maupun ancaman terhadap sistem.
e. Tinjaunan kontinuitas bisnis dengan memastikan ketersediaan prosedur backup dan menyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana/ kontinuitas bisnis yang dimiliki.

f. Tinjauan intergritas data yang bertujuan untuk memastikan ketelitian data beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

1.3.Pengertian Motivasi

Pengertian Motivasi Kata Motivasi berasal dari kata Latin "Motive" yang berarti dorongan, daya penggerak atau kekuatan yang terdapat dalam diri organism yang menyebabkan organism itu bertindak atau berbuat. Selanjutnya diserap dalam bahasa Inggris motivation berarti pemberian motiv, penimbulan motiv atau hal yang menimbulkan dorongan atau keadaan yang menimbulkan dorongan.

Menurut Landy dan Becker (2011:59) pengertian motivasi adalah : *"The term motivation has at least two connotations in the field organization behavior, the first is a management process, used this way. Motivation is seen as a management activity, something that management do to induce others to act in a way to produce result desired by organization or perhaps by the manager. In this context we might say role of every manager is to motivate employee to work harder or to do betteras a psychological concept motivation refers to internal mental state of a person, which relates to the initiation, direction, persistence intensity and termination of behavior."*

Dalam pernyataan Landy dan Becker menjelaskan bahwa Istilah motivasi setidaknya memiliki dua konotasi dalam perilaku organisasi lapangan, yang pertama adalah proses manajemen, yang digunakan dengan cara ini. Motivasi dipandang sebagai kegiatan manajemen, sesuatu yang dilakukan manajemen untuk mendorong orang lain bertindak dengan cara menghasilkan hasil yang diinginkan oleh organisasi atau mungkin oleh manajer. Dalam konteks ini kita bisa mengatakan peran setiap manajer adalah memotivasi karyawan untuk bekerja lebih keras atau melakukan yang

lebih baik sebagai motivasi konsep 24 psikologis mengacu pada keadaan mental internal seseorang, yang berkaitan dengan inisiasi, arahan, intensitas ketekunan dan penghentian perilaku.

1.4.**Tujuan Audit Sistem Informasi Dan Keuntungan Diaudit, Jenis Audit**

Tujuan Audit Sistem Informasi dapat dikelompokkan ke dalam dua aspek utama dari ketatakelolaan IT, yaitu :

a. *Conformance* (Kesesuaian)

Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kesesuaian, yaitu:

Confidentiality (Kerahasiaan), *Integrity* (Integritas), *Availability* (Ketersediaan) dan *Compliance* (Kepatuhan).

b. *Performance* (Kinerja)

Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kinerja, yaitu: *Effectiveness*

(Efektifitas), *Efficiency* (Efisiensi), *Reliability* (Kehandalan).

Menurut Gallegos dalam bukunya "*Audit And Control Of Information System*" menyatakan audit sistem informasi meliputi beberapa tahapan yakni:

1. Perencanaan (Planning)

Meliputi aktivitas utama, yakni:

- Menetapkan ruang lingkup dan tujuan audit
- Mengorganisasikan tim audit
- Memahami tentang oprasi bisnis klien
- Mengkaji ualgn hasil audit sebelumnya
- Menyiapkan program audit

2. Pemeriksaan Lapangan (Field Work)

   Pada tahap ini yang dikerjakan yaitu mengumpulkan informasi yang dilakukan dengan cara mengumpujlkan data dengan pihak-pihak yang berhubungan. Hal ini bisa dilakukan dengan cara penerapan metode pengumpulan data yakni wawancara, quisioner atau melakukan survey.

3. Pelaporan (Reporting)

   Setelah pengumpulan data, maka akan diperoleh data yang akan diproses untuk dihitung menurut perhitungan maturity level. Di tahapan ini akan dilakukan pemberian informasi dalam bentuk hasil-hasil dari audit.

4. Tindak Lanjut (Follow Up)

   Tahapan ini dilakukan dengan pemberian laporan hasil audit dalam bentuk rekomendasi tindakan perbaikan kepada pihak manajemen objek yang diteliti, untuk kemudian wewenang perbaikan menjadi tanggung jawah manajemen objek yang diteliti apakah akan diterapkan atau hanya menjadi acuan untuk perbaikan di masa yang akan datang

Pertemuan 2

Jenis Pendekatan Audit SI, Kelompok Pendekatan Audit SI, Langkah dari Metode Audit SI, Jenis jenis resiko

2.1. Jenis Pendekatan Audit SistemInformasi

A. Pendekatan temuan *(Exposures Approach*)

B. Pendekatan Kendali (*Control Approach*)

Pesatnya perkembangan dunia komputer , diikuti dengan peningkatan penegetahuan auditor, ternyata mengandung dua perlakuan terhadap komputer , yaitu :

1. Komputer dipergunakan sebagai alat bantu auditor dalam melaksanakan audit.
2. Komputer dijadikan sebagai target audit, karena data di *entry* ke komputer dan hasilnya untuk menilai kehandalan pemrosesan dan keakuratan komputer.

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

2.2.Jenis Audit Sistem Informasi/Teknologi Informasi

Jenis audit Sistem Informasi /Teknologi Informasi antara lain:

a. System Audit Audit terhadap sistem terdokumentasi untuk memastikan sudah memenuhi standar nasional atau internasional

b. *Compliance* Audit Untuk menguji efektifitas implementasi dari kebijakan, prosedur, kontrol dan unsur hukum yang lain

c. Product/*Service* Audit Untuk menguji suatu produk atau layanan telah sesuai seperti spesifikasi yang telah ditentukan dan cocok digunakan

2.3. Kelompok Pendekatan Audit Sistem Informasi

Dalam berjalannya evolusi tersebut, maka munculah pendekatan audit sistem informasi yang dapat dikategorikan kedalam tiga kelompok :

1. *Auditing around the computer*

   Dalam pendekatan audit di sekitar komputer, auditor (dalam hal ini harus akuntan yang registered, dan bersertifikasi akuntan publik) dapat mengambil kesimpulan dan merumuskan opini dengan hanya menelaah struktur pengendalian dan melaksanakan pengujian transaksi dan prosedur verifikasi saldo perkiraan dengan cara sama seperti pada sistem akuntansi manual.

   Kunci pendekatan audit ini ialah pada penelusuran transaksi terpilih mulai dari dokumen sumber sampai ke bagan-perkiraan (akun) dan laporannya.

   Keunggulan metode audit di sekitar komputer adalah:

   a. Pelaksanaan audit lebih sederhana.
   b. Auditor yang memiliki pengetahuan minimal di bidang komputer dapat dilatih dengan mudah untuk melaksanakan audit.

   Kelemahannya adalah jika kondisi (*user requirements*) berubah, mungkin sistem itupun perlu diredesain dan perlu penyesuaian (*update*) program-program, bahkan mungkin struktur data/file, sehingga auditor perlu menilai/menelaah ulang apakah sistem masih berjalan dengan baik.

2. *Audit with the computer*

   Audit dengan komputer untuk kegiatan pendukung dan administrasi paling sering digunakan, bahkan meskipun sistem klien yang diaudit telah berbasis komputer. Selain untuk kegiatan administratif, penyusunan program audit dan kuesioner serta pencatatan-pencatatan dan pelaporan hasil audit, komputer biasanya juga digunakan oleh auditor atau pegawai perusahaan klien untuk

melakukan analisis atau pengikgtisaran, pembuatan grafik dan tabel-tabel tentang hasil audit, sertapemaparan atau presentasi hasil audit (misalnya dengan Microsoft Word, PowerPoint, dan Excel).

3. *Audit throught the computer*

   Dalam pendekatan audit ke sistem komputer *(audit through the computer*) auditor melakukan pemeriksaan langsung terhadap program-program dan file-file komputer pada audit SI berbasis TI. Auditor menggunakan komputer *(software*) atau dengan cek logika atau listing program (*desk test on logic or programs source code*) untuk menguji logika program dalam rangka prngujian pengendalianyang ada pada komputer. Selain itu auditor juga dapat meminta penjelasan dari para teknisi komputer mengenai spefikasi sistem dan/atau program yang diaudit.

Keunggulan pendekatan audit dengan pemeriksaan sistem komputerisasi, ialah:

(a) Auditor memperoleh kemampuan yang besar dan efektif dalam melakukan pengujian terhadap sistem komputer.

(b) Auditor akan merasa lebih yakin terhadap kebenaran hasil kerjanya.

(c) Auditor dapat menilai kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan

Ada 3 kategori strategi ketika *Auditing Through the computer*, yaitu :

1) Test data approach (Test data *)*

Metode ini menggunakan data masukan yang telah dipersiapkan auditor dan menguji data tersebut dengan salinan (copy) dari perangkat lunak aplikasi auditan. Hasil pemrosesan data tersebut akan dibandingkan dengan ekspektasi auditor. Jika ada hasil yang tidak sesuai, mungkin ini suatu indikasi penyimpangan logika atau mekanisme pengendalian.

2) *Paralel simulation*

Pendekatan ini mengharuskan auditor untuk membuat suatu program yang menyimulasikan fungsi utama tertentu dari aplikasi yang sedang diuji.Sedangkan untuk melakukan pengujian substantif (misalnya detail transaksi atau saldo perkiraan),makaauditordapatmemilihteknik:

3) *Embeded audit module approach*

Merupakan suatu teknik dimana satu atau lebih modul program tertentu dilekatkan di suatu aplikasi untuk mencatat secara tersendiri serangkaian transaksi yang telah ditentukan ke dalam file yang akan dibaca oleh auditor

Dalam Merancang organisasi perusahaan perlu memperhatikan dan dipertimbangkan sistem pengendalian internt sebagai berikut :

1. Struktur organisasi yang memisahkan tanggung jawab fungsional secara tegas.
2. Sistem berwenang dan prosedur pencatatan yang memberikan perlindungan yang cukup terhadap kekayaan, utang, pendapatan, dan biaya.
3. Praktek yang sehat dalam melaksanakan tugas dan fungsi tiap unit organisasi
4. Karyawan yang mutunya sesuai dengan tanggungjawab

2.4.Metode Proses Audit Sistem Informasi

Metode dalam proses Audit SI, dapat dilakukan dengan langkah-langkah sebagai berikut :

A. Metode pemahaman
    1. Mendokumentasikan aktivitas yang mendasari control objective demikian juga untuk mengidentifikasi stade control measure/procedure yang berlaku
    2. .Melakukan wawancara dengan manajemen dan staf untuk mendapatkan pemahaman tentang : kebutuhan bisnis dan resikonya, struktur organisasi,

peran dan tanggung jawab, kebijakan *procedure*, hukum dan peraturan, *control measure* yang berlaku, laoran manajemen

3. Mendokumentasikan proses yang berhubungan dengan sumber daya TI terutama yang dipengaruhi oleh proses direview.

B. Evaluasi Kendali

1. Menilai keefektifan *control maesure* yg berlaku atau tingkat pencapaian *control objective* .
2. Mengevaluasi kesesuaian *control measure* dari proses yang direview dengan mempertimbangkan kriteria yg diidentifikasikan dan praktik standar industri, *Critical Success Factor* dan *Control measure* dan mengaplikasikan keputusan profesional audit.
3. Melakukan proses dokumentasi, deliverable yang sesuai dihasilkan, tanggung jawab dan akuntabilitas yang jelas dan efektif, adanya pengendalian kompensasi sebagaimana mestinya
4. Simpulkan sesuai tingkat *Control Objective*

C. Menilai Kepatuhan

1. Menjamin control measure yg ditetapkan , berjalan sebagaimana mestinya, secara konsisten dan berkelanjutan, serta menyimpulkan kesesuaian *control environment.*
2. Mendapatkan bukti langsung dan tidak langsung untuk item / periode yg dipilih untuk menjamin bahwa prosedur telah dipatuhi untuk periode yang direview menggunakan alat bukti langsung dan tidak langsung.
3. Melakukan review terbatas ttg kecukupan proses *deliverable.*
4. Menentukan tingkat pengujian substatif dan kerja tambahan yg dibutuhkan unt menyediakan jaminan proses IT adalah cukup.

D. Penilaian Resiko.

1. Memperkirakan resiko dari control objective yg tidak dipenuhi, dengan menggunakan teknik analitik dan atau mengkonsultasikan sumber sumber alternative.
2. Mendokumentasikan kelemahan kendali, serta ancaman dan kerawanan yang dihasilkan.
3. Mengidentifikasikan dan mendokumentasikan dampak yang potensial maupun aktual.
4. Menyediakan informasi komparatif, misalnya melalui *benchmark*

Secara Garis besar Metodologi dalam Audit SI dan TI akan terdiri atas beberapa tahapan anatara lain :

A. Analisis Kondisi Eksisteing

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

B. Penentuan tingkat resiko

   Dengan mengklasifikasikan proses bisnis yang tingkat resikonya tinggi maupun proses bisnis pendukung. Hasil penentuan tingkat resiko tersebut kemudian dijadikan sebagai bahan dalam penyusunan ruang lingkup pelaksanaan audit yang diarahkan kepada proses bisnis yang didukung oleh TI

C. Pelaksanaan Audit SI/TI dengan mengacu kerangka kerja COBIT yang akan didahului dengan proses penentuan ruang lingkup dan tujuan audit berdasarkan hasil penentuan tingkat resiko pada tahapan sebelumnya.

D. Penentuan rekomendasi beserta laporan dari hasil audit yang dilakukan.

2.4.1. Tinjauan Penting dalam Audit SI/TI

Adapun elemen utama dari aktivitas peninjauan yang dilakukan dalam Audit SI/TI dapat diklasifikasi kedalam tinjauan penting sebagai berikut:

1. Tinjauan terkait dengan fisik dan lingkungan yakni : hal hal yang terkait dengan keamanan fisik, suplai sumber daya, temperatur, kontrol kelembaban dan faktor lingkungan
2. Tinjauan Administrasi sistem yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen database seluruh prosedur administrasi sistem dan pelaksanaannya.
3. Tinjauan Perangkat Lunak. Perangkat lunak yang dimaksud merupakan aplikasi bisnis yang didaat berupa sistem berbasis web untuk pemrosesan permintaan pelanggan hingga ERP yang kini menjadi inti dari proses bisnis diperusahaan.
4. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan sistem, batasan tingkat keamanan, tinjauan terhadap firewall daftar kontrol akses router, port scaning serta pendeteksian akan gangguan maupun ancaman terhadap sistem.
5. Tinjauan Kontinuitas bisnis dengan memastikan ketersediaan prosedur backup dan penyimpanan, dokumentasi dari prosedure tersebut serta dokumentasi pemulihan bencana yang dimiliki.
6. Tinjauan intergritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

2.5. Konsep Resiko dan Jenis-jenis resiko

2.5.1. Konsep Resiko

Agar segala sesuatu berjalan sesuai yang seharusnya, maka perlu ada pengawasan. Salah satu bentuk/cara pengawasan ialah yang disebut system pengendalian intern (internal control system) yang melekat pada system dan prosedur organisasi tersebut.

Pendekatan Audit SI /TI berbasis resiko digunakan untuk menilai resiko dari poses bisnis yang berlangsung diorganisasi atau perusahaan dan yang terpenting dapat membantu pengaudit SI/TI dalam memutuskan metode pengujian yang digunakan dalm pelaksaaan audit nantinya dengan melakukan uji kepatutan atau uji secara substantif

2.5.2. **Jenis Jenis Resiko**

Adapun Jenis jenis resiko sebagai berikut :

1. **Risiko Bisnis (*Bussiness Risks*)**

   Risiko bisnis adalah risiko yang dapat disebabkan oleh faktor-faktor intern maupun ekstern yang berakibat kemungkinan tidak tercapainya tujuan organisasi (*business goals objectives).*

   a. **Risiko *ekstern*** *(risk from externa*l *environment*) ialah misalnya antara lain perubahan kondisi perekonomian tingkat kurs yang berubah mendadak, dan munculnya pesaing baru yang mempunyai potensi bersaing tinggi

   b. **Risiko *internal*** *ialah* risiko yang berasal dari internal misalnya antara lain permasalahan kepegawaian, risiko-risiko yang berkaitan dengan peralatan atau mesin, risiko keputusan yang tidak tepat, dan kecurangan manajemen (Manajement Fraud)

2. **Risiko Bawaan (*Inherent Risks*)**

Risiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan, jika tidak ada pengendalian intern. Misalnya kegiatan kampus, apabila tidak ada absensi/daftar kehadiran kuliah akan banyak mahasiswa yang cenderung tidak disiplin hadir mengikuti kuliah.

Inherent risk atau resiko bawaan merupakan resiko kesalahan audit yang merupakan aktivitas bawaan dari proses bisnis.Resiko kesalahan tersebut bersifat indenpenden dan akan semakin tinggi jika *compensating control* tidak tersedia.

3. **Risiko Pengendalian (*Control Risks*)**

Dalam suatu organisasi yang baik seharusnya sudah ada risks assessment, dan dirancang pengendalian intern secara optimal terhadap setiap potensi risiko. Risiko pengendalian ialah masih adanya risiko meskipun sudah ada pengendalian.

Control Risk atau resiko kontrol merupakan resiko kesalahan yang tidak terdeteksi oleh kontrol internal itu sendiri selama proses audit berlangsung. Resiko kontrol tersebut menjadi rendah jika prosedur validasi tersedut dilakukan secaraterkomputerisasi.

Risiko pengendalian tidak pernah mencapai keyakinan penuh bahwa semua salah saji material akan dapat dideteksi ataupun dicegah. Risiko pengendalian merupakan fungsi dari efektivitas struktur pengendalian inter. Semakin efektif struktur pengendalian intern perusahaan klien, semakin kecil risiko pengendaliannya. Penetapan risiko pengendalian didasarkan atas kecukupan bukti audit yang menyatakan bahwa struktur pengendalian inter klien adalah efektif. Ada dua macam risiko pengendalian, yaitu:

1. *Actual level of control risk Assessed level of control risk* yang ditentukan dengan melakukan modifikasi prosedur untuk menghimpun pemahaman struktur pengendalian intern terkait dengan asersi, dan prosedur untuk melaksanakan test of control. Pada saat perencanaan audit, auditor menentukan besarnya risiko pengendalian yang direncanakan untuk setiap asersi yang signifikan.
2. *Planned assessed level of control risk* ini ditentukan berdasar asumsi tentang efektivitas rancangan dan operasi struktur pengendalian intern yang relevan.

4. **Risiko Deteksi (*Detection Risks*)**

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 auditor ternyata dalam prosedur auditnya tidak dapat mendeteksi terjadinya *existing control failures* (system pengendalian intern yang ada ternyata tidak berjalan baik).

5. Audit (*Audit Risks*)

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

Ada Pun rumus mengetahui Resiko Audit dengan rumus dibawah:

Model Risiko Audit (audit risk) yang paling lumrah digunakan (dan diajarkan) adalah: **AR = IR x CR x DR**

Dimana:

AR = Audit Risk

IR = Inherent Risk

CR = Control Risk

DR = Detection Risk

Mengenai jenis – jenis risiko, dalam bukunya yang berjudul Accounting Information System, F.L. Jones dan D.V. Rama (2003,p127-134) tidak membahas masalah business risk, tetapi menyebut risiko – pelaksanaan (execution risks) yang mungkin lebih sempit ruang lingkupnya. Jones dan Rama berpendapat risiko pada hakekatnya dapat dikelompokkan kedalam 4 jenis risiko, yaitu execution risks, information risks, asset protection risks, dan performance risks.

1. Execution risk

   Execution risk adalah risiko yang berkaitan dengan tidak tercapainya sesuatu yang seharusnya dilaksanakan.

2. Information risk

   Risiko informasi yang dimaksud oleh Jones dan Rama ini ialah risiko yang berkaitan dengan kemungkinan kesalahan atau penyalahgunaan data informasi. Risiko terjadi waktu mencatat/entri data (recording risks) serta updating risks.

3. Asset protection risk

   Risiko yang berkaitan dengan save guarding assets ini ialah kerusakan, hilang, atau asset tidak digunakan seperti yang seharusnya, maupun risiko yang dapat timbul terhadap assets perusahaan akibat keputusan yang salah.

4. Performance Risk

   Risiko kinerja ini adalah resiko berkaitan dengan kinerja pegawai/ kinerja perusahaan yang tidak dapat dilaksanakan sesuai tujuan/standar/ukuran yang ditetapkan. Pada hakekatnya yang bertanggung jawab dan akan mempertanggung jawabkan pengelolaan perusahaan kepada para share/stockholder dan stakeholder adalah para pengurus perusahaan, yang

menurut Undang-undang Perseroan Terbatas di Indonesia ialah para anggota Dewan Direksi dan anggota Dewan Komisaris.

Dalam pelaksanaan kegiatan sehari-hari, yang melakukan tugas operasional ialah para manajer tingkat menengah, supervisor, staf dan pegawai pelaksana, yang melaksanakan tugas sesuai dengan kebijakan yang ditetapkan pimpinan. Jika mereka tidak melakukan tugas sesuai dengan yang seharusnya, atau kalau kinerjanya tidak sesuai dengan yang seharusnya. Hal ini merupakan risiko yang dipreventif, dideteksi, atau dikoreksi/diperbaiki.

Audit resiko merupakan risiko kemungkinan auditor ekstern memberikan opini yang salah terhadap fairness laporan keuangan auditee, atau temuan dan rekomendasi yang salah pada laporan hasil pemeriksaan auditor intern. Risiko ini sangat berbahaya karena auditor sudah memberikan opini atau rekomendasi bahwa "Things are okay and fine, but they are not"

Efek Risiko dalam sistem informasi ditemui pada:

1. Strategi (Strategic): risiko dimana sistem informasi tidak sesuai dengan tujuan organisasi dan tidak mendukung pencapaian misi.
2. Operasi (Operations): risiko dimana sistem informasi menimbulkan beban yang terlalu besar bagi organisasi. Selain itu ketergantungan organisasi terhadap suatu sistem informasi berarti apabila sistem tersebut tidak tersedia selama waktu tertentu dapat menimbulkan risiko besar bagi operasional.
3. Pelaporan (Reporting): risiko dimana sistem informasi tidak dapat diandalkan untuk menghasilkan informasi yang akurat, lengkap dan tepat waktu.

4. Kepatuhan (Compliance): risiko dimana sistem informasi malah menimbulkan pelanggaran hukum dan regulasi yang merugikan bagi organisasi baik secara finansial maupun reputasi.

Keterkaiatan antar Tujuan Bisnis dan TI akan dipaparkan dengan mengacu pada kerangka kerja COBIT. Kerangka kerja tersebut memberikan pemetaan keterkaitan antara tujuan bisnis dengan tujuan TI sehingga dapat dijadikan acuan bagi perusahaan dalam menerjemakan kebutuhan bisnis akan tersediaan TI.

PERTEMUAN 3

Pengertian Sistem Pengendalian Internal, Sistem pengendalian Umum, Jenis-jenis pengendalian, Pengendalian Pucuk Pimpinan, Jenis Perancangan pengendalian, Struktur Organisasi Fungsi Sistem Informasi, Perancangan Sistem, Interaksi Manusia dan komputer

3.1. Pengertian Sistem Pengendalian Internal

Dari beberapa referensi yang kita pelajari kita dapat mengetahui bahwa sampai pada awal abad 19 terminologi Internal Control System belum merupakan konsep yang dipahami meluas. Sebelumnya yang lebih dikenal adalah internal check, maksudnya ialah kegiatan klerikal pemeriksaan akurasi (kecermatan) book keeping yang pada saat ini lazimnya disebut verifikasi "independen" (pemeriksaan ulang secara independen, artinya orang atau unit lain bukan yang mengerjakan pertama).

Sistem Pengendalian Internal (Internal Control System) dalam sistem informasi dapat di kelompokkan dalam beberapa kategori , berdasarkan Jenis :

1. reventive Detective, Dan Corrective (Pencegahan, Deteksi Dan Koreksi)
2. Discretionary Dan Non-discretinary (Kebikjakan Dan Kebebasan)
3. Volumtary Dan Mandated (Sukarela Atau Diwajibkan)
4 Manual Atau Automated (Control Secara Manual Atau Dengan Computer)
5 Kontrol Perspektif Manajemen Dan Perspektif Teknis
6. Application Dan General Controls.

Menurut Gramling, Ri0enberg, dan Johnstone (2012: 208), "Internal control is a process related to the achievement of the organiza5on' s objec5ves. Organiza5ons iden5fy the risks to achieving those objec5ves and implement various controls to

mi5gate those risks". Pengendalian internal diperlukan untuk mengidentifikasi risiko agar proses bisnis perusahaan tidak terganggu.

Pengendalian Internal adalah Pengendalian dalam suatu organisasi bertujuan untk menjaga aset perusahaan, pemenuhan terhadap kebijakan dan prosedur, kehandalan dalam proses dan operasi yang efesien.

3.1.1 **Tujuan Pengendalian internal.**

Tujuan disusunnya system control atau pengendalian internal komputer adalah sebagai berikut:

1. Meningkatkan pengamanan (improve safeguard) aset sistem informasi (data/catatan akuntansi (accoun5ng records) yang bersifat logical assets, maupun physical assets seperti hardware, infrastructures, dan sebagainya).
2. Meningkatkan integritas data (improve data integrity), sehingga dengan data yang benar dan konsisten akan dapat dibuat laporan yang benar.
3. Meningkatkan efekAfitas sistem (improve system effec5veness).
4. Meningkatkan efisiensi sistem (improve system efficiency).

Tujuan sistem pengendalian internal direncanakan atau dirancang dengan tujuan untuk :

1. Menjaga kekayaan organisasi,
2. Mengecek keteliAan dan kehandalan data akuntasi,
3. Mendorong efisiensi,
4. Mendorong dipatuhinya kebijakan manajemen

3.2. Sistem Pengendalian Umum

Menurut Sawyer, Di0enhofer, & Scheiner (2005, hal. 549), general control consist of those controls in the IS and user environment that are pervasive over all or most applica5on. They include such controls as segrega5on of incompa5ble du5es, system

development procedures, data security, all administra5ve controls, and disaster recovery capabili5es.

Pengendalian umum didefinisikan sebagai sistem pengendalian internal komputer yang berlaku umum meliputi seluruh kegiatan komputerisasi sebuah organisasi secara menyeluruh. Artinya ketentuan – ketentuan dalam pengendalian tersebut berlaku untuk seluruh kegiatan komputerisasi yang digunakan di perusahaan tersebut.

Sistem pengendalian Umum yaitu manajemen menetapkan kebijakan yang dirumuskan untuk melaksanakan didalam organisasi atau perusahaan, setiap orang melaksanakan kebijakan ini dengan memberikan tanggung jawab untuk setiap pekerjaannya, dalam batasan yang telah ditetapkan dalam suatu peraturan.

Pengendalian umum (general control) adalah sistem pengendalian intern computer yang berlaku umum meliputi seluruh kegiatan komputerisasi sebuah organisasi secara menyeluruh. artinya ketentuan– ketentuan yang di atur dalam pengendalian intern tersebut berlaku untuk seluruh kegiatan komputerisasi pada organisasi / perusahaan tersebut.

Pengendalian umum adalah merupakan " Payung" atau kebijakan umum pengendalian dalam suatu organisasi , apabila tidak dilakukan pengendalian dapat berakibat negative terhadap aplikasi atau kegiatan komputerisasi organisasi . Pengendalian umum adalah kebijakan umum pengendalian dalam suatu suatu organisasi, apabila tidak dilakukan pengendalian dapat berakibat negative terhadap aplikasi atau kegiatan komputerisasi oraganisasi atau perusahaan.

Karena Pengendalian umum mengatur seluruh seluruh kegiatan perusahaan yang berkaitan dengan komputerisasi / teknologi informasi maka keputusan pengendalian jenis ini merupakan wewenang atau domain manajemen (bersifat

manajemen framework) dan oleh sebab itu beberapa textbook tidak menggunakan istilah pengendalian umum, melainkan Pengendalian Perspektif Manajemen.

Oleh karena pengendalian umum ini menyangkut seluruh kegiatan komputerisasi pada suatu organisasi, maka berwenang menentukan struktur pengendalian adalah pimpinan organisasi tersebut,atau dalam prakteknya wewenang tersebut didelegasikan kepada kepala unit komputer

Ikatan Akutansi Indonesia (IAI,2001,SA319, par.06 mengkelasifikasikan pengendalian umu sebagai berikut :

a) Pengendalian organisasi dan manajemen

b) Pengendalian terhadap pengembangan dan pemeliharaan sistem aplikasi

c) Pengendalian terhadap pengembangan operasi sistem

d) Pengendalian terhadap perangkat lunak sistem

e) Pengendalian terhadap TI (Pengolahan Data Elektronis)

3.2.1. Ruang lingkup Pengendalian Umum

Ruang lingkup yang termasuk dalam pengendalian umum (pengendalian perspektif manajemen) diantaranya adalah :

1. Pengendalian manajemen puncak (top management controls).
2. Pengendalian manajemen pengembangan sistem (information system management controls).
3. Pengendalian manajemen sumber data (data resources management controls).
4. Pengendalian manajemen operasi (operations management controls).
5. Pengendalian manajemen keamanan (security administration Management controls).

6. Pengendalian manajemen jaminan kualitas (quality assurance management controls).

3.3.Jenis-jenis pengendalian

Jenis Pengendalian Umum dan katergori pengendalian:

1. Organisasi dan Manajemen
    a) Pemisahan fungsi Depertemen TI dan Non TI
    b) Pemeriksaan fungsi dalam Depertemen TI
    c) Otorisasi Tranksasi
    d) Pengendalian Porsonil
    e) Perencanaan , Penganggaran dan sistem pembebasan kepada pemakai (user)
2. Piranti Lunak Dan Keras
    a) Pengendalian Piranti Keras (Hardware)
    b) Pengendalian Piranti Lunak (Software)
3. Pengendalian Akses
    a) Pembatasan Akses fisik dan Lojik
    b) Dokumentasi Program
    c) Fasilitas- Fasilitas On-line
4. Data dan Procedur
    a) Control Group
    b) File dan database
    c) Procedur- procedure standar
    d) Keamanan fisik
    e) Pemeriksaan Interen
5. Pengembangan Sistem Baru

a) Partisipasi manajemen dan Pemakai

b) Pengembangan Standar & pedoman

c) Manajemen Proyek

d) Pengujian sistem dan konversi

e) Penelaahan setelah pemasangan

6. Pemeriharaan Program

a) Otorisasi dan persetujuan

b) Prosedur standar dan dekomentasi

c) Pengendalian pemrogram dan pelaksanaan

d) Pengujian terhadap perubahaan

7. Dokumentasi

a) Dokumentasi standar dan dekomentasi pendefinisian masalah

b) Dokumentasi sistem

c) Dokumentasi program

d) Dokumentasi operasional

e) Domentasi pemakai

3.4.**Pengendalian Pucuk Pimpinan**

Pengendalian pucuk pimpinan adalah sistem pengendalian intern yang ada pada suatu organisasi yang mendorong keterlibatan, kepedulian dan tanggung jawab pucuk pimpinan organisasi terhadap kegiatan TI pada organisasi .

Pucuk pimpinan (Top management) adalah board of director atau di sebut direksi, terdiri dari direktur utama dan para direktur lainnya. Direksi bertanggung jawab terhadap seluruh operasi perusahaan , termasuk bidang Teknologi Informasi

Bagaimana Auditor menganalisa perhatian / kepedulian top management terhadap fungsi sistem informasi? Salah Satu cara yang dapat di lakukan adalah dengan melihat bagaimana Top Management terkait dengan sistem Informasi seperti layaknya tugas pokok dan fungsi management pada umumnya.

3.4.1. Fungsi Internal Auditor.

Seorang auditor TI sebaiknya mampu melakukan pekerjaan-pekerjaan sebagai berikut:

1. Mengevaluasi pengendalian atas aplikasi-aplikasi tertentu, yang mencakup analisis terhadap risiko dan pengendalian atas aplikasi-aplikasi seperti e-business, sistem perencanaan sumber daya perusahaan.
2. Memberikan asersi (assurance) atas proses-proses tertentu, seperti audit dengan prosedur-prosedur tertentu yang disepakat bersama dengan auditee mengenai lingkup asersi.
3. Memberikan asersi atas akAfitas pengolahandata pihak ketiga dengan tujuan untuk memberikan asersi bagi pihak lain yang memerlukan informasi mengenai aktifitas pengendalian data yang dilakukan oleh pihak ketiga tersebut.
4. Pengujian penetrasi, yaitu upaya untuk mengakses sumber daya informasi guna menemukan kelemahan-kelemahan yang ada dalam pengolahan data tersebut. Memberikan dukungan atas pekerjaan audit keuangan yang mencakup evaluasi atas risiko dan pengendalian TI yang dapat mempengaruhi kehandalan sistem pelaporan keuangan.
5. Mencari kecurangan yang berbasis TI, yaitu menginvestigasi catatan-catatan

komputer dalam invesAgasi kecurangan.

3.5. **Jenis Perancangan pengendalian**

Top Management bertanggung jawab untuk membuat master-plan sistem informasi, meliputi rencana jangka Panjang& jangka pendek .

Penyusunan Rencana meliputi 3 hal :

1. Mengetahui kesempatan dan masalah yang di hadapi organisasi sehingga teknologi informasi dan system Informasi dapat di gunakan secara efektif.
2. Mengindentifikasi sumber daya yang di perlukan untuk menyedikan Teknologi dan sistem informasi yang di perlukan.
3. Membuat strategi dan takti yang di perlukan untuk memperoleh sumber daya tersebut

Jenis perancangan pengendalian dibedakan dalam 2 jenis, yaitu :

1. *Strategi Plan*

   Strategi Plan bersifat jangka anjang dan berisi dibawah ini :

   a) Penilaian terhadap kondisi teknologi informasi saat ini, kekuatan kelemahan, serta, tantangan dan ancaman saat ini.
   b) Tujuan atau arah jangka panjang, jasa informasi masa depan harus disediakan, strategi keseluruhan terhadap intra organisasi maupun interorganisasi.
   c) Strategi pengembangan, visi dibidang teknologi informasi, aplikasi masa depan, kebutuhan dana, pendekatan dan monotoring terhadap pelaksanaan strategi.

2. *Operational Plan,*

   Operational Plan (Rencana Jangka Pendek) :

a) Progress report berisi keterangan tentang keberhasilan dan kegagalan pencapaian rencana sekarang. Perubahaan yang besar terhadap *platform hardware-software*, hal-hal yang baru harus di lakukan.

b) *Initiatives to be undertaken*, berisi keterangan tentang perkembangan sistem perubahaan *hardware-soft ware,* tambahan karyawan dan pengembangannya, penambahaan sumber daya keuangan.

c) *Implementation Scheduler*, berisi keterangan tentang kapan mulai selesainya, setiap proyek utama , kejadian yang penting, prosedur control , proyek yang di terapkan.

3.6. Perencanaan Sistem

Rancangan sistem adalah penentuan proses dan data di perlukan oleh sistem baru, jika sistem itu berbasis komputer, rancangannya dapat menyertakan spesifikasi jenis peralatan yang digunakan. Perencanaan Sistem terdiri dari kegiatan- kegiatan desain untuk menghasilkan spesifikasi sistem yang dapat memenuhi kebutuhan fungsional yang dikembangkan ke dalam proses analis sistem.

Jadi dengan demikian perancangan sistem merupakan proses-proses atau aktivitas-aktivitas untuk menentukan atau menghasilkan speksifikasi system yang diperlukan oleh sistem baru yang memenuhi kebutuhan fungsional dengan tujuan untuk memberikan gambaran secara umum oleh pemakai pada sistem yang baru.

Menurut O'Brien (2005p351) perancangan sistem terdiri dari tiga aktivitas yaitu :

a. *Desain User Interface,* yaitu merancang layar, Formulir dan dialog
b. Desain Data yaitu menentukan *entitiy* (Objek), atribut , relationship , kaidah intregritas dan lain –lain
c. Desain Proses yaitu membuat program dan prosedur seperti *user services, application services, dan data Services*

Interaksi manusia dan komputer(Imk) merupakan disiplin ilmu yang mempelajari mengenai suatu hubungan diantara manusia dan komputer yang diantaranya itu meliputi perancangan, evaluasi, serta implementasi antarmuka pengguna komputer supaya dapat mudah digunakan oleh manusia. Sedangkan *interaksi manusia dan komputer* itu juga merupakan serangkaian proses, dialog serta kegiatan(aktivitas) yang dilakukan oleh manusia untuk dapat berinteraksi dengan komputer dengan secara interaktif untuk dapat melaksanakan serta menyelesaikan tugas yang diinginkan.

Menurut Shneiderman dan Plaisant (2010, p22), Interaksi Manusia dan Komputer (IMK) adalah disiplin ilmu yang berhubungan dengan perancangan, evaluasi, dan implementasi sistem komputer interaktif untuk digunakan oleh manusia. Titik berat IMK adalah perancangan dan evaluasi antarmuka pemakai (*user interface*). Antarmuka pemakai adalah bagian sistem komputer yang memungkinkan manusia berinteraksi dengan komputer.

Menurut Pressman (2001, p20-29) rekayasa Software adalah aplikasi dari pendekatan kuantifiabel, displin, dan sistematis pada pengembangan, operasi, dan pemeliharaan perangkat lunak, salah satu model rekayasa perangkat Lunak yang di sebut Linear Sequential Model yang biasa disebut dengan Classic Life Cycle atau Waterfall Model.

Dalam model ini pendekatan pengembangan software di lakukan sistematik dan sequential yang di awali dengan System Enginering, Analysis, Design, Coding, Testing dan Maintanence.

3.7.Struktur Organisasi Fungsi Sistem Informasi

Secara umum sistem informasi di letakan pada fungsi depertemen sistem informasi, di dalam depertemen Ini berisi bagian pengembangan sistem. Bagian

programming, bagian pengeoprasian , penyiapan data dan bagian Pendukung atau control.

Stuktur Organisasi pusat komputer secara Tradisional terdiri dari :

1. Bagian Aplikasi (terdiri dari para sistem analis dan Programmer)
2. Bagian Produksi (terdiri dari para Operator yang secara langsung menjalankan operasional computer
3. Bagian dukungan Teknis (terdiri dari para Spesialis Operating sistem, ahli

Dalam control terhadap pemakai jasa sistem informasi , Top Manager harus menbuat policy dan Prosedur yang akan membuat user menggunakan jasa sistem informasi secara Efektif dan Efisien.

3.7.1. Pengendalian Manajemen Pengembangan Sistem

Pengendalian, pengembangan dan pemeliharaan sistem diperlukan untuk mencegah dan mendeteksi Kemungkinan kesalahan pada waktu pengembangan dan pemeliharaan sistem, serta untuk menperoleh keyakinan memadai bahwa sistem berbasis teknologi informasi di kembangkan dan di pelihara dengan cara efesien dan melalui proses otorisasi dengan semestinya.

Pengendalian pengembangan sistem adalah sebagai berikut :

1.Pengembang sistem harus melibatkan partisipasi pemakai, manajemen,auditor

2. Adanya standard dan pedoman maupun prosedur

3.Dilaksanakannya pengujian sistem dan konversi dengan cermat.

4.Penelaahan setelah pemasangan atau instalasi .

3.8.Interaksi Manusia dan komputer

Dalam merancang suatu sistem harus di perlukan satu hal sangat pentng yaitu interaksi anatara user /pengguna dengan sistem. Interaksi ini haruslah user friendly,

yang artinya mudah di gunakan oleh pengguna yang awan sekalipun. (Shneiderman ,1998,pp 74-75).

Dalam merancang suatu sistem interkasi manusia dengan dan komputer yang baik , maka ada delapan (8) aturan yang diperhatikan :

1. Konsisten dalam warna, tampilan, jenis huruf, perintah/ menu
2. Memungkinkan *Frequent users* menggunakan shortcuts, penggunaan shortcuts untuk memudahkan Pemakai saat berintraksi dengan komputer sehingga perintah dan fasilitas yang tersedia lebih mudah di mengerti dan lebih cepat di akses.
3. Memberikan umpan balik yang imformatif, setipa aksi pemakai sebaliknya ada umpan balik dari system dan umpan balik (respon) atau message di layar , harus di buat sederhana agar mudah di megerti untuk menetukan langkah selanjutnya.
4. Merancang dialog yang baik, dari awal sampai penutupan. urutan dari aksi sebaliknya di atur dengan baik yaitu dengan pembukaan , isi dan penutup.
5. Memberikan pencegahan dan penanganan kesalahan yang sederhana sebisa mungkin rancangan sistem di buat agar pemakai tidak menbuat kesalahan contohnya jika suatu kolom isian tidak di perbolehkan pengisian jenis alphabet , maka jika di isi alphabet layar harus segera menberikan error message.
6. Memungkinkan pembalikan aksi yang mudah, dalam merancang sistem sebaiknya aksi dapat dikembalikan . pengembalian aksi dapat berupa aksi tunggal, tugas entry atau kelompok yang lengkap.
7. Mendukung pusat kendali internal, pemakai dapat mengusai sistem , dan sistem merespon intruksi-Intruksi dari mereka.

8. Mengurangi beban ingatan dari jangka pendek, manusia memiliki keterbatasan dalam meningat memory singkat, tampilan halaman yang banyak menggabungkan frekuensi gerakan window sebaliknya dikurangi, buatlah tampilan sederhana, dengan menyediakan penyingkatan kode dan informasi lain.

3.9.System Development Life Cycle Approach

System development life cycle approach adalah metode pengembahan sistem aplikasi yang terdiri dari beberapa tahap, setiap tahap mempunyai jenis kegiatan tertentu :

a. *Feasibility Study*

   Dengan kriteria *cost benefit* untuk mengusulkan aplikasi.

b. *Information Analysis*

   *M*enentukan keperluan user

c. *Sistem Design*,

   Mendesain *user interface* , file yang di gunakan dan fungsi proses informasi yang di lakukan oleh sistem.

d. *Program Development*

   Design, *codding*, compiling, *testing*, dan dokumentasi program

e. *Procedures And From Development*

   Desain dan dokumentasi prosedur sistem dan formulir yang di gunakan user pada sistem.

f. *Acceptance Test*

   Testing terakhir terhadap sistem dan persetujuan formal serta penerimaan oleh management dan user.

g. *Conversion*

Konversi atau perubahan dari sistem lama ke sistem baru

h. *Operation and maintance*

Penambahan sistem selama implementasi dan modifikasi serta maintances bila di ketahui ada masalah

PERTEMUAN 4

Sistem berbasis Teknologi Informasi, Tugas data Adiministration (DA) dan database administrator (DBA), Definisi Database, Database Intergrity, Konsep dan kontrol dan Audit PL

4.1. Sistem berbasis Teknologi Informasi

Di dalam suatu sistem berbasis teknologi informasi, pengendalian sumber data yang baik adalah :

a. User harus dapat berbagi data

b. Data harus tersedia di gunakan kapan saja, dimana pun, dan dalam bentuk apa pun.

c. Sistem manajemen data harus menjamin adanya sistem penyimpanan yang efisien tidak terjadi redundancy data , adanya data security

d. data harus dapat di modifikasi dengan mudah.

Setiap organisasi tentu mengakui bahwa data merupakan sumber daya yang kritis dan harus di kelolah dengan baik , karena itu kita mencari cara untuk menangani sistem manajemen data . Solusi teknis adalah dengan database management sistem (DBMS) dan data repository system (DRS) , selain itu di perkenalkan dua keahlian penting yaitu data administration (DA) dan database administrator (DBA)

4.2. Tugas data Adiministration (DA) dan database administrator (DBA)

Database administrator adalah orang yang bertugas untuk menyimpan dan mengelola data perusahaan dengan menggunakan jenis perangkat lunak khusus. Data yang dimaksud dapat mencakup berbagai informasi seperti data finansial, informasi sensus, akun pengguna.

Seorang database administrator atau DBA akan memastikan bahwa data-data yang ada dalam perusahaan tadi tersedia, tersimpan dengan baik dan aman agar tidak hilang atau diakses oleh orang-orang yang tidak memiliki kepentingan.

Seorang data administrator memiliki peran dan tugas yang beragam di dalam perusahaan. Beberapa tanggung jawab dan tugas database administrator adalah:

1. Mengevaluasi pembelian software database
2. Melakukan pengawasan terhadap modifikasi dari software database yang ada untuk memenuhi kebutuhan employer
3. Menjaga integritas dan kinerja basis data perusahaan
4. Menjamin bahwa data disimpan dengan aman dan optimal
5. Memberi tahu end user tentang perubahan dalam database dan melatih mereka cara untuk memanfaatkan sistem
6. Membuat user accounts baru dan perizinan
7. Menguji modifikasi pada struktur database
8. Mengoptimalkan sistem database dengan menginstal pembaruan secara teratur
9. Memperbarui program anti virus di server database secara teratur
10. Mendiagnosis masalah yang ada pada sistem database dan memecahkan masalah tersebut
11. Menggabungkan database lama
12. Melakukan perencanaan kapasitas
13. Memantau perangkat keras dan sistem operasi server database
14. Membuat back up dan memulihkannya untuk mencegah kehilangan data

4.2.1. **Jenis-jenis *database administrator***

Ada jenis database administrator serba guna yang melakukan semua jenis pekerjaan yang terkait dengan administrasi data. Yaitu:

1. System database administrator.

   Bertanggung jawab atas aspek fisik dan teknis dari database seperti menginstal upgrade dan patch untuk memperbaiki bug program. Biasanya jenis database administrator ini memiliki latar belakang dalam arsitektur sistem dan bertugas memastikan bahwa database di sistem komputer berfungsi dengan baik.

2. Application database administrator.

   Fokus mendukung database yang telah dirancang untuk aplikasi atau serangkaian aplikasi tertentu seperti software customer service.

4.2.2. Pemahaman yang baik terhadap tugas DA dan DBA karena alasan berikut :

1. Jika DA dan DBA tidak bekerja baik, maka keamanan harta , keutuhan data efektivitas dan efesiensi system pada lingkungan database dapat rusak berat.
2. DA dan DBA , merupakan sumber daya yang penting untuk memberikan informasi tentang kekuatan dan kelemahan lingkungan database, karena mereka merupakan pusat kmunikasi antara pemakai dan database

Fungsi pengeloaan sumberdaya data dilakukan oleh Data Administrator (DA) dan Database Administrator (DBA). Kedua administrator ini melakukan fungsi pendefinisian data, pencatatan data, perbaikan data, penghapusan data, penyajian data, pendidikan dan pelayanan pemakai, pengamanan data, dan memonitor penggunaan data. Antara DA dan DBA memeran tugas yang berbeda dalam menjalankan fungsi tersebut.

1. Definiting (pendefinisian) data

   Fungsi DA yaitu menentukan kebutuhan pengguna guna menetapkan definisi skema eksternal dan konseptual. Sedangkan fungs DBA yaitu menentukan definisi skema internal yang lebih banyak berhubungan dengan programer.

2. Creating (pencatatan) data

   Fungsi DA adalah memberitahukan pengguna tentang prosedur pengumpulan data, cara memeriksa, dan validasi. Sedangkan fungsi DBA adalah menyiapkan program untuk membuat data.

3. Redefining / restructuring (perbaikan) data

   Fungsi DA adalah menetapkan definisi baru skema konseptual, skema eksternal dan membuat pengguna nyaman dengan konsep baru tersebut. Sedangkan fungsi DBA adalah menetapkan definisi skema internal yang baru, megubah database agar sesuai dengan definisi skema yang baru.

4. Retiring (pebuangan) data

   Fungsi DA adalah menetapkan kebijakan retiring data atau membuang data yang tidak diperlukan. Sedangkan fungsi DBA adalah melakukan kebijakan retirement atau memisahkan data yang sudah tidak digunakan lagi.

5. Making database available to users (penyajian data)

   Fungsi DA adalah menentukan peralatan yang dibutuhkan user, menguji dan mengevaluasi peralatan tersebut. Sedangkan fungsi DBA adalah menentukan peralatan yang dibutuhkan programmer, menguji dan mengevaluasi peralatan tersebut.

6. Informing and servicing users (Pelatihan dan pelayanan pemakai).

   Fngsi DA adalah menjawab pertanyaan user dan mendidik user, menyampaikan informasi tentang kebijakan dan menyediakan informasi

tentang skema konseptual dan skema eksternal. Sedangkan fungsi DBA adalah menjawab pertanyaan programmer dan mendidiknya, menyiapkan skema internal.

7. Maintaining database integrity (Memelihara dan menganankan data).

   Fungsi DA adalah mengembangkan dan mengumumkan standar mutu organisasi, membantu pengguna untuk merumuskan aplikasi . Sedangkan fungsi DBA adalah melakukan pengendalian database, membantu programmer untuk merancang dan emngimplementasikan kontrol aplikasi.

8. Monitoring operations (memonitor pemakain data). Fungsi DA adalah mengawasi aktivitas pengguna dalam pemakaian database. Sedangkan fungsi DBA adalah mengawasi aktivitas programmer dalam pemakaian database, mengumpulkan tenaga kerja dan memperbaiki database.

Penyimpangan oleh DA dan DBA:

1) Ketidak kompetenan dalam menjalankan peran DA dan DBA, adanya resiko DA dan DBA tidak mampu menjalankan perannya, jadi auditor harus memastikan adanya pengendalian manajemen.
2) DA dan DBA mempunyai peluang untuk melakukan penyelewengan karena DA dan DBA mempunyai kekuasaan dalam fungsi komunikasi dan koordinasi pada lingkungan database.
3) Adanya alat yang dapat digunakan untuk mengabaikan kontrol

Cara mengatasi exposure DA dan DBA:

1. Menempatkan jabatan DA dan DBA dengan tepat
2. Perlu adanya pelatihan bagi DA dan DBA
3. Adanya pemisahan tugas yang jelas bagi DA dan DBA

4.3. Definisi Database

Pada sistem database ada tiga tipe pendefinisian yang harus di lakukan yaitu :

a. External schema, sebuah schema eksternal menperlihatkan keterangan tentang pandangan pemakai terhadap database sebagai suatu objek/ entity , attribute dari objek/ entity , data integrity costains pada objek / entity yang di minta oleh pemakai , karena banyak pemakai maka eksternal skema ini juga banyak

b. Conceptual schema : skema ini memperlihatkan database dari perspektif users, Isi skema konsep adalah semua objek / entity yang ada pada database , semua attribute , semua hubungan antara objek/entity dan semua integrity constraint pada objek / entity

c. Internal Schema : skema ini menunjukkan peta database (Map) ke fisik media penyimpanan , Hal ini berisi records, fields.access paths, dan proses yang di gunakan untuk menggambarkan objek / entity , attribute objek relasi/ hubungan antara objek/entity seperti yang di cantumkan pada skema konseptual.

4.4. Database Intergrity

Integritas data (Everest ,1986) mengidentifikasi ke dalam 6 hal yang harus di lakukan oleh DA dan DBA untuk Mengontrol aktivitas mereka , yaitu :

a. *Definition Control* : DA dan DBA menetapkan control untuk memastikan bahwa database selalu sesuai dengan definisinya ,DA mengembangkan dan menyebar luaskan standar definisi data yang telah di buat dan melakukan pengawasan terhadap pencapaian standar tersebut.

b. *Existence control* : DA dan DBA melakukan pengamanan terhadap database yang ada dengan melakukan backup dan recovery yang di perlukan .

c. *Access control* : control akses, seperti password , mencegah kelalaian atau memperlihatkan data yang tidak seharusnya pada database.. berbagai akses level control di perlukan untuk jenis data . group jenis data , dan file , untuk mencegah hal yang tidak sama , pemisahan fungsi harus di lakukan agar orang yang memiliki akses control pada semua level tidak sama.

d. *Update control* : membatasi pengubahaan database hanya oleh user database yang sah saja. Otorisasi update terdiri dari dua hal : penambahaan database pada database dan wewenang untuk mengubah dan menghapus data yang ada.

e. *Concurrency control* (pemakaian simultan) , integritas data dapat bermasalah, bila satu data yang sama di akses oleh dua proses dalam waktu yang bersamaan , jika akses bersama-sama tidak di atur , database dapat menjadi error

f. *Quality control* : control kwalitas bertugas untuk memastikan keakuratan data , kelengkapan, dan konsisitensi data yang maintance pada database.

g. Auditor harus melakukan wawancara dengan DA dan DBA untuk mengetahui bagaimana control yang Mereka lakukan untuk mengawasi keutuhan database . auditor juga harus mewawancara pemakai database Untuk menentukan level peringatan terhadap control itu.

Strategi Implementasi pengintegrasian Tiga strategi utama dari implementasi dan integrasi modul adalah sebagai berikut:

1. Top-Down, strategi ini digunakan jika, modul level atas (high-level modules) dibuat (coding), di test, dan diintegrasikan sebelum modul level bawah (low-level modules). Keuntungannya adalah kesalahan pada modul level atas dapat teridentifikasi lebih dini, kerugiannya adalah pada saat uji coba program akan menemui kesulitan ketika modul level bawah menemukan kesalahan fungsi input-output yang sangat sulit.

2. Bottom up, strategi ini digunakan jika, modul level bawah di buat (coding), di test dan diintegrasikan sebelum modul level atas di buat. Keuntungannya adalah modul level rendah yang merupakan operasi yang paling sulit di implementasikan dan diuji terlebih dahulu. Kerugiannya adalah pendekatan ini sangat sulit untuk di teliti seluruh operasinya, sebelum programnya selesai dibuat.
3. Threads, strategi ini digunakan jika, keputusan dibuat terlebih dahulu untuk fungsi program yang akan dibuat, kemudian modul yang akan mendukungnya baru dibuat dan kemudian diimplementasikan untuk menghasilkan fungsi yang penting. Keuntungannya adalah fungsi yang paling penting di implementasikan terlebih dahulu. Kerugiannya adalah integrasi dari modul yang berikutnya mungkin akan lebih sulit, jika dibandingkan dengan pendekatan top-down atau bottom-up.

Auditor perlu mencari bukti bahwa strategi yang dipilih manajemen adalah tepat khususnya pada program yang besar, penggunaan strategi yang salah dapat mengakibatkan program yang dihasilkan menjadi kurang berkualitas. Auditor dapat melakukan wawancara untuk menguji apakah manajemen menggunakan pendekatan sistematik untuk memilih strategi implementas dan integrasi.

Mereka juga dapat menguji dokumentasi program untuk memperoleh bukti tipe strategi yang telah di pilih.

Untuk memonitor agar pelaksanaan tidak bertentangan dengan rencana awal, beberapa teknik dapat digunakan seperti :

a) Work Breakdown Structures (WBS), dengan teknik ini kita dapat mengidentifikasi tugas-tugas yang spesifik untuk pengembangan, pengadaan, dan implementasi software yang dibutuhkan.
b) Gantt Chart, dapat digunakan untuk membantu mengatur tugas. Teknik ini akan menunjukan kapan tugas harus dimulai dan diselesaikan, tugas apa yang

harus dibuat bersama-sama, dan tugas apa yang harus dihasilkan secara serial, serta membantu mengidentifikasi konsekuensi dari keterlambatan penyelesaian tugas tersebut. Kemajuan dari sebuah software dapat di plot pada gantt charts untuk menunjukkan apakah proyek telah berjalan dengan seharusnya.

c) Program Evaluation and review technique (PERT), menunjukan tugas-tugas yang harus diselesaikan, bagaimana hubungannya, kebutuhan sumber daya apa untuk setiap tugas-tugasnya. Evaluasi program dan tinjauan teknis *(PERT) charts* menunjukkan tugas yang harus dilakukan, keterkaitan dan kebutuhan sumber daya untuk setiap tugas. PERT charts membiarkan masalah sepanjang keterlambatan dalam penyelesaian tugas yang tertunda akan menghasilkan software secara keseluruhan. PERT charts juga memungkinkan manajemen untuk menentukan konsekuensi penyelesaian awal atau akhir tugas.

Tanggung Jawab DBA adalah menangani Struktur basis data adalah :

1. Merancang skema

   DBA biasanya tidak terlibat dalam perancangan basisdata mulai dari awal. Oleh karena itu, setiap terjadi perubahan struktur basis data yang berpengaruh pada skema / relasi antar tabel harus selalu dicatat

2. Mengawasi terjadinya redundancy

   Redundancy dapat terjadi pada dua hal, yaitu performance dan data integrity. DBA harus menetapkan prosedur tertentu untuk melakukan rekonsiliasi data untuk menghindari terjadinya redundancy

3. Melakukan pengawasan konfigurasi permintaan atas perubahan struktur basisdata

DBA bertugas menyusun laporan secara berkala mengenai pemakai yang aktif, serta file dan data yang dipakai, dan metode akses yang digunakan. Disamping itu juga dicatat terjadinya kesalahan. Hal tersebut diperlukan untuk menentukan apakah diperlukan adanya perubahan struktur basisdata demi peningkatan performance

4. Menjadwalkan dan mengadakan pertemuan apabila terjadi perubahan struktur basisdata
5. Menerapkan perubahan skema

   Perubahan harus dilakukan pada basisdata ujicoba, agar pemakai dapat mengujinya sebelum diterapkan pada sistem yang sesungguhnya
6. Merawat dokumentasi pemakai

   Merawat dokumentasi DBA – untuk memperoleh informasi tentang perubahan yang telah dilakukan, bagaimana dan kapan dilakukanManajemen DBMS

4.5. Konsep dan kontrol dan Audit PL

Audit Software adalah software yang digunakan oleh auditor untuk membantu tugas auditnya terutama untuk menguji keandalan sistem dan integritas data.

Software audit ini beraneka ragam, dan sebagian besar tersedia secara luas dalam bentuk paket jadi. Berikut ini akan dibahas beberapa jenis audit software:

1. Generalized Audit Software (GAS)

   Merupakan audit yang digunakan untuk hampir seluruh pekerjaan audit..

   Misal: ACL (audit common language). GAS memiliki kemampuan fungsional sbb:

a) Untuk akses file

b) Untuk menyusun ulang file

c) Untuk seleksi(mengambil data yang diinginkan)

d) Untuk statistik

e) Untuk aritmatik, penambahan, pengurangan dan pembagian

f) Untuk analisi pengelompokkan data dan frekuensi

g) Untuk membuat file baru dan up-date data

h) Untuk pelaporan

Pekerjaan audit yang dapat dilakukan dengan GAS adalah:

a) Memeriksa mutu data, auditor dapat menggunakan GAS untuk menguji eksistensi, keakuratan, kelengkapan, konsistensi dan jangka waktu pemeliharaan data dan tempat penyimpanan.

b) Memeriksa kualitas dari proses sistem, Auditor dapat menggunakan teknik paralel simulation

c) Memeriksa eksistensi/ keberadaan aset yang diwakili oleh data klien

d) Melakukan analisis analitik, membandingkan angka dalam laporan keuangan dengan angka yang lain atau dari catatan klien

Keterbatasan GAS :

a) Hanya dapat digunakan untuk ex-post audit/ audit untuk transaksi yang sudah terjadi, tidak bisa melakukan audit pada saat terjadi transaksi (concurrent audit).

b) Kemampuan terbatas dalam menguji mutu dari prose pengolaan data dari klien.

c) Kemampuan terbatas dalam menemukan kemungkinan terjadi kesalahan atau kegagalan pada sistem.

Cara GAS untuk mengakses data klien. Ada berbagai cara auditor dapat mengakses data auditan dengan menggunakan GAS:

a) Data di copy ke disk

b) Melalui modem

c) Melalui LAN klien

2. Industry Spesifik Audit software (ISAS)

Merupakan software audit yang di buat khusus berdasarkan jenis industri yang akan diaudit. Perbedaan utama ISAS dengan GAS

a) IASA dapat dikembangkan untuk mengakses data spesifik yang digunakan secara luas dalam industri.

b) ISAS di implementasikan kepada industri tertentu yang menyediakan perintah high- level yang memuat fungsi audit umum yang dibutuhkan untuk mengaudit industri tersebut.

3. High- Level Language (4GL)

Memiliki fungsi yang sama dengan GAS dalam audit, contoh adalah Fourth generation languages seperti SQL, QBE, SPSS dan SAS.

Alasan penggunaan Fourth- generation languages

a) Fungsi yang terdapat pada GAS yang ada pada 4GL.

b) Auditor lebih menguasai 4GL dapat digunakan lebih mudah di banding GAS

c) 4GL digunakan secara luas dalam organisasi yang akan membantu auditor dalam pekerjaan

4. Utility software

Software untuk berbagai keperluan umum yang tidak hanya diperlukan oleh auditor. Jenis-jenis kegunaan utility audit software

a) Untuk keamanan Integritas

b) Untuk menguji mutu dari data,

c) Untuk mengamani sistem klien

d) Untuk memeriksa utility

e) Untuk mengukur efisiensi operasi

Auditor menggunakan utility software dengan alasan:

a) dapat digunakan untuk melakukan keamanan khusus atau fungsi yang berhubungan dengan integritas.

b) dapat digunakan untuk mendownlod data

c) dapat melaksanakan fungsi yang tidak dapat dilakukan oleh GAS atau software audit lainnya.

d) dapat menyelesaikan tugas audit dengan cara efektif dan efisien dibanding software audit .

e) dapat digunakan auditor untuk membantu mengembangkan software audit baru.

5. Expert System Software (ES)

Merupakan program yang di buat berdasarkan keahlian manusia yang mempunyai kemampuan untuk menggantikan tenaga ahli tersebut pada saat terjadi masalah. Alasan auditor mengembangkan , memelihara dan menggunakan ES:

a) ES menyediakan penetahuan yang hanya di miliki sebagian kecil auditor.

b) Karena perkembangan teknologi yang pesat, sulit bagi auditor untuk menguasai pengetahuan yang mungkin atau dihadapkan dalam fungsi audit.

6. Special Audit Software

Merupakan software audit khusus untuk pelaksanaan pekerjaan audit tertentu.

Alasan menggunakan special audit software

a) Tidak tersedianya software alternatif

b) Keterbatasan fungsi dari software alternatif

c. Pertimbangan efisiensi

d. Meningkatkan pemahaman tentang sistem

e. Kesempatan untuk implementasi yang mudah

f. Peningkatan kemandirian auditor

Pertemuan 5

Definisi Tata Kelola TI, Tata Kelola TI, Manfaat tata Kelola. Fokus Utama Area Tata Kelola, Model Tata Kelola teknologi informasi.

5.1. **Definisi Tata Kelola TI**

Definisi Tata Kelola TI adalah suatu cabang dari tata kelola perusahaan yang terfokus pada Sistem / Teknologi informasi serta manajemen kinerja dan risikonya. Tata kelola TI adalah struktur kebijakan atau prosedur dan kumpulan proses yang bertujuan untuk memastikan kesesuaian penerapan TI dengan dukungannya terhadap pencapaian tujuan institusi, dengan cara mengoptimalkan keuntungan dan kesempatan yang ditawarkan TI, mengendalikan penggunaan terhadap sumber daya TI dan mengelola resiko-resiko terkait TI

Tatakelola teknologi informasi bukan bidang yang terpisah dari pengelolaan perusahan, 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 menerap kan strategi perusahaan.

3. Memastikan proses-proses tersebut menghasilkan keluaran yang terukur.

4. Memastikan adanya informasi mengenai hasil yang dipero leh dan mengukurnya.

5. Memastikan keluaran yg dihasilkan sesuai dgn yg diharap

5.2. Tata Kelola TI

Tata kelola TI adalah struktur kebijakan atau prosedur dan kumpulan proses yang bertujuan untuk memastikan kesesuaian penerapan TI dengan dukungannya

terhadap pencapaian tujuan institusi, dengan cara mengoptimalkan keuntungan dan kesempatan yang ditawarkan TI, mengendalikan penggunaan terhadap sumber daya TI dan mengelola resiko-resiko terkait TI

Menurut Kridanto Surendro, 2009 menerangkan Tata Kelola Teknologi Informasi adalah upaya menjamin pengelolaan teknologi informasi agar mendukung bahkan selaras dengan strategi bisnis suatu enterprise yang dilakukan oleh dewan direksi, manajemen eksekutif, dan juga oleh manajemen teknologi informasi" .

Menurut U. Tresna Lenggana, 2007 menerangkan bahwa: "Tata Kelola TI adalah sebuah kerangka kerja kebijakan, prosedur dan kumpulan proses-proses yang bertujuan untuk mengarahkan dan mengendalikan organisasi dalam waktu rangka pencapaian tujuan organisasi dengan memberikan tambahan nilai bisnis, melalui penyeimbangan dan resiko TI beserta proses-proses yang ada didalamnya".

5.3. Manfaat tata Kelola.

Manfaat tata kelola TI adalah untuk mengatur penggunaan TI, dan memastikan kinerja TI sesuai dengan tujuan/fokus utama area tata kelola TI

Di lingkungan yang sudah memanfaatkan Teknologi Informasi (TI), 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 TI dengan kualitas yang bagus, tepat waktu, dan sesuai dengan anggaran.
2. Menguasai dan menggunakan TI untuk mendatangkan keuntungan.
3. Menerapkan TI untuk meningkatkan efisiensi dan produktifitas sambil menangani risiko TI.

Tatakelola teknologi informasi bukan bidang yang terpisah dari pengelolaan perusahan, 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 menerap kan strategi perusahaan.
3. Memastikan proses-proses tersebut menghasilkan keluaran yang terukur.
4. Memastikan adanya informasi mengenai hasil yang dipero leh dan mengukurnya.
5. Memastikan keluaran yg dihasilkan sesuai dgn yg diharap

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

1. Kerugian bisnis, berkurangnya reputasi, dan melemahnya posisi kompetisi.
2. Tenggang waktu yang terlampaui, biaya lebih tinggi dari yang di perkirakan, dan kualitas lebih rendah dari yang telah diantisipasi.
3. Efisiensi dan proses inti perusahaan terpengaruh secara negatif oleh rendahnya kualitas penggunaan TI.
4. Kegagalan dari inisiatif TI untuk melahirkan inovasi atau memberikan keuntungan yang dijanjikan

Menurut IMPACT's IT Governance Special Interest Group (SIG), manfaat Tata Kelola TI adalah sebagai berikut :

a. Transparansi dan Akuntabilitas :
    1) Meningkatkan transparansi dari biaya TI, proses TI, portofolio TI (proyek dan layanan)

2) Mengklarifikasi akuntabilitas dari pembuat keputusan. Definisi yang jelas dari user dan provider.

b. ROI (*Return of Investment/Stakeholder Value*):
   1) Meningkatkan pemahaman atas biaya TI secara keseluruhan dan pengaruhnya terhadap ROI
   2) Dapat menjelaskan alasan pemotongan biaya investasi TI
   3) Stakeholder mendapat informasi mengenai risiko dan keuntungan yang didapatkan dari investasi TI
   4) Meningkatkan kontribusi stakeholder
   5) Melindungi reputasi perusahaan

c. Peluang dan Partnership
   1) Mengetahui jenis-jenis peluang yang mungkin tidak akan mendapat perhatian ataupun sponsor
   2) Dapat memposisikan TI sebagai partner bisnis
   3) Memfasilitasi kerjasama dengan perusahaan lain
   4) Memberikan fasilitas pada hubungan bisnis dengan partner TI (vendor, suplier)
   5) Memungkinkan partisipasi TI dalam strategi bisnis
   6) Meningkatkan responsiveness terhadap tantangan dan kesempatan yang ada di pasar

d. Peningkatan perfoma bisnis :
   1) Mencapai penjelasan mengenai bagaimana TI dapat mendukung aktivitas bisnis
   2) Meningkatkan peforma bisnis, dan mendorong pada peningkatan best practices tata kelola perusahaan

e. Pencapaian Extrnal:

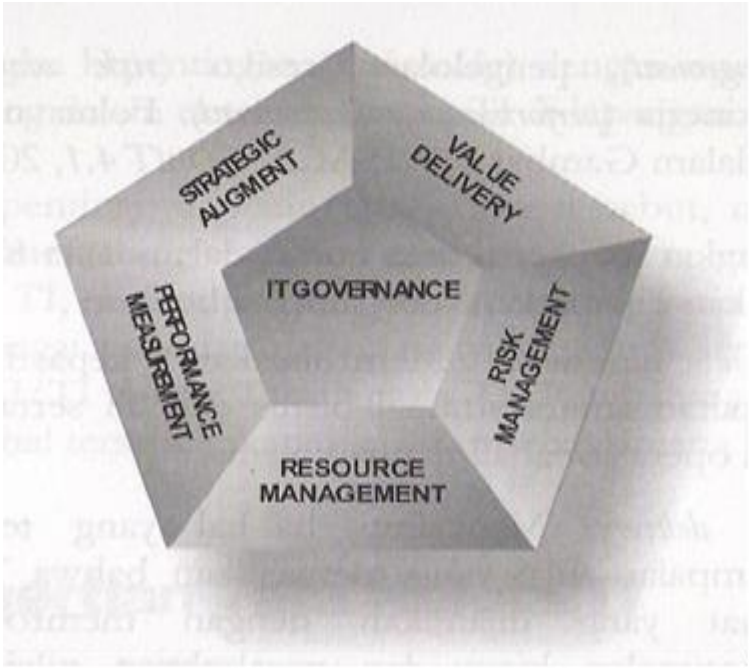
   Memingkinkan terjadinya pendekatan yang terintregrasi untuk keperluan urusan hukum dan peraturan / kebijakan.

Prinsip Keselarasan

- TI mengelola sumber dayanya secara efektif dan efisien agar selaras dengan kebutuhan organisasi
- TI merupakan penyedia layanan. Outsourcing juga dapat terjadi dalam hubungan antara TI dan bisnis
- TI secara aktif tergabung dalam pengembangan dan inovasi organisasi
- TI mengembangkan dan menjaga kompetensi yang selaras dengan dan mendukung keinginan para ahli dalam organisasi
- TI harus selaras dengan tujuan strategis organisasi, melalui perencanaan yang terintegrasi
- Semua aplikasi TI harus selaras dengan aturan dan kebijakan yang telah disepakati bersama oleh manajemen bisnis dan manajemen TI
- TI secara aktif ikut dalam mengulas dan merancang proses bisnis yang efisien
- Adanya transparansi mengenai layanan TI yang harus disediakan untuk mendukung keperluan bisnis dan layanan tersebut harus selalu diawasi
- Mulai dari pengembangan awal proyek baru, akibat dari investasi TI harus sudah dianalisa

5.4. Fokus Utama Area Tata Kelola,

Fokus Area



Gambar V.1 ISACA, COBIT 4.1, 2007

Faktor Utama Tata Kelola TI :

1. Penyelarasan Strategis (Stategic Aligment).

   Memastikan adanya hubungan perencanaan organisasi dan TI dengan cara menetapkan, memelihara, serta menyesuaikan operasional TI dengan operasional organisasi

   Fokus kepastian terhadap keterkaitan antara strategi bisnis dan TI serta penyelarasan antara operasional TI dengan Bisnis

2. Penyampaian Nilai (Value Delivery)

   Fokus dengan melaksanakan proses TI agar supaya proses tersebut sesuai dengan siklusnya, mulai dari menjalankan rencana, memastikan TI dapat memberikan

manfaat yang diharapkan, meng optimalkan penggunaan biaya sehingga pada akhirnya TI dapat mencapai hasil yang diinginkan

Mencakup hal yang terkait dengan penyampaian nilai yang memastikan bahwa TI memenuhi manfaat yang dijanjikan dengan memfokuskan pada pengoptimalan biaya dan pembuktian nilai hakiki akan keberadaan TI

3. Pengelolaan Sumber Daya (resource Management).

   Fokus pada kegiatan yang dapat mengoptimal kan dan mengelola sumber daya TI, yang terdiri dari aplikasi, informasi, infrastruktur, dan sumber daya manusia

   Berkaitan dengan pengoptimalan investasi yang dilakukan dan pengelolaan secara tepat dari sumber dya TI yang kritis mencakup aplikasi, informasi, infrastruktur dan SDM. Berhubungan dengan pengoptimalan pengetahuan dan infrastruktur.

4. Pengelolaan Resiko (Risk Management)

   Untuk melaksanakan pengelolaan terhadap risiko, dibutuhkan kesadaran anggota organisasi dalam memahami adanya risiko, kebutuhan organisasi, dan risiko – risiko signifikan yang dapat terjadi, serta menanamkan tanggung jawab dalam mengelola risiko yang ada di organisasi.

   Membutuhkan kepekaan akan resiko oleh manajemen senior pemahaman yang jelas akan perhatian perusahaan terhadap keberadaan resiko, memahaman kebutuhan akan kepatutanm transparansi akan resiko yang sifgnifikan terhadap proses bisnis perusahaan dan tanggung jawab pengelolaan resiko kedalam organisasi itu sendiri.

5. Pengukuran Kinerja (Performance Maintenance).

   Mengikuti dan mengawasi jalannya pelaksanaan rencana, pelaksanaan proyek, pemanfaaatan sumber daya, kinerja poses, penyampaian layanan sampai dengan pencapaian hasil TI

Penelusuran dan pengawasan implementasi dari strategi, pemenuhan proyek yang berjalan, penggunaan sumber daya, kinerja proses dan penyam,paian layanan dengan menggunakan kerangka kerja seperti balanced scorecard yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan terukur dibandingkan dengan akuntansi konvensional.

5.5. Model Tata Kelola teknologi informasi.

Model Tata Kelola teknologi Informasi terdiri dari :

1. *The IT 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 TI (IT Service Management – ITSM) yang sudah diadopsi sebagai standar industri pengembangan industri perangkat lunak di dunia.

   ITSM memfokuskan diri pada 3 (tiga) tujuan utama, yaitu:

   1. Menyelaraskan layanan TI dengan kebutuhan sekarang dan akan datang dari bisnis dan pelanggannya.

   2. Memperbaiki kualitas layanan-layanan TI.

   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 TI yang dikembangkan.

2. ISO/IEC 17799

ISO/IEC 17799 dikembangkan oleh The International Organization for Standardization (ISO) dan The International Electrotechnical Commission (IEC) ISO/IEC 17799 bertujuan memperkuat 3 (tiga) element 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.
3. Availability – memastikan bahwa user yang terotorisasi mendapatkan akses kepada informasi dan aset yang terhubung dengannya ketika memerlukannya

3. COSO

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.*

***COSO** framework terdiri dari 3 dimensi yaitu:*

***1.** Komponen kontrol COSO*

COSO mengidentifikasi 5 komponen kontrol yang diintegrasikan dan dijalankan dalam semua unit bisnis, dan akan membantu mencapai sasaran kontrol internal:

a. Monitoring.

b. Information and communications.

c. Control activities.

d. Risk assessment.

e. Control environment.

2. Sasaran kontrol internal

Sasaran kontrol internal dikategorikan menjadi beberapa area sebagai berikut:

a. Operations – efisisensi dan efektifitas operasi dalam mencapai sasaran bisnis yang juga meliputi tujuan performansi dan keuntungan.

b. Financial reporting – persiapan pelaporan anggaran finansial yang dapat dipercaya.

c. ***Compliance*** *– pemenuhan hukum dan aturan yang dapat dipercaya.*

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

COBIT Framework dikembangkan oleh IT Governance Institute, sebuah organisasi yang melakukan studi tentang model pengelolaan TI yang berbasis di Amerika Serikat

COBIT Framework terdiri atas 4 domain utama:

1. Planning & Organisation.
2. Acquisition & Implementation.
3. Delivery & Support.
4. Monitoring.

1. Planning & Organisation.

Domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi TI dengan strategi perusahaan.

2. Acquisition & Implementation.

Domain ini menitikberatkan pada proses pemilihan, pengadaaan dan penerapan teknologi informasi yang digunakan.

3. Delivery & Support.

Domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya.

4. Monitoring.

Domain ini menitikberatkan pada proses pengawasan

COBIT mempunyai model kematangan (maturity models), 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 optimised (dari 0 sampai 5).

COBIT juga mempunyai ukuran-ukuran lainnya sebagai berikut:

1. Critical Success Factors (CSF) – mendefinisian

2. Key Goal Indicators (KGI) – mendefinisikan

3.Key Performance Indicators (KPI) – mendefinisikan

1. Critical Success Factors (CSF) – mendefinisian

Mendefinisian hal-hal atau kegiatan penting yang dapat digunakan manajemen untuk dapat mengontrol proses-proses TI di organisasinya.

2. Key Goal Indicators (KGI)

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:

a. Ketersediaan informasi yang diperlukan dalam mendukung kebutuhan bisnis.

b. Tidak adanya resiko integritas dan kerahasiaandata.

c. Efisiensi biaya dari proses dan operasi yangdilakukan.

d. Konfirmasi reliabilitas, efektifitas, dan compliance.

3. Key Performance Indicators (KPI)

Mendefinisikan ukuran-ukuran untuk menentukan kinerja proses-proses TI dilakukan untuk mewujudkan tujuan yang telah ditentukan. KPI biasanya berupa indikator kapabilitas, pelaksanaan, dan kemampuan sumber daya TI.

Control Objectives for Information and related technology (COBIT) menyediakan standar dalam kerangka kerja dokumen yang terdiri dari sekumpulan proses TI yang mempresentasikan aktivitas yang dapat dikendalikan dan terstruktur.

Memfokuskan pada kontrol dan sedikit eksekusi, dimana lebih ditujukan kepada pendefinisian strategi dan kontrol yang biasa dilakukan oleh manajemen tingkat atas.

Pertemuan 6

Implementasi Cobit : 1. Tantangan Manajemen dalam penggunaan SIM; 2. Kendala Penggunaan SI; 3. Tujuan Keamanan sistem Informasi; 4. Pengertian COBIT; 5. Pengertian Domain

6. Implementasi Cobit

COBIT Framework (Business Requrement)

1. Efektivitas

Informasi yang relevan yang berhubungan pada proses bisnis, serta disampaikan secara tepat waktu, benar, konsisten dan mudah

2. Evisiensi

   Terkait dengan ketentuan informasi melalui penggunaan sumber daya yang optimal

3. Kerahasiaan

   Terkait dengan pengamanan terhadap informasi yang sensitif dari pihak yang tidak berhak

4. Integritas

   Terkait dengan keakuratan dan kelengkapan informasi serta validitasnya sesuai dengan nilai dan harapan bisnis

5. Ketersediaan

   Terkait dengan ketersediaan informasi pada saat kapanpun diperlukan

6. Kepatuhan

   Terkait pada kepatuhannya terhadap hukum, regulasi maupun perjanjian kontrak

7. Keandalan

   Terkait dengan penyediaan informasi yang tepat bagi manajemen untuk mendukung operasional suatu entitas dan menjalankan tanggung jawab tata kelolanya

6.1. **Tantangan Manajemen dalam Penggunaan SIM**

Ada banyak teknologi alternatif untuk membantu perusahaan mencapai keamanan dan kontrol, tapi disiplin organisasi diminta untuk menggunakan teknologi-teknologi tersebut secara efektif.:

1. Tantangan investasi sistem informasi

2. Tantangan strategik bisnis

3. Tantangan globalisasi

4. Tantangan infrastruktur teknologi informasi

5. Tantangan tanggung jawab dan pengawasan: etika dan keamanan.

Tantangan dalam implementasi pengembangan system informasi adalah orang-orang yang terlibat dalam pengembangan system informasi yaitu departemen operasional sebagai end-user dan IT sebagai pengembang dan tentu saja sebagai support dan manajemen sebagai leader yang membuat definisi goal yang akan dicapai. Jika system yang akan di-implementasikan adalah system informasi yang terintegrasi maka tantangannya akan sangat besar karena meliputi keseluruhan organisasi yang bisa saja melibatkan pihak eksternal.

Masalah yang dihadapi dalam implementasi tersebut biasanya adalah sebagai berikut :

1. Pengguna tidak mengetahui kemampuan teknologi yang dapat digunakan untuk membantu proses bisnis yang dikerjakannya setiap hari, dan pada tahap analisa developer juga tidak mengetahui benar-benar proses bisnis yang berlangsung atau juga karena standard dari developer yang kurang dalam membuat program sehingga program yang dihasilkan adalah program yang baik dari kacamata developer bukan dari kedua belah pihak. Karena ketidak tahuan pengguna maka masalah ini bisa diabaikan dimana pengguna juga tidak keberatan dengan program yang diberikan untuk digunakan.
2. Kedua belah pihak tidak memahami asumsi dan ketergantungan yang ada dalam system dan bisnis proses, sehingga pada tahap implementasi jika ada bagian dari proses bisnis yang belum di cover oleh system dan kemudian dibuatkan fungsi baru yang ternyata menimbulkan masalah, dan penyelesaian

masalah menimbulkan masalah baru seperti melakukan tambal sulam yang berakibat pada benang kusut akan membuat suatu aplikasi yang tidak dapat di andalkan. Dan aplikasi hanya dibuat sebagai program untuk melakukan entry data.

3. Dalam implementasi system terintegrasi, dimana pengguna tidak dapat menjadikan implementasi sebagai prioritas pertama, dimana pengguna yang sudah disibukkan dengan kegiatan operasional akan berpura-pura menyetujui, menjalankan dan mengikutinya tetapi pada kenyataannya semuanya tidak berjalan sesuai dengan harapan.

6.2. **Kendala Penggunaan SI**

Kendala Penggunaan SI

1. Bencana (*disaster)*

   Untuk pencegahan atau meminimalkan dampak bencana:

   a. Rencana Kesinambungan Kegiatan (pada perusahaan dikenal dengan *Bussiness Continuity Plan)* yaitu suatu fasilitas atau prosedur yang dibangun untuk menjaga kesinambungan kegiatan/layanan apabila terjadi bencana

   b. Rencana Pemulihan Dampak Bencana "*disaster recovery plan",* yaitu fasilitas atau prosedur untuk memperbaiki dan/atau mengembalikan kerusakan/dampak suatu bencana ke kondisi semula.

2 Sistem Pengamanan (*security)*. Merupakan kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian, atau kerusakan fisik terhadap sistem informasi.

3. Kesalahan (*errors)* dalam sistem yang terotomatisasi dapat terjadi di berbagai titik di dalam siklus prosesnya, misalnya: pada saat entri-data, kesalahan program, operasional komputer, dan perangkat keras.

6.3. **Tujuan Keamanan Sistem Informasi**

1. Kerahasiaan. Setiap organisasi berusaha melindungi data dan informasinya dari pengungkapan kepada pihak-pihak yang tidak berwenang.
2. Ketersediaan. Sistem dimaksudkan untuk selalu siap menyediakan data dan informasi bagi mereka yang berwenang untuk menggunakannya.
3. Integritas. Semua sistem dan subsistem yang dibangun harus mampu memberikan gambaran yang lengkap dan akurat dari sistem fisik yang diwakilinya

6.4. **Pengertian COBIT**

Sejarah perkembangan COBIT yang pertama kali muncul adalah pada tahun 1996 dengan COBIT versi 1 yang menekankan pada audit dilanjutkan dengan COBIT versi 2 pada tahun 1998 yang menekankan pada tahap pengendalian, lalu COBIT 3 pada tahun 2000 yang berorientasi pada aspek manajemen. Pada tahun 2005, COBIT kembali muncul dengan versi 4 tepatnya pada bulan Desember dan

dilanjutkan pada bulan Mei 2007 muncul COBIT versi 4.1 yang lebih beorientasi pada tata kelola TI. Dan terakhir, saat ini COBIT versi 5 tepatnya pada bulan Juni 2012 yang berorientasi pada tata kelola TI perusahaan dan manajemen

COBIT (*Control Objectives for Information and Related Technology*) merupakan audit sistem informasi dan dasar pengendalian yang dibuat oleh *Information Systems Audit and Control Association* (ISACA) dan *IT Governance Institute* (ITGI) pada tahun 1992.

COBIT Framework adalah standar kontrol yang umum terhadap teknologi informasi, dengan memberikan kerangka kerja dan kontrol terhadap teknologi informasi yang dapat diterima dan diterapkan secara internasional.

COBIT bermanfaat bagi manajemen untuk membantu menyeimbangkan antara resiko dan investasi pengendalian dalam sebuah lingkungan IT yang sering tidak dapat diprediksi. Bagi user, ini menjadi sangat berguna untuk memperoleh keyakinan atas layanan keamanan dan pengendalian IT yang disediakan oleh pihak internal atau pihak ketiga. Sedangkan bagi Auditor untuk mendukung atau memperkuat opini yang dihasilkan dan memberikan saran kepada manajemen atas pengendalian internal yang ada.

COBIT merupakan kombinasi dari prinsip-prinsip yang telah ditanamkan yang dilengkapi dengan balance scorecard dan dapat digunakan sebagai acuan model (seperti COSO) dan disejajarkan dengan standar industri, seperti ITIL, CMM, BS779, ISO 9000

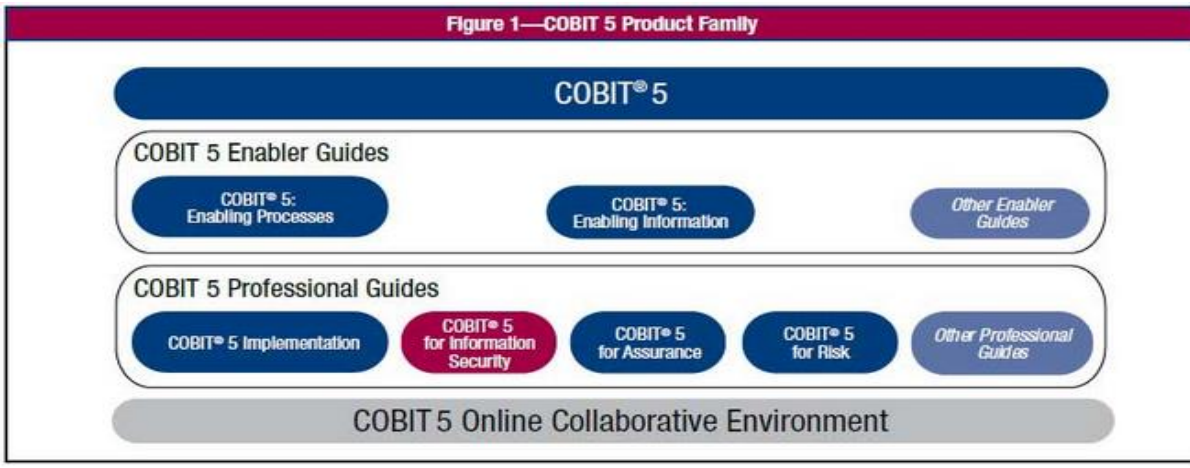
COBIT versi 4.1 adalah model standar pengelolaan IT yang telah mendapatkan pengakuan secara luas, dikembangkan oleh Information Technology Governance Institute (ITGI) dari Information System Audit and Control Association (ISACA). Menurut IT Governance Institute, 2007, menyatakan bahwa pada versi 4.1 ini diuraikan good practices, domain-domain dan proses kerangka kerja (framework) TI

yang ada. COBIT 5 adalah evolusi dari framework sebelumnya yakni, COBIT 4.1 yang ditambah dengan Val IT 2.0 dan Risk IT

COBIT 5 adalah kerangka bisnis untuk tata kelola dan manajemen perusahaan IT (IT gevornance framework), dan juga kumpulan alat yang mendukung para manager untuk menjembatani jarak (gap) antara kebutuhan yang dikendalikan (control requirments), masalah teknis (technical issues) dan resiko bisnis (business risk)

Pengertian COBIT 5 adalah Informasi merupakan sumber daya utama bagi enterprise. Teknologi memegang peranan penting yang dapat meningkatkan fungsi informasi pada enterprise, sosial, publik dan lingkungan bisnis. COBIT 5 memberikan layanan kerangka kerja secara komprehensif untuk membantu pemerintah dan manajemen IT dalam sebuah perusahaan mencapai tujuan yang diharapkan

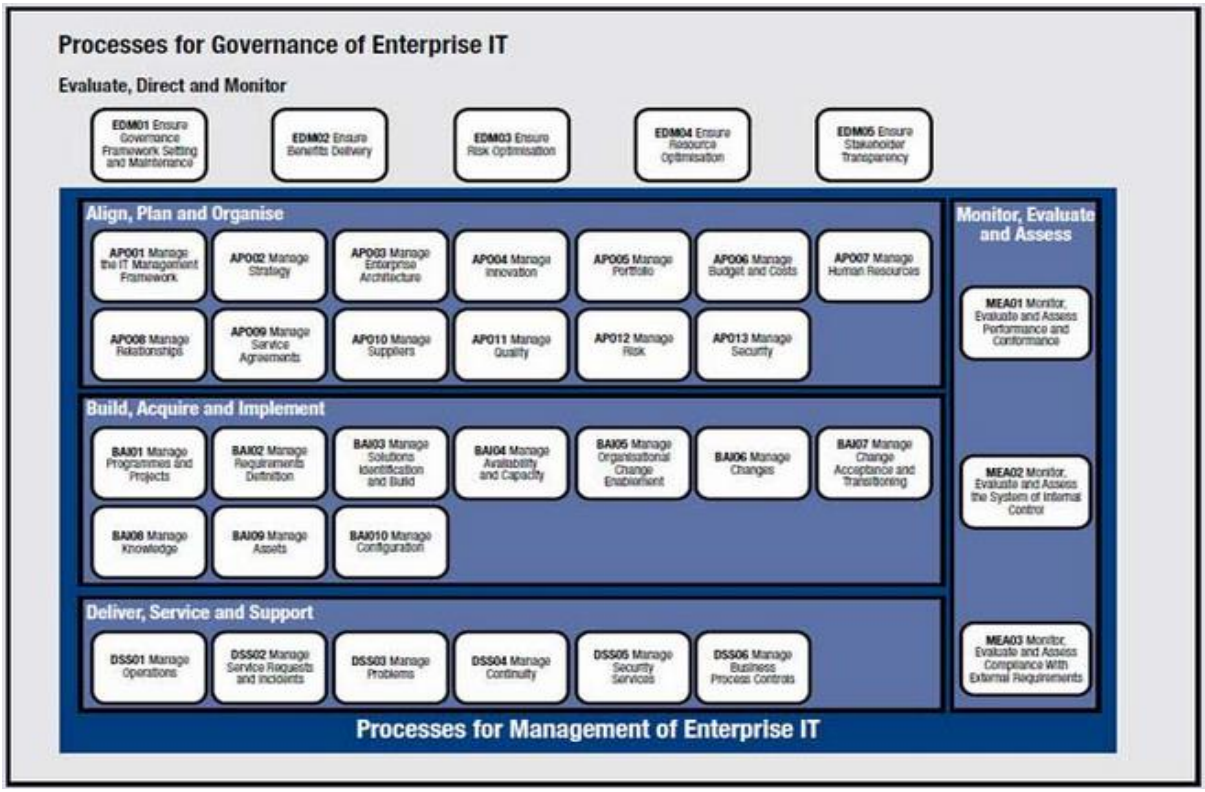
Pengertian COBIT 5 adalah sebuah framework atau kerangka kerja yang memberikan layanan kepada enterprise, baik itu sebuah perusahaan, organisasi, maupun pemerintahan dalam mengelola dan memanajemen aset atau sumber daya IT untuk mencapai tujuan enterprise tersebut.



Gambar VI.1 Cobit 5

Pada COBIT 5, proses-proses seperti APO13 Manage Security, DSS04 Manage Continuity dan DSS05 Manage Security Services memberikan panduan dasar

mengidentifikasi, mengoperasikan dan memonitor sistem untuk manajemen keamanan secara umum. Gambaran mengenai proses-proses tersebut dapat dilihat pada Gambar 2 berikut ini



Gambar VI.2 Proses Manajemen IT pada Cobit 5

Menggambarkan keamanan informasi pada enterprise termasuk:

1. Responsibilities terhadap fungsi IT pada keamanan informasi.
2. Aspek-aspek yang akan meningkatkan efektivitas kepemimpinan dan manajemen keamanan informasi seperti struktur organisasi, aturan-aturan dan kultur.
3. Hubungan dan jaringan keamanan informasi terhadap tujuan enterprise.

Memenuhi kebutuhan enterprise untuk:

1. Menjaga risiko keamanan pada level yang berwenang dan melindungi informasi terhadap orang yang tidak berkepentingan atau tidak berwenang untuk melakukan modifikasi yang dapat mengakibatkan kekacauan.

2. Memastikan layanan dan sistem secara berkelanjutan dapat digunakan oleh internal dan eksternal stakeholders.
3. Mengikuti hukum dan peraturan yang relevan.

Sebagai tambahan, pengembangan COBIT 5 for Information Security untuk memberikan fakta bahwa keamanan informasi merupakan salah satu aspek penting dalam operasional sehari-hari pada enterprise.

Keunggulan:

Menggunakan COBIT 5 for Information Secutiry memberikan sejumlah kemampuan yang berhubungan dengan keamanan informasi untuk perusahaan sehingga dapat menghasilkan manfaat perusahaan seperti:

1. Mengurangi kompleksitas dan meningkatkan efektivitas biaya karena integrasi yang lebih baik dan lebih mudah.
2. Meningkatkan kepuasan pengguna.
3. Meningkatkan integrasi keamanan informasi dalam perusahaan.
4. Menginformasikan risiko keputusan dan risk awareness.
5. Meningkatkan pencegahan, deteksi dan pemulihan.
6. Mengurangi insiden (dampak) keamanan informasi.
7. Meningkatkan dukungan untuk inovasi dan daya saing.
8. Meningkatkan pengelolaan biaya yang berhubungan dengan fungsi keamanan informasi.
9. Pemahaman yang lebih baik dari keamanan informasi.

6.4.1. **Kriteria Informasi berdasarkan COBIT**

Untuk memenuhi tujuan bisnis, informasi perlu memenuhi kriteria tertentu, adapun 7 kriteria informasi yang menjadi perhatian COBIT, yaitu sebagai berikut:

1. Effectiveness (Efektivitas). Informasi yang diperoleh harus relevan dan berkaitan dengan proses bisnis, konsisten dapat dipercaya, dan tepat waktu.
2. Effeciency (Efisiensi). Penyediaan informasi melalui penggunaan sumber daya (yang paling produktif dan ekonomis) yang optimal.
3. Confidentially (Kerahasiaan). Berkaitan dengan proteksi pada informasi penting dari pihak-pihak yang tidak memiliki hak otorisasi/tidak berwenang.
4. Intergrity (Integritas). Berkaitan dengan keakuratan dan kelengkapan data/informasi dan tingkat validitas yang sesuai dengan ekspetasi dan nilai bisnis.
5. Availability (Ketersediaan). Fokus terhadap ketersediaan data/informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun dimasa yang akan datang. Ini juga terkait dengan pengamanan atas sumber daya yang diperlukan dan terkait.
6. Compliance (Kepatuhan). Pemenuhan data/informasi yang sesuai dengan ketentuan hukum, peraturan, dan rencana perjanjian/kontrak untuk proses bisnis.
7. Reliability (Handal). Fokus pada pemberian informasi yang tepat bagi manajemen untuk mengoperasikan perusahaan dan pemenuhan kewajiban mereka untuk membuat laporan keuangan.

6.4.2. **Komponen Control Objective**

Berdasarkan IT Governance Institute (2012), Framework COBIT disusun dengan karakteristik yang berfokus pada bisnis (bussiness focused). Pada edisi keempatnya ini, COBIT Framework terdiri dari 34 high level control objectives dan kemudian mengelompokan proses tersebut menjadi 4 domain, keempat domain

tersebut antara lain: *Plannig and Organization, Acquisition and Implementation, Delivery and Support, dan Monitoring and Evaluation*

6.4.3. **Prinsip dari OBIT 5**

Prinsip COBIT 5 :

Prinsip 1. Meeting Stakeholder Needs

Keberadaan sebuah perusahaan untuk menciptakan nilai kepada stakeholdernya – termasuk stakeholders untuk keamanan informasi – didasarkan pada pemeliharaan keseimbangan antara realisasi keuntungan dan optimalisasi risiko dan penggunaan sumber daya yang ada. Optimalisasi risiko dianggap paling relevan untuk keamanan informasi. Setiap perusahaan memiliki tujuan yang berbeda-beda sehingga perusahaan tersebut harus mampu menyesuaikan atau melakukan customize COBIT 5 ke konteks perusahaan yang dimiliki.

Prinsip 2. Covering the Enterprise End-to-End

COBIT 5 mengintegrasikan IT enterprise pada organisasi pemerintahan dengan cara:

- Mengakomodasi seluruh fungsi dan proses yang terdapat pada enterprise. COBIT 5 tidak hanya fokus pada ‘fungsi IT’, namun termasuk pada pemeliharaan informasi dan teknologi terkait sebagai aset layaknya aset-aset yang terdapat pada enterprise.
- Mengakomodasi seluruh stakeholders, fungsi dan proses yang relevan dengan keamanan informasi.

Prinsip 3. Applying a Single, Integrated Network

COBIT 5 dapat disesuaikan dengan standar dan framework lain, serta mengizinkan perusahaan untuk menggunakan standar dan framework lain sebagai lingkup manajemen kerangka kerja untuk IT enterprise. COBIT 5 for Information Security

membawa pengetahuan dari versi ISACA sebelumnya seperti COBIT, BMIS, Risk IT, Val IT dengan panduan dari standar ISO/IEC 27000 yang merupakan standar ISF untuk keamanan informasi dan U.S. National Institute of Standars and Technology (NIST) SP800-53A.

Prinsip 4. Enabling a Holistic Approach

Pemerintahan dan manajemen perusahaan IT yang efektif dan efisien membutuhkan pendekatan secara holistik atau menyeluruh. COBIT 5 mendefinisikan kumpulan pemicu yang disebut enabler untuk mendukung implementasi pemerintahan yang komprehensif dan manajemen sistem perusahaan IT dan informasi. Enablers adalah faktor individual dan kolektif yang mempengaruhi sesuatu agar dapat berjalan atau 7 7enablers yang digunakan pada COBIT 5 meliputi:

1. Principles, Policies and Frameworks
2. Processes
3. Organisational Strucutres
4. Culture, Ethics and Behaviour
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies

Prinsip 5. Separating Governance from Management

COBIT 5 dengan tegas membedakan pemerintahan dan manajemen. Kedua disiplin ini memiliki tipe aktivitas yang berbeda, membutuhkan struktur organisasi yang berbeda dan memiliki tujuan yang berbeda. COBIT 5 melihat perbedaan tersebut berdasarkan sudut pandang berikut bekerja

6.5 **Pengertian Domain**

A. Cobit 4 mempunyai ada beberapa domain:

1. Perencanaan dan Organisasi (Plan and Organisation)

Domain ini mengutamakan tentang proses perencanaan dan penyelarasan strategi TI dengan strategi perusahaan, mencakup masalah strategi, taktik dan identifikasi cara terbaik IT dengan tujuan untuk mencapai tujuan bisnis organisasi sehingga dapat membentuk organisasi yang baik,

Domain ini mencakup :

a. PO1 – Menentukan rencana strategis
b. PO2 – Menentukan arsitektur informasi
c. PO3 – Menentukan arah teknologi
d. PO4 – Menentukan proses TI, organisasi dan hubungannya
e. PO5 – Mengelola investasi TI
f. PO6 – Mengkomunikasikan tujuan dan arahan manajemen
g. PO7 – Mengelola sumber daya manusia
h. PO8 – Mengelola kualitas
i. PO9 – Menilai dan mengelola resiko TI
j. PO10 – Mengelola proyek

Domain PO terdiri dari 10 sub proses.

a. PO1. Define a strategic IT plan Perencanaan IT yang strategis dibutuhkan untuk mengelola dan mengarahkan semua sumber daya IT agar sejalan dengan prioritas dan strategi bisnis. IT dan stakeholder bertanggung jawab untuk memastikan bahwa portofolio proyek dan layanan akan menghasilkan nilai yang optimal. NI telah memahami investasi wajib dalam bidang TI dan telah memiliki portofolio perusahaan. Namun pengolahan dan pengawasan terhadap penyimpanganpenyimpangan yang terjadi terhadap jadwal atau dana masih belum berjalan dengan baik.

b. PO2.Define the Information Architecture Sistem informasi berfungsi untuk menciptakan dan memperbarui model informasi bisnis secara teratur, serta menentukan sistem yang sesuai untuk mengoptimalkan penggunaan informasi. Prosesnya meliputi pengembangan kamus data perusahaan dengan aturan sintaks data organisasi, skema klasifikasi data dan tingkat keamanan. NI telah memahami tentang mengelola data untuk kepentingan perusahaan.

c. PO3. Determine technological direction Layanan informasi menentukan arah teknologi untuk mendukung bisnis. Harus ada rencana untuk membuat sebuah infrastruktur teknologi yang menetapkan dan mengelola harapan yang jelas dan realistis terhadap apa yang dapat ditawarkan oleh teknologi dalam hal produk, layanan, dan mekanisme pengiriman. NI telah mengetahui pentingnya strategi TI pada sebuah perusahaan dan masih memperbaiki infrastruktur yang belum optimal untuk sekarang.

d. PO4. Define the IT processes, organisation and relationships. Sebuah organisasi IT didefinisikan dengan mempertimbangkan persyaratan untuk staf, ketrampilan, fungsi, akuntabilitas, kewenangan, peran dan tanggung jawab, serta pengawasan. NI telah mengetahui kerangka proses teknologi informasi untuk melaksanakan rencana strategis teknologi informasi. Serta membentuk dan mengkomunikasikan peran dan tanggung jawab untuk personil teknologi informasi.Namun masih rendahnya praktek-praktek pengawasan yang memadai untuk memastikan bahwa peran dan tanggung jawab dilakukan dengan benar.

e. PO5 Manage the IT investment Sebuah kerangka ditetapkan dan dipertahankan untuk mengelola program investasi IT, dan yang mencakup

biaya, manfaat, prioritas dalam anggaran, proses penyusunan anggaran yang resmi, dan pengelolaan anggaran. Masih lemahnya pengelolaan aset dan anggaran IT guna mempertahankan kerangka keuangan untuk mengelola investasi pada PT. Nusantara Indah. Sehingga tidak terlaksanan penyediaan dan pemeliharaan kemampuan teknologi informasi yang tepat.

f. PO6 Communicate management aims and direction Manajemen mengembangkan sebuah kerangka pengendalian IT, serta menentukan dan menyampaikan kebijakan-kebijakan. Sebuah program komunikasi dilaksanakan secara terus menerus untuk menyuarakan misi, tujuan layanan, kebijakan dan prosedur, serta didukung dan disetujui oleh manajemen. NI menggelar dan menegakkan kebijakan teknologi informasi kepada semua staf yang relevan, tetapi peninjauan kebijakan tidak dilakukan secara berkala.

g. PO7 Manage IT human resources Seorang tenaga kerja yang kompeten diperoleh dan dipertahankan untuk menciptakan dan mengirimkan layanan IT kepada bisnis. NI melaksanakan proses untuk memastikan bahwa organisasi memiliki penempatan tenaga kerja teknologi informasi yang sesuai dengan ketrampilan yang diperlukan untuk mencapai tujuan organisasi. Namun proses verifikasi atas kopetensi personel masih kurang pengawasan dan transfer pengetahuan yang belum di atur dengan tepat.

h. PO8 Manage quality QMS dibangung dan dikelola yang berisi proses serta standar akusisi dan pengembangan yang telah teruji. Hal ini dicapai dengan cara perencanaan, implementasi serta pengelolaan QMS dengan memnyediakan kebutuhan kualitas, prosedur, dan peraturan yang jelas. Kebutuhan kualitas dinyatakan dan dikomunikasikan dalam indikator yang

dapat dicapai dan diukur secara quantitatif. NI telah menentukan dan merencanakan pengukuran untuk terus memantau kepatuhan terhadap quality management system dan nilai-nilainya pada semua staffnya.

i. PO9 Assess and manage IT risks Kerangka kerja manajemen resiko dibuat dan dikelola. Kerangka kerja mendokumentasikan resiko biasa ataupun resiko lain berdasarkan level yang sudah disetujui sebelumnya, strategis mitigasi, dan resiko residu. Dampak potensial apapun terhadap tujuan organisasi yang disebabkan oleh hal yang tak terencana diidentifikasi, dianalisa, dan dinilai. Strategi mitigasi resiko diadopsi untuk meminimalkan resiko residual sampai tingkat yang dapat diterima. NI telah melakukan penentuan konteks dimana kerangka penilaian risiko diterapkan untuk memastikan hasil yang tepat. NI telah mengidentifikasikan prioritas dan merencanakan kegiatan pengawasan disemua tingkatan untuk melaksanakan tanggapan resiko.\

j. PO10 Manage projects. Kerangka kerja manajemen proyek dan program untuk pengelolaan dari seluruh proyek IT dibangun. Keranga kerja menjamin prioritas dan koordinasi yang tepat dari seluruh proyek. Kerangka kerja meliputi master plan, penugasan sumber daya, definisi dari deliverables, persetujuan dari pengguna, pendekatan yang bertahap untuk delivery, QA, rencana pengujian formal, pengujian, dan peninjauan paska implementasi setelah instalasi untuk menjami manajemen resiko proyek dan value delivery ke bisnis. NI belum menetapkan rencana formal dan integrasi (meliputi bisnis dan sumber daya sistem informasi) untuk memandu pelaksanaan proyek. Tidak adanya penetapan tanggung jawab, wewenang dan kriteria kinerja anggota tim proyek

2. Pengadaan dan Implementasi (Acquire and Implement)

Domain ini berkaitan dengan implementasi solusi IT dan integrasinya dalam proses bisnis organisasi untuk mewujudkan strategi TI, juga meliputi perubahan dan *maintenance* yang dibutuhkan sistem yang sedang berjalan untuk memastikan tidak ada perubahan dalam proses mewujudkan tujuan organisasi

Domain ini meliputi:

AI1 – Mengidentifikasi solusi yang dapat diotomatisasi.

AI2 – Mendapatkan dan *maintenance* software aplikasi.

AI3 – Mendapatkan dan *maintenance* infrastuktur teknologi

AI4 – Mengaktifkan operasi dan penggunaan

AI5 – Pengadaan sumber daya IT.

AI6 – Mengelola perubahan

AI7 – Instalasi dan akreditasi solusi dan perubahan.

Adapun domain acquire and implement (AI) pada COBIT 4.1 membahas 7 sub domain sebagai berikut:

a) AI1 – Identify automated solutions; kebutuhan untuk aplikasi baru memerlukan analisis sebelum adanya akuisisi atau penciptaan untuk memastikan bahwa kebutuhan bisnis puas dalam pendekatan yang efektif dan efisien. Proses ini meliputi definisi kebutuhan, pertimbangan sumber alternatif, review kelayakan teknologi dan ekonomi, pelaksanaan analisis risiko dan analisis biaya-manfaat, dan kesimpulan atas keputusan akhir untuk 'membuat' atau 'membeli'. Semua

langkah memungkinkan organisasi untuk meminimalkan biaya untuk memperoleh dan menerapkan solusi sementara memastikan bahwa ada kemungkinan untuk mencapai tujuan.

b) AI2 – Acquire and maintain application software; aplikasi yang dibuat tersedia sesuai dengan kebutuhan bisnis. Proses ini meliputi desain aplikasi, memasukkan kontrol ke aplikasi sesuai persyaratan keamanan, dan pengembangan konfigurasi sesuai dengan standar. Hal ini memungkinkan organisasi untuk benar mendukung operasi bisnis dengan aplikasi otomatis yang benar.

c) AI3 – Acquire and maintain technology infrastructure; organisasi memiliki proses untuk pelaksanaan, akuisisi, dan upgrade dari infrastruktur teknologi. Ini membutuhkan pendekatan yang direncanakan untuk diakuisisi, pemeliharaan dan perlindungan infrastruktur sejalan dengan yang telah disepakati strategi teknologi dan penyediaan lingkungan pengembangan dan pengujian. Hal ini memastikan bahwa ada dukungan teknologi yang sedang berlangsung untuk aplikasi bisnis.

d) AI4 – Enable operation and use; tersedianya pengetahuan tentang sistem baru. Proses ini membutuhkan pembuatan dokumentasi dan manual bagi pengguna dan bagian IT. Penyediaan pelatihan untuk memastikan penggunaan yang tepat dan pengoperasian aplikasi dan infrastruktur.

e) AI5 – Procure IT resources; Sumber daya TI, termasuk SDM, hardware, software dan jasa, perlu diperoleh. Hal ini memerlukan definisi dan penegakan prosedur pengadaan, pemilihan vendor, setup pengaturan kontrak, dan akuisisi itu sendiri.

Memastikan bahwa organisasi memiliki semua yang diperlukan sumber daya TI secara tepat waktu dan hemat biaya.

f) AI6 – Manage changes; semua perubahan, termasuk perawatan darurat dan patch yang berkaitan dengan infrastruktur dan aplikasi dalam lingkungan produksi secara resmi dikelola dengan cara yang terkendali. Perubahan (termasuk parameter prosedur, proses, sistem dan layanan) akan dicatat, dinilai dan diberlakukan sebelum pelaksanaan dan ditinjau terhadap hasil yang direncanakan menyusul implementasi.

g) AI7 – Install and accredit solutions and changes; sistem baru perlu dibuat operasional setelah pembangunan selesai. Hal ini membutuhkan pengujian yang tepat dalam lingkungan khusus dengan data uji yang relevan, instruksi peluncuran dan migrasi, perencanaan rilis dan promosi yang sebenarnya untuk produksi, dan kajian pasca implementasi. Hal ini menjamin bahwa sistem operasional sejalan dengan yang disepakati

3. Pengantaran dan Dukungan (Deliver and Support)

Domain yang ketiga ini mencakup proses pemenuhan layanan IT, keamanan sistem, kontinyuitas layanan, pelatihan dan pendidikan untuk pengguna, dan pemenuhan proses data yang sedang berjalan.

Pada domain ini meliputi :

DS1 – Menentukan dan mengelola tingkat layanan.

DS2 – Mengelola layanan dari pihak ketiga

DS3 – Mengelola performa dan kapasitas.

DS4 – Menjamin layanan yang berkelanjutan

DS5 – Menjamin keamanan sistem.

DS6 – Mengidentifikasi dan mengalokasikan dana.

DS7 – Mendidik dan melatih pengguna

DS8 – Mengelola service desk dan insiden.

DS9 – Mengelola konfigurasi.

DS10 – Mengelola permasalahan.

DS11 – Mengelola data

DS12 – Mengelola lingkungan fisik

DS13 – Mengelola operasi.

Domain DS (Delevery and Support) pada cobit 4.1.

Deliver and Support (DS), domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan dan pendidikan untuk pengguna, dan pengelolaan data yang sedang berjalan. Domain DS terdiri dari 13 control objectives, yaitu : DS1 – Define and manage service levels, DS2 – Manage third-party services, DS3 – Manage performance and capacity, DS4 – Ensure continuous service, DS5 – Ensure systems security. DS6 – Identify and allocate costs, DS7 – Educate and train users,DS8 – Manage service desk and incidents, DS9 – Manage the configuration, DS10 – Manage problems, DS11 – Manage data, DS12 – Manage the physical environment, DS13 – Manage operations.

4. Pengawasan dan Evaluasi (Monitor and Evaluate)

Domain ini berfokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan intern dan ekstern dan jaminan independent dari proses pemeriksaan yang dilakukan. Semua proses TI perlu dinilai secara

teratur dan berkala bagaimana kualitas dan kesesuaiannya dengan kebutuhan kontrol.

Domain ini meliputi:

ME1 – Mengawasi dan mengevaluasi performansi TI.

ME2 – Mengevaluasi dan mengawasi kontrol internal

ME3 – Menjamin kesesuaian dengan kebutuhan eksternal.

ME4 – Menyediakan *IT Governance*.

Domain ME (Monitor and Evaluate) pada COBIT 4.

a. ME1 Monitor and Evaluate IT Peformance

Proses ini bertujuan untuk mengetahui apakah organisasi sadar akan kebutuhan proses pengawasan. Proses pengawasan ini termasuk dalam mendefinisikan indikator peforma pengendalian yang relevan, sistematik, dan sebuah laporan yang dilakukan secara berkala serta penanganan yang cepat saat terjadi masalah. Domain ini terbagi menjadi 6 sub-domain yaitu:

ME1.1 Monitoring Approach ,ME1.2 Definition and Collection of Monitoring Data, ME1.3 Monitoring Method ,ME1.4 Performance Assessment ,ME1.5 Board and Executive Reporting,ME1.6 Remedial Actions

b. ME2 Monitor and Evaluate Internal Control Membentuk program pengendalian internal yang efektif untuk TI membutuhkan proses monitoring yang jelas. Proses ini mencangkup pengawasan dan pelaporan kontrol pengecualian, hasil atas penilaian diri sendiri. Manfaat utama pengwasaan pengendalian internal adalah untuk memberikan kepastian mengenai efektifas dan efisiensi operasi dan kepatuhan dengan peraturan dan regulasi yang ada.

c. Domain ini terbagi menjadi 7 subdomain yaitu: ME2.1 Monitoring of Internal Control Framework, ME2.2 Supervisory Review, ME2.3 Control Exceptions,

ME2.4 Control Self-assessment , ME2.5 Assurance of Internal Control ,ME2.6 Internal Control at Third Parties , ME2.7 Remedial Actions Hasil evaluasi maturity l.ME3 Ensure Compliance with External Requirements Pengawasan kepatuhan yang efektif mengharuskan pembentukan proses review untuk memastikan kepatuhan terhadap undang-undang dan peraturan persyaratan kontrak. Proses ini mencakup indentifikasi persyaratan kepatuhan, optimalisasi dan evaluasi respon, mendapatkan jaminan bahwa persyaratan telah dipenuhi dan akhirnya mengintegrasikan laporan kepatuhan TI dengan bagian bisnis lainnya. Domain ini terbagi menjadi 5 sub-domain yaitu: ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements , ME3.2 Optimisation of Response to External Requirements, ME3.3 Evaluation of Compliance With External Requirements , ME3.4 Positive Assurance of Compliance ,ME3.5 Integrated Reporting.

d. ME4 Provide IT Governance

Membangun kerangka kerja tata kelola yang efektif termasuk pendefinisian struktur organisasi, proses, kepemimpinan, peran, dan tanggung jawab untuk memastikan bahwa investasi perusahaan IT selaras dan disampaikan sesuai dengan strategi dan objektif perusahaan. Domain ini terbagi menjadi 7 sub-domain yaitu: ME4.1 Establishment of an IT Governance Framework • ME4.2 Strategic Alignment,ME4.3 Value Delivery, ME4.4 Resource Management ,ME4.5 Risk Management, ME4.6 Performance Measurement , ME4.7 Independent Assurance

B. Dimensi Proses tata Kelola TI dalam COBIT 5

1. Evaluate, Direct, and Monitor (EDM)

Proses tata kelola berhubungan dengan tata kelola tujuan stakeholder (pengantaran nilai, optimasi risiko dan optimasi sumberdaya), serta termasuk di dalamnya praktik dan aktivitas yang bertujuan untuk mengevaluasi pilihan strategis, pengarahan menuju TI dan monitoring outcome (pengawasan terhadap hasil)

EDM Defined Process :

1. EDM01 Ensure governance framework setting and maintenance
2. EDM02 Ensure benefits delivery
3. EDM03 Ensure risk optimasion
4. EDM04 Ensure resource optimasion
5. EDM05 Ensure stakeholder transparancey

2. Align, Plan and Organise (APO)

Menyediakan panduan untuk Solution Delivery dan Service Delivery (BAI) serta pendukung (DSS).

Area ini melingkupi strategi dan taktik, serta mengidentifikasi cara terbaik dimana TI dapat berkontribusi dalam pencapaian tujuan bisnis.

Realisasi dari visi strategis harus direncanakan, dikomunikasikan dan dikelola pada perspektif yang berbeda.

Pengelolaan organisasi dan infrastruktur teknologi dengan layak

APO Proses terdiri dari :

1. APO01 Manage The IT management Framework
2. APO02 Manage Strategy
3. APO03 Manage Enterprise architecture
4. APO04 Manage innovation
5. APO05 Manage portfolio
6. APO06 Manage budget and costs

7. APO07 Manage human resources
8. APO08 Manage relationship
9. APO09 Manage service agreement
10. APO10 Manage suppliers
11. APO11 Manage quality
12. APO12 Manage risk
13. APO13 Manage security

3. Build, Acquire, and Implement (BAI)

• Menyediakan solusi dan mengantarkannya dalam sebuah layanan.

• Untuk merealisasikan strategi TI, solusi TI harus dapat diidentifikasi, dikembangkan dan diperoleh, serta diimplementasi dan diintegrasikan ke dalam proses bisnis

• Domain ini juga melingkupi perubahan dalam proses maintenance sistem yang ada,

untuk menjamin bahwa solusi TI dapat terus memenuhi tujuan bisnis.

BAI Defined Process :

1. BAI01 Manage programmes and projects
2. BAI02 Manage requirements anddefinitions
3. BAI03 Manage solutions identificationand build
4. BAI04 Manage availability adn capacity
5. BAI05 Manage organisational changeenablement
6. BAI06 Manage changes
7. BAI07 Manage change acceptance andtransitioning
8. BAI08 Manage knowledge
9. BAI09 Manage assets

10. BAI10 Manage configuration

4 . Deliver, Service and Support (DSS)

Domain ini fokus pada bagaimana penerimaan solusi dan kegunaannya dalam membantu user

Bagaimana pengantaran dan dukungan dari layanan yang dibutuhkan, termasuk di dalamnya pengantaran nilai, manajemen keamanan, layanan pendukung untuk user serta manajemen data dan fasilitas operasional.

DSS Defined Process :

1. DSS01 Manage opreations
2. DSS02 Manage service requests and incidents
3. DSS03 Manage problems
4. DSS04 Manage continuity
5. DSS05 Manage security services
6. DSS06 Manage business process control

5. Monitor, Evaluate, and Assess (MEA)

• Pengawasan terhadap semua proses menjamin bahwa arahan/panduan benarbenar dijalankan.

• Semua proses TI harus sering diukur untuk kualitas serta pemenuhannya dengan sebuah kebutuhan pengendalian.

• Domain ini meliputi manajemen performa, pengawasan terhadap pengendalian internal, kepatuhan terhadap peraturan dan tata kelola

MEA Defined Process:

1. MEA01 Monitor, evaluate and assess performance and conformance
2. MEA02 Monitor, evaluate and assess the system of internal control
3. MEA03 Monitor, evaluate and assess compliance with external requirements

6.6. MODEL KEMATANGAN dan Rumus Gab

Dalam Cobit ada tingkat kematangan yaitu:

a. Model kematangan (*maturity model*) digunakan sebagai alat untuk melakukan benchmarking dan self-assessment oleh manajemen teknologi informasi secara lebih efisien.
b. Model kematangan untuk pengelolaan dan kontrol pada proses teknologi informasi didasarkan pada metoda evaluasi perusahaan atau organisasi, sehingga dapat mengevaluasi sendiri, mulai dari level 0 (non-existent) hingga level 5 (optimised)

Capability Level yang diukur ada 2 (dua) macam yaitu *existing capability level* dan *target capability level* (ISACA, 2012).

Existing Capability Level

Pengukuran *existing capability level* menggunakan metode wawancara terhadap beberapa ahli di pemerintah daerah yang berhubungan dengan teknologi informasi, keuangan, sumber daya manusia dengan alat bantu COBIT 5 *Self Assessment Template* yang merupakan bagian dari COBIT 5 PAM. Terdapat beberapa tingkatan *capability level* pada proses pengukuran ini yaitu:

a. Level 0: Pada level ini proses tidak diimplementasikan atau gagal mencapai tujuannya, tidak ada atau sedikit sekali bukti yang menyatakan pencapaian tujuan proses.
b. Level 1: Pada level ini, proses yang dilaksanakan sudah mencapai tujuannya.
c. Level 2: Proses yang sudah dilaksanakan pada level sebelumnya, pada level ini pelaksanaan proses sudah dilaksanakan dengan perencanaan,

pengawasan dan penyesuaian serta hasil kerjanya sudah ditetapkan,diawasi dan dirawat dengan baik.

d. Level 3: Proses di level sebelumnya yang sudah diatur dengan baik, pada level ini proses didefinisikan untuk mencapai hasil prosesnya.
e. Level 4: Proses yang sudah dijalankan sebelumnya, pada level ini sudah beroperasi dalam batas yang ditentukan untuk mencapai hasil yang diharapkan.
f. Level 5: Proses yang sudah dijalankan di level sebelumnya, pada level ini ditingkatkan secara terus menerus untuk memenuhi tujuan organisasi saat ini dan yang diproyeksikan di masa mendatang.

Rumus dari perhitungan Audit Sistem Informasi

GAP yaitu Current Maturity – Expected Mantury

Current Manurity =Jumlah dari responden / Jumlah Responden

Nilai Rata Rata Yaitu : Jumlah per sub domain / jumlah domain yang dipakai

Indeks Kematangan	Level	Keterangan
0 - 0.49	0	0 – Non-Existent
0.50 – 1.49	1	1 – Initial/Ad Hoc
1.50 – 2.49	2	2 – Repeatable But Intutitive
2.50 – 3.49	3	3 – Defined Process
3.50 – 4.49	4	4 – Managed and Measureabel
4.50 – 5.00	5	5 - Optimized