



# **PERTEMUAN 1**

## **PENGANTAR AUDIT TEKNOLOGI INFORMASI**

# Kontak Perkuliahan

- Audit TI Merupakan mata kuliah berbasis Kompetensi
- Pertemuan 1 s.d 6 disampaikan dengan metode ceramah, metode diskusi dan latihan soal
- Pertemuan 7 diadakan QUIZ / review materi
- Pertemuan 8 diadakan UTS dimana materi diambil dari pertemuan 1-6
- Pada pertemuan 9 s.d 14 dilakukan presentasi per kelompok. Setiap pertemuan menampilkan beberapa kelompok



# Penjelasan Tugas KBK

1. Buat project kelompok (Max 5 mahasiswa)
2. Kelompok sudah ditentukan pada pertemuan 1
3. Tugas membuat Audit TI di sebuah perusahaan dengan menggunakan cobit.

# PENGERTIAN AUDIT TEKNOLOGI INFORMASI

“Audit Teknologi informasi adalah proses pengumpulan dan penilaian bukti – bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien”. Ron Weber (1999,10) mengemukakan bahwa audit sistem informasi adalah :

*” Information systems auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently”.*

# TUJUAN AUDIT TEKNOLOGI INFORMASI

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

## a. *Conformance* (Kesesuaian)

Pada kelompok tujuan ini audit teknologi 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).

# **TUJUAN AUDIT TEKNOLOGI INFORMASI (Lanjutan)**

Tujuan audit teknologi informasi menurut Ron Weber tujuan audit yaitu :

1. Mengamankan asset
2. Menjaga integritas data
3. Menjaga efektivitas sistem
4. Mencapai efisiensi sumberdaya.

# KEUNTUNGAN AUDIT

- Menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi
- Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
- Mengukur tingkat efektifitas dari sistem
- Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidaksesuaian di masa datang
- Menyediakan informasi untuk proses peningkatan
- Meningkatkan saling memahami antar departemen dan antar individu
- Melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen

# JENIS AUDIT IT

- System Audit
  - Audit terhadap sistem terdokumentasi untuk memastikan sudah memenuhi standar nasional atau internasional
- Compliance Audit
  - Untuk menguji efektifitas implementasi dari kebijakan, prosedur, kontrol dan unsur hukum yang lain
- Product / Service Audit
  - Untuk menguji suatu produk atau layanan telah sesuai seperti spesifikasi yang telah ditentukan dan cocok digunakan

# SIAPA YANG DI AUDIT ?

- Management
- IT Manager
- IT Specialist (network, database, system analyst, programmer, dll.)
- User

# SIAPA YG MENGAUDIT ?

Tergantung Tujuan Audit

- Internal Audit (First Party Audit)
  - Dilakukan oleh atau atas nama perusahaan sendiri
  - Biasanya untuk management review atau tujuan internal perusahaan
- Lembaga independen di luar perusahaan
  - Second Party Audit
    - Dilakukan oleh pihak yang memiliki kepentingan terhadap perusahaan
  - Third Party Audit
    - Dilakukan oleh pihak independen dari luar perusahaan. Misalnya untuk sertifikasi (ISO 9001, BS7799 dll).

# TUGAS AUDITOR SISTEM INFORMASI

- Memastikan sisi-sisi penerapan IT memiliki kontrol yang diperlukan
- Memastikan kontrol tersebut diterapkan dengan baik sesuai yang diharapkan

# HAL-HAL YANG DILAKUKAN AUDITOR

- Persiapan
- Review Dokumen
- Persiapan kegiatan on-site audit
- Melakukan kegiatan on-site audit
- Persiapan, persetujuan dan distribusi laporan audit
- Follow up audit

# OUTPUT KEGIATAN AUDIT

Hasil akhir adalah berupa laporan yang berisi:

- Ruang Lingkup audit
- Metodologi
- Temuan-temuan
- Ketidaksesuaian (sifat ketidaksesuaian, bukti2 pendukung, syarat yg tdk dipenuhi, lokasi, tingkat ketidaksesuaian)
- Kesimpulan (tingkat kesesuaian dengan kriteria audit, efektifitas implementasi, pemeliharaan dan pengembangan sistem manajemen, rekomendasi)

# Ketrampilan Yang Dibutuhkan

- **Audit skill :**  
sampling, komunikasi, melakukan interview, mengajukan pertanyaan, mencatat
- **Generic knowledge :**  
pengetahuan mengenai prinsip2 audit, prosedur dan teknik, sistem manajemen dan dokumen2 referensi, organisasi, peraturan2 yang berlaku
- **Specific knowledge :**  
background IT/IS, bisnis, specialist technical skill, pengalaman audit sistem manajemen, perundangan

# PRINSIP-PRINSIP AUDIT

- **Ethical conduct**
  - Berdasar pada profesionalisme, kejujuran, integritas, kerahasiaan dan kebijaksanaan
- **Fair Presentation**
  - Kewajiban melaporkan secara jujur dan akurat
- **Due Professional Care**
  - Implementasi dari kesungguhan dan pertimbangan yang diberikan
- **Independence**
- **Evidence-base Approach**

# Peraturan dan Standar Yang Biasa Digunakan

- ISO / IEC 17799 and BS7799
- Control Objectives for Information and related Technology (CobiT)
- ISO TR 13335
- IT Baseline Protection Manual
- ITSEC / Common Criteria
- Federal Information Processing Standard 140-1/2 (FIPS 140-1/2)
- The “Sicheres Internet” Task Force [Task Force Sicheres Internet]
- The quality seal and product audit scheme operated by the Schleswig-Holstein Independent State Centre for Data Privacy Protection (ULD)
- ISO 9000

# Kebutuhan Auditor IT

- Internal Audit -> setiap perusahaan memerlukan
- Perusahaan penyedia layanan audit
- Perusahaan penyedia sertifikasi

# Peluang

- Ketergantungan terhadap IT semakin besar sehingga muncul kebutuhan untuk melakukan audit IT
- Auditor IT yang sekarang banyak yang berasal bukan dari bidang IT
- Banyak permasalahan (bisnis) dalam pengelolaan IT



# **PERTEMUAN 2**

## **PENDEKATAN AUDIT TEKNOLOGI INFORMASI**

# Jenis Pendekatan Audit TI

Jenis Pendekatan Audit TI :

1. Pendekatan temuan (*Exposures Approach*)
2. Pendekatan Kendali (*Control Approach*)

Pesatnya perkembangan dunia komputer , diikuti dengan peningkatan pengetahuan 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.

# Kelompok Pendekatan Audit TI

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

- 1. Auditing around the computer*
- 2. Audit with the computer*
- 3. Audit through the computer*

# Kelompok Pendekatan Audit TI (Lanjutan)

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

1. *Test data approach*
2. *Paralel simulation*
3. *Embeded audit module approach*

# METODE AUDIT TI

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

- a. Metode pemahaman
- b. Evaluasi Kendali
- c. Menilai Kepatuhan
- d. Penilaian Resiko

# METODE AUDIT TI (Lanjutan)

## Langkah 1 : Metode pemahaman

- a. Mendokumentasikan aktivitas yang mendasari control objective demikian juga untuk mengidentifikasi stade control measure/procedure yang berlaku
- b. 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, laporan manajemen
- c. Mendokumentasikan proses yang berhubungan dengan sumber daya TI terutama yang dipengaruhi oleh proses direview.

# METODE AUDIT TI (Lanjutan)

## Langkah 2 :Evaluasi Kendali

- a. Menilai keefektifan *control maesure* yg berlaku atau tingkat pencapaian *control objective* .
- b. Mengevaluasi kesesuaian *control measure* dari proses yang direview dg mempertimbangkan kriteria yg diidentifikasi dan praktik standar industri, *Critical Success Factor* dan *Control measure* dan mengaplikasikan keputusan profesional audit.
- c. Melakukan proses dokumentasi, deliverable yang sesuai dihasilkan, tanggung jawab dan akuntabilitas yang jelas dan efektif, adanya pengendalian kompensasi sebagaimana mestinya
- d. Simpulkan sesuai tingkat *Control Objective*

# METODE AUDIT TI (Lanjutan)

## Langkah 3 : Menilai Kepatuhan

- a. Menjamin control measure yg ditetapkan , berjalan sebagaimana mestinya, secara konsisten dan berkelanjutan, serta menyimpulkan kesesuaian *control environment*.
- b. 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.
- c. Melakukan review terbatas ttg kecukupan proses *deliverable*.
- d. Menentukan tingkat pengujian substatif dan kerja tambahan yg dibutuhkan unt menyediakan jaminan proses IT adalah cukup.

# METODE AUDIT TI (Lanjutan)

## Langkah 4 : Penilaian Resiko

- a. Memperkirakan resiko dari control objective yg tidak dipenuhi, dg menggunakan teknik analitik dan atau mengkonsultasikan sumber2x alternative.
- b. Mendokumentasikan kelemahan kendali, serta ancaman dan kerawanan yg dihasilkan.
- c. Mengidentifikasikan dan mendokumentasikan dampak yg potensial maupun aktual.
- d. Menyediakan informasi komparatif, misalnya melalui *benchmark*.

# 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.

# JENIS-JENIS RESIKO

## 1. Risiko Bisnis (Business 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 external 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).

# JENIS-JENIS RESIKO (Lanjutan)

## 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.

## 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.

# JENIS-JENIS RESIKO (Lanjutan)

## 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 yang belum dapat mencerminkan keadaan sesungguhnya.

# JENIS-JENIS RESIKO (Lanjutan)

## 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.

# Jenis Resiko Menurut Jones dan Rama

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.***

# Jenis Resiko Menurut Jones dan Rama

## 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.

# Jenis Resiko Menurut Jones dan Rama

## 4. Performance Risk

Risiko kinerja ini adalah 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.

# Jenis Resiko Menurut Jones dan Rama

## 5. IT Security Risks

IT Security risks berkaitan dengan data integrity dan akses. Data integrity ialah keandalan dan konsistensi data di dalam system manajemen data organisasi akses ke komputer atau data oleh pihak tidak berwenang perlu ditanggulangi karena terkait dengan data integrity, privacy, dan seluruh keamanan system.

## 6. Continuity Risks

Continuity Risks berkaitan dengan ketersediaan/stabilitas (availability), back-up site, back-up file serta recovery pada system berbasis teknologi informasi. Back-up site adalah cadangan system (mesin cadangan atau mungkin instalasi yang berbeda lokasinya), sedangkan back-up file ialah cadangan file pada media off-line. Recovery ialah system pengembalian status terakhir bila suatu proses mengalami gangguan atau terhenti secara tidak normal.

# AUDIT RESIKO

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”.



# **PERTEMUAN 3**

## **PENGENDALIAN SISTEM KOMPUTERISASI**

# 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).

# Pengertian Sistem Pengendalian Internal (Lanjutan)

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

Berdasarkan Jenis :

1. *Preventive Detective, Dan Corrective* (Pencegahan, Deteksi Dan Koreksi )
2. *Discretionary Dan Non-discretionary* (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

# Sistem Pengendalian Umum (*General Control*)

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 .

# Sistem Pengendalian Umum *(General Control)*- Lanjutan

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**.

# Jenis-jenis Pengendalian

## 1. Organisasi & Manajemen

- Pemisahaan fungsi Depertemen TI dan Non TI
- Pemeriksaan fungsi dalam Depertemen TI
- Otorisasi Tranksasi
- Pengendalian Porsonil
- Perencanaan , Penganggaran dan sistem pembebasan kepada pemakai (user)

## 2. Piranti Lunak Dan Keras

- Pengendalian Piranti Keras (Hardware)
- Pengendalian Piranti Lunak (Software)

## 3. Pengendalian Akses

- Pembatasan Akses fisik dan Lojik
- Dokumentasi Program
- Fasilitas- Fasilitas On-line

# Jenis-jenis Pengendalian (Lanjutan)

## 4. Data dan Procedur

- Control Group
- File dan database
- Procedur- procedure standar
- Keamanan fisik
- Pemeriksaan Interen

## 5. Pengembangan Sistem Baru

- Partisipasi manajemen dan Pemakai
- Pengembangan Standar & pedoman
- Manajemen Proyek
- Pengujian sistem dan konversi
- Penelaahan setelah pemasangan

# Jenis-jenis Pengendalian (Lanjutan)

## 6. Pemeriharaan Program

- Otorisasi dan persetujuan
- Prosedur standar dan dekomentasi
- Pengendalian pemrogram dan pelaksanaan
- Pengujian terhadap perubahan

## 7. Dokumentasi

- Dokumentasi standar dan dekomentasi pendefinisian masalah
- Dokumentasi sistem
- Dokumentasi program
- Dokumentasi operasional
- Domentasi pemakai

# Pengendalian Pucuk Pimpinan

Pucuk pimpinan (*Top management*) adalah *board of director* atau disebut 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 teknologi informasi? Salah satu cara yang dapat dilakukan adalah dengan melihat bagaimana Top Management terkait dengan sistem informasi seperti layaknya tugas pokok dan fungsi management pada umumnya.

# Pengendalian Pucuk Pimpinan (Lanjutan)

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. Mengidentifikasi sumber daya yang di perlukan untuk menyediakan Teknologi dan sistem informasi yang di perlukan.
3. Membuat strategi dan takti yang di perlukan untuk memperoleh sumber daya tersebut.

# Jenis Perancangan Pengendalian

Jenis perancangan pengendalian dibedakan dalam 2 jenis, yaitu :

1. *Strategi Plan*
2. *Operational Plan,*

Hal ini harus selalu di review secara berkala dan di perbaharui jika di perlukan.

# Jenis Perancangan Pengendalian (Lanjutan)

*Strategi Plan* bersifat jangka panjang :

1. Penilaian terhadap kondisi Teknologi informasi saat ini, kekuatan ,kelemahan ,serta tantangan dan ancaman saat ini.
2. Tujuan dan arah jangka panjang , Jasa informasi masa depan harus di sediakan Strategi keseluruhaannya terhadap intraorganisasi maupun interotganisasi.
3. Strategi pengembang, Visi di bidang Teknologi informasi, Aplikasi masa depan, kebutuhan dana, Pendekatan dari monitoring terhadap pelaksanaan Strategi.

# Jenis Perancangan Pengendalian (Lanjutan)

## Operational Plan (Rencana Jangka Pendek) :

1. Progress report berisi keterangan tentang keberhasilan dan kegagalan pencapaian rencana sekarang. Perubahan yang besar terhadap *platform hardware-software*, hal-hal yang baru harus di lakukan.
2. *Initiatives to be undertaken*, berisi keterangan tentang perkembangan sistem perubahan *hardware-soft ware*, tambahan karyawan dan pengembangannya, penambahan sumber daya keuangan.
3. *Implementation Scheduler*, berisi keterangan tentang kapan mulai selesainya, setiap proyek utama , kejadian yang penting, prosedur control , proyek yang di terapkan.

# Operasional Komputer

Letak unit komputer di dalam suatu organisasi perlu di terapkan secara Tepat :

- a. Apakah merupakan unit fungsional sendiri yang di kepala oleh salah satu Eksecutive.
- b. Sebagai bagian dari unit fungsional administratif, atau sebagai bagian dari unit operasional.

# Struktur Organisasi Fungsi Teknologi Informasi

Secara Umum Teknologi 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 database, ahli komunikasi data)

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

# Pengendalian Manajemen Pengembangan Sistem

Pengendalian, pengembangan dan pemeliharaan sistem diperlukan untuk mencegah dan mendeteksi Kemungkinan kesalahan pada waktu pengembangan dan pemeliharaan sistem, serta untuk memperoleh keyakinan memadai bahwa sistem berbasis teknologi informasi di kembangkan dan di pelihara dengan cara efisien 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 .

# 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 .

# Perencanaan Sistem (Lanjutan)

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

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

# Perencanaan Sistem (Lanjutan)

Menurut Pressman (2001, p20-29 ) rekayasa Software adalah aplikasi dari pendekatan kuantifiabel, disiplin, 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 Engineering, Analysis, Design, Coding, Testing dan Maintanence*.

# 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).

# Interaksi Manusia dan Komputer (Lanjutan)

Dalam merancang suatu sistem interaksi manusia dengan 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 berinteraksi dengan komputer sehingga perintah dan fasilitas yang tersedia lebih mudah di mengerti dan lebih cepat di akses.
3. Memberikan umpan balik yang informatif, 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.

# Interaksi Manusia dan Komputer (Lanjutan)

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 membuat kesalahan contohnya jika suatu kolom isian tidak di perbolehkan pengisian jenis alphabet , maka jika di isi alphabet layar harus segera memberikan error message

## Interaksi Manusia dan Komputer (Lanjutan)

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.

# ***System Development Life Cycle Approach***

*System development life cycle approach* adalah metode pengembangan 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*

Menentukan keperluan user

c. *Sistem Design,*

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

# ***System Development Life Cycle Approach***

## *d. Program Development*

*Design, coding, 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 maintenance*

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

# PERTEMUAN 4

## PENGENDALIAN MANAJEMEN SUMBER DATA

- ✓ Pengendalian manajemen adalah proses yang digunakan oleh organisasi untuk memastikan bahwa tujuan dan sasaran tercapai dengan efektif dan efisien.
- ✓ Proses ini melibatkan pemantauan kinerja dan pengambilan tindakan korektif jika diperlukan.
- ✓ Dalam konteks pengendalian manajemen, **sumber data** memainkan peran yang sangat penting untuk membantu membuat keputusan yang informasional dan berbasis bukti.

- Pengendalian sumber data dalam **teknologi informasi (TI)** merujuk pada proses dan mekanisme yang digunakan untuk memastikan bahwa data yang digunakan dalam sistem TI dikelola dengan baik, terlindungi, dan dapat diakses dengan tepat untuk mendukung pengambilan keputusan serta operasi organisasi.
- Dalam konteks TI, pengendalian sumber data melibatkan kontrol atas kualitas, keamanan, dan keberlanjutan data yang digunakan di berbagai sistem informasi.



# Tujuan Pengendalian Sumber Data dalam Teknologi Informasi

- Menjamin Keakuratan dan Kualitas Data
- Keamanan Data
- Aksesibilitas dan Ketersediaan Data
- Integritas Data
- Pemantauan dan Pelaporan

# Jenis Pengendalian Sumber Data dalam Teknologi Informasi

- Pengendalian Akses (Access Control)
- Pengendalian Keamanan Data
- Backup dan Pemulihan Data (Data Backup and Recovery)
- Pengendalian Kualitas Data (Data Quality Control)
- Audit dan Pemantauan (Audit and Monitoring)
- Manajemen Siklus Hidup Data (Data Lifecycle Management)

# Teknologi yang Mendukung Pengendalian Sumber Data

## ✓ **Sistem Manajemen Basis Data (DBMS)**

DBMS dilengkapi dengan fitur-fitur pengendalian akses, enkripsi, dan backup

## ✓ **Sistem Keamanan TI**

Menggunakan perangkat lunak keamanan seperti firewall, antivirus, dan alat deteksi intrusi untuk melindungi data dari ancaman eksternal dan internal

## ✓ **Cloud Storage and Backup Solutions**

Solusi penyimpanan berbasis cloud seperti Google Cloud, AWS, atau Microsoft Azure menyediakan pengendalian akses, backup otomatis, dan pemulihan data secara terpusat.

## ✓ **Platform Pemantauan dan Analisis**

Alat seperti Splunk, Datadog, atau Zabbix digunakan untuk memantau penggunaan data dan kinerja sistem secara real-time

# 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).



# Tugas data administration ( DA) dan database administrator ( DBA)

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 efisiensi 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 komunikasi antara pemakai dan database.

# Definisi Sistem Database

Pada sistem database ada tiga tipe pendefinisian yang harus dilakukan 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

# Definisi Sistem Database (Lanjutan)

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.

## Database integrity

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.

# Database integrity

*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 pengubahan database hanya oleh user database yang sah saja. Otorisasi update terdiri dari dua hal : penambahan database pada database dan wewenang untuk mengubah dan menghapus data yang ada.

# Database integrity (Lanjutan)

- 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 konsistensi 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.

# PERTEMUAN 5

## TATA KELOLA TEKNOLOGI INFORMASI

# 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

# Tata Kelola TI

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

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

# Pentingnya 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.

# Pengabaian Tata Kelola TI

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

# Manfaat Tata kelola TI

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

# Fokus utama Area Tata Kelola TI



# *Strategic alignment*

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

# *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

# *Resource management*

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

# *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.

# *Performance measurement*

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

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (1)

## *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.

# MODEL TATA KELOLA TEKNOLOGI INFORMASI (2)

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.

# MODEL TATA KELOLA TEKNOLOGI INFORMASI (3)

## 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

# MODEL TATA KELOLA TEKNOLOGI INFORMASI (4)

## 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*

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (5)

COSO framework terdiri dari 3 dimensi yaitu:

## 3. 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.*

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (6)

## 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.

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (7)

## 3.3. Unit/Aktifitas Terhadap Organisasi

Dimensi ini mengidentifikasi 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.

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (8)

## *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.*

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (9)

## ***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 pengelolaan TI pada organisasi.

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (10)

**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*).

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (11)

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*

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (12)

## 1. *Critical Success Factors (CSF) –*

**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 yang dilakukan.
- d. Konfirmasi reliabilitas, efektifitas, dan compliance.

# MODEL TATAKELOLA TEKNOLOGI INFORMASI (13)

## *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.

# PERTEMUAN 6

IMPLEMENTASI COBIT  
*Control Objectives for Information  
and related Technology*

# Tantangan Manajemen dalam Penggunaan SIM

1. Bagaimana merancang sistem yang tidak mengakibatkan terjadinya pengendalian yang berlebih (*overcontrolling*) atau pengendalian yang terlalu lemah (*undercontrolling*).
2. Bagaimana pemenuhan standar jaminan kualitas (*quality assurance*) dalam aplikasi sistem informasi.

# Mengapa informasi begitu rentan?

1. Kerusakan perangkat keras.
2. Perangkat lunak tidak berfungsi.
3. Tindakan-tindakan personal.
4. Penetrasi akses ke terminal.
5. Pencurian data atau peralatan.
6. Kebakaran.
7. Permasalahan listrik.
8. Kesalahan-kesalahan pengguna.
9. Program berubah.
10. Permasalahan-permasalahan telekomunikasi.

# Kendala Penggunaan SI

## 1. Bencana (*disaster*)

untuk pencegahan atau meminimalkan dampak bencana:

- a. Rencana Kesinambungan Kegiatan (pada perusahaan dikenal dengan *Business 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.



# Kendala Penggunaan SI

## 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*)

Kesalahan (error) 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.

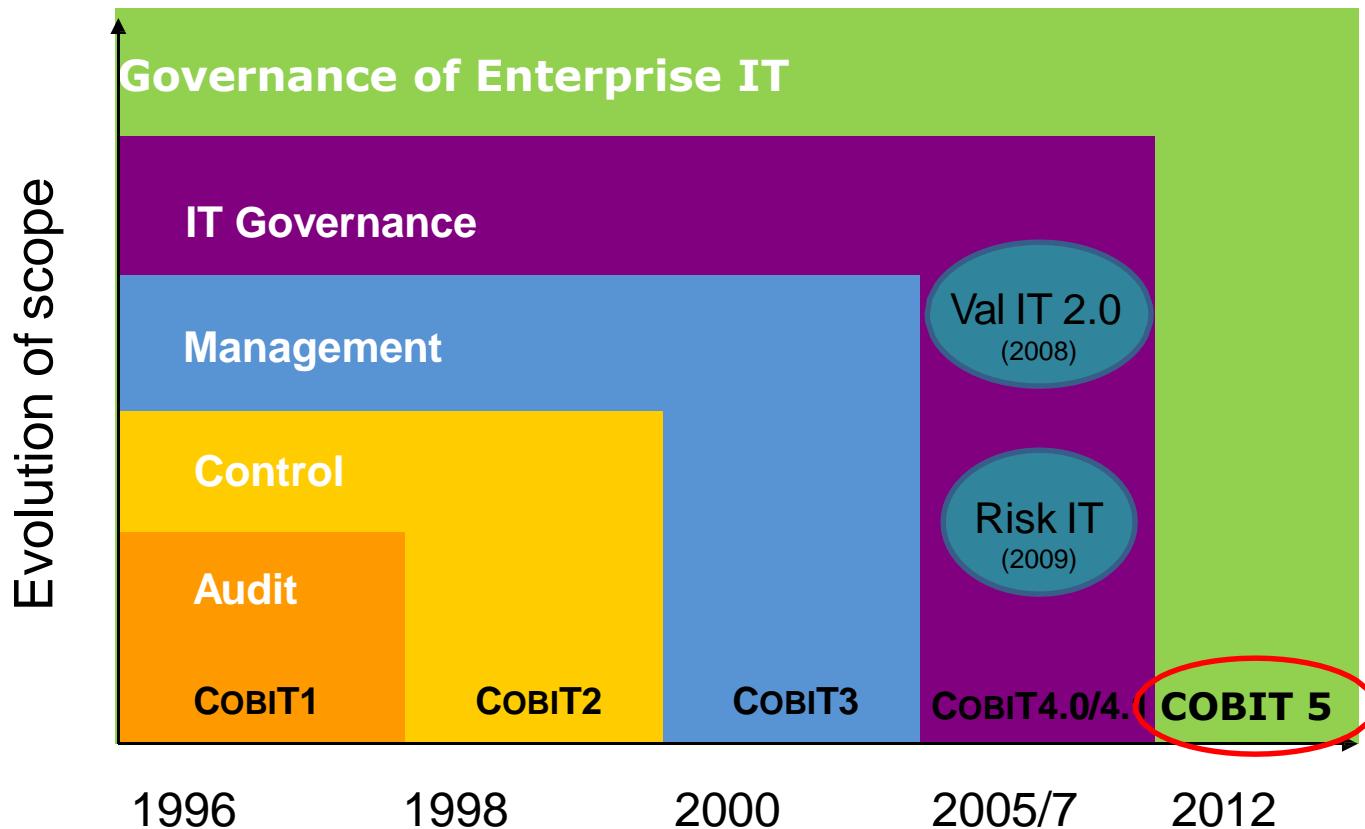
# Tujuan Keamanan Sistem Informasi

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.

# Apa itu COBIT...?

- Cobit dirancang sebagai alat penguasaan IT yang membantu dalam pemahaman dan mengelola resiko, manfaat serta evaluasi yang berhubungan dengan IT
- *Control Objectives for Information and related Technology*

# COBIT 5: Now One Complete Business Framework



An business framework from ISACA, at [www.isaca.org/cobit](http://www.isaca.org/cobit)

# COBIT: Sebuah kerangka kontrol TI

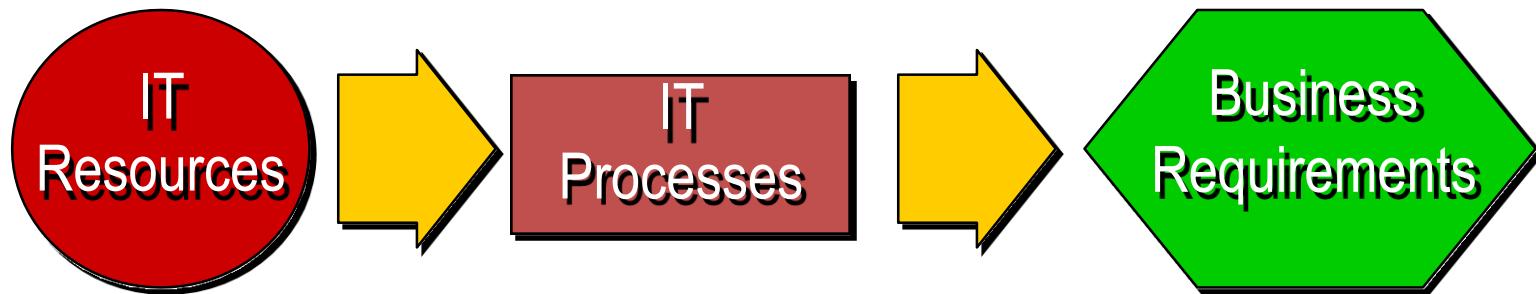
## COBIT's Vision

Sebagai model untuk penguasaan IT

## COBIT's Mission

Melakukan penelitian, pengembangan, publikasi dan promosi terhadap control objective dari teknologi informasi yang secara umum diterima di lingkungan internasional untuk pemakaian sehari-hari oleh manager dan auditor

# COBIT Framework



- ➲ Data
- ➲ Information Systems
- ➲ Technology
- ➲ Facilities
- ➲ Human Resources

- ➲ Plan and Organise (Perencanaan & Org.)
- ➲ Acquire and Implement (Pengadaan & Implementasi)
- ➲ Deliver and Support (Pengantaran & dukungan)
- ➲ Monitor and Evaluate (Pengawasan &Evaluasi)

- ➲ Effectiveness(efektifitas)
- ➲ Efficiency (Efisiensi)
- ➲ Confidentiality (Rahasia)
- ➲ Integrity (Integritas)
- ➲ Availability (Ketersediaan)
- ➲ Compliance (Pemenuhan)
- ➲ Information Reliability (Kehandalan Informasi)

# COBIT Framework

?  
ate  
rel  
  
they  
o  
d  
  
How  
Facilities  
Technology

- ➡ Data
- ➡ Information Systems
- ➡ Facilities Technology
- ➡ Human Resources



Tersedianya IT sumber daya

Bagaimana IT diorganisir utk bereaksi thd suatu kebutuhan

Apa yang stakeholders harapkan dari IT



- ➡ Planning and organisation
- ➡ Acquisition and implementation
- ➡ Delivery and Support
- ➡ Monitoring



- ➡ Effectiveness
- ➡ Efficiency
- ➡ Confidentiality
- ➡ Integrity
- ➡ Availability
- ➡ Compliance
- ➡ Information Reliability

# COBIT terdiri dari 4 domain, yaitu:

- Planning & Organization
- Acquisition & Implementation
- Delivery & Support
- Monitoring & Evaluation

# COBIT Framework (IT Proses) 1

## Domains

### *Plan and Organise/ Perencanaan & Pengorganisasi*

#### Topics

- Strategi dan taktik
- Merencanakan Visi
- Organisasi and infrastruktur

#### Questions

- Apakah IT dan strategi bisnis sudah ditetapkan?
- Apakah perusahaan sudah menggunakan secara maksimum sumber dayanya?
- Apakah semua orang di dlm org. sudah memahami sasaran IT?
- Apakah resiko IT sudah dipahami & diatur?
- Apakah mutu sistem IT sudah sesuai dgn kebutuhan bisnis?

### *Acquire and Implement Pengadaan & implemtasi*

#### Topics

- IT solutions
- Perubahan dan Pemeliharaan

#### Questions

- Apakah proyek baru dapat memberikan solusi terhadap kebutuhan bisnis?
- Apakah proyek baru dapat selesai tepat waktu dan sesuai anggaran?
- Apakah sistem kerja yg baru bisa diterapkan dgn baik?
- Apakah perubahan yg dibuat tdk merepotkan kegiatan bisnis yg berjalan?

# COBIT Framework (IT Proses) 2

## *Deliver and Support / Layanan & dukungan*

### Topics

- Layanan pengantaran& dukungan
- Dukungan proses penyusunan
- Pengolahan sistem aplikasi

### Questions

- Apakah layanan IT yg diberikan sesuai dgn prioritas bisnis?
- Apakah biaya IT dapat dioptimalkan?
- Apakah pekerja mampu menggunakan sistem IT lebih produktif dan aman?
- Apakah keamanan, integritas dan ketersediaan sudah pada tempatnya?

## *Monitor and Evaluate/ Kontrol & evaluasi*

### Topics

- Penilaian over time, jaminan pengiriman
- Sistem pengendalian manajemen kesalahan
- Pengukuran pekerjaan

### Questions

- Dapatkan IT mendeteksi suatu permasalahan sebelum semuanya terlambat?
- Apakah jaminan kemandirian yg diperlukan dpt memastikan bidang2 kritis bisa beroperasi sesuai dgn yg diharapkan?

# COBIT Framework (Business Requirement)

## 1. Efektivitas

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

## 2. Evisensi

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

# COBIT Framework (Business Requirement)

## 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

# COBIT Framework

## Waterfall Model

*The control of*  
*(kendali)*

IT Processes

*which satisfy*  
*(yang mencakupi)*

Business Requirements

*is enabled by*  
*(dimungkinkan)*

Control Statements

*Considering*  
*(mempertimbangkan)*

Control Practices

## Business Objectives

### Criteria

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

# COBIT Framework

- PO1 Define a strategic IT plan (menggambarkan)
- PO2 Define the information architecture
- PO3 Determine the technological direction (menentukan)
- PO4 Define the IT organisation and relationships
- PO5 Manage the IT investment
- PO6 Communicate management aims and direction
- PO7 Manage human resources
- PO8 Ensure compliance with external requirements (memastikan)
- PO9 Assess risks (menilai)
- PO10 Manage projects
- PO11 Manage quality

- M1 Monitor the process
- M2 Assess internal control adequacy
- M3 Obtain independent assurance
- M4 Provide for independent audit

### IT RESOURCES

- Data
- Application systems
- Technology
- Facilities
- People

### PLAN AND ORGANISE

### MONITOR AND EVALUATE

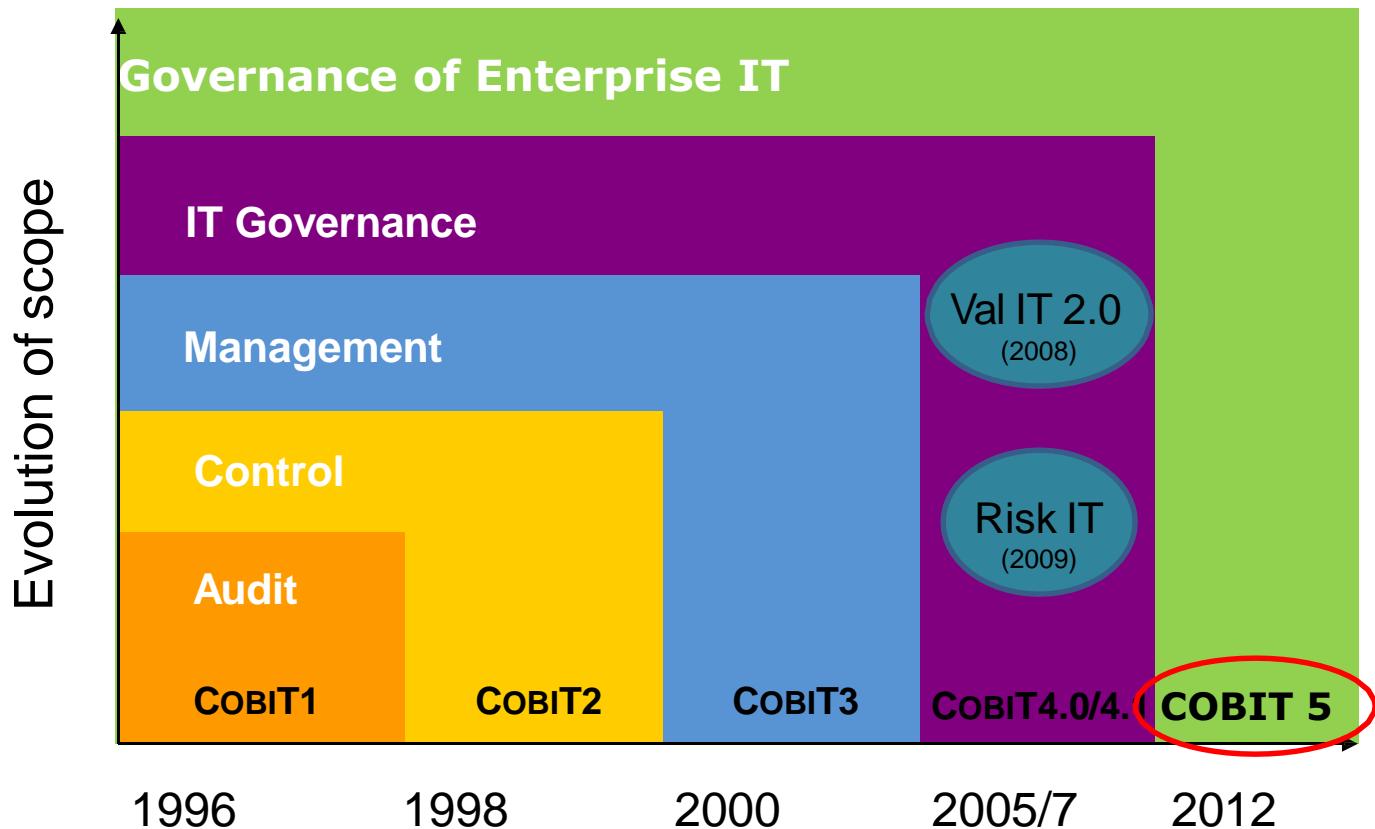
- DS1 Define service levels
- DS2 Manage third-party services
- DS3 Manage performance and capacity
- DS4 Ensure continuous service
- DS5 Ensure systems security
- DS6 Identify and attribute costs
- DS7 Educate and train users
- DS8 Assist and advise IT customers
- DS9 Manage the configuration
- DS10 Manage problems and incidents
- DS11 Manage data
- DS12 Manage facilities
- DS13 Manage operations

### ACQUIRE AND IMPLEMENT

- AI1 Identify automated solutions
- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology infrastructure
- AI4 Develop and maintain IT procedures
- AI5 Install and accredit systems
- AI6 Manage changes

### DELIVER AND SUPPORT

# COBIT 5: Now One Complete Business Framework



An business framework from ISACA, at [www.isaca.org/cobit](http://www.isaca.org/cobit)

© 2012 ISACA® All rights reserved.

# MODEL KEMATANGAN

- Model kematangan (*maturity model*) digunakan sebagai alat untuk melakukan benchmarking dan self-assessment oleh manajemen teknologi informasi secara lebih efisien.
- 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).

# Tabel Model Kematangan (maturity Model)

Level	Kriteria Kematangan
0 Non Existent	Kekurangan yang menyeluruh terhadap proses apapun yang dapat dikenali. Perusahaan bahkan tidak mengetahui bahwa terdapat permasalahan yang harus diatasi
1 Initial / Ad Hoc	Terdapat bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Bagaimanapun juga tidak terdapat proses standar, namun menggunakan pendekatan <i>ad hoc yang cenderung diperlakukan secara individu atau per kasus. Secara umum pendekatan kepada pengelolaan proses tidak terorganisasi.</i>
2 Repeatable but intituitive	Proses dikembangkan ke dalam tahapan yang prosedur serupa diikuti oleh pihak-pihak yang berbeda untuk pekerjaan yang sama. Tidak terdapat pelatihan formal atau pengkomunikasian prosedur standar dan tanggung jawab diserahkan kepada individu masing-masing. Terdapat tingkat kepercayaan yang tinggi terhadap pengetahuan individu sehingga kemungkinan terjadi <i>error sangat besar</i> .

# Tabel Model Kematangan (maturity Model)

Level	Kriteria Kematangan
3 Defined	Prosedur distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Kemudian diamanatkan bahwa proses-proses tersebut harus diikuti. Namun penyimpangan tidak mungkin dapat terdeteksi. Prosedur sendiri tidak lengkap namun sudah memformalkan praktek yang berjalan.
4 Managed and measurable	Manajemen mengawasi dan mengukur kepatutan terhadap prosedur dan mengambil tindakan jika proses tidak dapat dikerjakan secara efektif. Proses berada dibawah peningkatan yang konstan dan penyediaan praktek yang baik. Otomatisasi dan perangkat digunakan dalam batasan tertentu
5 Optimised	Proses telah dipilih ke dalam tingkat praktek yang baik, berdasarkan hasil dari perbaikan berkelanjutan dan permodelan kedewasaan dengan perusahaan lain. Teknologi informasi digunakan sebagai cara terintegrasi untuk mengotomatisasi alur kerja, penyediaan alat untuk peningkatan kualitas dan efektifitas serta membuat perusahaan cepat beradaptasi