Controlling & Auditing
Information System

Magister SI UNIKOM

Konstruksi Kontrol TI & Audit TI Step-by-Step

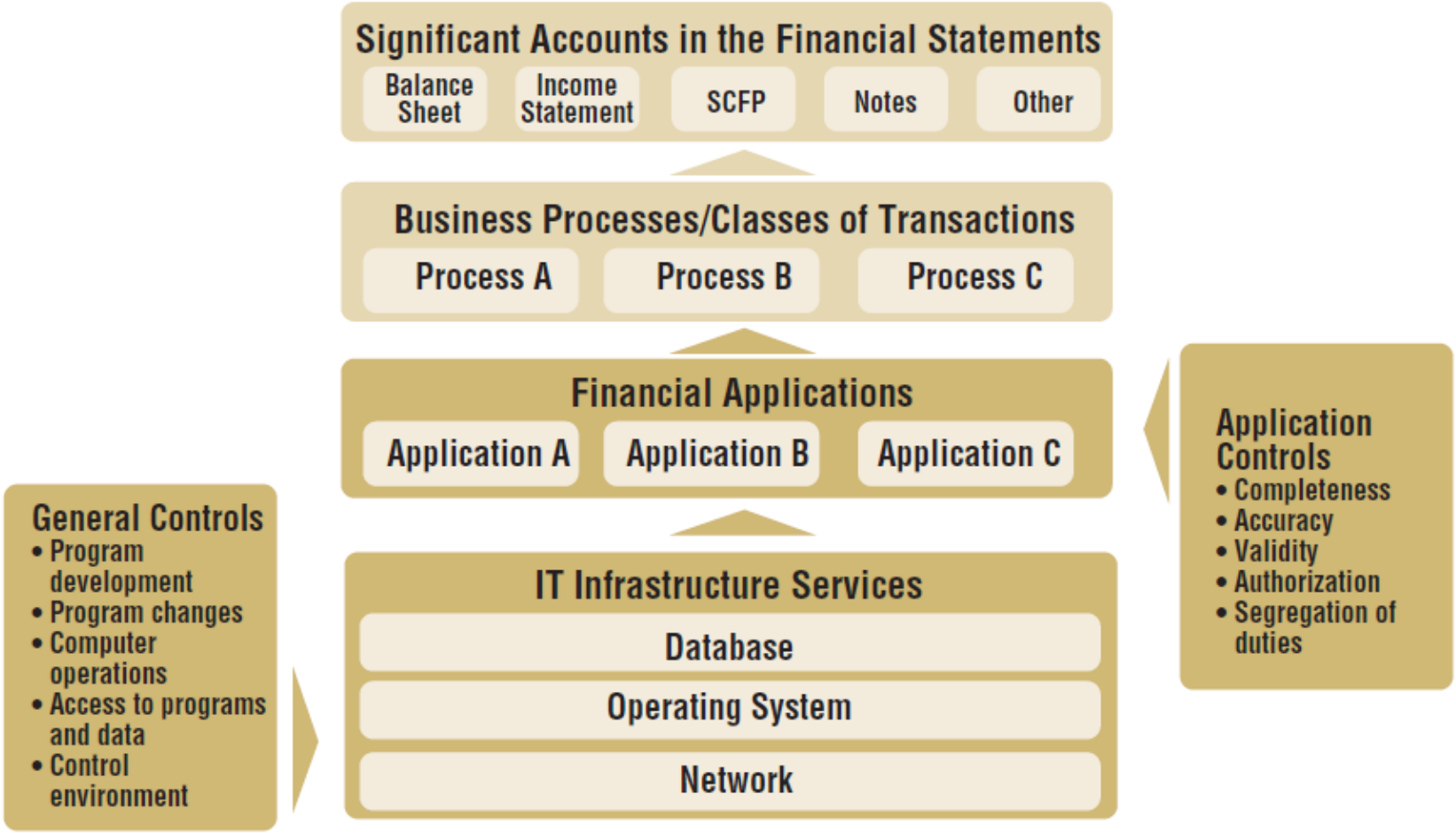
Basuki Rahmad, Dr, CISA, CISM

Agenda

- **Konstruksi Kontrol TI**
  - General Control
  - Application Control
- Metodologi Audit TI: Step-by-Step

Mengapa *IT Controls* dibutuhkan?

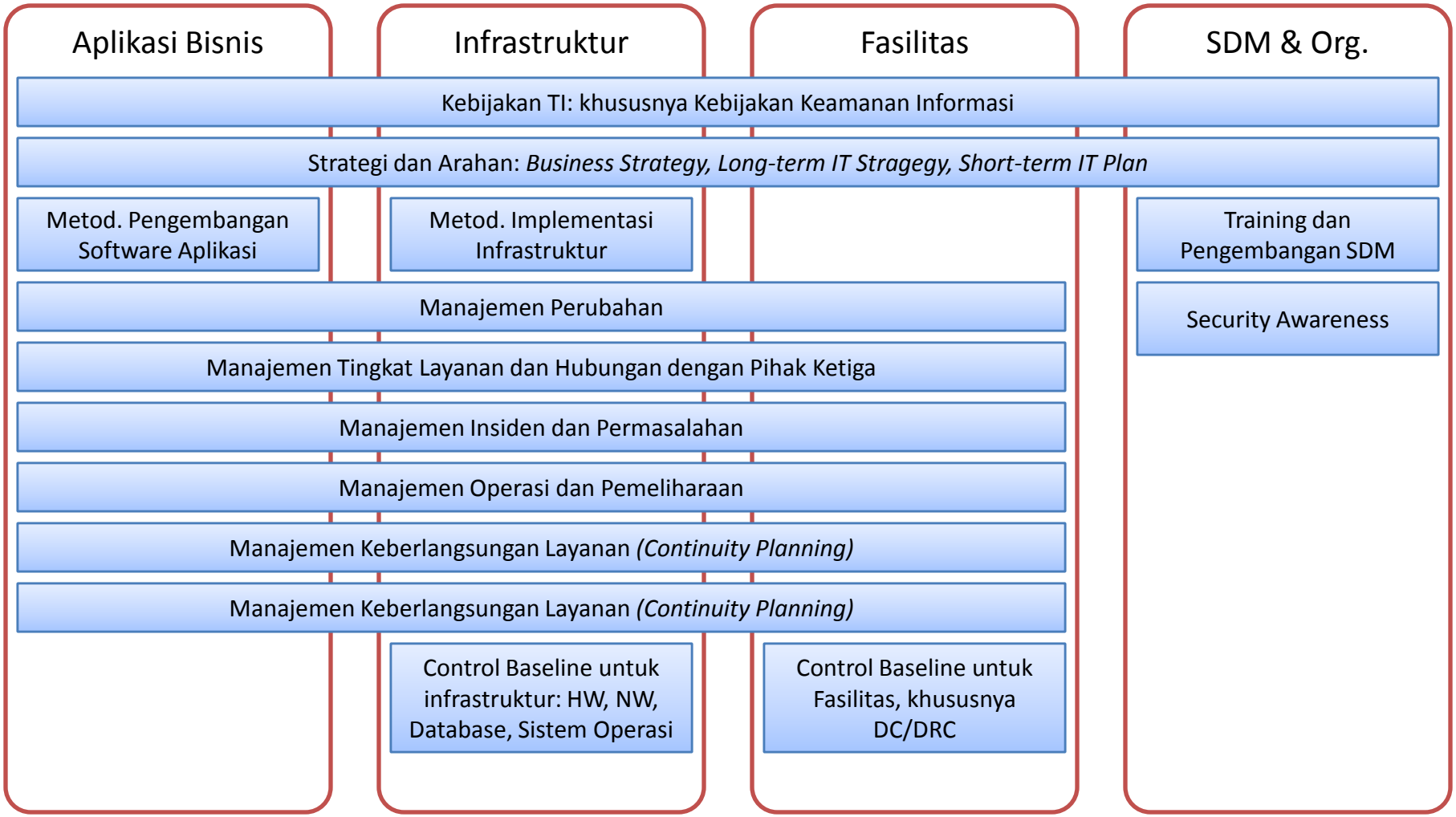
Kontrol TI = General Controls + Application Controls



Application Controls

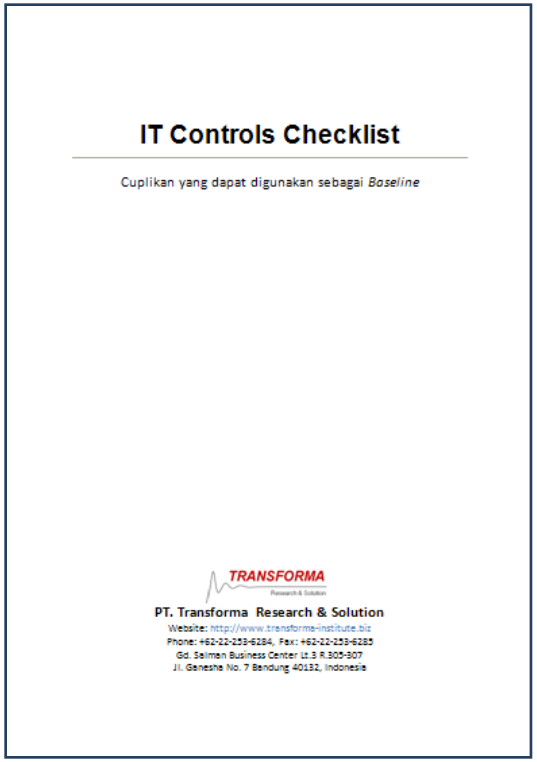
Logical Access Controls	Siapa sajakah yang berhak mengakses aplikasi? Bagaimana kontrol atas akses sehingga hanya terbatas pada yg berhak?
Input Controls	Apakah input data akurat, lengkap dan otentik? Bagaimana memvalidasi input ? Bagaimana memastikan input dilakukan oleh pihak yang terotorisasi ? Bagaimana melakukan koreksi?
Processing Controls	Bagaimana memastikan integritas dan validitas siklus pemrosesan? Deteksi pemrosesan error tidak mengganggu pemrosesan transaksi valid?
Output Controls	Apakah output ditangani dengan tepat, disampaikan kepada penerima yang tepat dan dilindungi dalam transmisinya?
Authorization Controls	Bagaimana mengelola otorisasi dalam aplikasi sehingga memimalkan fraud karena aspek tidak terpenuhinya *Segregation of Duties?*

General Controls



Referensi IT Controls

Dikarenakan lingkup *IT Controls* yang cukup luas, dapat digunakan referensi standar, framework atau *good practices* serta regulasi, misalnya COBIT, ISO 27000 series, ISO 20000/ITIL, NIST, dsb. Dalam CPE ini disajikan IT Controls Checklist untuk membantu memberikan deskripsi detail tentang konstruksi IT Controls.

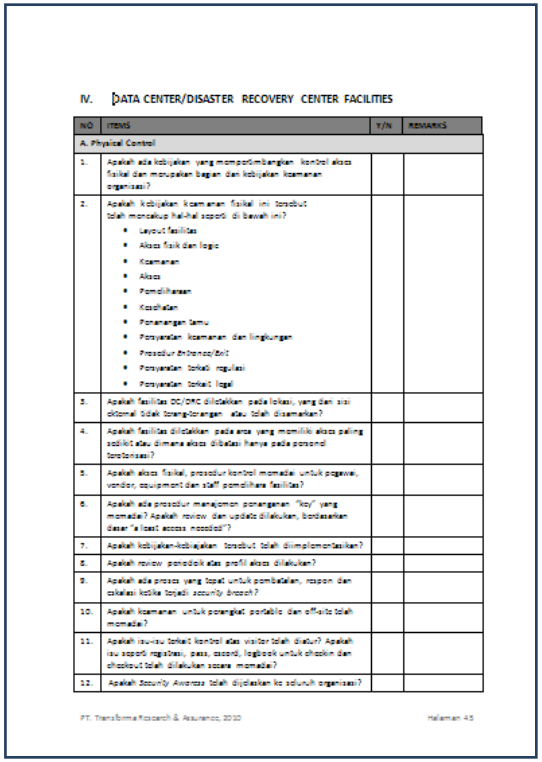


IT Controls Checklist

Cuplikan yang dapat digunakan sebagai *Baseline*

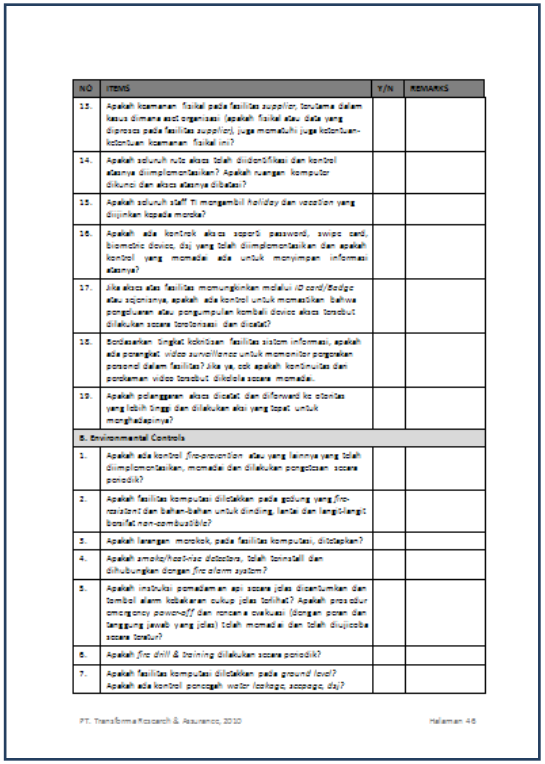
TRANSFORMA
Research & Solution

PT. Transforma Research & Solution
Website: http://www.transforma-institute.biz
Phone: +62-22-253-6284, Fax: +62-22-253-6285
Gd. Salman Business Center Lt.3 R.305-307
Jl. Ganesha No. 7 Bandung 40132, Indonesia



IV. DATA CENTER/DISASTER RECOVERY CENTER FACILITIES

NO	ITEMS	Y/N	REMARKS
A. Physical Control			
1.	Apakah ada kebijakan yang memperhitungkan kontrol akses fisikal dan merupakan bagian dari kebijakan keamanan organisasi?		
2.	Apakah kebijakan keamanan fisikal ini tersebut telah mencakup hal-hal seperti di bawah ini? • Layout fasilitas • Akses fisik dan logic • Keamanan • Akses • Pemeliharaan • Kesehatan • Penanangan tamu • Persyaratan keamanan dan lingkungan • Prosedur Entrance/Exit • Persyaratan terkait regulasi • Persyaratan terkait legal		
3.	Apakah fasilitas DC/DRC ditaktikan pada lokasi yang dari sisi eksternal tidak terang-terangan atau telah disamarkan?		
4.	Apakah fasilitas ditaktikan pada area yang memiliki akses paling sedikit atau dimana akses dibatasi hanya pada personil tertentusaja?		
5.	Apakah akses fisikal, prosedur kontrol memadai untuk pegawai, vendor, equipment dan staff pemelihara fasilitas?		
6.	Apakah ada prosedur manajemen penanganan "key" yang memadai? Apakah review dan update dilakukan, berdasarkan dasar "a least access necessity"?		
7.	Apakah kebijakan-kebijakan tersebut telah diimplementasikan?		
8.	Apakah review periodik atas profil akses dilakukan?		
9.	Apakah ada proses yang tepat untuk pembatalan, respon dan eskalasi ketika terjadi security breach?		
10.	Apakah keamanan untuk perangkat portable dan offsite telah memadai?		
11.	Apakah isu-isu terkait kontrol atas visitor telah diatur? Apakah isu seperti registrasi, pass, escord, logbook untuk checkin dan checkout telah dilakukan secara memadai?		
12.	Apakah Security Awarnes telah dijelaskan ke seluruh organisasi?		



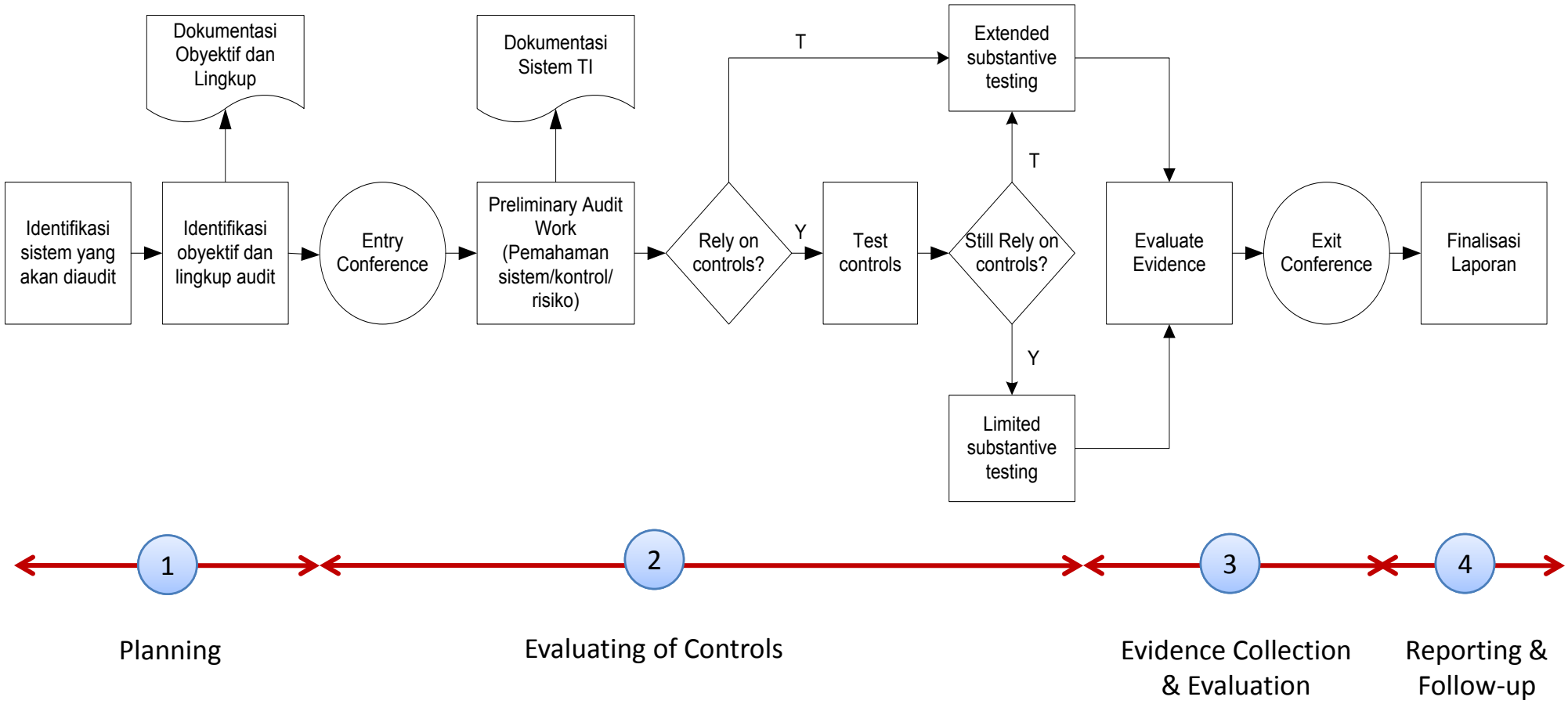
NO	ITEMS	Y/N	REMARKS
13.	Apakah keamanan fisikal pada fasilitas supplier, terutama dalam kasus dimana asset organisasi (apakah fisikal atau data yang diproses pada fasilitas supplier), juga memenuhi juga ketentuan-ketentuan keamanan fisikal ini?		
14.	Apakah seluruh nuts akses telah diidentifikasi dan kontrol atasnya diimplementasikan? Apakah ruangan komputer dikunci dan akses atasnya dibatasi?		
15.	Apakah seluruh staff TI mengambil holiday dan vacation yang diijinkan kepada mereka?		
16.	Apakah ada kontrak akses seperti password, swipe card, biometric device, dsj yang telah diimplementasikan dan apakah kontrol yang memadai ada untuk menyimpan informasi atasnya?		
17.	Jika akses atas fasilitas memungkinkan melalui ID card/Badge atau sejenisnya, apakah ada kontrol untuk memastikan bahwa pengeluaran atau pengumpulan kembali device akses tersebut dilakukan secara tepat waktu dan dicatat?		
18.	Berdasarkan singkat kebutuhan fasilitas sistem informasi, apakah ada perangkat video surveillance untuk memonitor pergerakan personil dalam fasilitas? Jika ya, cek apakah kontinuitas dan perekaman video tersebut dikelola secara memadai.		
19.	Apakah pelanggaran akses dicatat dan diforward ke otoritas yang lebih tinggi dan dilakukan aksi yang tepat untuk menghadapinya?		
B. Environmental Controls			
1.	Apakah ada kontrol fireprevention atau yang lainnya yang telah diimplementasikan, memadai dan dilakukan pengetesan secara periodik?		
2.	Apakah fasilitas komputasi ditaktikan pada gedung yang fire-resistant dan bahan-bahan untuk dinding, lantai dan langit-langit bersifat non-combustible?		
3.	Apakah larangan merokok, pada fasilitas komputasi, ditetapkan?		
4.	Apakah smoke/heat/fire detectors, telah terinstall dan dihubungkan dengan fire alarm system?		
5.	Apakah instruksi pemadaman api secara jelas dicantumkan dan tombol alarm kebakaran cukup jelas terlihat? Apakah prosedur emergency power off dan rencana evakuasi (dengan peran dan tanggung jawab yang jelas) telah memadai dan telah diujicoba secara tertur?		
6.	Apakah fire drill & training dilakukan secara periodik?		
7.	Apakah fasilitas komputasi ditaktikan pada ground level? Apakah ada kontrol pencegah water leakage, seepage, dsj?		

Agenda

- Konstruksi Kontrol TI
  - General Control
  - Application Control

- **Metodologi Audit TI: Step-by-Step**

Metodologi Audit TI



A. Planning

Technical Planning

Pemahaman akan organisasi, lingkungan bisnis, mekanisme kontrol internal, risiko dalam penggunaan sistem TI

Logistical Planning

Perencanaan sumberdaya SDM, Biaya dan Teknikal: Teaming-up, metodologi yang akan digunakan, lingkup audit, budget, time schedule, identifikasi cara-cara mendapatkan finding, penyusunan kerangka kebutuhan pelaporan

Risk Assessment

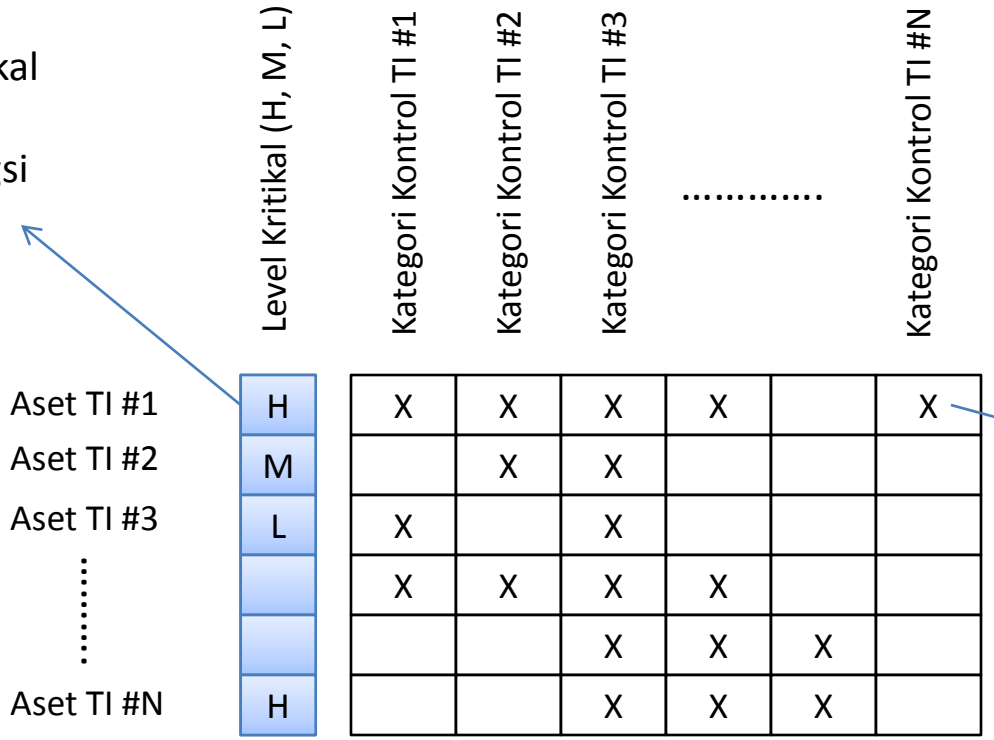
Iventori dan kategorisasi SI yang digunakan, penentuan dampak atas fungsi atau aset kritikal, penilaiain risiko awal dan potensi level severity-nya, penetapan prioritas audit, sumberdaya dan jadwal



A. Planning (cont.)

Satu tahapan paling krusial dalam Risk Assessment adalah melakukan penilaian level kritikal setiap aset dan apa saja kontrol yang relevan untuk setiap aset. Penentuan lingkup kontrol apa saja yang harus dipenuhi akan menjadi dasar dalam penentuan lingkup audit TI.

Penentuan level kritikal didasarkan atas dampaknya atas fungsi bisnis jika aset tsb bermasalah



	Level Kritikal (H, M, L)	Kategori Kontrol TI #1	Kategori Kontrol TI #2	Kategori Kontrol TI #3	.....		Kategori Kontrol TI #N
Aset TI #1	H	X	X	X	X		X
Aset TI #2	M		X	X			
Aset TI #3	L	X		X			
		X	X	X	X		
				X	X	X	
Aset TI #N	H			X	X	X	

Analisa lingkup kontrol dapat merujuk kepada referensi-referensi kontrol yang dibagi berdasarkan tipe aset

A. Planning (cont.)

Hasil dari fase *Planning* yang paling utama adalah tersusunya *Audit Programme,* yang akan menjadi dasar dalam pelaksanaan *Field Audit* nantinya.

1. Latar belakang dari entitas yang diaudit

   Pernyataan tentang *key drivers,* tujuan dan obyektif high-level

   - ❑ Obyektif
   - ❑ Struktur
   - ❑ Outline sistem hardware dan software
   - ❑ Ukuran operasi sistem komputer

2. Obyektif dan lingkup detail Audit
   - ❑ Outline obyektif detail audit
   - ❑ Outline lingkup dan pendekatan audit
   - ❑ Outline lingkup peran Auditor TI
3. Highlight area-area kritikal yang akan diuji: area-area dengan risiko terbesar
4. Kebutuhan sumberdaya:
   - ❑ Staffing/ Budgets/ scheduling
   - ❑ Sunberdaya teknikal yang diperlukan

B. Audit Execution

Dalam pelaksanaan audit, pengumpulan *evidence* akan menentukan sejauh mana analisa dapat dilakukan untuk menjawab obyektif yang ditentukan. Independensi dan kualifikasi sumber akan menentukan kualitas evidence.



- Proses yang diobservasi dan keberadaan item-item fisikal
- *Documentary audit evidence* (mencakup *electronic records*)
- Analysis(mencakuo *IT enabled analysis using CAATs*)

B. Audit Execution (cont.)

Auditor TI menggunakan dua tipe tes: **“Compliance Test”** dan **“Subtantive Test”**

- **“Compliance Test”** digunakan untuk mengetahui status kepatuhan kepada *rules* atau *regulation* organisasi dan memberikan *evidence* akan eksistensi dan efektifitas kontrol-kontrol internal.
- **“Subtantive Test”** memberikan *evidence* tentang validitas dan properti transaksi dan *balance,* digunakan untuk mengetes *monetary errors* yg secara langsung akan mempengaruhi *Financial statement balances.*
  - system availability analysis
  - system storage media analysis
  - system outage analysis
  - Comparing computer inventory as per book vis-à-vis actual count
  - Reconciling account balances



B. Audit Execution (cont.)

Setelah melakukan *Audit Test,* langkah selanjutnya adalah melakukan evaluasi atas evidence yang telah dapat dikumpulkan. Evaluasi atas evidence akan menghasilkan FINDING, jika ditemukan *significant variation.* Sebuah *Finding* harus bersifat faktual, didasarkan pada analisa komparasi atas standar/guideline dan disertai analisa *effect, impact, significance.* Defiensi finding menyertakan lima atribut berikut:

- Criteria (what should be)
- Condition (what is)
- Cause (why condition occurred)
- Effect (what is the consequence)
- Recommendation (what is to be done)



B. Audit Execution (cont.)

B. Environmental Controls			
1.	Apakah ada kontrol *fire-prevention* atau yang lainnya yang telah diimplementasikan, memadai dan dilakukan pengetesan secara periodik?		
2.	Apakah fasilitas komputasi diletakkan pada gedung yang *fire-resistant* dan bahan-bahan untuk dinding, lantai dan langit-langit bersifat *non-combustible?*		
3.	Apakah l		
4.	Apakah *s* dihubungkan dengan *fire alarm system?*		
5.	Apakah instruksi pemadaman api secara jelas dicantumkan dan tombol alarm kebakaran cukup jelas terlihat? Apakah prosedur emergency *power-off* dan rencana evakuasi (dengan peran dan		

Analisa efektifitas kontrol

Form Dokumentasi Finding dan Analisanya

IP	Vulnerability			Severity	Potensi Dampak	Rekomendasi
	Port	Serv	Finding			
192.168.2.1	53/ udp	domain	The host is running BIND and is prone to Security Bypass High.	Med	Successful exploitation could allow remote attackers to bypass the certificate validation checks and can cause man-in-the-middle attack via signature checks on DSA and ECDSA keys used with SSL/TLS.	Upgrade to version 9.6.0 P1, 9.5.1 P1, 9.4.3 P1, 9.3.6 P1
192.168.2.2	443/ tcp	https			CSRF queries.	plution or patch is available as on March, 2009. Information rding this issue will be updated the solution details are available. pdates refer, http://www.apachefriends.org/en/xampp.htm
	80/ tcp	http	The host is running PHP and is prone to Buffer Overflow vulnerability.	High	Successful exploitation could allow attackers to execute arbitrary code via a crafted string containing an HTML entity.	Upgrade to version 5.2.7 or later

Working paper teknikal

B. Audit Execution (cont.)

2 Aplikasi Bisnis

KONTROL TI		TEMUAN DEFISIENSI				ANALISA DAMPAK	
NO	NAMA	DESKRIPSI TEMUAN		D	O	DESKRIPSI	LEVEL
A.	**Akuisisi dan Implementasi Paket Software**						
A.1	Identifikasi dan Analisa Requirement	1.					
		2.					
		3.					
A.2	Kriteria pemilihan vendor	1.					
		2.					
		3.					
A.3	Proses pemilihan vendor	1.					
		2.					
		3.					
A.4	Kontrak	1.					
		2.					
		3.					
A.5	Implementasi	1.					
		2.					
		3.					
A.6	Post-Implementation	1.					

Contoh form utk Finding

B. Audit Execution (cont.)

Hal-hal praktis dan operasional yang akan menentukan eksekusi audit TI disumbangkan pada aspek teknikal dan non teknikal

- "Entry Conference" yang representatif dan menghasilkan persetujuan kesepakatan dan sponsorship atas pelaksanaan Audit TI
- Risk Assessment yang tepat untuk menghasilkan lingkup teknikal Audit TI
- Akses atas sistem dan lingkungan pada auditee yang cukup, sehingga pengetesan audit dapat dilakukan secara memadai
- Analisa evidence yang berorientasi bisnis
- "Exit Conference" untuk mendapatkan verifikasi, persetujuan dan komentar auditee dan manajemen



"First, I'll need to see an audited statement of revenue and expenses."

C. Reporting & Follow-up

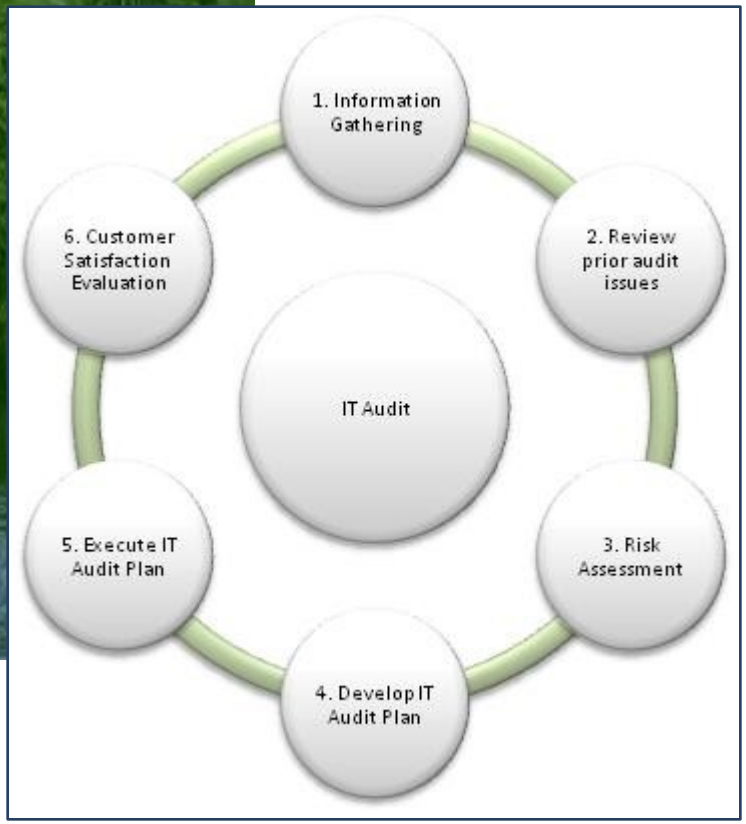
Laporan Audit TI harus lengkap, akurat, obyektif, meyakinkan dan jelas-padat sesuai dengan subyek yang ditetapkan. Laporan ini berisi seluruh Finding audit yang signifikan. Jika Finding memerlukan penjelasan, auditor harus memberikan deskripsi Finding, penyebab dan risikonya.

- Pendahuluan
- Obyektif, lingkup dan metodologi audit
- Audit Findings
- Kesimpulan Audit
- Rekomendasi

Adalah penting untuk menetapkan juga “Program Follow-up”, yang akan menjadi dasar dalam menutup defisiensi yang ditemukan dalam durasi waktu tertentu, sehingga risiko bisa dikelola secara memadai.




it should
always be
this easy


1. Information Gathering
2. Review prior audit issues
3. Risk Assessment
4. Develop IT Audit Plan
5. Execute IT Audit Plan
6. Customer Satisfaction Evaluation
IT Audit



Terimakasih

Thank You

Matur Nuwun

Hatur Nuhun