

# KENDALI DAN AUDIT SISTEM INFORMASI (KASI)

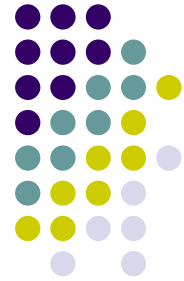


Oleh :

**Solikin, M.T.**

solikin2004@yahoocom

# KENDALI DAN AUDIT SISTEM INFORMASI (KASI)



Beban Kredit 3 SKS

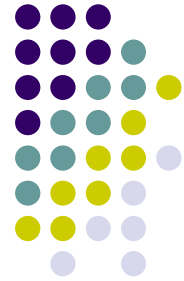
Tujuan :

- Mempelajari Pengelolaan SI pada lingkungan Enterprise
- Memahami Pengendalian SI suatu Enterprise
- Memahami Audit SI suatu Enterprise

Prasyarat :

Analisis dan Perancangan Sistem Informasi

# SILABUS MATA KULIAH



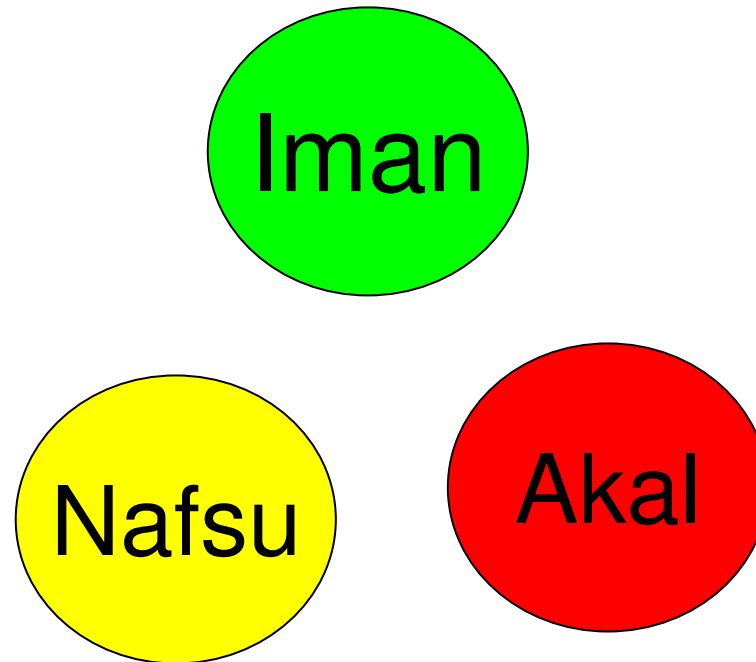
1. Pendahuluan : Auditing SI, Pelaksanaan Audit SI
2. Kerangka Kerja Pengendalian Manajemen : Pengendalian Top Manajemen, Pengendalian Manajemen Pengembangan Sistem, Pengendalian Manajemen Programming, Pengendalian Manajemen Sumber Data, Pengendalian Manajemen Keamanan, Pengendalian Manajemen Operasional, Pengendalian Manajemen Jaminan Kualitas.
3. Kerangka Kerja Pengendalian Aplikasi : Pengendalian Batasan (*Boundary*), Pengendalian Masukan, Pengendalian Komunikasi, Pengendalian Pemrosesan, Pengendalian Basis Data, Pengendalian Keluaran
4. Pengumpulan Bukti : Audit Software; Tinjauan pengkodean, Tes Data, dan Perbandingan Data; Teknik Auditing Concurrent; Interview, Kuesioner dan Flowchart Pengendalian; Alat Pengukuran Kinerja.
5. Evaluasi Bukti : Evaluasi Perlindungan aset dan integritas data, Evaluasi efektifitas sistem, Evaluasi efisiensi sistem.
6. Manajemen Audit SI : Pengelolaan Fungsi Audit SI

# KEPUSTAKAAN

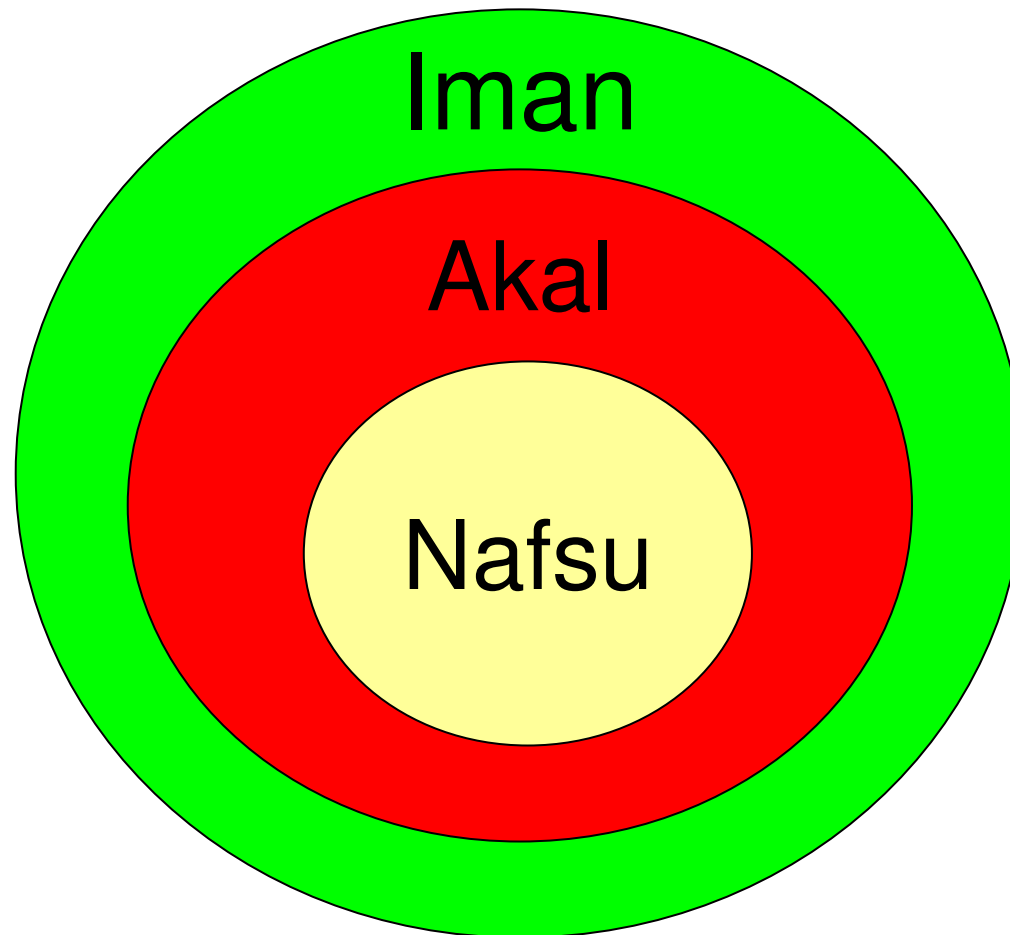
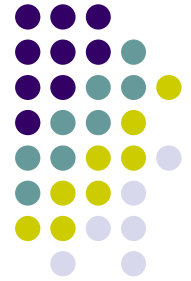


1. Indikator Bacaan :
2. Ron Weber, *“Information Systems Control and Audit”*, Prentice-Hall, USA., 1999.
3. GAO, *“Federal Information System Controls Audit Manual, Volume I :Financial Statement Audits”*, 1999
4. Edi Purwono, *“Aspek-aspek EDP Audit Pengendalian Internal pada Komputerisasi”*, Andi, Jogjakarta, 2004
5. IT Governance Institute (2000), *Executive Summary*, COBIT 3rd Edition, <http://www.isaca.org>.
6. IT Governance Institute (2000), *Audit Guidelines*, COBIT 3rd Edition, <http://www.isaca.org>.
7. IT Governance Institute (2000), *Management Guidelines*, COBIT 3rd Edition, <http://www.isaca.org>.
8. IT Governance Institute (2000), *Implementation Tool Set*, COBIT 3rd Edition, <http://www.isaca.org>.
9. Yayasan Pendidikan Internal Audit (2002), Institut Pendidikan dan Pelatihan Audit dan Manajemen, *Audit Sistem Informasi II*, Jakarta.

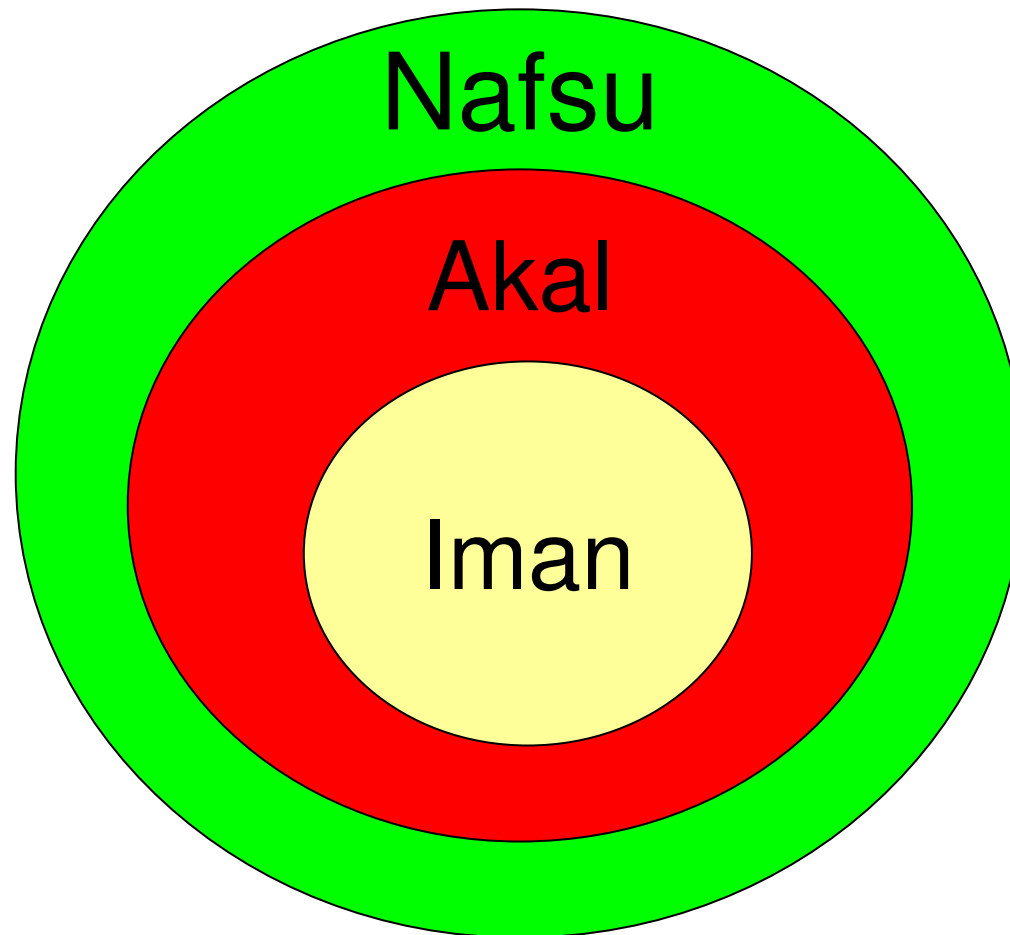
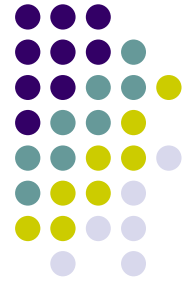
# Mengukur Diri Kita



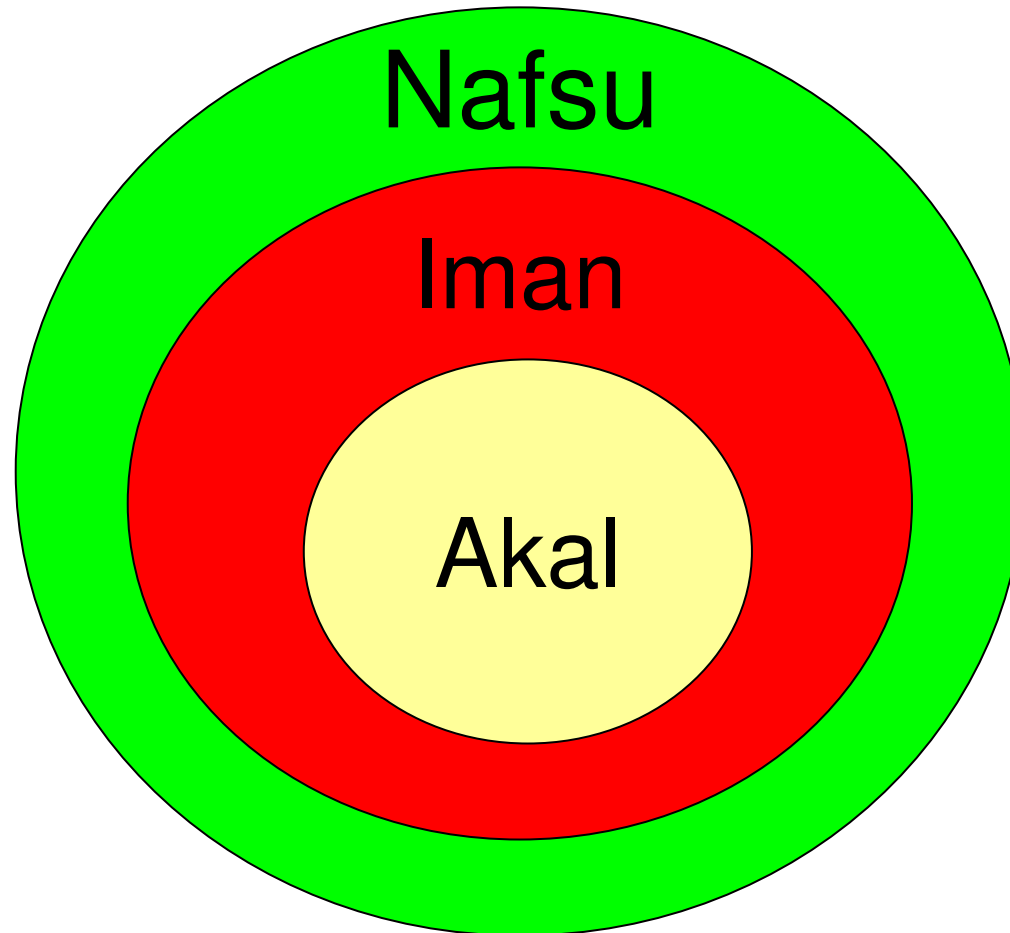
# Mengukur Diri Kita



# Mengukur Diri Kita

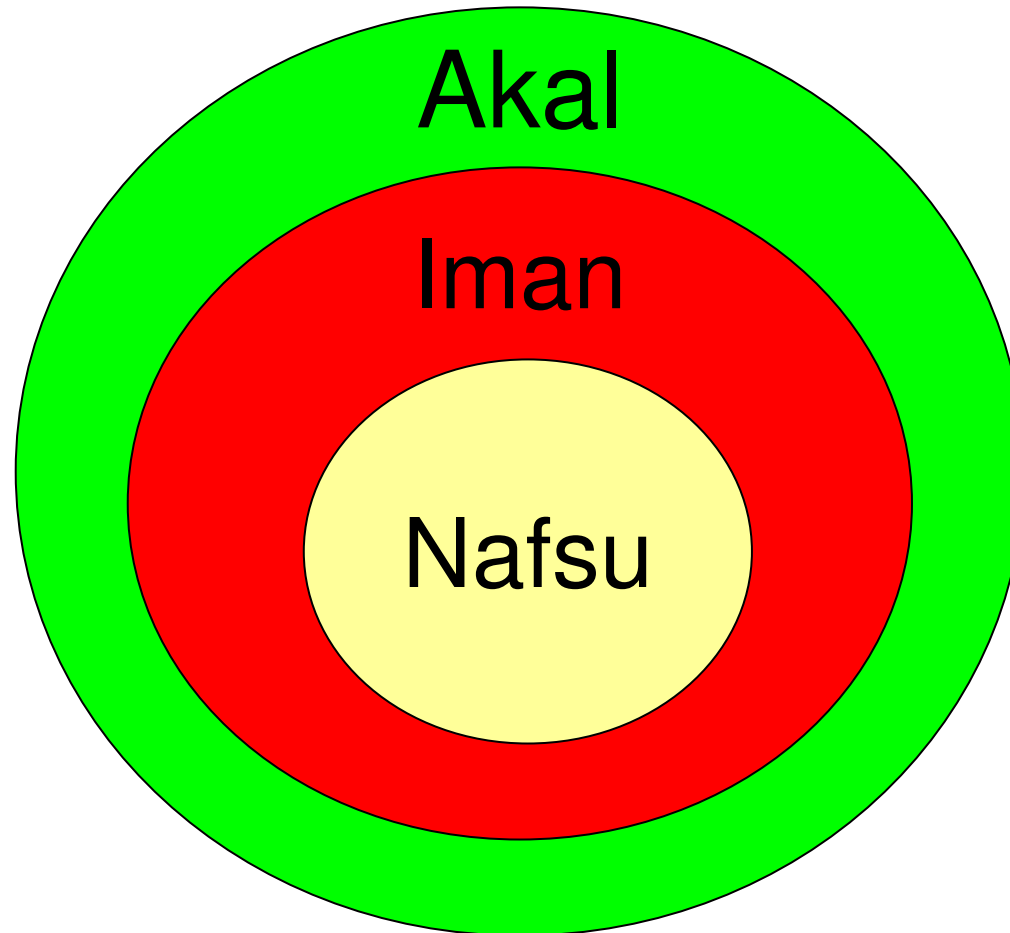
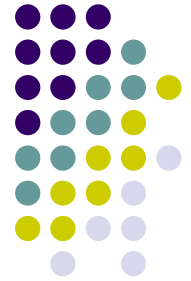


# Mengukur Diri Kita

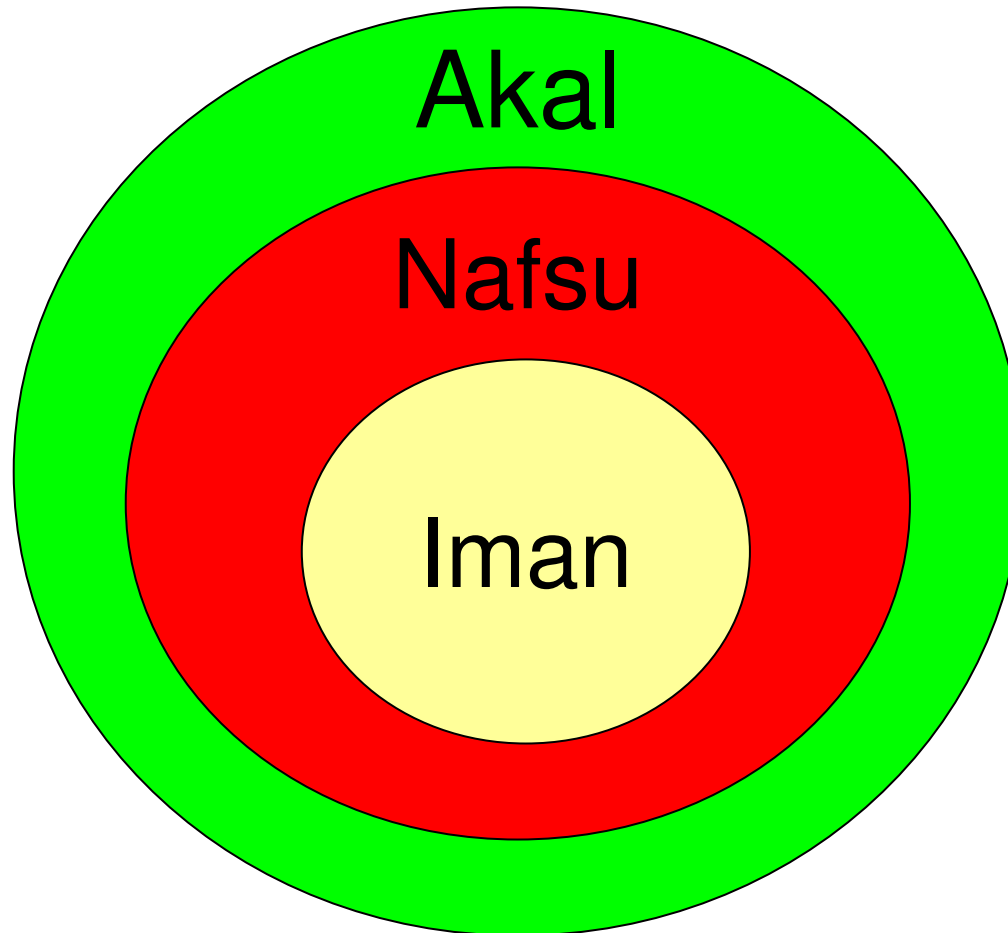




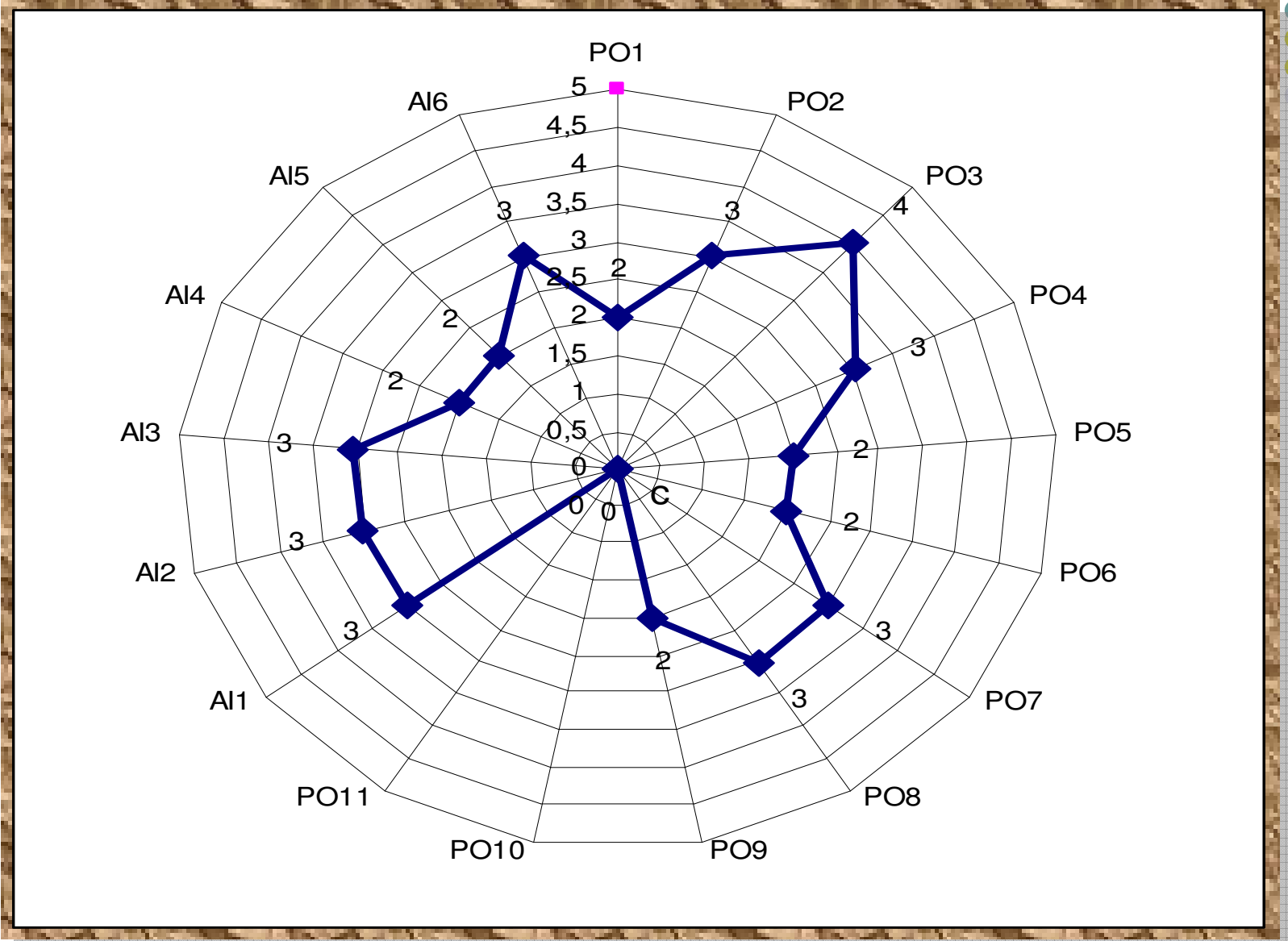
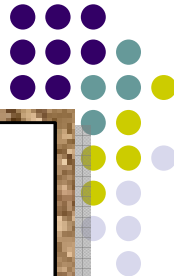
# Mengukur Diri Kita



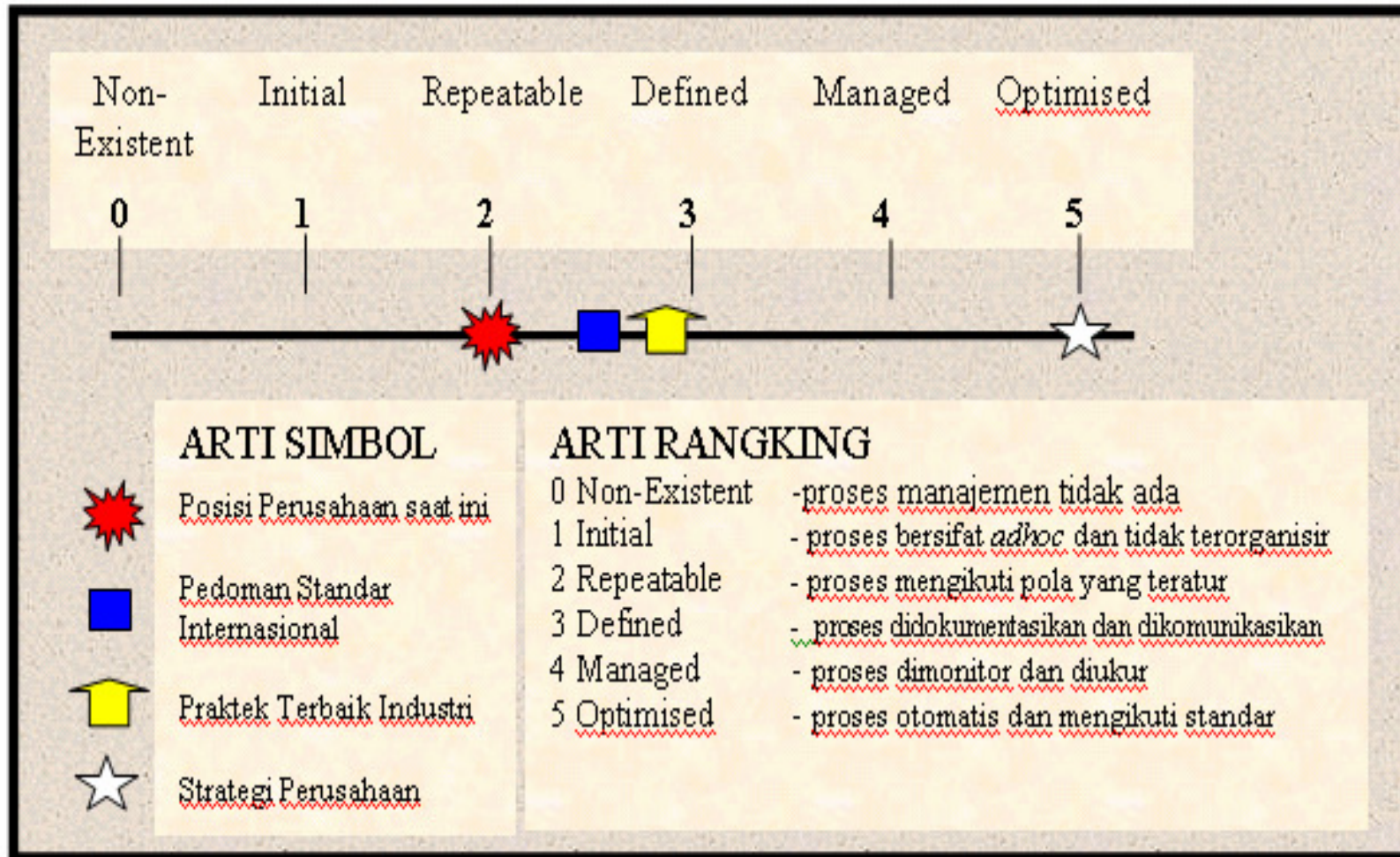
# Mengukur Diri Kita



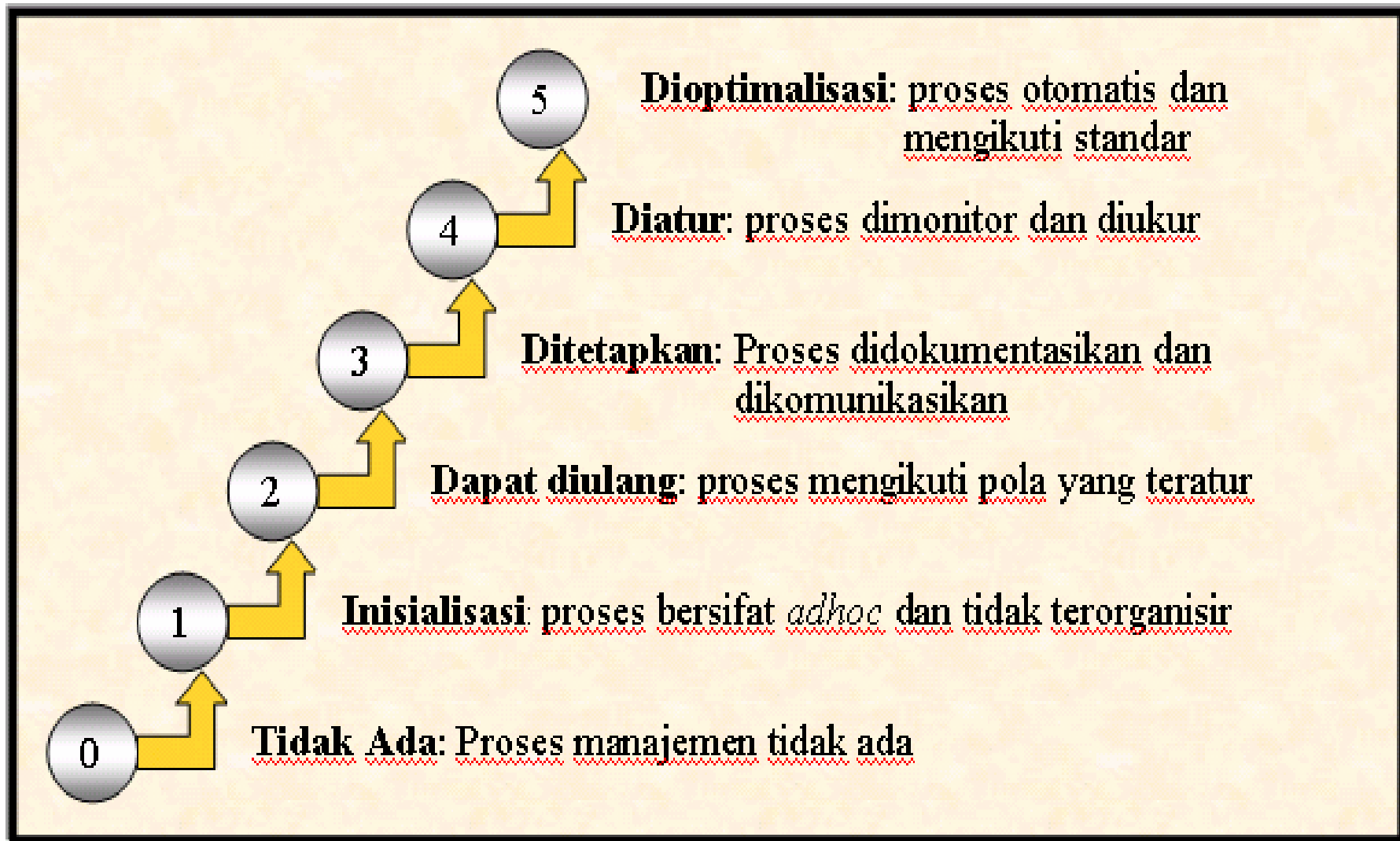
# Hasil Analisis SI Institusi



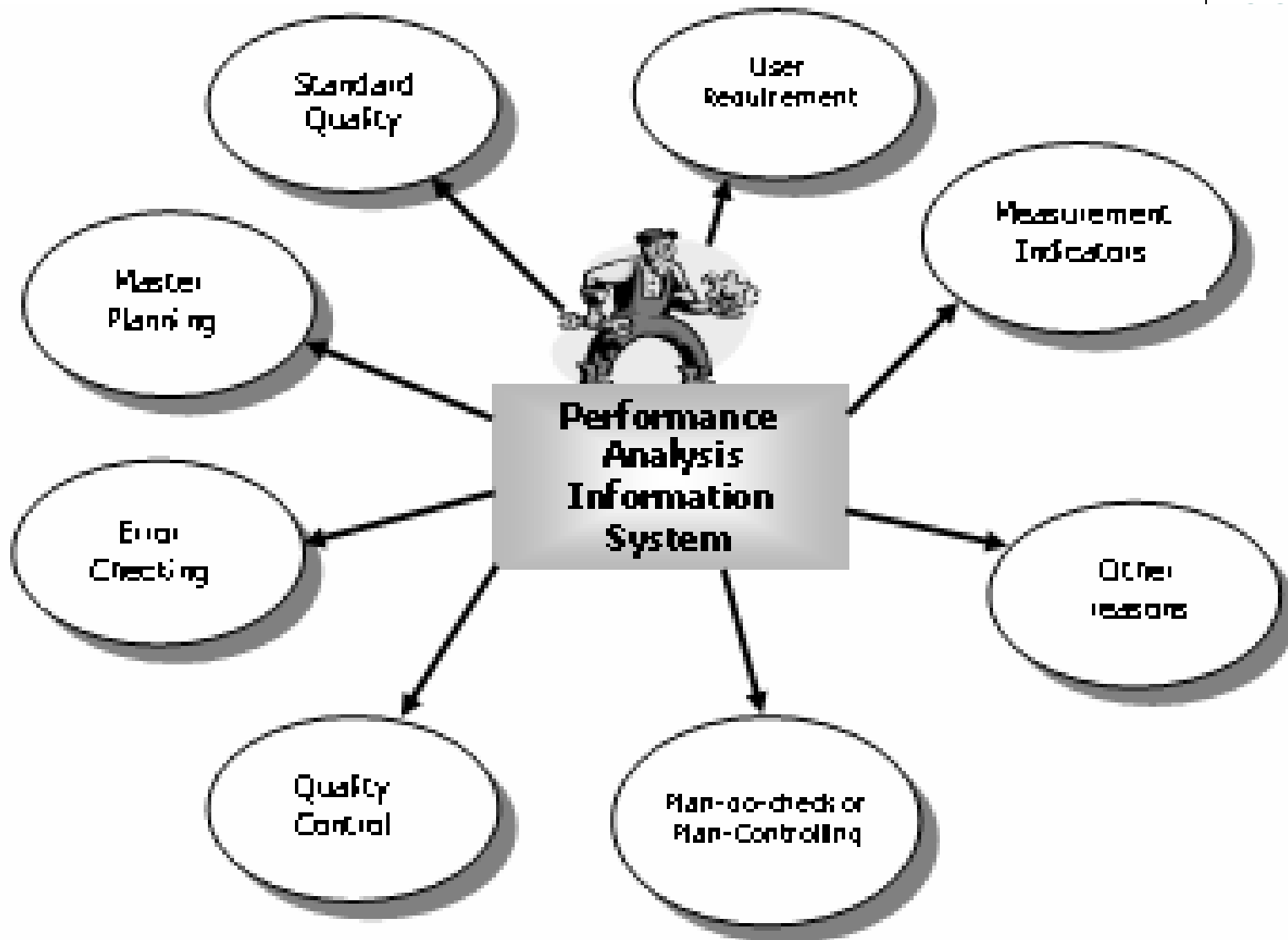
# Model Maturity



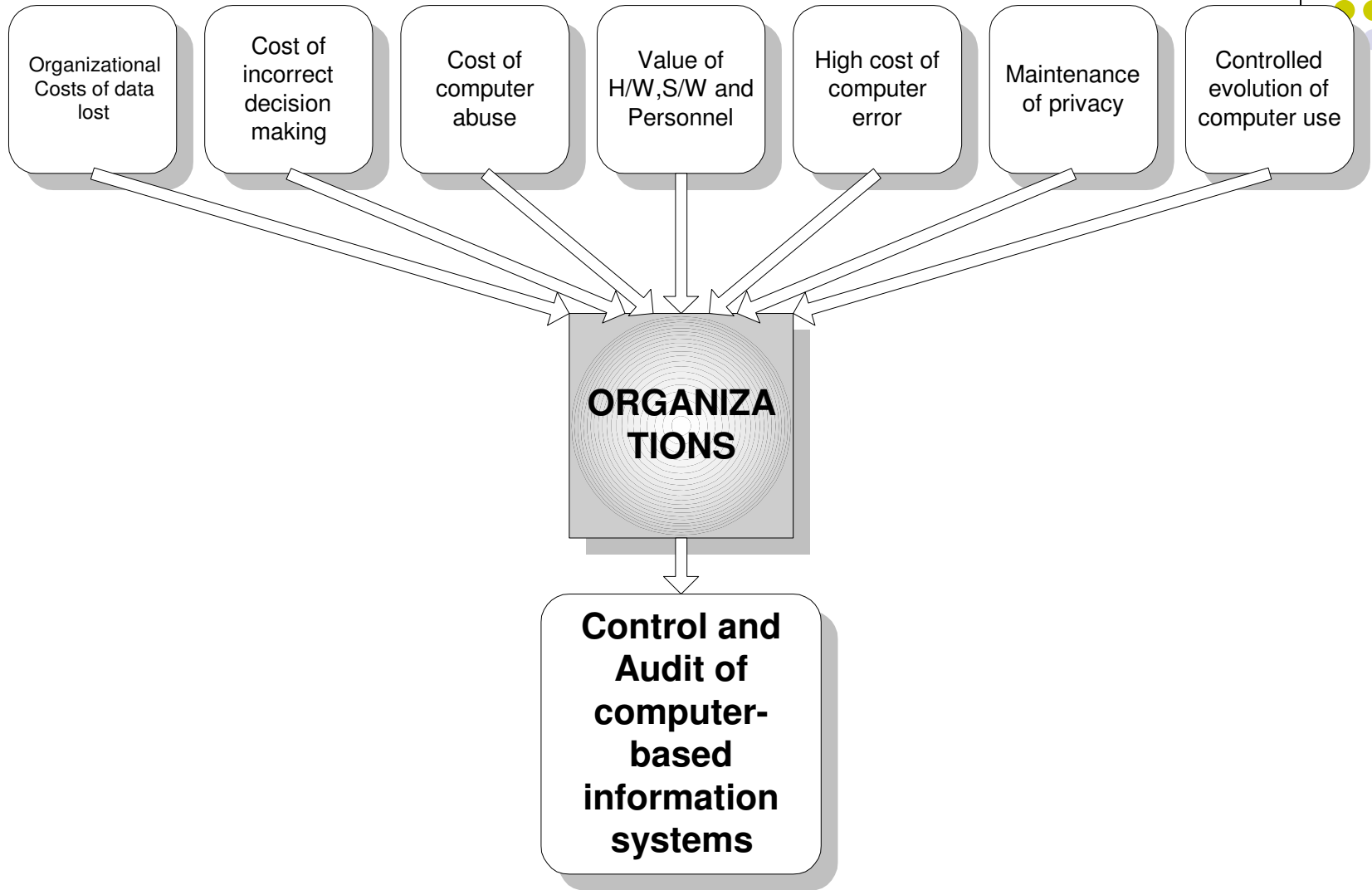
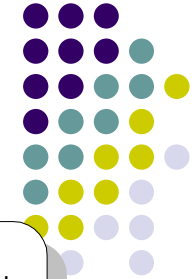
# Tingkat Model Maturity SI Institusi



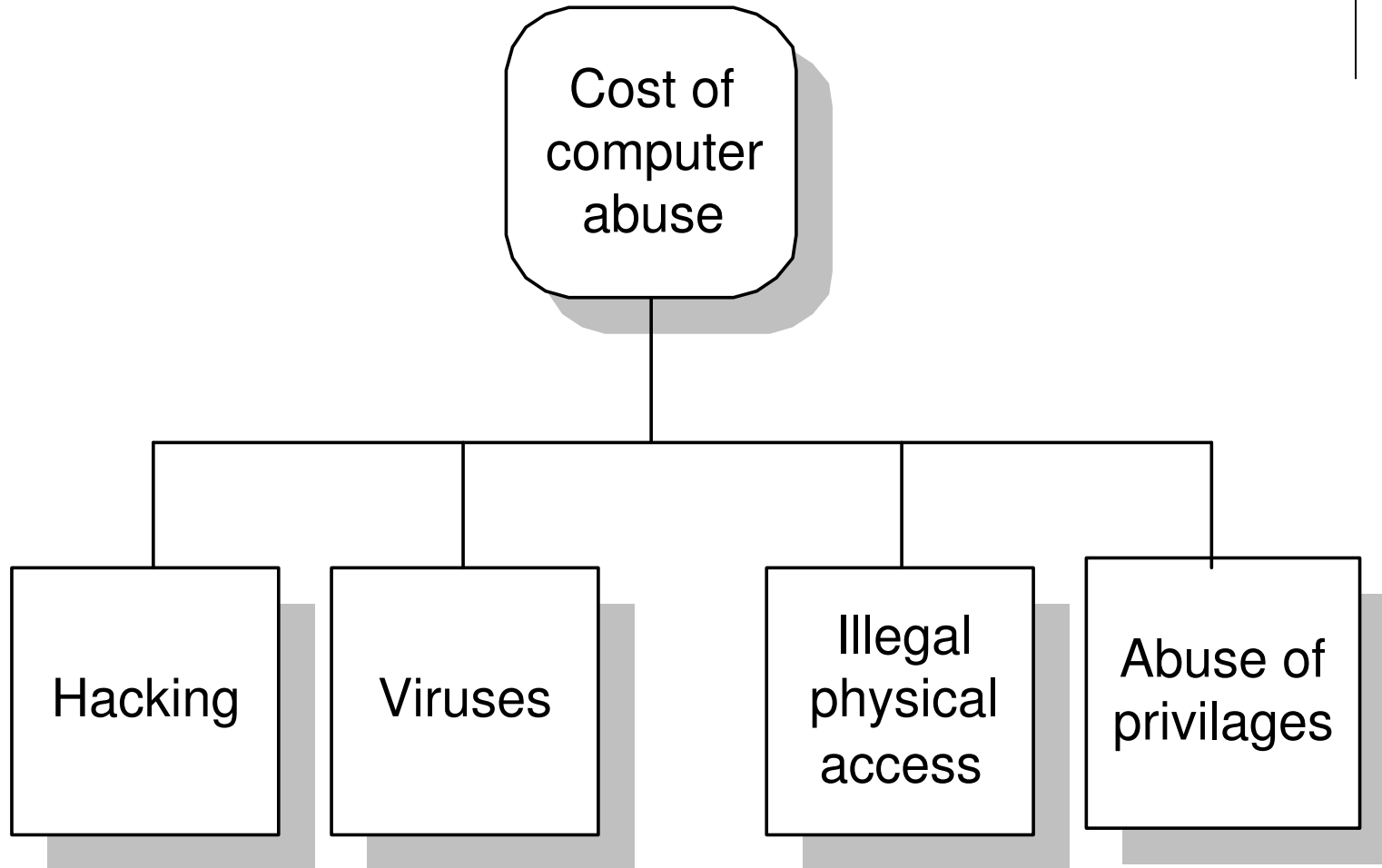
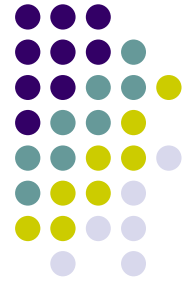
# Performance Information System Reasons



# Need For Control and Audit of Computers

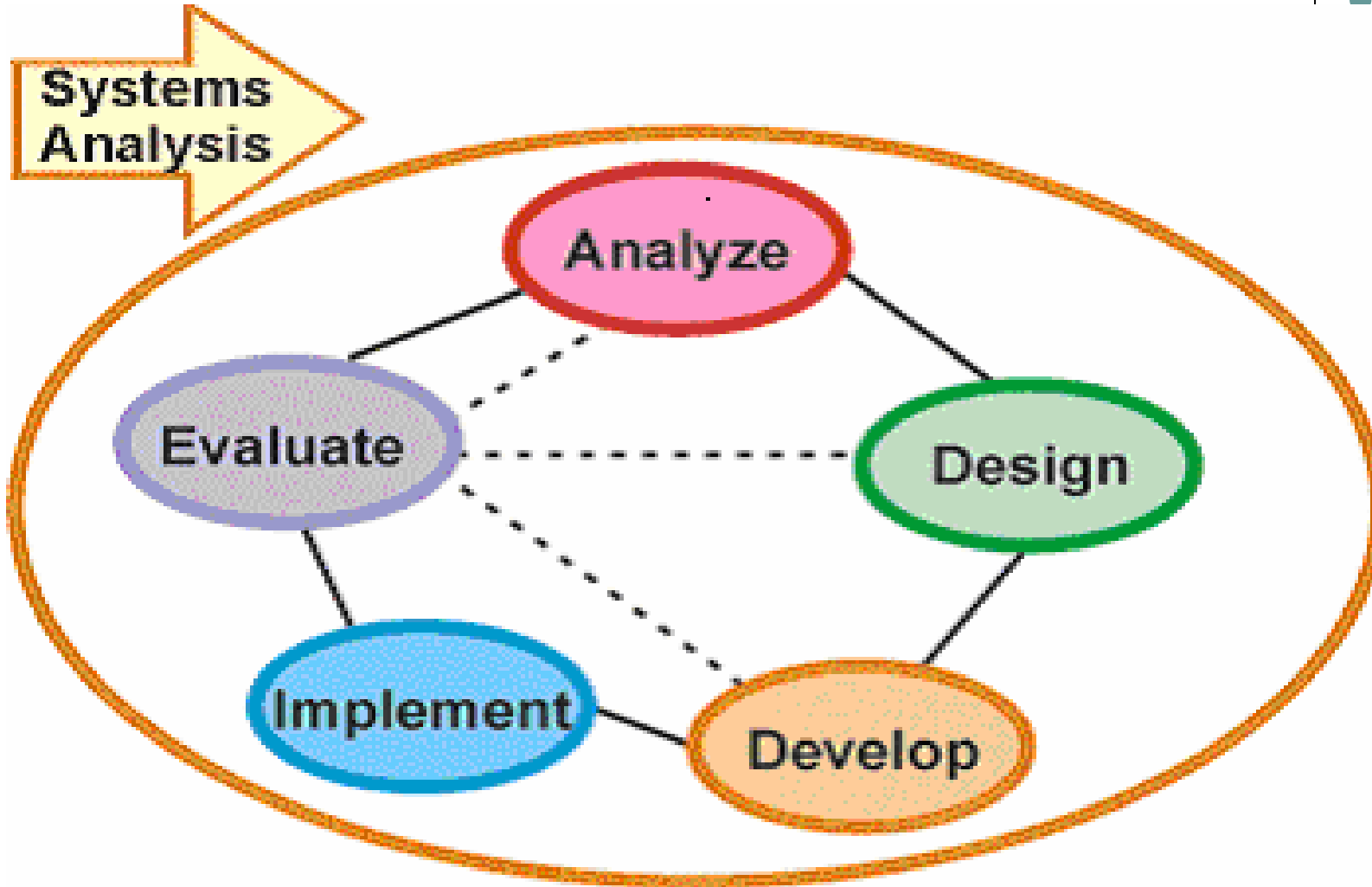


# Cost of computer abuse

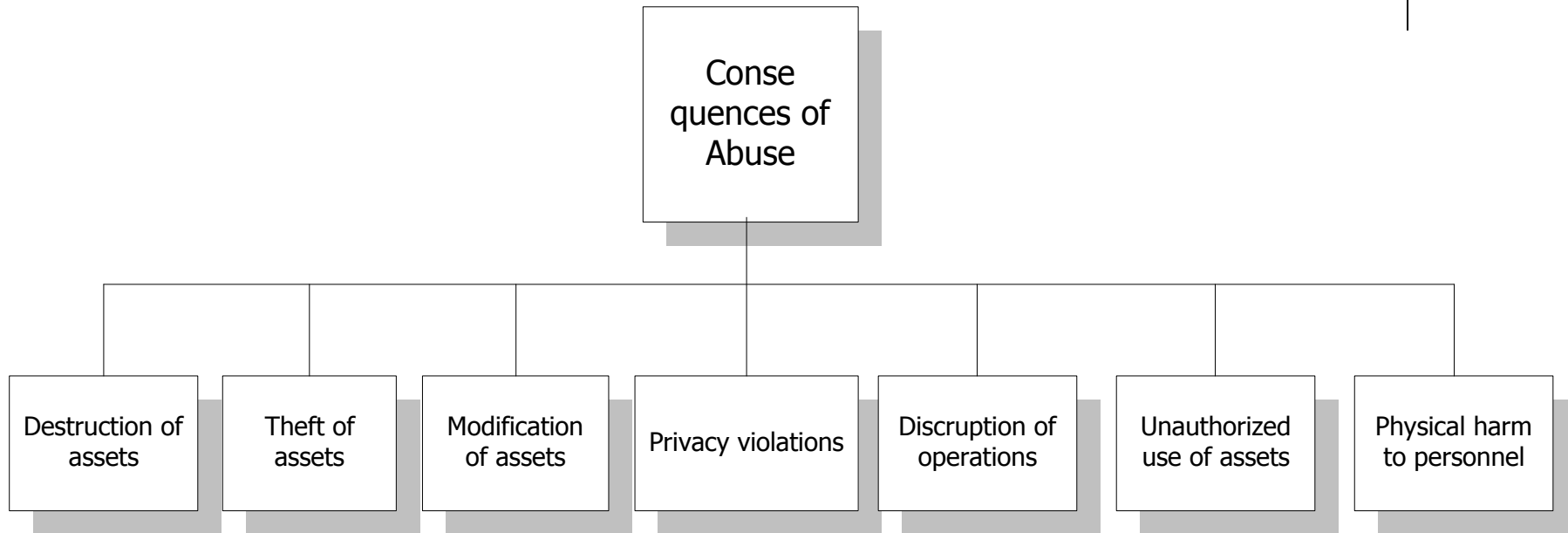




# Evaluate of the System Analysis



# Consequences of Abuse



# Impact of the IS audit function on organization

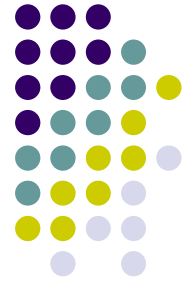


# Memeriksa Sistem Informasi (1)



- **Pemeriksaan Tradisional** (*The Nature of Controls*)
  - Pemeriksaan menyangkut pengendalian evaluasi kehandalan atau efektivitas operasi.
  - Kita harus memahami apa pengertian dari pengendalian (*control*)

“Pengendalian (*control*) adalah sebuah sistem yang digunakan untuk mencegah (*prevents*), mendeteksi (*detects*), atau mengkoreksi kejadian yang tidak dibenarkan (*unlawful events*).



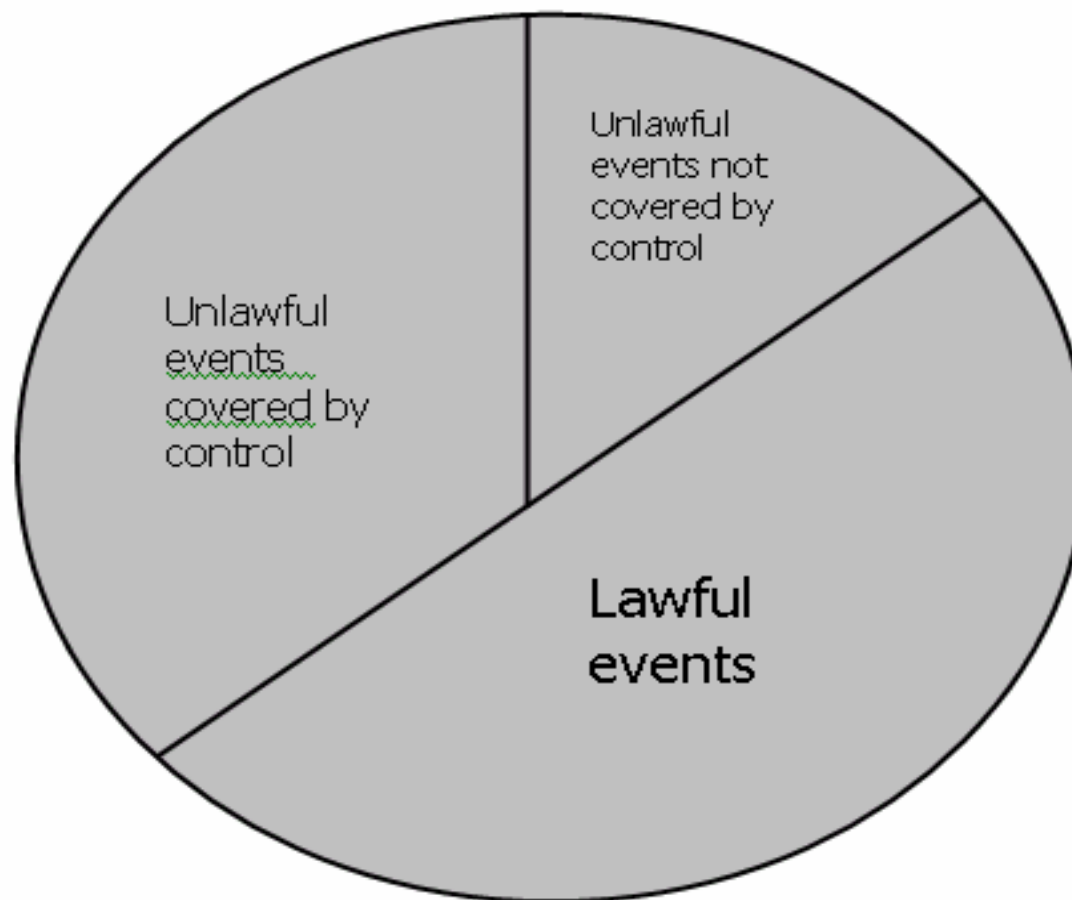
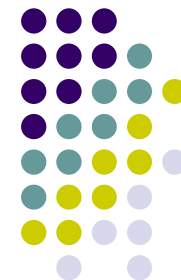
# Memeriksa Sistem Informasi(2)

- Tiga aspek kata kunci definisi pengendalian, yaitu :
  1. Pengendalian adalah sebuah sistem (*a control is a system*)  
Dengan kata lain, terdiri dari sekumpulan komponen yang saling berelasi yang berfungsi secara bersama-sama untuk menyelesaikan suatu maksud atau tujuan.
  2. Kejadian yang tidak dibenarkan (*unlawful events*)  
Ke tidakabsahan kegiatan dapat muncul jika tidak ada otorisasi (*unauthorized*), tidak akurat (*inaccurate*), tidak lengkap (*incomplete*), redundansi (*redundant*), tidak efektif (*ineffective*) atau tidak efisien (*inefficient*) pemasukan data kedalam sistem.
  3. Ketiga, pemeriksaan digunakan untuk mencegah (*prevent*), mendeteksi (*detect*), atau mengkoreksi (*correct*) kejadian yang tidak dibenarkan (*unlawful events*).



# Memeriksa Sistem Informasi(3)

- Beberapa contoh dapat dipertimbangkan :
  - Pemeriksaan Pencegahan (*Preventive control*)
  - Instruksi yang ditempatkan pada dokumen dasar (sumber) untuk mencegah kemungkinan petugas salah DALAM mengisi dokumen (*out incorrectly*).
  - Pemeriksaan Detektif / pengintaian (*Detective control*)
  - Program dapat mengidentifikasi kesalahan pemasukan data ke dalam sistem melalui terminal (alat masukan).
  - Pemeriksaan Koreksi (*Corrective control*)
  - Program menggunakan kode khusus yang memungkinkan sistem dapat mengkoreksi kesalahan data akaibat gangguan (*noise*) komunikasi.



Gbr. 2.1a Kejadian yang tidak dibenarkan atau tidak sesuai dengan aturan / hukum dalam SI.

# Kaitan dengan Kompleksitas

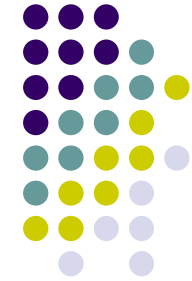
## *(Dealing with Complexity)*



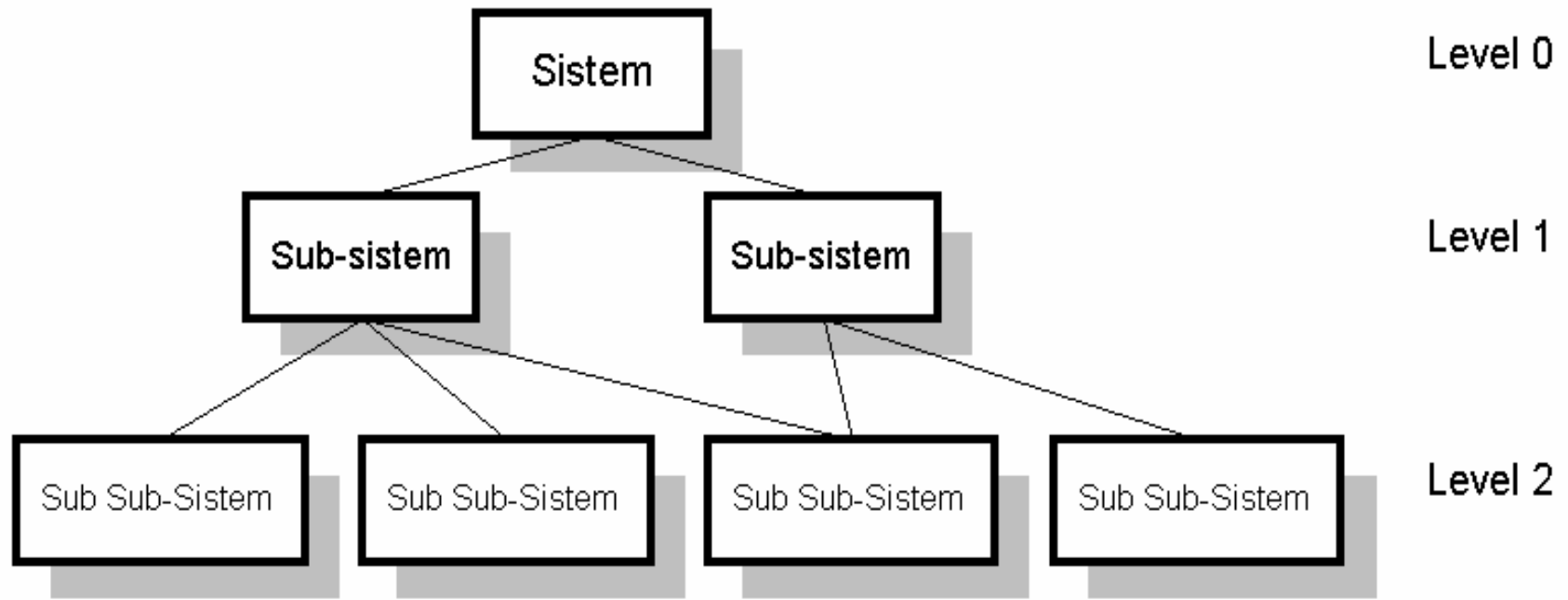
- Dua pedoman pendekatan sewaktu pemeriksaan kinerja SI :
  - Penentuan rencana kinerja SI, faktor sistem di evaluasi kedalam sub sistem.
  - Menentukan keandalan dari tiap sub-sistem dan implikasi kehandalan dari tiap level sub-sistem untuk kehandalan sistem secara menyeluruh.



# Struktur dari Level Sistem dan Sub-Sistem



Faktor sub-sistem



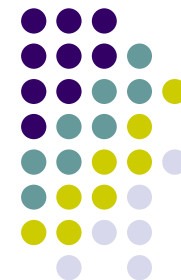
Gbr. 2.2a Struktur dari level sistem dan sub-sistem

# Beberapa tipe sub-sistem manajemen dapat diidentifikasi berdasarkan hubungan antara hirarki organisasi dan sebagian besar tugas fungsi sistem informasinya :



## a. Sistem Manajemen

<u>Sub-sistem Manajemen</u>	<u>Penjelasan</u>
<u>Top Manajemen</u>	<u>Top manajemen harus memastikan fungsi sistem informasi di kelola dengan baik. Bertanggung jawab terutama untuk pengambilan keputusan dalam jangka panjang dan bagaimana sistem informasi akan di gunakan di dalam organisasi</u>
<u>Manajemen Sistem Informasi</u>	<u>Manajemen sistem informasi, secara keseluruhan bertanggung jawab dalam perencanaan dan pengendalian aktivitas sistem informasi. Juga menyampaikan masukan (saran) bagi top manajemen dalam kaitannya dengan kebijakan pengambilan keputusan jangka panjang dan menerjemahkan kebijakan jangka panjang tersebut ke dalam sasaran (<i>goal</i>) dan tujuan (<i>objectives</i>).</u>
<u>Manajemen Pengembangan Sistem</u>	<u>Manajemen pengembangan sistem, bertanggung jawab atas desain, implementasi, dan pemeliharaan dari sistem aplikasi.</u>
<u>Manajemen Pemrograman</u>	<u>Manajemen Pemrograman, bertanggung jawab untuk pembuatan program sistem yang baru, pemeliharaan sistem yang lama, dan menyediakan dukungan sistem softwarena.</u>



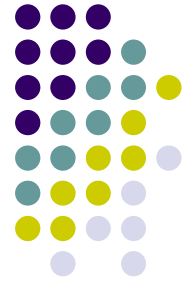
## a. Sistem Manajemen (*cont*)

<u>Administrasi Data</u>	<u>Administrasi data, bertanggung jawab untuk mengarahkan perencanaan dan pengendalian dalam hubungannya dengan akses dan pengorganisasian data.</u>
<u>Manajemen Jaminan Kualitas</u>	<u>Manajemen Jaminan Kualitas, bertanggung jawab untuk penjaminan pengembangan sistem informasi, implementasi, operasional, dan pemeliharaan untuk meningkatkan standar kualitas.</u>
<u>Administrasi Keamanan</u>	<u>Administrasi keamanan, bertanggung jawab untuk pengendalian akses dan keamanan fisik dari fungsi sistem informasi.</u>
<u>Manajemen Operasional</u>	<u>Manajemen Operasional, bertanggung jawab untuk perencanaan dan pengendalian operasional sehari-hari (<i>day-to-day operations</i>) dari system informasi.</u>



## b. Sistem Aplikasi

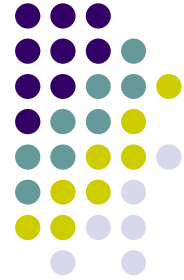
Sub-sistem Aplikasi	Penjelasan
Pembatasan ( <i>Boundary</i> )	Berupa komponen yang menetapkan hubungan (pembatasan) antara user dan sistem.
Input	Berupa komponen yang menangkap ( <i>capture</i> ), menyiapkan, dan memasukan perintah dan data kedalam sistem.
Communication	Berupa komponen yang mengirimkan data antar sub-sistem dan sistem.



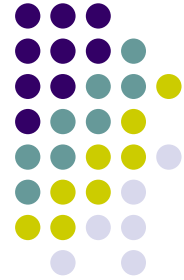
## b. Sistem Aplikasi (*cont*)

Processing	Berupa komponen yang melaksanakan (memproses) pengambilan keputusan, perhitungan, klasifikasi, pemesanan, peringkasan data dalam sistem.
Database	Berupa komponen yang mendefinisikan, menambah, mengakses, memodifikasi, dan menghapus data dalam sistem.
Output	Berupa komponen yang mengambil dan mempresentasikan data untuk user dari sistem.

# PENGENDALIAN INTERNAL

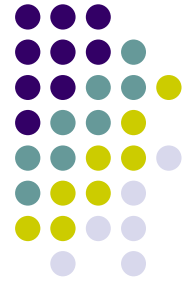


- **Konsep Pengendalian Intern**
- **Konsep Pengendalian Preventif, Detektif, Korektif**



- **Konsep Pengendalian merupakan konsep deskriptif bukan normatif**
- **Konsep Deskriptif : konsep yg dikembangkan berdasarkan pada pengamatan atas pengelolaan yg dilakukan oleh para manajer organisasi perusahaan.**
- **Sedangkan konsep normatif lebih berdasarkan pada landasan teori.**

# Tujuan Pengendalian Internal



- Tujuan pengendalian TI didefinisikan sebagai suatu pernyataan hasil yang diinginkan atau maksud yang dicapai oleh prosedur pengendalian implementasi dalam kegiatan TI khusus.





# Tujuan Pengendalian Internal

- **Tujuan dari pengendalian internal adalah**
  1. Memeriksa ketelitian dan kebenaran data yang akan menghasilkan laporan-laporan yang dapat diandalkan.
  2. Efektivitas dan efisiensi dalam operasi, yaitu efektif dalam mencapai tujuan organisasi secara keseluruhan dan efisien dalam pemakaian sumberdaya yang tersedia.
  3. Membantu agar tidak terjadi penyimpangan terhadap hukum dan peraturan yang berlaku
  4. Mengamankan harta milik organisasi atau perusahaan termasuk data yang tersedia

# Dua Pendekatan Pengendalian Intern :



1. **Pendekatan Statis**
2. **Pendekatan Dinamis**

# Pendekatan Statis

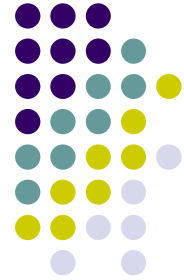


- 1. Berdasarkan pertimbangan pada pembagian wewenang di dalam pengelolaan perusahaan atau entitas pada masa lalu yg bersifat sentralisasi.**
- 2. Metoda sentralisasi artinya jika kita telusuri bahwa intelektualitas berada pd pucuk pimpinan perusahaan. Semakin rendah posisi seseorang, maka semakin sedikit pengetahuannya ttg pencapaian tujuan perusahaan, artinya hanya sekedar menjalankan perintah atasannya.**
- 3. Artinya bahwa pendekatan statis akan berorientasi pada sistem yg dpt dg mudah ditelusuri keberadaannya.**

# Pendekatan Dinamis



1. **Pengendalian intern sbg sebuah proses**
2. **Konsep ini terkait dg perkembangan metoda pengelolaan sumber daya manusia pada organisasi yg bersangkutan.**
3. **Perubahan metoda pengelolaan tersebut adalah perubahan ke metoda pengelolaan manajemen melalui tujuan (management by objective) menggantikan manajemen melalui kekuasaan (management by drive).**
4. **Hal tersebut di dorong oleh :**
  - **Peningkatan kualitas SDM, sehingga intensitas pengendalian intern dpt di kurangi**
  - **Spesialisasi dpt meningkatkan kinerja seseorang**
  - **Kepuasan kerja dpt meningkatkan produktivitas.**
  - **Persaingan yg semakin ketat, membutuhkan pengambilan keputusan yg cepat.**

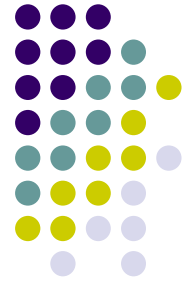


- **Berdasarkan perkembangan di bidang manajemen SDM tersebut, konsep pengendalian intern jg mengalami perubahan dari konsep ketersediaan pengendalian inetern beralih ke konsep proses pencapaian tujuan.**
- **Dg konsep baru tersebut disadari bahwa intelektualitas tdk lg terletak pd pucuk pimpinan, tetapi terletak dilapisan bawah.**
- **Mereka yg dekat dg konsumenlah yg paling mengerti dg kebutuhan pasar.**
- **Pengorganisasian yg paling tepat untuk kondisi seperti ini adalah seperti pengorganisasian orkes simponi.**



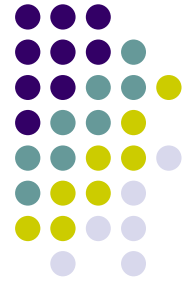
- **Organisasi ini sepenuhnya akan digerakan oleh dinamika para pekerja (ujung tombak) sesuai spesialisai masing-masing.**
- **Untuk menjaga kekompakan agar terjadi irama yg serasi dibutuhkan seorang manajer yg berfungsi sbg konduktor.**
- **Manajer tersebut tdk lg hrs memiliki pengetahuan teknis seperti yg dimiliki pemain orkesnya, tetapi yg diperlukan hanya seorang yg mampu mengatur tempo dan menguasai tingkatan nada.**

# Pengendalian Dilingkungan SI



- 1. Dpt dilakukan dg cara manual atau otomatis**
- 2. Dpt diklasifikasikan dalam :**
  - **Pengendalian Umum dan**
  - **Pengendalian Aplikasi**

# Pengaruh Komputer dalam Pengendalian



- 1. Perubahan dalam Pengumpulan fakta  
(*Changes to Evidence Collection*)**
- 2. Perubahan dalam Evaluasi Fakta  
(*Changes to Evidence Evaluation*)**



# Pengaruh Komputer dalam Pengendalian Internal (#1)



**Tujuan dari perlindungan aset, integritas data, efektivitas sistem, dan efisiensi sistem dapat dicapai dengan baik jika manajemen organisasi meningkatkan sistem pengendalian internalnya, yaitu dengan cara :**

# Pengaruh Komputer dalam Pengendalian Internal (#2)



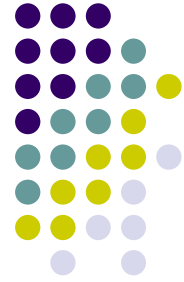
1. **Pemisahan Tanggung Jawab (*Separation of Duties*)**
2. **Pendelegasian Wewenang dan Tanggung Jawab *Delegation of Authority and Responsibility***
3. **Personal yang Kompeten dan Dapat dipercaya (*Competent and Trustworthy Personnel*)**
4. **Otorisasi Sistem (*System of Authorizations*)**
5. **Kecukupan Catatan dan Dokumen (*Adequate Documents and Records*)**

# Pengaruh Komputer dalam Pengendalian Internal (#3)



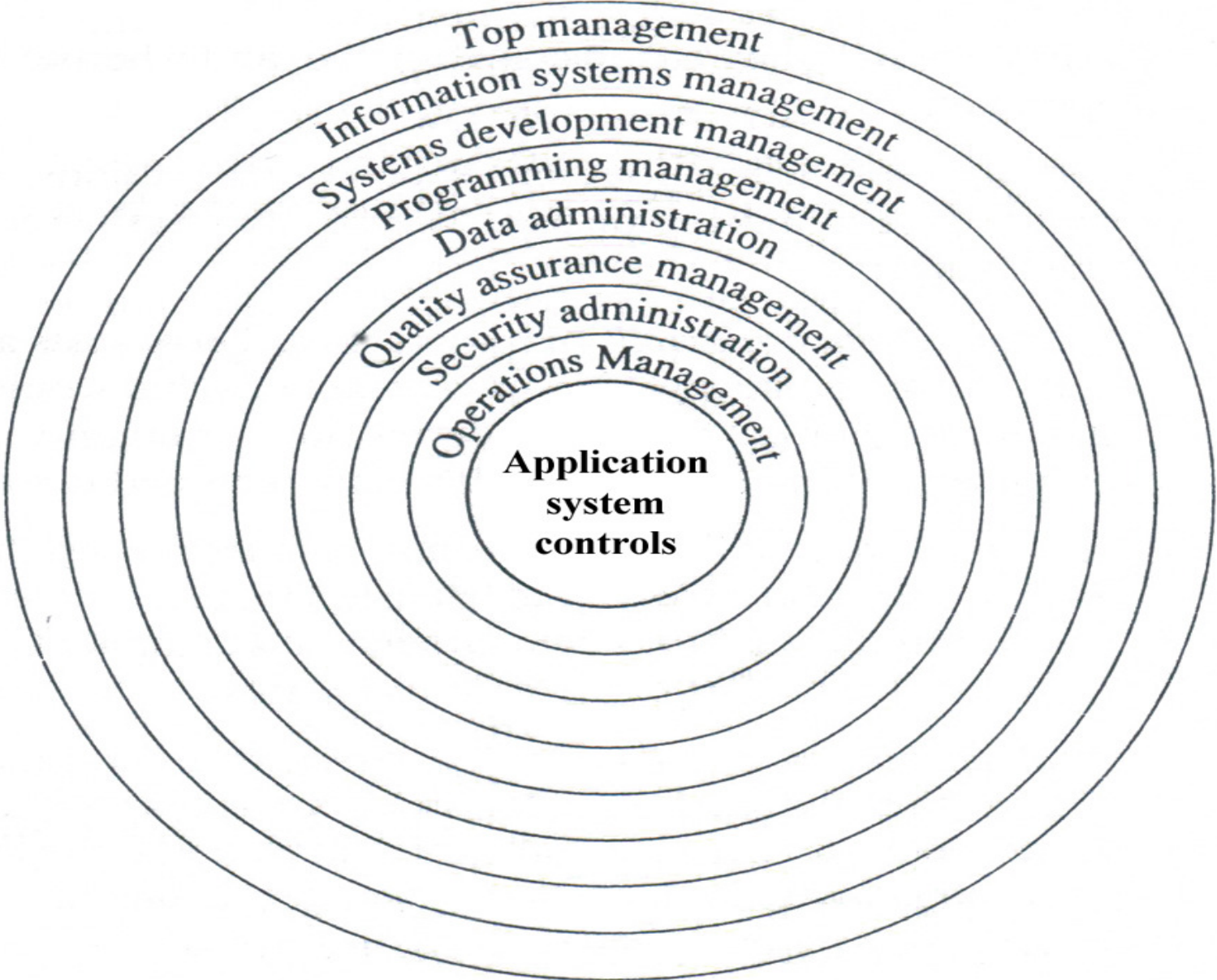
6. **Pengendalian Fisik atas banyaknya Rekord dan Aset (*Physical Control over Assets and Records*)**
7. **Kecukupan Supervisi dari pihak Manajemen (*Adequate Management Supervision*)**
8. **Bentuk Pengecekan yang Independen (*independent Checks on Performance*)**
9. **Perbandingan Akuntabilitas Rekord dengan Aset (*Comparing Recorded Accountability with Assets*)**

# Dua Pendekatan Pengendalian



- **Pengendalian manajemen (*management control*)**, terdiri dari *Top Management Controls, Systems Development Management Controls, Programming Management Controls, Data Resource Management Controls, Security Management Controls, Operations Management Controls, dan Quality Assurance Management Controls*
- **Pengendalian aplikasi (*application control*)**, terdiri dari, *Boundary Controls, Input Controls, Communication Controls, Processing Controls, Database Controls, dan Output Controls.*

# Dua Pendekatan Pengendalian

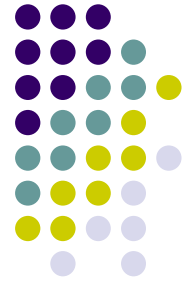




# Pengendalian Umum

1. **Pengendalian Organisasi dan Operasi**
2. **Pengendalian Pengembangan dan Dokumentasi Sistem**
3. **Pengendalian H/W**
4. **Pengendalian Akses H/W dan Data**

# Pengendalian Organisasi & Operasi



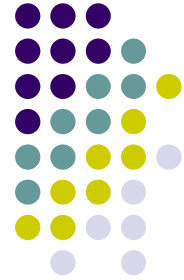
- 1. Struktur org.hrs disusun sedemikian rupa sehingga terdapat pemisahan antara fungsi atau tugas yg memadai.**
- 2. Pemisahan tersebut yaitu : fungsi analisis sistem, pemrograman, pengoperasian komputer, librarian dan pengendali data**
- 3. Pemisahan antara USER dg Unit pengolah data.**

# Pengendalian Pengembangan dan Dokumentasi Sistem



- 1. Pengendalian oleh Komite pengarah yg anggotanya dari pimpinan puncak user.**
- 2. Studi Kelayakan ekonomi, operasional dan teknik hrs dilakukan terhadap eksisting system.**





## **Pengendalian Pengembangan Sistem yg dilakukan antara lain :**

- a) Proposal atau permintaan pengembangan dan modifikasi sistem hrs di buat secara tertulis oleh user dan di otorisasi oleh komite.**
- b) Menetapkan standar sistem desain dan pemrograman.**
- c) Modifikasi hanya boleh terhadap salinan sistem**
- d) Sistem hrs di uji**
- e) Pengembangan sistem hrs di dokumentasikan dg baik**



## **Pengendalian Dokumentasi Sistem** **Beberapa jenis dokumentasi :**

- 1) Pendefinisian masalah,**
- 2) Dokumentasi sistem : flowchart, input dan output, proses, dan pengendalian yg dirancang.**
- 3) Dokumentasi Program**
- 4) Dokumentasi Operasi**
- 5) Dokumentasi Pemakai**

# Pengendalian H/W



1. H/W sdh di lengkapi dg pengendalian otomatis dari pabrikan
2. Beberapa pengendalian H/W sbb :
  - a) **Boundary (storage) Protection** melindungi program dan data
  - b) **Diagnostic Routines**, mengecek permasalahan yg terjadi di S/W (dialkukan pd awal kerja)
  - c) **Dual Read**, pengendalian membaca input dua kali pd tape drive.
  - d) **Duplicate Circuitry**, menghitung 2 kali dan membandingkannya (pada ALU).
  - e) **Echo Check**, mengirim balik sinyal yg telah dikirim.
  - f) **Parity Check**, memberikan digit atau bit tambahan.
  - g) **Read-Write Suppression**, pengendalian dlm disk drive agar tdk dpt di tulis dan dibaca.

# Pengendalian Akses H/W dan Data



1. Untuk mencegah adanya pemakaian yg tdk benar
2. Beberapa pengendalian Akses H/W sbb :
  - a) Password, namun demikian pemakain Password yg berlebihan dpt membuat user bosan dan sistem bekerja lambat.
  - b) System Accses Log, menggunakan log yg mencatat semua usaha untuk menggunakan sistem a.l. tgl, kode, tipe akses, dan data yg digunakan.
  - c) Encryption, menggunakan algortima atau formula tertentu untuk mengacak atau memanipulasi data.
  - d) Callback, melindungi sistem melalui terminal remote tanpa otorisasi.
  - e) Biometric Technologies, pengendalian melalui ciri fisik seseorang, misal melalui sidik jari, retina mata, telapak tangan tanda tangan atau suara.
  - f) Automatic Log-Off, akan memutus hub.secara otomatis terminal yg tdk aktif.

# Pengendalian Aplikasi

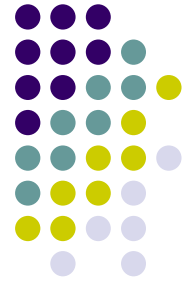
Meliputi pengendalian INPUT, PROSES dan OUTPUT.



## 1. Pengendalian INPUT :

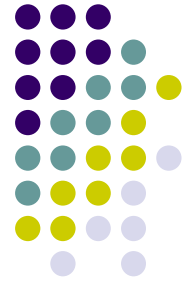
- a) **Error Listing.**kesalahan yg baru ditemukan dan kesalahan sebelumnya yg belum dikoreksi
- b) **Filed Check,** format field dpt berupa alphabet, Numeric date atau format lainnya.
- c) **Financial Total,**
- d) **Hasil Total**
- e) **Limit Check,** membatasi data masukan
- f) **Ranga Check,** kisaran batasan

# Pengendalian INPUT (Cont..#1)



- g) **Record Count**, mengecek jml transaksi yg di proses sistem
- h) **Self Checking Digit**, digit tambahan untuk pengecekan
- i) **Sequence Check**, mengecek data yg tdk berurut.
- j) **Sign Check**, mengecek tanda aritmatik, misal jam kerja selalu bernilai positif.
- k) **Validity Check**, mengecek no. identifikasi atau kode valid.
- l) **Key Verification**, re-keying, biasanya dilakukan oleh petugas yg lain.
- m) **Redundancy Check**
- n) **Echo Check**,

# Pengendalian INPUT (Cont..#2)



- g) Record Count, mengecek jml transaksi yg di proses sistem**
- h) Self Checking Digit, digit tambahan untuk pengecekan**
- i) Sequence Check, mengecek data yg tdk berurut.**
- j) Sign Check, mengecek tanda aritmatik, misal jam kerja selalu bernilai positif.**
- k) Validity Check, mengecek no. identifikasi atau kode valid.**
- l) Key Verification, re-keying, biasanya dilakukan oleh petugas yg lain.**
- m) Redundancy Check**
- n) Echo Check,**

# Pengendalian INPUT (Cont..#3)

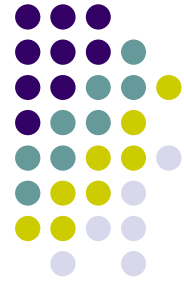
- o) **Completeness Check**
- p) **Internal Reader dan Trailer Label, pemakaian internal label di awal dan di akhir suatu file data.**





## 2. Pengendalian PROSES

1. **Limit, Reasobable dan Sign Test**
2. **Posting, Crossfooting dan Zero Balance Check**
3. **Run to Run Tools**
4. **End Of File Procedure**
5. **Audit Trail**

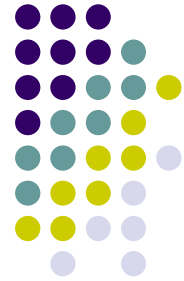


# 3. Pengendalian OUTPUT



1. **Console Log**
2. **Distribution**
3. **User Review**

# 15 Area Pengendalian



- 1. Integritas Sistem**
- 2. Manajemen Sumber Daya (Perencanaan Kapasitas)**
- 3. Pengendalian Perubahan S/W Aplikasi dan S/W sistem**
- 4. Backup dan Recovery**
- 5. Contingency Planning**
- 6. System S/W Support**
- 7. Dokumentasi**
- 8. Pelatihan atau Training**

# 15 Area Pengendalian (*cont..*)



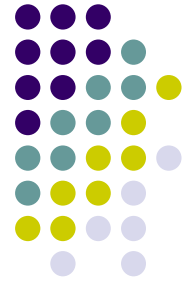
- 9. Administrasi**
- 10. Pengendalian Lingkungan dan Keamanan Fisik**
- 11. Operasi**
- 12. Telekomunikasi**
- 13. Program Libraries**
- 14. Application Support (SDLC)**
- 15. Pengendalian Mikrokomputer**

# 1. Integritas Sistem



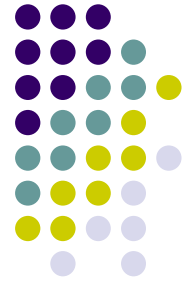
1. **Ketersediaan dan kesinambungan sistem komputer untuk user**
2. **Kelengkapan, Keakuratan, Otorisasi, serta proses yg auditable**
3. **Persetujuan dari user atas kinerja sistem yang di inginkan**
4. ***Preventive maintenance agreements* untuk seluruh perlengkapan**
5. **Kesesuaian kinerja antara S/W dan jaringan dengan yang diharapkan**
6. **Serta adanya program yang disusun untuk operasi secara menyeluruh**

## 2. Manajemen Sumber Daya



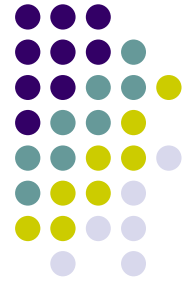
- 1. Faktor-faktor yang melengkapi integritas sistem**
- 2. Yaitu meyakini kelangsungan (*ongoing*) H/W, S/W, SO, S/W aplikasi, dan komunikasi jaringan komputer, telah di pantau dan dikelola pada kinerja yang maksimal namun tetap dengan biaya yang wajar.**
- 3. Hal-hal tersebut di dokumentasikan secara formal, demi proses yang berkesinambungan**

### 3. Pengendalian Perubahan S/W Aplikasi dan S/W sistem



- 1. Menentukan adanya keterlibatan dan persetujuan user dalam hal adanya perubahan terhadap s/w aplikasi dan s/w sistem**
- 2. Setiap pengembangan dan perbaikan aplikasi harus melalui proses formal dan di dokumentasikan serta telah melalui tahapan-tahapan pengembangan sistem yang dibakukan dan disetujui.**

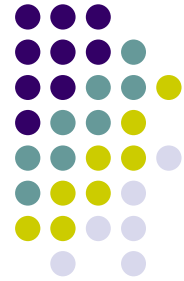
## 4. Backup dan Recovery



1. Demi kelangsungan usaha, harus tersedia ***data processing disaster recovery planning*** (rencana pemulihan data dan pusat sistem informasi apabila terjadi kehancuran),
2. Baik berupa backup dan pemulihan normal, maupun rencana ***contingency*** untuk kerusakan pusat SI (lokasi gedung, peralatanya, SDM-nya maupun manualnya).

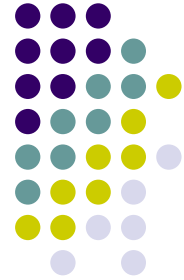


# 5. Contingency Planning

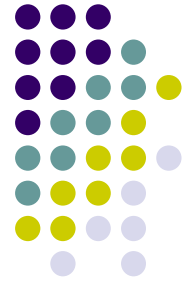


1. **Perencanaan yang komprehensif di dalam mengantisipasi terjadinya ancaman terhadap fasilitas pemrosesan SI,**
2. **Dimana sebagian besar komponen utama dari *disaster recovery plan* telah dirumuskan dengan jelas, telah di koordinasikan dan disetujui, seperti *critical application systems*, identifikasi peralatan dan fasilitas penunjang H/W, sistem S/W dan sebagainya.**

## 6. System S/W Support



1. Pengukuran pengendalian dalam pengembangan, penggunaan, dan pemeliharaan dari S/W SO, biasanya lebih canggih dan lebih cepat perputarannya dibandingkan dengan S/W aplikasi,
2. Dengan ketergantungan yang lebih besar kepada staf teknik untuk integritas fungsionalnya
3. Pengukuran kendali pengamanan aplikasi individu maupun pengamanan logika sistem secara menyeluruh (*systemwide logical security*)



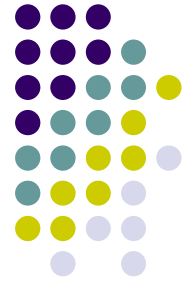
## 7. Dokumentasi

- 1. Integritas dan ketersediaan dokumen operasi, pengembangan aplikasi, user dan S/W sistem**
- 2. Diantaranya dokumentasi program dan sistem, buku pedoman operasi dan schedule operasi,**
- 3. Untuk setiap aplikasi sebaiknya tersedia dokumentasi untuk tiap jenjang user.**

## 8. Pelatihan atau Training



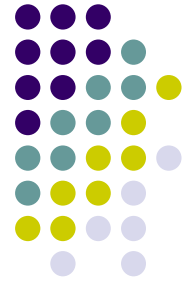
- 1. Adanya penjenjangan berdasarkan kemampuan untuk seluruh lapisan manajemen dan staf, dalam hal penguasaannya atas aplikasi-aplikasi dan kemampuan teknisnya**
- 2. Serta rencana pelatihan yang berkesinambungan**



## 9. Administrasi

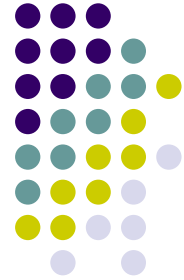
1. **Struktur organisasi dan bagannya, rencana strategis, tanggungjawab fungsional, job description, sejalan dengan metoda *job accounting* dan/atau *charge out* yang digunakan**
2. **Termasuk didalamnya pengukuran atas proses pengadaan dan persetujuan untuk semua sumber daya SI.**

## 10. Pengendalian Lingkungan dan Keamanan Fisik



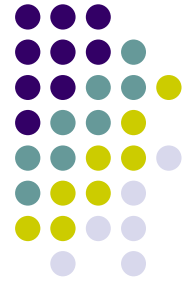
- 1. Listrik, peyejuk udara, penerang ruangan, pengaturan kelembaban, serta kendali akses ke sumber daya informasi**
- 2. Pencegahan kebakaran, ketersediaan sumber listrik cadangan,**
- 3. Juga pengendalian dan backup sarana telekomunikasi**

# 11. Operasi



- 1. Diprogram untuk merespon permintaan/keperluan SO**
- 2. Review atas kelompok SO berdasarkan job scheduling, review yang terus-menerus terhadap operator, retensi terhadap *console log message*, dokumentasi untuk *run/restore/backup* atas seluruh aplikasi,**
- 3. Daftar personel, dan nomor telepon yang harus dihubungi jika muncul masalah SO, penerapan sistem sift dan rotasi serta pengambilan cuti untuk setiap operator.**

# 12. Telekomunikasi



1. **Review terhadap logical and *physical access controls*,**
2. **Metodologi pengacakan (*encryption*) terhadap aplikasi *electronic data interchange* (EDI)**
3. **Adanya supervisi yang berkesinambungan terhadap jaringan komputer dan komitmen untuk ketersediaan jaringan tersebut dan juga redundansi saluran telekomunikasi.**

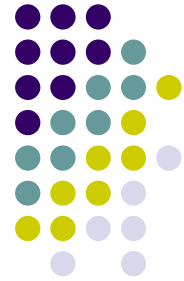


# 13. Program Libraries



1. Terdapat pemisahan dan prosedur pengendalian formal untuk *application source code* dan *compiled production program code* dengan yang disimpan di *application test libraries development*,
2. Terdapat review atas prosedur *quality assurance*.

# 14. Application Support



- 1. Bahwa proses tetap dapat berlangsung walaupun terjadi kegagalan sistem**
- 2. Sejalan dengan kesinambungan proses untuk inisiasi sistem baru, manajemen proyek, proses pengujian yang menyeluruh antara user dan staf SI**
- 3. Adanya review baik formal maupun informal terhadap tingkat kepuasan atas SDLC yang digunakan.**

# 15. Microcomputer Controls



- 1. Pembatasan yang ketat dalam pengadaan, pengembangan aplikasi, dokumentasi atas aplikasi produksi maupun aplikasi dengan misi yang kritis, sekuriti logika, dan fisik terhadap microcomputer yang dimiliki,**
- 2. Serta pembuatan daftar inventaris atas H/W, S/W, serta legalitas dari S/W untuk menghindari tuntutan pelanggaran hak cipta.**

- Teknik Kalkulasi Nilai Pengendalian Intern (#1)

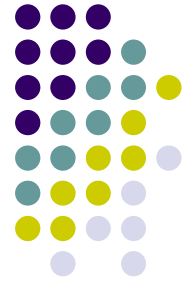


- **Bobot :**

**1,0 : resiko adalah kritis**

**0,5 : resiko kurang kritis**

**2,0 : resiko sangat kritis**



- Teknik Kalkulasi Nilai Pengendalian Intern (#2)

- **Standar Penilaian 1-5 :**

**1 : Lemah**

**2 : Kurang**

**3 : Sedang**

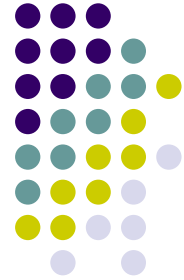
**4 : Memadai**

**5 : Memuaskan**



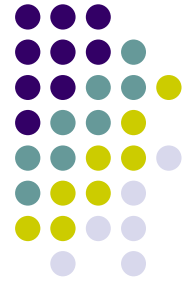
- # Teknik Kalkulasi Nilai Pengendalian Intern (#3)
- **Cara Penghitungan :**
  1. Hasil review atas masing2 resiko dikalikan dengan bobotnya.
  2. Kemudian seluruh hasil perkalian ini dijumlahkan dan dicatat dikolom jumlah (nila x bobot)
  3. Angka ini kita bagi dengan banyaknya area pengendalian yang kita uji (dari 15 area mungkin hanya 10 atau kurang)
  4. Hasil pembagian kita catat di kolom nilai rata-rata (NR), kemudian kita bulatkan ke bawah sesuai prinsip conservatism, dan kita catat di kolom NR di bulatkan ke bawah.
  5. Terakhir, angka ini kita konversikan kembali, sehingga kita mendapatkan rating yang sesuai untuk pusat informasi ybs yaitu apakah MEMUASKAN, MEMADAI, SEDANG, KURANG atau LEMAH.

# Pengendalian Manajemen Puncak



1. **Evaluasi Fungsi Perencanaan**
2. **Evaluasi Fungsi Organisasi**
3. **Evaluasi Fungsi Kepemimpinan**
4. **Evaluasi Fungsi Pengendalian**

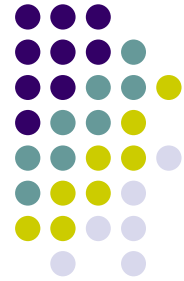
# Pengendalian Manajemen Pengembangan Sistem



- Evaluasi Sebagian Besar Tahap Proses Pengembangan Sistem

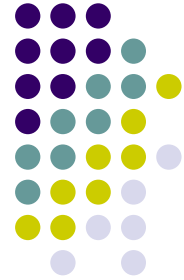


# Pengendalian Manajemen Pemrograman



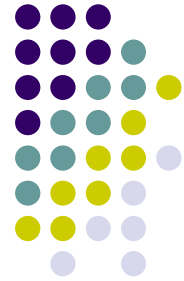
1. Siklus Hidup Pengembangan Program
2. Pengorganisasian Tim Pemrograman
3. Pengelolaan Kelompok Pemrograman

# Pengendalian Manajemen Keamanan



1. Pelaksanaan Program Keamanan
2. Sebagian Besar Ancaman dan Pengukuran Perbaikan
3. Pengendalian Muara Akhir

# Pengendalian Manajemen Operasi



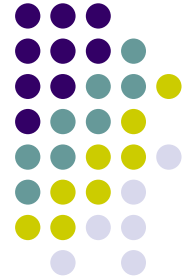
1. Operasi Komputer
2. Operasi Jaringan
3. Penyiapan dan Pengentrian Data
4. Pengendalian Produksi
5. Pustaka File
6. Dokumentasi dan Pustaka Program
7. Help Desk / Dukungan Teknik
8. Perencanaan Kapasitas dan Pengawasan Kinerja
9. Pengelolaan Operasi Outsource

# Pengendalian Manajemen Jaminan Kualitas



1. Fungsi QA
2. Pertimbangan Pengorganisasian
3. Hubungan Antara QA dan Auditing

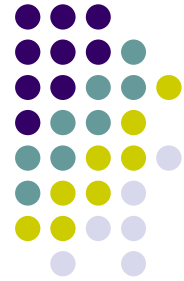
# Pengendalian Pembatasan (*Boundary*)



1. Pengendalian Cryptographic
2. Pengendalian Akses
3. Nomor Identifikasi Personal
4. Tandatangan Digital
5. Kartu Kredit
6. Pengendalian Audit Trail

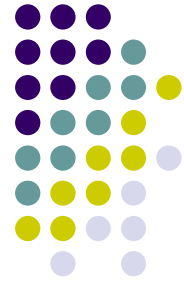
# Pengendalian Masukan

1. Metode Input Data
2. Rancangan Dokumen Sumber / Dasar
3. Rancangan Layar Entri Data
4. Pengendalian Kode Data
5. Pengecekan Digit
6. Pengendalian Batch
7. Validasi Input Data
8. Instruksi Masukan
9. Validasi Instruksi Masukan
10. Pengendalian Audit Trail



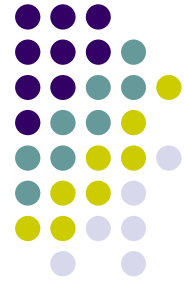
# Pengendalian Komunikasi

1. Ekspos Sub sistem Komunikasi
2. Pengendalian Komponen Fisik
3. Pengendalian Baris Kesalahan
4. Pengendalian Flow
5. Pengendalian Hubungan
6. Pengendalian Topologi
7. Pengendalian Akses Chanel
8. Pengendalian Atas Ancaman Subversif
9. Pengendalian Antar Jaringan
10. Pengendalian dan Arsitektur Komunikasi
11. Pengendalian Audit Trail
12. Pengendalian Eksistensi



# Pengendalian Pemrosesan

1. Pengendalian Pemroses
2. Pengendalian Memori Nyata
3. Pengendalian Memori Virtual
4. Integrasi Sistem Operasi
5. Pengendalian Integritas
6. Pengendalian Software Aplikasi
7. Pengendalian Audit Trail
8. Pengendalian Eksistensi



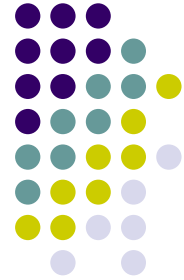


# Pengendalian Database



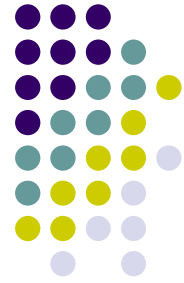
1. Pengendalian Akses
2. Pengendalian Integritas
3. Pengendalian Software Aplikasi
4. Pengendalian Konkuren
5. Pengendalian Cryptographic
6. Pengendalian Penanganan File
7. Pengendalian Audit Trail
8. Pengendalian Eksistensi

# Pengendalian Output



1. Pengendalian Inferensi
2. Pengendalian Distribusi dan Produksi Output Batch
3. Pengendalian Rancangan Laporan Batch
4. Pengendalian Distribusi dan Produksi Output On-line
5. Pengendalian Audit Trail
6. Pengendalian Eksistensi

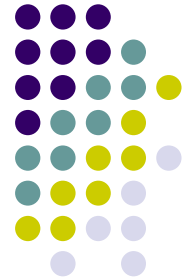
# Klasifikasi Proses Pengendalian SI



1. Perencanaan dan pengorganisasian (PO : *Planning and Organisation*)
2. Akuisisi dan implementasi (AI : *Acquisition and Implementation*)
3. Penyampaian dan dukungan (DS : *Delivery and Support*)
4. Pemantauan (M : *Monitoring*)

COBIT *Framework* sebagaimana disebutkan dalam *IS Auditing Guidelines* pada bab '*Effect of Perfasive IS Control*' yang mulai berlaku efektif sejak 1 Maret 2000

# Klasifikasi Proses Pengendalian SI



Keempat domain tersebut diatas kemudian dijabarkan menjadi 34 faktor resiko yang harus dievaluasi jika ingin diperoleh suatu kesimpulan mengenai seberapa besar kepedulian manajemen terhadap teknologi informasi, serta bagaimana teknologi informasi dapat memenuhi kebutuhan manajemen akan informasi

## PLANNING AND ORGANISATION (PO)

1. **PO1** Menetapkan Rencana Strategis Teknologi Informasi (*Define a Strategic IT Plan*)
2. **PO2** Menetapkan Arsitektur Informasi (*Define the Information Architecture*)
3. **PO3** Menetapkan Arah Teknologi (*Determine Technological Direction*)
4. **PO4** Menetapkan Organisasi TI dan Hubungannya (*Define the IT Organisation and Relationships*)
5. **PO5** Mengatur Investasi TI (*Manage the IT Investment*)
6. **PO6** Mengkomunikasikan Tujuan dan Arah Manajemen (*Communicate Management Aims and Direction*)
7. **PO7** Mengelola Sumberdaya Manusia (*Manage Human Resources*)
8. **PO8** Memastikan Kesesuaian dengan Kebutuhan-kebutuhan eksternal (*Ensure Compliance with External Requirements*)
9. **PO9** Menilai Resiko (*Assess Risks*)
10. **PO10** Mengatur Proyek (*Manage Projects*)
11. **PO11** Mengatur Kualitas (*Manage Quality*)

## ACQUISITION AND IMPLEMENTATION (AI)

12. **AI1** Identifikasi solusi-solusi otomatisasi (*Identify Automated Solutions*)
13. **AI2** Memperoleh dan memelihara Perangkat Lunak Aplikasi (*Acquire and Maintain Application Software*)
14. **AI3** Memperoleh dan memelihara Infrastruktur Teknologi (*Acquire and Maintain Technology Infrastructure*)
15. **AI4** Mengembangkan dan memelihara prosedur (*Develop and Maintain Procedures*)
16. **AI5** Instalasi dan pengakuan sistem (*Install and Accredite Systems*)
17. **AI6** Mengatur Perubahan (*Manage Changes*)

# DELIVERY AND SUPPORT (DS)

18. **DS1** Menetapkan dan mengatur tingkatan pelayanan (*Define and Manage Service Levels*)
19. **DS2** Mengelola layanan pihak ke tiga (*Manage Third-Party Services*)
20. **DS3** Mengelola kapasitas dan kinerja (*Manage Performance and Capacity*)
21. **DS4** Menjamin layanan berkelanjutan (*Ensure Continuous Service*)
22. **DS5** Menjamin keamanan sistem (*Ensure Systems Security*)
23. **DS6** Mengidentifikasi dan mengalokasikan biaya (*Identify and Allocate Costs*)
24. **DS7** Mendidik dan melatih user (*Educate and Train Users*)
25. **DS8** Membantu dan memberikan masukan kepada pelanggan (*Assist and Advise Customers*)
26. **DS9** Mengelola konfigurasi (*Manage the Configuration*)
27. **DS10** Mengelola kegiatan dan permasalahan (*Manage Problems and Incidents*)
28. **DS11** Mengelola Data (*Manage Data*)
29. **DS12** Mengelola Fasilitas (*Manage Facilities*)
30. **DS13** Mengelola Operasi (*Manage Operations*)

# MONITORING (M)

31. **M1** Mengawasi proses (*Monitor the Processes*)
32. **M2** Menilai kecukupan pengendalian internal (*Assess Internal Control Adequacy*)
33. **M3** Memperoleh jaminan independen (*Obtain Independent Assurance*)
34. **M4** Menyediakan Audit Independen (*Provide for Independent Audit*)



# COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS

