iValueIT

CONSULTING

Delivering Integrated Value Through IT

www.ivitc.com

Workshop Auditor Internal

PT Bukit Asam, Tbk.

Fasilitator:

1. Umar Alhabsyi, MT, CISA, CRISC.
2. Kurnia, MT, CISA, CISM, CRISC, ITILF

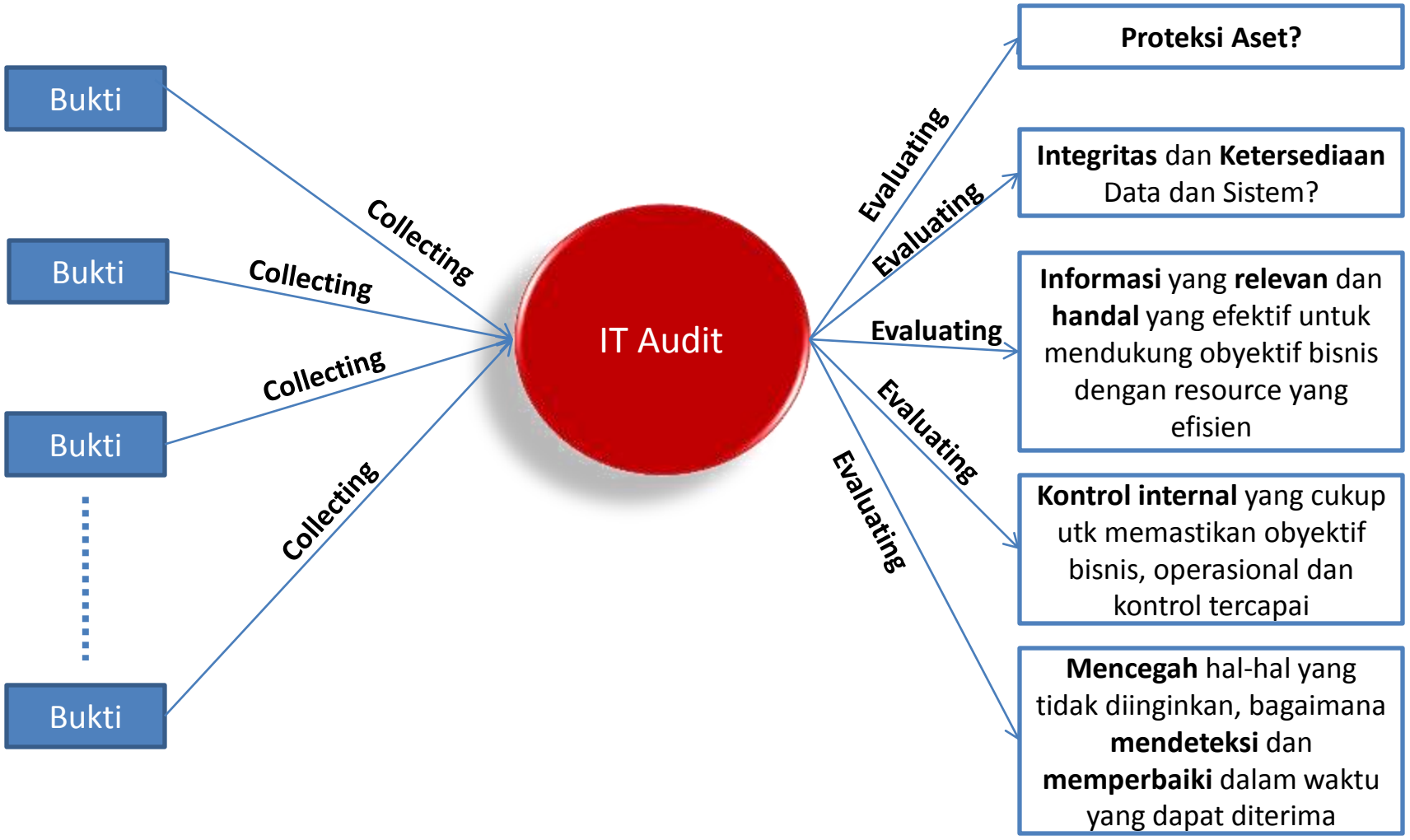
Hotel Jayakarta Bandung,
20-23 April 2015

Program Persiapan Auditor Teknologi Informasi

Audit Teknologi Informasi

Resume, Materi Tambahan dan Contoh-Contoh

IT Audit


Bukti
Bukti
Bukti
Bukti
Collecting
Collecting
Collecting
Collecting
IT Audit
Evaluating
Evaluating
Evaluating
Evaluating
Evaluating
Proteksi Aset?
Integritas dan Ketersediaan Data dan Sistem?
Informasi yang relevan dan handal yang efektif untuk mendukung obyektif bisnis dengan resource yang efisien
Kontrol internal yang cukup utk memastikan obyektif bisnis, operasional dan kontrol tercapai
Mencegah hal-hal yang tidak diinginkan, bagaimana mendeteksi dan memperbaiki dalam waktu yang dapat diterima

Basis dalam IT Audit?

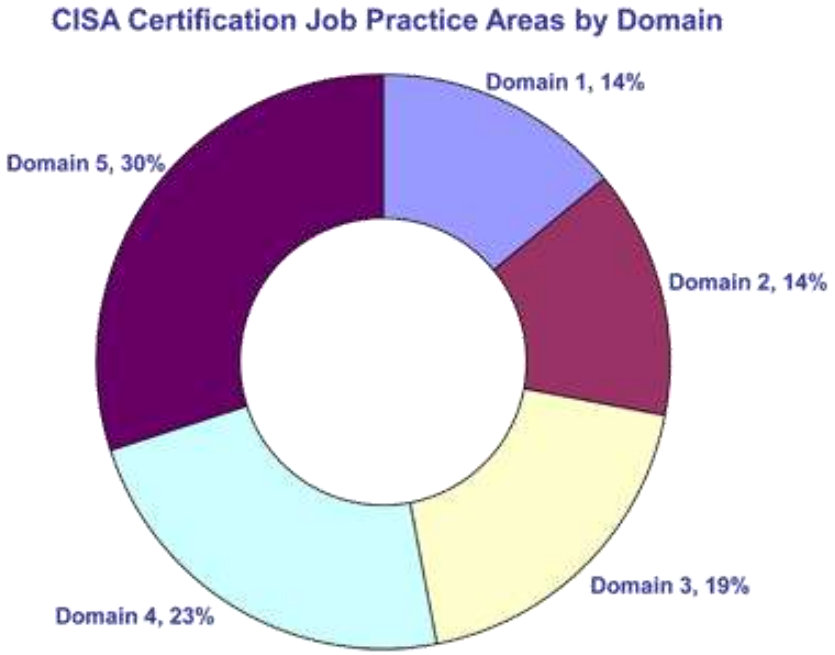
Tugas seorang IT Auditor adalah **mengidentifikasi Risiko** pada area dalam cakupan Audit, serta **identifikasi kebutuhan dan evaluasi penerapan kontrol** yang mengelolanya.

IS Auditor harus memahami Audit Subject

Kompetensi Standard untuk Auditor TI

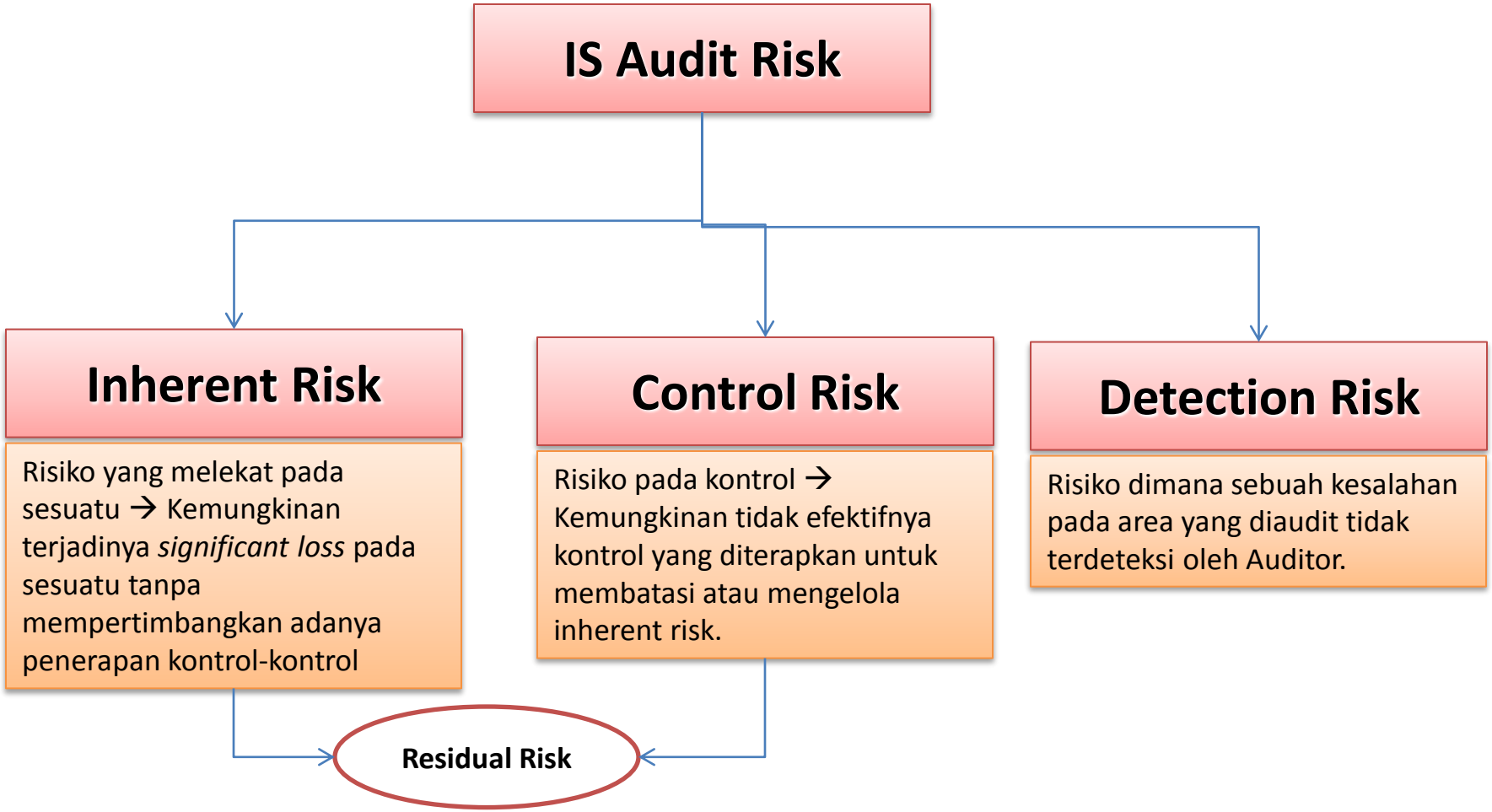
Domain 1—The Process of Auditing Information Systems (14%)
Domain 2—Governance and Management of IT (14%)
Domain 3—Information Systems Acquisition, Development and Implementation (19%)
Domain 4—Information Systems Operations, Maintenance and Support (23%)
Domain 5—Protection of Information Assets (30%)

CISA Certified Information Systems Auditor
An ISACA Certification



Risiko dalam Proses IS Audit

Audit Risk = Risiko yang diakibatkan IS Auditor tidak akurat dalam memberikan judgment terkait area yang diaudit



Tipe Kontrol Internal

Kontrol Internal

Preventive Control

Kontrol yang didesain untuk **mencegah** terjadinya kesalahan, kelalaian atau kejadian lain yang **telah diketahui** dapat berdampak negatif.

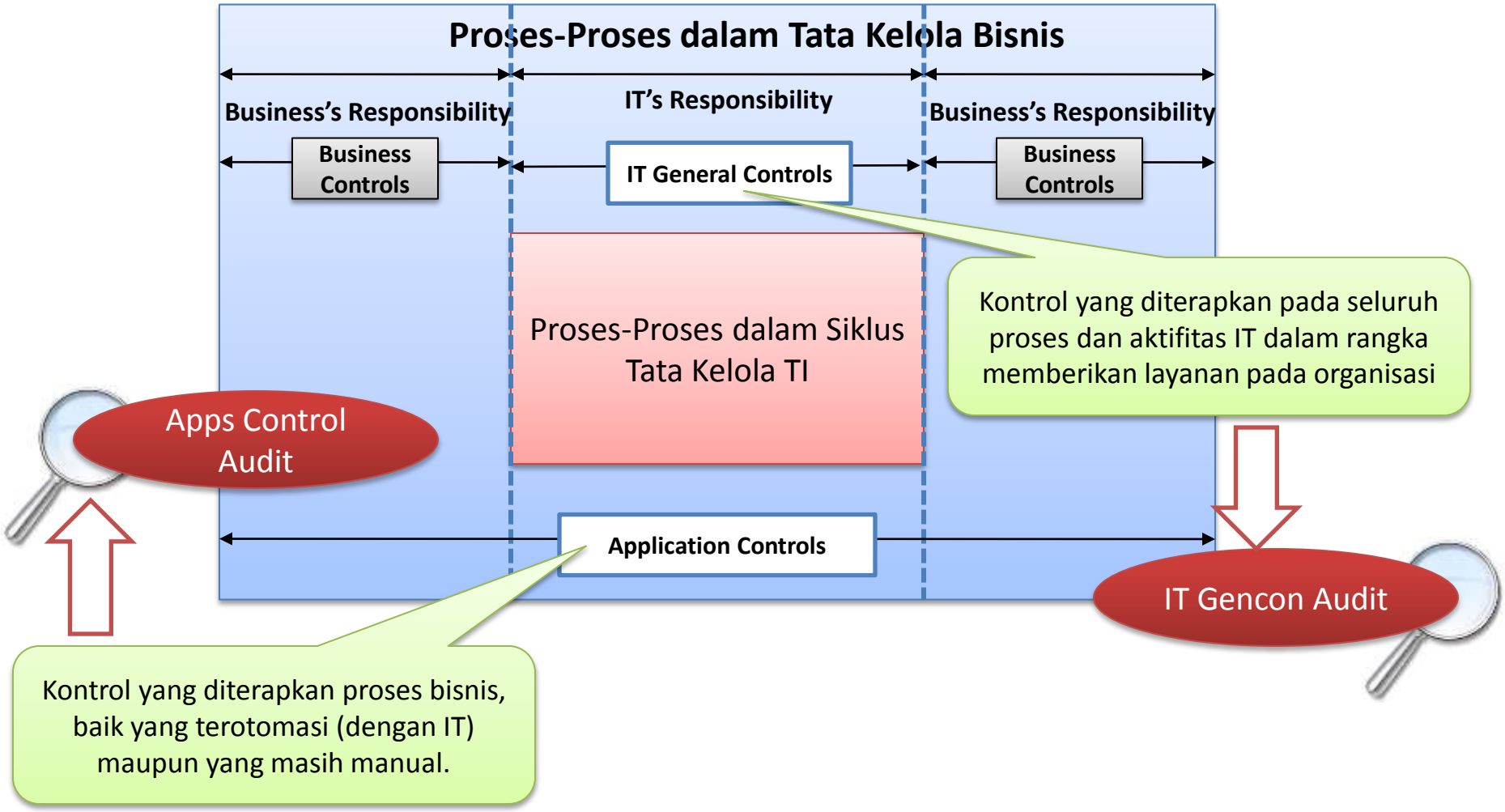
Detective Control

Kontrol yang digunakan untuk mengidentifikasi suatu kejadian, kesalahan atau hal lain yang terjadi dimana telah diketahui akan berdampak signifikan

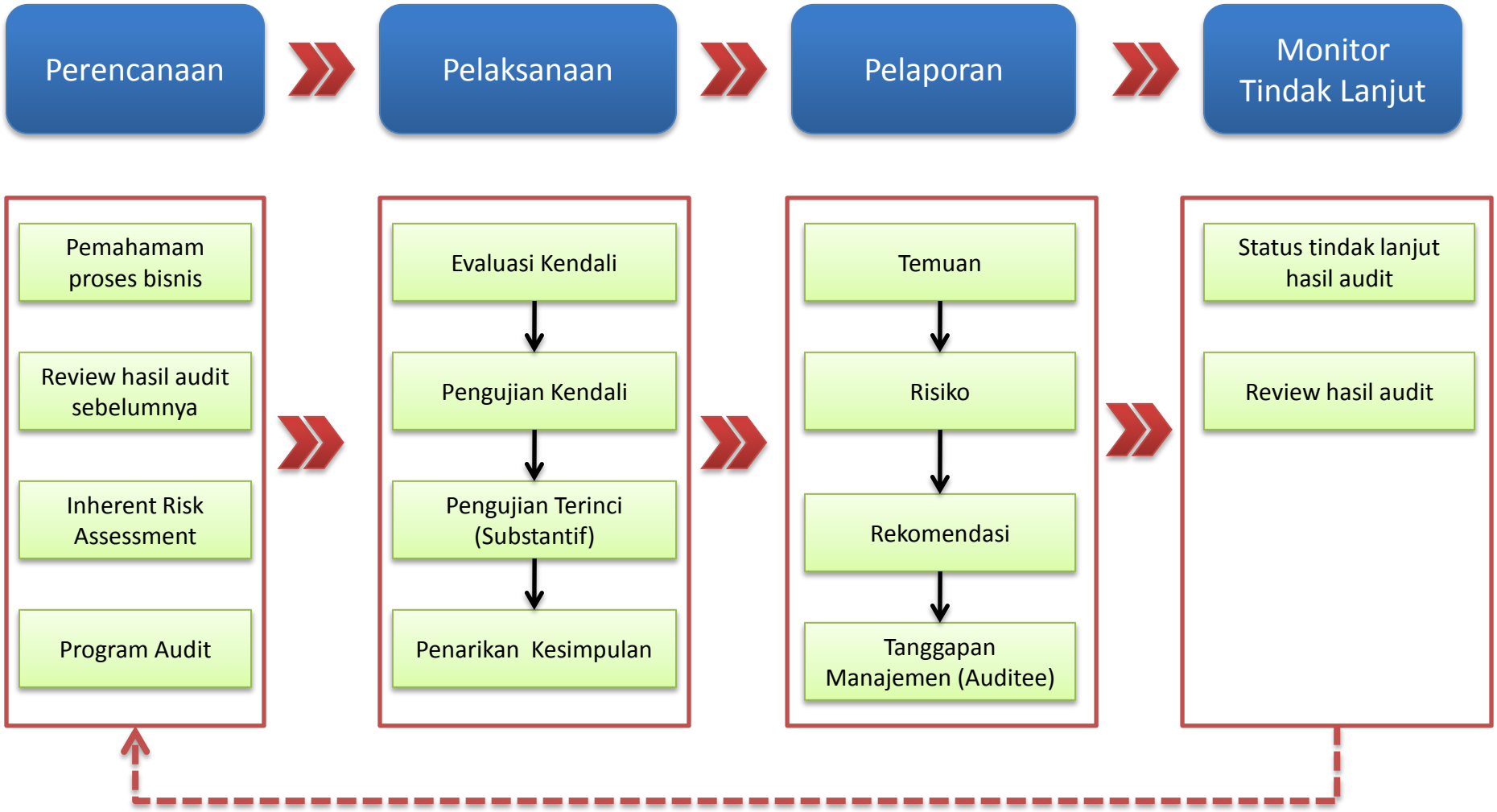
Corrective Control

Kontrol yang digunakan untuk melakukan perbaikan pada hal-hal yang berjalan tidak benar atau semestinya

Bisnis dan Kontrol TI



Proses IT Audit



1. Perencanaan Audit TI:

Kebijakan dan Prosedur

KEBIJAKAN
1. Fungsi AITI harus melakukan suatu proses penilaian risiko yang menggambarkan risiko inheren di Satuan Kerja TI dan Satuan Kerja Pengguna TI, yang diperbaharui secara berkala dan dijadikan dasar untuk perencanaan audit intern TI;
2. Fungsi AITI harus melaksanakan audit terhadap penyelenggaraan TI, yang direncanakan dan dilaksanakan sekurang-kurangnya 1 (satu) kali dalam setahun terhadap aspek-aspek yang terkait TI sesuai kebutuhan, prioritas, dan hasil analisis risiko TI perusahaan;
3. Fungsi AITI harus melakukan audit untuk aplikasi inti perusahaan, dimana keseluruhan modul aplikasi tersebut hendaknya diperiksa oleh audit intern TI sekurang-kurangnya sekali dalam 3 (tiga) tahun;
4. Fungsi AITI wajib menyusun suatu program untuk setiap penugasan yang akan dilaksanakan sesuai dengan rencana tahunan audit intern TI.

Contoh

Perencanaan Audit TI:

Kebijakan dan Prosedur

PROSEDUR
1. Sebelum melaksanakan analisis risiko TI, Fungsi AITI harus mengidentifikasi terlebih dahulu hal-hal sebagai berikut :
a) Sumber daya TI yang ada (informasi, aplikasi, infrastruktur, dan personil TI) serta aspek finansial yang terkait (Anggaran Belanja dan Anggaran Operasional TI);
b) Proses tata kelola TI yang ada (perencanaan dan organisasi, pengembangan dan implementasi, operasional dan layanan, serta monitoring dan pengawasan);
c) Kegiatan dan proses bisnis perusahaan yang telah menggunakan TI baik secara keseluruhan maupun sebagian.
2. Analisis risiko TI yang dilakukan oleh Fungsi AITI harus sesuai dengan Kebijakan dan Prosedur Manajemen Risiko dari Satuan Kerja Manajemen Risiko, serta memperhatikan Kebijakan dan Prosedur Manajemen Risiko TI yang diterapkan oleh Satuan Kerja TI, dan jika dipandang layak maka Fungsi AITI dapat memanfaatkan hasil analisis risiko TI yang telah disusun oleh Satuan Kerja TI dan/atau Satuan Kerja Manajemen Risiko.
3. Pelaksanaan Analisis Risiko TI oleh Fungsi AITI dapat dilakukan seperti contoh pada Lampiran– Formulir Analisis Risiko TI.
4. Fungsi ATI harus menyusun alokasi seluruh sumber daya audit berdasarkan suatu skala prioritas tertentu, dengan mempertimbangkan berbagai faktor, seperti : a) Hasil penilaian profil risiko yang terkait dengan aset/proses TI; b) Berbagai informasi audit yang terkait dengan aset/proses TI tersebut; c) Kewajiban audit intern TI berdasarkan peraturan dan perjanjian;
5. Pelaksanaan Alokasi Sumber Daya AITI oleh Fungsi AITI dapat dilakukan seperti contoh pada Lampiran– Rencana Tahunan AITI.
6. Fungsi AITI harus menyusun suatu Program Audit yang mencantumkan prosedur yang harus dilaksanakan oleh auditor intern TI dalam mengumpulkan, menganalisis, menginterpretasikan, dan mendokumentasikan informasi selama pelaksanaan audit.
7. Pelaksanaan penyusunan Program Audit oleh Fungsi AITI dapat dilakukan seperti contoh pada Lampiran– Program Audit TI.

Contoh

Perencanaan Audit TI:

Analisis Risiko

FORMULIR ANALISIS RISIKO TEKNOLOGI INFORMASI DALAM RANGKA PENYUSUNAN RENCANA AUDIT INTERN TI TAHUN ...

ASET/PROSES TI	ANCAMAN	RISIKO INHEREN	TINDAK LANJUT	RISIKO RESIDUAL	PENGENDALIAN			VARIABEL LAIN	PRIORITAS
					EKSISTING	MITIGASI	PIC		
Aplikasi									
Infrastruktur									
Personil									
Perencanaan TI									
Pengembangan TI									
Operasional TI									
... dsb.									

Contoh

Perencanaan Audit TI:

Rencana Audit Intern TI

RENCANA AUDIT INTERN TEKNOLOGI INFORMASI TAHUN ...

AUDIT UNIVERSE	LINGKUP AUDIT	TUJUAN AUDIT	JUMLAH HARI	JADWAL PELAKSANAAN	TIM AUDITOR	BIAYA AUDIT
Berdasarkan Aset						
Aplikasi						
Infrastruktur						
Personil						
Berdasarkan Kendali						
Perencanaan TI						
Pengembangan TI						
Operasional TI						
Lainnya						
Berdasarkan Lokasi						
Berdasarkan Bisnis						
Audit Wajib/Rutin						

Contoh

Perencanaan Audit TI:

Program Audit Intern TI

(LEMBAR RINCIAN) PROGRAM AUDIT INTERN TEKNOLOGI INFORMASI				
TUJUAN PROGRAM AUDIT				
LINGKUP PROGRAM AUDIT				
PENGENDALIAN		PROSEDUR AUDIT		REFERENSI
NO.	URAIAN SINGKAT	KODE	LANGKAH-LANGKAH	

Contoh

2. Pelaksanaan Audit TI:

Kebijakan dan Prosedur

KEBIJAKAN
1. Pelaksanaan seluruh audit pada Fungsi AITI harus disupervisi untuk menjamin bahwa tujuan audit telah tercapai dan pelaksanaannya telah sesuai dengan Kebijakan dan Prosedur AITI serta Standar Audit Intern TI.
2. Auditor intern TI harus memperoleh bukti audit yang cukup dan layak serta dapat diandalkan untuk mencapai tujuan audit, dimana kesimpulan dan seluruh temuan audit harus didukung oleh interpretasi dan analisis yang memadai atas bukti-bukti audit.
3. Fungsi AITI harus mendokumentasikan seluruh proses audit intern TI, dengan mencatat seluruh langkah audit yang telah dilaksanakan dan bukti audit yang relevan dengan tujuan dan lingkup audit yang diperoleh.
4. Pendokumentasian proses pelaksanaan audit harus memperhatikan mengenai aspek kerahasiaan, kelengkapan, dan ketersediaan dari informasi yang terkait dengan audit.

Contoh

2. Pelaksanaan Audit TI:

Kebijakan dan Prosedur

PROSEDUR

1. Supervisi atas setiap penugasan audit intern TI harus dilakukan untuk memastikan bahwa :
   a) Seluruh prosedur audit telah dilaksanakan dan didokumentasikan, dimana tidak terdapat prosedur audit yang terkait dengan risiko dan kendali TI yang material dan signifikan yang belum dilaksanakan oleh auditor intern TI;
   b) Seluruh dokumentasi pelaksanaan prosedur audit, kertas kerja audit serta bukti-bukti audit yang diperoleh, telah direviu dengan memadai;
   c) Berbagai kendala dan hambatan teknis dan non-teknis terkait yang dapat mengganggu pelaksanaan dan pencapaian tujuan penugasan dapat segera ditindaklanjuti.
2. Auditor intern TI harus memperoleh bukti audit yang cukup dan layak serta dapat diandalkan untuk mencapai tujuan audit, yang antara lain mencakup :
   a) Prosedur audit yang telah dilaksanakan dan hasilnya;
   b) Temuan dan kesimpulan hasil pelaksanaan audit Intern TI.
3. Auditor intern TI harus mendokumentasikan seluruh informasi yang terkait dengan pelaksanaan prosedur audit dan berbagai bukti yang diperolehnya di dalam Kertas Kerja Audit Intern TI, yang harus :
   a) Disusun dengan lengkap, jelas, terstruktur, dan memiliki indeks, agar mudah untuk dipahami dan digunakan, serta mencantumkan identitas pihak yang melaksanakan setiap tahapan dan pengujian serta peranannnya, serta telah direviu oleh pihak lain di dalam tim.
   b) Memungkin dilakukannya pelaksanaan ulang kegiatan yang telah dilaksanakan auditor intern TI, dan memperoleh hasil dan kesimpulan yang sama;
4. Kertas Kerja Audit dapat menggunakan bentuk seperti pada Lampiran– Formulir Kertas Kerja Audit.

Contoh

2. Pelaksanaan Audit TI:

Kertas Kerja Audit Intern TI

(ISI) KERTAS KERJA AUDIT INTERN TI	
JUDUL PENUGASAN	
BAGIAN PENUGASAN	
TAHAPAN PENUGASAN	
TUJUAN PROSEDUR AUDIT	
RENCANA PROSEDUR AUDIT	
PELAKSANAAN PROSEDUR AUDIT	
HASIL PROSEDUR AUDIT	**INDEKS KKA**
KESIMPULAN PROSEDUR AUDIT	

Contoh

3. Pelaporan Audit TI:

Kebijakan dan Prosedur

KEBIJAKAN

1. Fungsi AITI harus menyampaikan laporan atas setiap penugasan yang telah selesai dilaksanakan, dan disampaikan kepada pihak-pihak yang terkait dengan penugasan tersebut;
2. Penyusunan dan persetujuan serta distribusi dan retensi berbagai laporan Audit Intern TI harus sesuai dengan peraturan yang berlaku dan Standar Audit Intern TI.

PROSEDUR

1. Fungsi AITI harus mengkomunikasi setiap ditemukan adanya kelemahan atau kekurangan atas rancangan dan/atau pelaksanaan pengendalian intern TI dan manajemen risiko, dimana komunikasi tersebut minimal mencakup :

   a) **Kondisi** – Yaitu berbagai fakta mengenai kelemahan atau kekurangan rancangan dan pelaksanaan atas rancangan dan/atau pelaksanaan pengendalian intern TI dan manajemen risiko TI yang didasarkan kepada bukti-bukti audit yang diperoleh dari hasil pelaksanaan prosedur pengujian Audit Intern TI;

   b) **Akibat/Risiko** – Yaitu dampak yang disebabkan oleh adanya kondisi tersebut diatas, yang secara aktual telah terjadi atau memiliki potensi untuk terjadi, yang telah atau akan dapat mempengaruhi pencapaian sebagian atau keseluruhan tujuan dari pengendalian intern TI dan manajemen risiko TI;

   c) **Rekomendasi** - Yaitu berbagai tindakan perbaikan yang menurut auditor intern TI dapat atau harus dilakukan oleh-oleh pihak yang terkait, untuk menghilangkan atau penyebab, serta menghilangkan atau mengendalikan berbagai dampak, dari adanya berbagai kelemahan atau kekurangan atas rancangan dan/atau pelaksanaan pengendalian intern TI dan manajemen risiko TI;

   d) **Tanggapan Manajemen** – Yaitu klarifikasi atau penjelasan dan argumentasi atau tanggapan resmi dari pihak-pihak yang terkait dan/atau bertanggungajawab atas hal-hal yang terkait dengan temuan dan rekomendasi yang disampaikan oleh auditor intern TI.

Contoh

3. Pelaporan Audit TI:

Kebijakan dan Prosedur

PROSEDUR

2. Bentuk komunikasi temuan dan rekomendasi audit intern TI dapat menggunakan bentuk seperti pada Lampiran – Lembar Temuan Pemeriksaan;
3. Fungsi AITI harus menyampaikan suatu Laporan Hasil Audit Intern TI kepada Komite Audit dan Direksi serta pihak-pihak yang terkait dengan suatu penugasan, segera setelah audit selesai dilaksanakan, yang minimal mencakup :
   a) Identitas organisasi, pihak-pihak yang berhak menerima, dan pembatasan distribusi atau sirkulasi laporan tersebut;
   b) Tujuan, aspek dan periode yang dicakup, serta sifat, waktu, dan kedalaman audit;
   c) Hasil Audit Intern TI berupa temuan, kesimpulan, dan rekomendasi Audit Intern TI, serta, jika ada, pengecualian dan pembatasan terkait dengan lingkup audit;
   d) Tanggapan dan/atau komentar resmi atas Laporan Hasil Audit Intern TI dari pihak-pihak yang bertanggungjawab atas entitas atau kegiatan yang diaudit;
   e) Tanggal pelaporan, serta nama, jabatan dan tanda tangan Ketua Tim dan/atau Kepala SKAI;
   f) Ringkasan Eksekutif, yang merupakan ringkasan dari Laporan Hasil Audit Intern TI, khususnya mengenai hal-hal yang menurut Auditor Intern TI cukup material dan signifikan dan perlu mendapatkan perhatian dari pihak-pihak yang bertanggungjawab atas kegiatan yang diaudit;

Contoh

3. Pelaporan Audit TI:

Kebijakan dan Prosedur

PROSEDUR

4. Kesimpulan Audit yang dapat digunakan oleh Tim Audit Intern TI untuk menunjukan tingkat kehandalan pengendalian intern TI dalam Laporan Hasil Audit Intern TI adalah sebagai berikut :

   a) **Dapat Diandalkan (*Satisfactory*)**, yaitu menunjukan bahwa rancangan atau implementasi atau pencapaian tujuan pengendalian intern TI yang dicakup dalam lingkup audit intern TI yang dilaporkan secara umum telah dapat diandalkan, dimana ……..;

   b) **Perlu Peningkatan (*Need Improvement*)**, yaitu menunjukan rancangan atau implementasi atau pencapaian tujuan pengendalian intern TI yang dicakup dalam lingkup audit intern TI yang dilaporkan relatif telah dipandang memadai, namun masih terdapat kelemahan atau kekurangan yang jika ditingkatkan akan dapat memberikan peningkatan ……;

   c) **Belum Dapat Diandalkan (*Weak*)**, yaitu menunjukan bahwa dalam rancangan atau implementasi atau pencapaian tujuan pengendalian intern TI masih terdapatnya kelemahan atau kekurangan yang signifikan ……..

5. Penetapan Kesimpulan Audit dalam Laporan Hasil Audit Intern TI dapat menggunakan matrikulasi seperti pada Lampiran - Matriks Penetapan Kesimpulan Audit Intern TI.

Contoh

3. Pelaporan Audit TI:

Lembar Temuan Audit

LEMBAR TEMUAN AUDIT	
JUDUL PENUGASAN	
BAGIAN LINGKUP PENUGASAN	
NOMOR KODE TEMUAN	
JUDUL TEMUAN	
KLASIFIKASI TEMUAN	
KONDISI	
RISIKO	
REKOMENDASI	
TANGGAPAN	

Contoh

3. Pelaporan Audit TI:

Matriks Penetapan Kesimpulan Audit TI

MATRIKS PENETAPAN KESIMPULAN AUDIT INTERN TI			
Kesimpulan Tahapan Evaluasi Kendali	**Kesimpulan Tahapan Pengujian Kendali**	**Kesimpulan Tahapan Pengujian Terinci**	**Kesimpulan Audit Intern TI**
Dapat Diandalkan (*Satisfactory*)	Dapat Diandalkan (*Satisfactory*)	Dapat Diandalkan (*Satisfactory*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Dapat Diandalkan (*Satisfactory*)"**
Dapat Diandalkan (*Satisfactory*)	Dapat Diandalkan (*Satisfactory*)	Perlu Peningkatan (*Need Improvement*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Dapat Diandalkan (*Satisfactory*)"**
Dapat Diandalkan (*Satisfactory*)	Dapat Diandalkan (*Satisfactory*)	Belum Dapat Diandalkan (*Weak*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Perlu Peningkatan (*Need Improvement*)"**
Dapat Diandalkan (*Satisfactory*)	Perlu Peningkatan (*Need Improvement*)	Dapat Diandalkan (*Satisfactory*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Dapat Diandalkan (*Satisfactory*)"**
Dapat Diandalkan (*Satisfactory*)	Perlu Peningkatan (*Need Improvement*)	Perlu Peningkatan (*Need Improvement*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Perlu Peningkatan (*Need Improvement*)"**
Dapat Diandalkan (*Satisfactory*)	Perlu Peningkatan (*Need Improvement*)	Belum Dapat Diandalkan (*Weak*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Belum Dapat Diandalkan (*Weak*)"**
Dapat Diandalkan (*Satisfactory*)	Belum Dapat Diandalkan (*Weak*)	Dapat Diandalkan (*Satisfactory*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Perlu Peningkatan (*Need Improvement*)"**
Dapat Diandalkan (*Satisfactory*)	Belum Dapat Diandalkan (*Weak*)	Perlu Peningkatan (*Need Improvement*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Belum Dapat Diandalkan (*Weak*)"**
Dapat Diandalkan (*Satisfactory*)	Belum Dapat Diandalkan (*Weak*)	Belum Dapat Diandalkan (*Weak*)	Auditor dapat menyimpulkan bahwa **"Pengendalian Intern TI Belum Dapat Diandalkan (*Weak*)"**

Contoh

4. Monitoring Tindak Lanjut Audit TI:

Kebijakan dan Prosedur

KEBIJAKAN
1. Fungsi AITI harus meminta tanggapan dari satuan kerja yang terkait terhadap hasil audit intern TI dan apabila terdapat rekomendasi yang perlu ditindaklanjuti maka satuan kerja yang terkait harus memberikan komitmen dan target waktu penyelesaiannya;
2. Fungsi AITI harus memonitor pelaksanaan rekomendasi audit intern TI dan melakukan verifikasi terhadap perbaikan yang sudah dilakukan, untuk mengevaluasi apakah tindak lanjut tersebut telah dilaksanakan secara memadai dan tepat waktu.

Contoh

4. Monitoring Tindak Lanjut Audit TI:

Kebijakan dan Prosedur

PROSEDUR

1. Funngsi ATI, bersama dengan Fungsi Manajemen Risiko TI, dalam melakukan pemantauan tindak lanjut atas rekomendasi audit intern TI, harus :
   a) Mencatat jangka waktu yang harus dipenuhi oleh satuan kerja untuk menindaklanjuti rekomendasi Audit Intern TI;
   b) Jika dipandang perlu, dapat melakukan penugasan khusus atau tambahan dalam rangka melakukan evaluasi dan verifikasi atas tindak lanjut yang telah dilaporkan;
   c) Apabila terdapat tindak lanjut yang belum dilaksanakan atau yang dipandang kurang memadai pelaksanaannya, Fungsi AITI harus menyampaikan hasil pemantauan tindak lanjut audit intern TI tersebut kepada satuan kerja yang terkait atau kepada pejabat yang lebih tinggi;
   d) Apabila satuan kerja yang bertanggungjawab untuk menindaklanjuti temuan dan rekomendasi audit intern TI memutuskan untuk tidak melaksanakan tindak lanjut yang telah disepakati, maka Fungsi AITI harus memperoleh keyakinan yang memadai bahwa tingkat risiko yang terkait dengan tindak lanjut temuan tersebut telah dipahami dan dapat diterima oleh satuan kerja dan/atau pejabat yang bertanggung jawab atas risiko terkait tersebut.
2. Fungsi AITI, dalam melakukan evaluasi dan verifikasi kelayakan tindak lanjut atas rekomendasi Audit Intern TI, harus memperhatikan :
   a) Signifikansi dari temuan dan rekomendasi Audit Intern TI tersebut;
   b) Adanya perubahan terhadap lingkungan TI yang dapat mempengaruhi signifikasi permasalahan atau risiko yang terkait dengan rekomendasi tersebut;
   c) Sumber daya dan kompleksitas serta jangka waktu yang dibutuhkan untuk melaksanakan tindak lanjut dari rekomendasi Audit Intern TI tersebut;
   d) Dampak yang mungkin ditimbulkan jika tindak lanjut dari rekomendasi tersebut tidak atau gagal dilakukan;

Contoh

Standard Audit Intern TI

STANDAR AUDIT

S-1 Penugasan Audit

S-1.1 Tanggung Jawab, Wewenang dan Akuntabilitas

Tanggung jawab, wewenang dan akuntabilitas dari Auditor Teknologi Informasi harus dinyatakan dengan jelas secara formal dan tertulis dalam piagam atau surat tugas audit teknologi informasi serta disetujui secara bersama oleh Auditor Teknologi Informasi dan pemberi tugas.

S-2 Independensi dan Obyektifitas

S-2.1 Independensi

Dalam berbagai hal yang berkaitan dengan audit teknologi informasi, Auditor Teknologi Informasi harus menjaga independensinya, baik secara faktual maupun penampilan dari organisasi atau hal yang diaudit.

S-2.2 Obyektifitas

Auditor Teknologi Informasi harus menjaga obyektifitasnya dalam merencanakan, melaksanakan dan melaporkan audit teknologi informasi.

S-3 Profesionalisme dan Kompetensi

S-3.1 Profesionalisme

Auditor Teknologi Informasi harus memenuhi berbagai standar audit yang berlaku serta menerapkan kecermatan dan keterampilan profesionalnya dalam merencanakan, melaksanakan, dan melaporkan audit teknologi informasi.

S-3.2 Kompetensi

Auditor Teknologi Informasi, secara kolektif, harus memiliki atau memperoleh pengetahuan dan keahlian yang diperlukan untuk melaksanakan audit teknologi informasi.

S-3.3 Pendidikan Profesi Berkelanjutan

Auditor Teknologi Informasi harus meningkatkan pengetahuan dan keahlian yang diperlukan untuk melaksanakan audit teknologi informasi melalui pendidikan profesi berkelanjutan.

Piagam Audit Intern TI

PENDAHULUAN
Piagam Audit Intern Teknologi Informasi ini merupakan dasar pelaksanaan fungsi dari Audit Intern Teknologi Informasi (AITI) serta penegasan komitmen dari berbagai pihak yang terkait di perusahaan terhadap arti pentingnya fungsi pengawasan atas proses dan fungsi TI.

TANGGUNG JAWAB
1. Mengidentifikasi area risiko TI yang akan menjadi fokus audit;
2. Melakukan evaluasi terhadap fungsi dan kecukupan pengendalian intern TI;
3. Mengevaluasi efektifitas perencanaan dan pengawasan penyelenggaraan TI;
4. Mengevaluasi kepatuhan TI terhadap ketentuan intern, ketentuan Regulator dan ketentuan perundang-undangan yang berlaku serta praktik-praktik terbaik internasional;

KEWAJIBAN
1. Merencanakan, melaksanakan, mengawasi dan melaporkan seluruh aktifitasnya sesuai dengan Standar Audit dan Kebijakan dan Prosedur AITI;
2. Menjaga independensi dan obyektifitas dan meningkatkan profesionalisme dan kompetensi, serta mematuhi dan Kode Etik AITI;

Piagam Audit Intern TI

RUANG LINGKUP
Ruang lingkup AITI adalah mencakup seluruh proses dan aset yang berkaitan langsung maupun tidak langsung dengan TI di Perusahaan, baik yang dilaksanakan oleh Perusahaan maupun yang dilaksanakan oleh pihak ketiga yang terkait;

WEWENANG	
Dalam melaksanakan tugasnya AITI berwenang untuk mengakses seluruh informasi yang relevan atas seluruh proses dan aset TI di Perusahaan, sesuai dengan kebutuhan penugasan dan peraturan yang berlaku.	
DEWAN KOMISARIS	**DEWAN DIREKSI**

Contoh

Contoh Program Audit TI

Contoh-1: Audit atas Organisasi TI

PROGRAM AUDIT INTERN TEKNOLOGI INFORMASI	
TUJUAN PROGRAM AUDIT	Evaluasi atas disain dan implementasi Organisasi TI dan Manajemen SDM TI, untuk memastikan bahwa : 1. Struktur organisasi TI telah menggambarkan secara spesifik garis kewenangan, pelaporan, tanggung jawab untuk setiap fungsi TSI yang harus dimiliki; 2. Struktur organisasi TI telah menerapkan prinsip pemisahan tugas dan tanggung jawab untuk mencegah seseorang mendapat tanggung jawab atas fungsi-fungsi yang berbeda dan kritikal sedemikian rupa yang dapat menyebabkan kesalahan tidak mudah dideteksi, dan telah menerapkan berbagai pengendalian TSI pengganti jika pemisahan tugas dan tanggungjawab belum dapat dilaksanakan secara memadai; 3. Penempatan personil TSI telah dilakukan berdasarkan pertimbangan kompetensi (pengetahuan dan keahlian) yang sesuai dengan posisi (jabatan/tugas);
LINGKUP PROGRAM AUDIT	**1. Organisasi TI** : Dewan Komisaris, Dewan Direksi, Komite Pengarah TI, Satuan Kerja TI, Satuan Kerja Manajemen Risiko, Pejabat Tertinggi Pengamanan Informasi, Satuan Kerja Pengguna TI **2. Manajemen SDM TI** : Rekrutmen dan Seleksi , Penugasan, Pendidikan dan Pelatihan

Contoh

Audit atas Organisasi TI

PENGENDALIAN	PROSEDUR AUDIT	REFERENSI
	PEMAHAMAN	
Organisasi TI	1. Pahami struktur organisasi, tugas pokok dan fungsi Satuan Kerja TI	
	2. Pahami wewenang dan tanggung jawab dari Dewan Komisaris, Dewan Direksi, Komite Pengarah TI, Satuan Kerja TI, Satuan Kerja Manajemen Risiko, Satuan Kerja Pengguna TI, khususnya yang berkaitan dengan fungsi penyelenggaraan TI dan manajemen risiko TI	
	3. Pahami alur kerja antara berbagai satuan kerja yang terkait dalam manajemen risiko TI	
Manajemen SDM TI	1. Pahami kebijakan dan prosedur pengelolaan SDM TI yang mencakup: rekruitmen, pengembangan, mutas/rotasi dan terminasi, standar penilaian kinerja, remunerasi.	
	2. Pahami kebijakan dan prosedur pengikatan hubungan kerja dengan konsultan, pegawai honorer, dan pegawai penyedia jasa TI	

Contoh

Audit atas Organisasi TI

	EVALUASI KENDALI	
Organisasi TI	1. Evaluasi kecukupan disain organisasi TI sesuai ketentuan yang berlaku	
Manajemen SDM TI	2. Evaluasi kecukupan disain kebijakan & prosedur manajemen SDM TI sesuai ketentuan yang berlaku	
	UJI KENDALI	
Organisasi TI	1. Uji apakah pihak-pihak berikut ini di dalam organisasi TI telah melaksanakan peranannya : ▪ Dewan Komisaris ▪ Dewan Direksi ▪ Komite Pengarah TI ▪ Pimpinan Satuan Kerja TI ▪ Satuan Kerja Manajemen Risiko ▪ Pejabat Tertinggi Pengamanan Informasi ▪ Satuan Kerja Pengguna TI	**Lampiran-1**
Manajemen SDM TI	2. Berdasarkan sampel, uji apakah kebijakan dan prosedur SDM telah dilaksanakan, khususnya untuk : ▪ Rekrutmen dan Seleksi ▪ Penugasan/Pengangkatan ▪ Pendidikan dan Pelatihan	**Lampiran-1**

Audit atas Organisasi TI

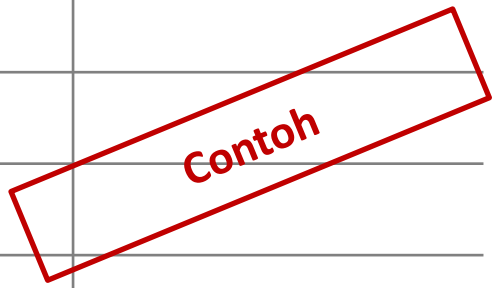
	UJI TERINCI
Organisasi TI	1. Analisis melalui matriks fungsi/peranan (RACI Chart) diantara pihak-pihak yang terkait dalam organisasi TI, apakah terdapat : a) perangkapan fungsi/peranan; b) fungsi/peranan yang belum dialokasikan; c) alokasi fungsi/peranan secara tumpang tindih.
Manajemen SDM TI	2. Berdasarkan sampel, uji apakah terdapat SDM TI yang : ■ Proses rekrutmen dan seleksi tidak sesuai dengan kebijakan dan prosedur; ■ Kelengkapan Penugasan/Pengangkatannya belum sesuai dengan kebijakan dan prosedur; ■ Memiliki kompetensi yang tidak sesuai dengan kerangka kompetensi untuk posisinya; ■ Belum memenuhi kebijakan dan prosedur Pendidikan dan Pelatihan.

Contoh

Lampiran-2: Evaluasi Kendali Organisasi TI

KUESIONER EVALUASI PENGENDALIAN INTERN

PENGENDALIAN INTERN	Ya	Tdk	Keterangan
1. Apakah tanggung jawab Dewan Komisaris sudah mencakup hal-hal sebagai berikut :			
a) Mengarahkan, memantau dan mengevaluasi Rencana Strategis TSI dan kebijakan Perusahaan terkait penyelenggaraan TSI;			
2. Apakah wewenang dan tanggung jawab Direksi sudah mencakup hal-hal sebagai berikut :			
a) Menetapkan Rencana Strategis TI dan rencana pelaksanaan dan/atau pengembangan TSI jangka pendek yang sejalan dengan rencana strategis dan rencana tahunan Perusahaan;			
b) Memastikan bahwa TI yang digunakan Perusahan dapat mendukung perkembangan usaha, pencapaian tujuan bisnis Perusahaan dan kelangsungan pelayanan kepada pelanggan;			
3. Apakah wewenang dan tanggung jawab Komite Pengarah TI sudah mencakup memberikan rekomendasi kepada Dewan Komisaris dan Dewan Direksi untuk hal-hal sebagai berikut :			
a) Rencana Strategis TI agar selalu sejalan dengan rencana strategis Perusahaan;			
b) Kesesuaian TI dengan kebutuhan sistem informasi manajemen dan kebutuhan kegiatan usaha Perusahaan;			



	PENGENDALIAN INTERN	Ya	Tdk	Keterangan
4.	Apakah wewenang dan tanggung jawab Pimpinan Satuan Kerja TSI (SKTSI) sudah mencakup hal-hal sebagai berikut :			
	a) Bersama dengan satuan kerja yang terkait, merumuskan kebijakan, rencana dan anggaran TI;			
	b) Bersama dengan satuan kerja yang terkait, menerapkan semua kebijakan TI dan rencana yang telah ditetapkan oleh Dewan Direksi,;			
	c) Melalui koordinasi dengan satuan kerja yang terkait, memberikan dukungan pemberian layanan TI kepada satuan kerja pengguna untuk mencapai target bisnisnya secara responsif dan tepat waktu;			
5.	Apakah wewenang dan tanggung jawab Pimpinan Satuan Kerja Manajemen Risiko (SKMR) sudah mencakup hal-hal sebagai berikut :			
	a) Menetapkan kebijakan dan prosedur manajemen risiko TI yang mencakup proses identifikasi, analisis (pengukuran), dan evaluasi serta pemantauan risiko TI;			
	b) Bersama dengan SKTI dan satuan kerja pengguna TI, memastikan bahwa pelaksanaan dari kebijakan dan prosedur manajemen risiko TI tersebut telah dilakukan secara memadai, serta atas setiap aktivitas bisnis Perusahaan yang terkait dengan penggunaan TI.			
6.	Apakah wewenang dan tanggung jawab Pimpinan Satuan Kerja Pengguna TI sudah mencakup hal-hal sebagai berikut :			
	a) Memastikan adanya proses komunikasi berkelanjutan kepada SKTI mengenai kebutuhan TSI terkait strategi bisnis Perusahaan;			
	b) Menetapkan kebutuhan sistem informasi manajemen dan mengkomunikasikannya ke SKTI;			

PENGENDALIAN INTERN		Ya	Tdk	Keterangan
7.	Apakah kebijakan dan prosedur manajemen SDM TI sudah mencakup hal-hal sebagai berikut :			
a)	Prosedur penerimaan pegawai baru, mutasi dan promosi, serta pemberhentian petugas TSI, yang berlaku untuk pegawai Perusahaan, konsultan, pegawai honorer dan pegawai pihak penyedia jasa, dimana untuk fungsi yang sensitif dalam pengelolaan TSI diperlukan penelitian latar belakang calon pegawai dalam proses penerimaan;			
b)	Penetapan tugas dan tanggung jawab secara jelas, dengan memperhatikan kelayakan pemisahan tugas dan tanggungjawab;			
c)	Penetapan target kinerja secara terstruktur dan transparan;			

Contoh

Lampiran-2: Uji Kendali Manajemen SDM TI

PENGENDALIAN INTERN	Ya	Belum	BUKTI
MANAJEMEN SDM TI			
1. Apakah rekrutmen SDM TI telah dilaksanakan melalui tahapan :			
a) Inventarisasi kondisi SDM TI yang ada dan identifikasi kebutuhan SDM TI, serta penetapan standar kompetensi atau kemampuan dan keahlian yang harus dimiliki oleh SDM TI dan calon SDM TI yang akan direkrut.			
a) Pembahasan dalam Rapat Komite Pengarah TI untuk memastikan kesesuaian rencana kebutuhan SDM TI dengan Rencana Strategis TI, untuk kemudian disetujui oleh Direksi sebagai bagian dari Rencana Tahunan Perusahaan.			
a) Seleksi calon SDM TI harus dilaksanakan berdasarkan faktor penilaian minimal sebagai berikut : 1. Pendidikan formal dan non-formal dievaluasi melalui tes tertulis; 2. Keahlian dan pengalaman dievaluasi melalui tes wawancara; 3. Karakteristik dievaluasi melalui psikotes, tes kesehatan, dan penelitian latar belakang calon SDM TI;			
2. Apakah penugasan SDM TI telah dilaksanakan oleh Pimpinan SKTI secara tertulis dan ditandatangani oleh SDM TI yang bersangkutan, dengan menyepakati hal-hal sebagai berikut :			
• Nama pegawai dan jabatan;			
• Fungsi dan tugas pokok;			
• Tanggungjawab dan wewenang;			
• Indikator kinerja;			
• Skema insentif;			
• Standar kompetensi;			

Lampiran-3: Uji Terinci Organisasi TI

Peranan	Dewan Komisaris	Dewan Direksi	Komite Pengarah TI	Pimpinan Satuan Kerja TI	Pimpinan Satuan Kerja MR	Information Security Officer	Pimpinan Satuan Kerja Pengguna
Perencanaan							
Pengembangan							
Operasional							
Monitoring							
atau							
COBIT PO1-PO10							
COBIT AI1-AI7							
COBIT DS1-DS13							
COBIT ME1-ME4							

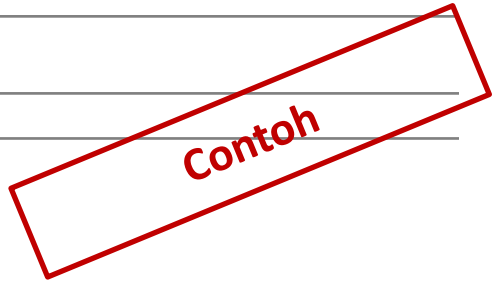
Contoh

Contoh-2: Audit Atas Pusat Data TI

PROGRAM AUDIT INTERN TEKNOLOGI INFORMASI		
TUJUAN PROGRAM AUDIT	Evaluasi atas manajemen Pusat Data TI untuk memastikan pengelolaan yang efektif atas proses pemrosesan data dan pemeliharaan yang memadai atas perangkat yang terkait, termasuk penetapan jadwal pemrosesan, perlindungan atas informasi yang sensitif, pengawasan atas kinerja infrastruktur, dan pelaksanaan pemeliharaan prefentif atas perangkat keras.	
LINGKUP PROGRAM AUDIT	Manajemen Pusat Data : Operasional Pusat Data, Manajemen Kapasitas Pusat Data, Pengamanan Fisik & Lingkungan Pusat Data	
PENGENDALIAN	**PROSEDUR AUDIT**	**REFERENSI**
	PEMAHAMAN	
Manajemen Pusat Data	1. Pahami kebijakan dan prosedur Manajemen Pusat Data;	
	1. Lakukan observasi ke Pusat Data;	
	1. Dapatkan daftar perangkat dan aplikasi serta personil di Pusat Data;	
	EVALUASI KENDALI	
Manajemen Pusat Data	1. Evaluasi kecukupan disain kebijakan dan prosedur Manajemen Pusat Data sesuai ketentuan yang berlaku;	Lampiran 1
	UJI KENDALI	
Manajemen Pusat Data	1. Uji apakah pelaksanaan Manajemen Pusat Data telah sesuai dengan kebijakan dan prosedur yang berlaku;	Lampiran 2
	UJI TERINCI	
Manajemen Pusat Data	• Identifikasi apakah terdapat pelaksanaan Manajamen Pusat Data TI yang tidak sesuai dengan kebijakan dan prosedur yang berlaku;	
	• Identifikasi apakah terdapat perangkat dan aplikasiyang tidak terdaftar berada di Pusat Data TI;	
	• Identifikasi apakah terdapat personil yang tidak berhak berada di Pusat Data TI;	
	• Identifikasi apakah terdapat aktifitas yang tidak sesuai dengan jadwal aktifitas di Pusat Data TI;	
	• Identifikasi apakah terdapat aktifitas di Pusat Data yang sudah dijadwalkan namun tidak dilakukan;	
	• Identifikasi apakah terdapat indikasi tidak memadainya kapasitas sumber daya TI di Pusat Data;	

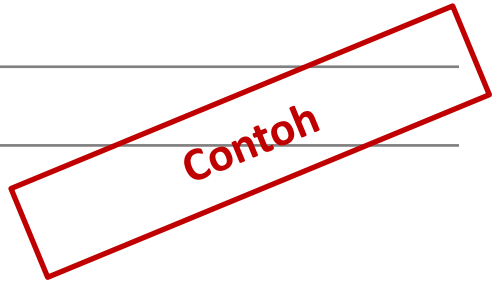
Lampiran-1: Evaluasi Kendali Pusat Data TI

KUESIONER EVALUASI PENGENDALIAN INTERN			
PENGENDALIAN INTERN	**Ya**	**Tdk**	**Keterangan**
1. Apakah kebijakan dan prosedur Manajemen Pusat Data TI sudah mencakup hal-hal sebagai berikut :			
a) SKTI harus menerapkan berbagai kendali yang terkait dengan dengan operasional Pusat Data TI, yang minimal mencakup :			
• Penjadwalan Tugas, dimana SKTI wajib memiliki dan melaksanakan jadwal semua tugas yang harus dijalankan di Pusat Data operasional TI dengan efektif dan aman dari perubahan yang tidak sah;			
• Pengoperasian Proses atas Data, dimana pemberian akses command line kepada operator TI harus dibatasi sesuai kewenangan pada fungsi pengoperasian tugas yang telah ditentukan;			
• Pendistribusian Laporan/Output, dimana hasil informasi yang diproduksi oleh sistem (output), dalam bentuk softcopy atau hardcopy, yang dapat merupakan informasi yang sensitif atau rahasia, sehingga SKTI harus menetapkan informasi apa yang akan diproduksi dan pendistribusian output baik secara fisik maupun logik, serta pemusnahan output yang sudah tidak diperlukan lagi, untuk menghindari terbukanya informasi yang bersifat rahasia dan meningkatnya biaya akibat adanya output yang tidak diperlukan, dan untuk dapat memastikan keamanan output;			
• Proses Backup, baik on-site maupun off-site, termasuk restore, download dan upload untuk data/database;			
• Pengaktifan jejak audit (Audit Trail);			
b) SKTI harus melaksanakan pengelolaan kapasitas Pusat Data dengan memadai untuk dapat memastikan bahwa perangkat keras dan perangkat lunak yang digunakan Perusahaan telah sesuai dengan kebutuhan operasional bisnis dan mengantisipasi perkembangan usaha Perusahaan.			



Lampiran-1: Evaluasi Kendali Pusat Data TI

KUESIONER EVALUASI PENGENDALIAN INTERN			
PENGENDALIAN INTERN	**Ya**	**Tdk**	**Keterangan**
a) SKTSI harus mengembangkan dan mengimplementasikan pengendalian akses fisik ke Pusat Data, yang minimal mencakup :			
• Akses fisik ke Pusat Data harus dibatasi dan dikendalikan dengan baik;			
• Pintu Pusat Data harus selalu terkunci, dilengkapi dengan kartu akses dan atau biometric device;			
• Ruang Pusat Data tidak boleh diberi label atau papan petunjuk sehingga orang mudah mengenalinya;			
• Harus terdapat buku catatan untuk mencatat tamu yang memasuki Pusat Data.			
a) SKTSI harus menghindari terjadinya lingkungan pemrosesan TSI yang tidak sesuai standar dapat menimbulkan gangguan pada operasi TSI, dan untuk itu SKTSI harus mengimplementasikan pengendalian lingkungan atas Pusat Data, yang minimal mencakup :			
• Mengawasi dan memantau faktor lingkungan data center, antara lain mencakup: sumber listrik, api, air, suhu, dan kelembaban udara.			
• Pendeteksi asap/api/panas dan sistem pemadaman api			
• Pengaturan suhu dan kelembaban udara (AC, termometer, dan hidrometer);			
• Lantai yang ditinggikan (raised floor), langit-langit ruangan yang diperkuat, penggunaan bahan ruangan tahan api;			
• Memastikan tersedianya sumber listrik yang cukup, stabil, dan tersedianya sumber alternatif untuk mengantisipasi tidak berfungsinya sumber listrik utama, dengan menggunakan UPS (Uninterruptible Power Supply) dan generator listrik;			



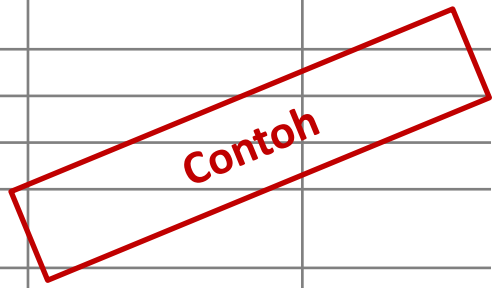
Lampiran-2: Uji Kendali Pusat Data

KERTAS KERJA PENGUJIAN PENGENDALIAN INTERN			
PENGENDALIAN INTERN	**Pusat Data Utama**	**Pusat Data Cadangan**	**Keterangan**
1. Operasional Pusat Data			
• Penjadwalan Tugas;			
• Pengoperasian Proses atas Data;			
• Pendistribusian Laporan/Output;			
• Proses Backup & Restore;			
• Pengaktifan Audit Trail;			
2. Manajemen Kapasitas Pusat Data			
• Inventarisasi dan Pemantauan kapasitas Pusat Data;			
• Laporan Manajemen kapasitas Pusat Data;			

Contoh

Lampiran-2: Uji Kendali Pusat Data

KERTAS KERJA PENGUJIAN PENGENDALIAN INTERN			
PENGENDALIAN INTERN	**Pusat Data Utama**	**Pusat Data Cadangan**	**Keterangan**
1. Pengendalian Akses Fisik Pusat Data			
• Akses fisik ke Pusat Data harus dibatasi dan dikendalikan dengan baik;			
• Pintu harus selalu terkunci, dilengkapi dengan kartu akses dan atau biometric device;			
• Ruang Pusat Data tidak boleh diberi label atau papan petunjuk;			
• Harus terdapat buku catatan untuk mencatat tamu yang memasuki Pusat Data.			
• Kamera pengawas yang direkam dan dimonitor secara terus menerus;			
2. Pengendalian lingkungan Pusat Data			
• Mengawasi dan memantau faktor lingkungan data center, mencakup: sumber listrik, api, air, suhu, dan kelembaban udara;			
• Pendeteksi asap/api/panas dan sistem pemadaman api;			
• Pengaturan suhu dan kelembaban udara (AC, termometer, dan hidrometer);			
• Lantai yang ditinggikan (raised floor);			
• Langit-langit ruangan yang diperkuat;			
• Penggunaan bahan ruangan tahan api;			
• Sumber listrik yang cukup, stabil, dan sumber alternatif (UPS dan generator listrik);			
• Pengatur voltase listrik dan automatic switching.			



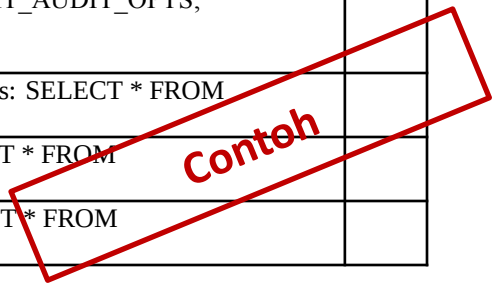
Contoh-3: Audit untuk Pelaksanaan RSTI

Tujuan Audit:
Mengevaluasi tingkat pelaksanaan Rencana Strategis TI yang telah ditetapkan

Item	Program Audit	Narasumber	Evaluasi Kendali	Pengujian Kendali	Evidence	Ref Item Audit
Pemanfaatan ECMS untuk Document Management System	1. Apakah aplikasi sudah operasional?	- IT - User				RSTI 5.3
	2. Apakah training/sosialisasi kepada pengguna sudah dilaksanakan?	- IT - User				
	3. Siapa sajakah pengguna aplikasi siapa tersebut?	IT				
	4. Apakah dukungan operasional (complaint, isu, request) sudah ada?	- IT - User				
	5. Tingkat penggunaan aplikasi (jarang, sering atau sangat dibutuhkan)? Berapa banyak dokumen yang sudah dihasilkan dan dikelola oleh sistem?	- IT - User				

Contoh-4: Oracle Database Audit

1. Patch Management	
1.1 Security patches are applied in a timely manner.	
• Determine if the database version is current and supported by reviewing the result of the following query and comparing the version to current versions supported by Oracle: • SELECT * FROM V$VERSION;	
• Discuss with the database and system administrators the process for reviewing and applying database, application and operating system patches.	
• Verify the number of database instances installed by obtaining the init<SID>.ora files under the $ORACLE_HOME directory.	
• Determine how DBAs monitor and are notified of new patches.	
• Review change control procedures to ensure that all database updates and patches are adequately tested before being applied to production environments.	
2. Security Monitoring	
2.1 Processes are in place to regularly monitor security on the system.	
• Discuss with the DBAs their processes for monitoring key database functions and security-related events to determine if system activity is regularly monitored. Obtain from the DBAs any reports or queries that are used to monitor the system.	
• Discuss with the DBAs the level of auditing that is performed on users' actions. Review the setting for the AUDIT_TRAIL parameter in the init<SID>.ora file to determine if auditing is enabled.	
• Review the retention policy on audit trails and logs.	
• Discuss with the DBAs procedures for monitoring sensitive accounts and privileges. Review the output of the following query to determine if updates made by the DBAs' account are monitored: SELECT * FROM SYS.DBA_STMT_AUDIT_OPTS;	
• Review the output of the following query to determine auditing in place for all system-level privileges: SELECT * FROM DBA_PRIV_AUDIT_OPTS;	
• Review the output of the following query to determine if statement-level auditing is enabled: SELECT * FROM DBA_STMT_AUDIT_OPTS;	
• Review the output of the following query to determine auditing in place for database objects: SELECT * FROM DBA_OBJ_AUDIT_OPTS;	



Contoh-5: Audit Microsoft Exchange Server 2010

1. Document the Configuration

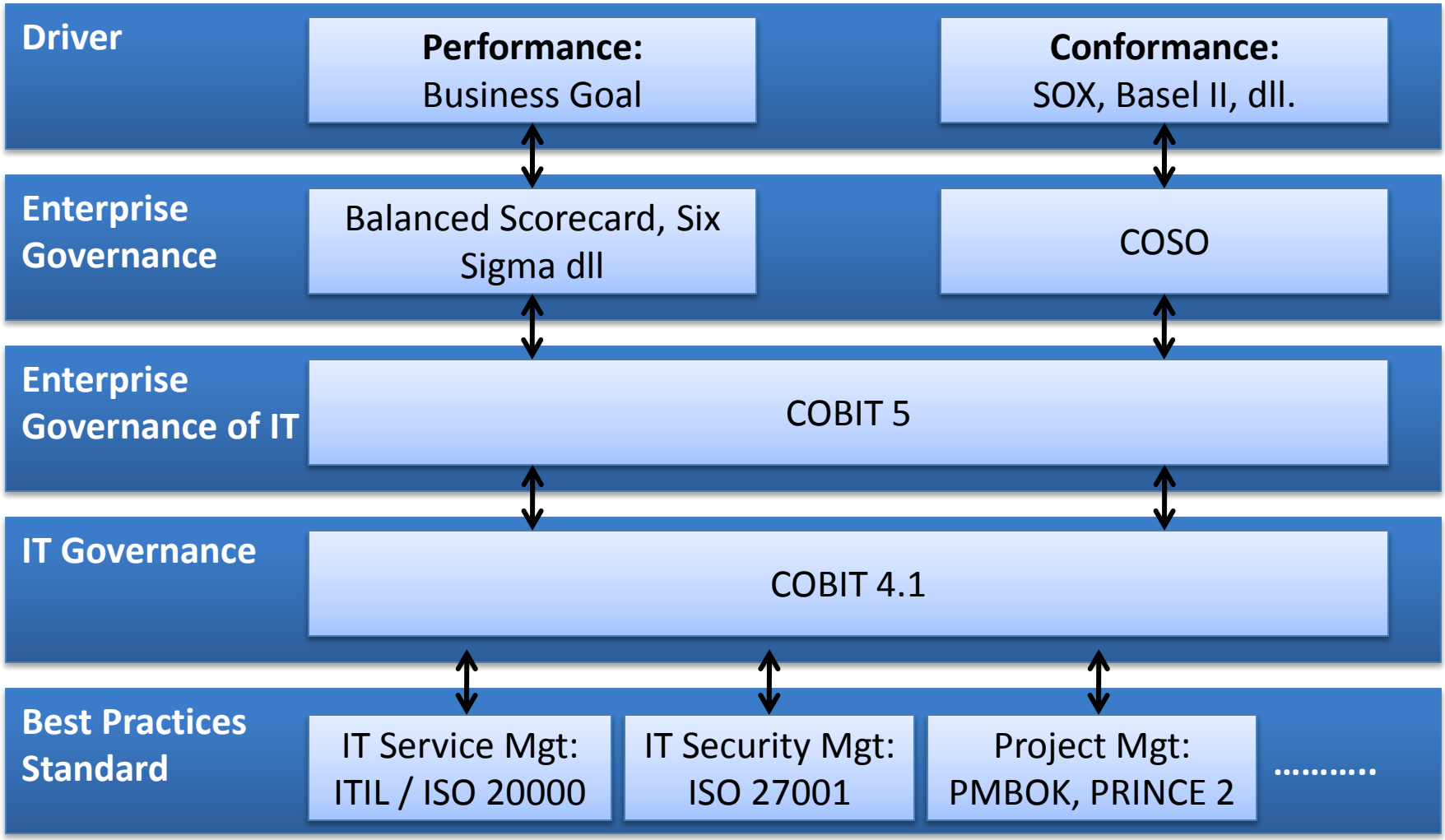
1. Use Exchange Management Console (EMC) to determine:

- Organization configuration – applies organization-wide to all Exchange servers
- Server configuration – details of specific servers, i.e., chosen for audit/review
- Service Pack level installed – compare to latest service pack at *www.microsoft.com/exchange/*
- Number and locations of all mounted Mailbox databases
- Installed Exchange Server roles, i.e., Client Access Server, Mailbox Server, Edge Transport Server, Hub Transport Server, Unified Messaging server (see schematic diagram in VIII. Exchange Server 2010 – server roles)
- Database Availability Groups – these groups drive database replication, failover and recovery
- Installed X.509 Digital Certificates – these drive e-mail encryption as well as secure Federated Sharing with third parties (if Federation is deployed)
- Outlook Anywhere – allows remote users (e.g., teleworkers or mobile devices) to access e-mail boxes securely over Secure Hypertext Transfer Protocol (HTTPS)

- If necessary, run the **Get-ExchangeServer** cmdlet in Exchange Management Shell (EMS) to display a list of installed Exchange Server 2010 server roles on the specified server. See *http://technet.microsoft.com/en-us/library/bb123873.aspx* for details of this cmdlet.
- Ensure that the edge Transport Server does not share hardware with any other Exchange Server 2010 server role (even running in separate virtual machines in a virtualized environment is discouraged).
- If this is a recent deployment of Exchange Server 2010, request the relevant Setup Log created during the installation and review for any unresolved warning or error messages. The Setup Log is located at **<*system drive*>\ExchangeSetupLogs\ExchangeSetup.log** (where **<*system drive*>** is the root directory of the drive where the OS is installed.)

Framework & Standards

Lautan Framework



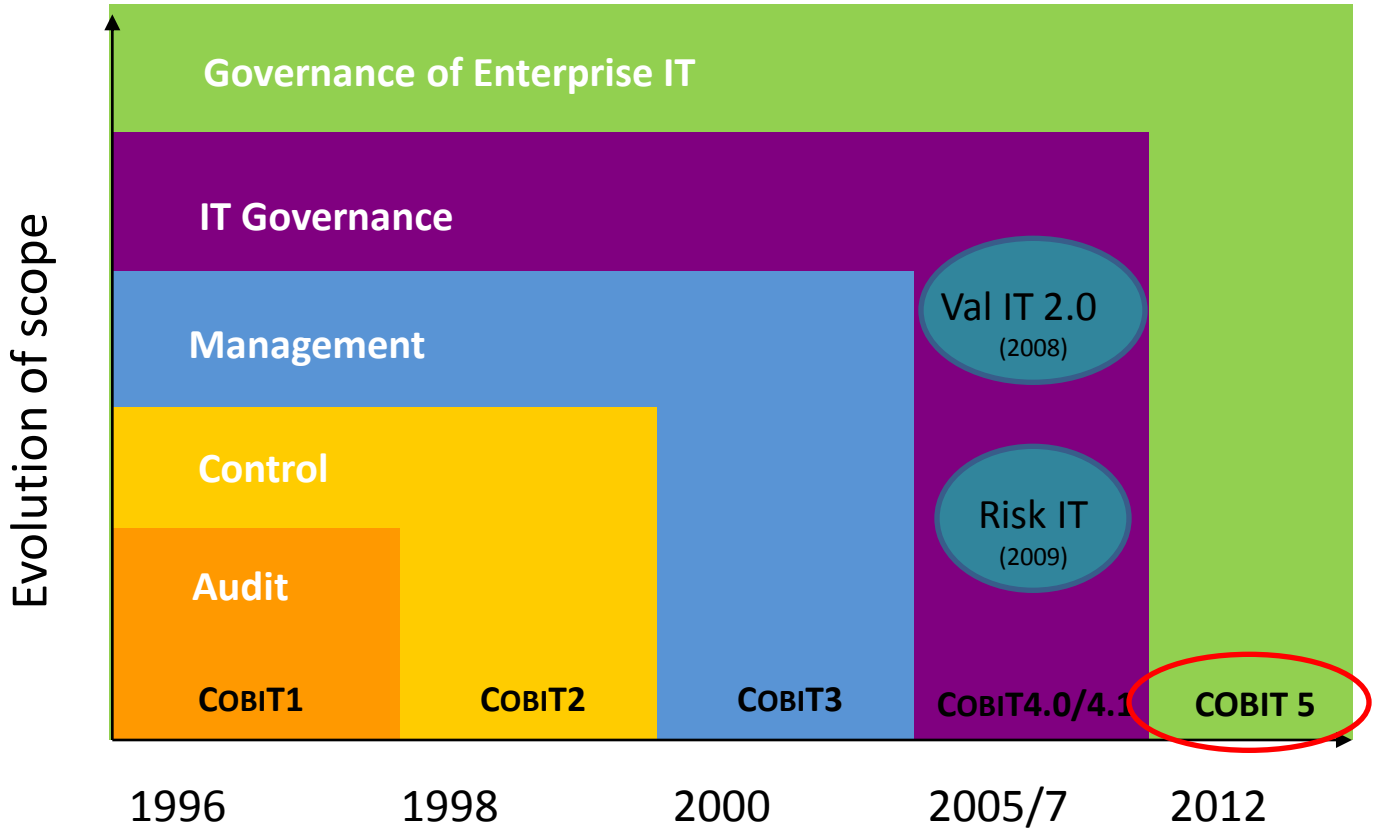
COBIT itu sebenarnya framework apa?

- **IT audit and control framework?**
  - COBIT (1996) and COBIT 2nd Edition (1998)
  - Fokus pada Control Objectives
- **IT management framework?**
  - COBIT 3rd Edition (2000)
  - Ada tambahan Management Guidelines
- **IT governance framework?**
  - COBIT 4.0 (2005) and COBIT 4.1 (2007)
  - Ditambahkan proses Governance dan compliance
  - Proses Audit/Assurance dihilangkan

Lalu apa bedanya antara **governance** dan **management**?

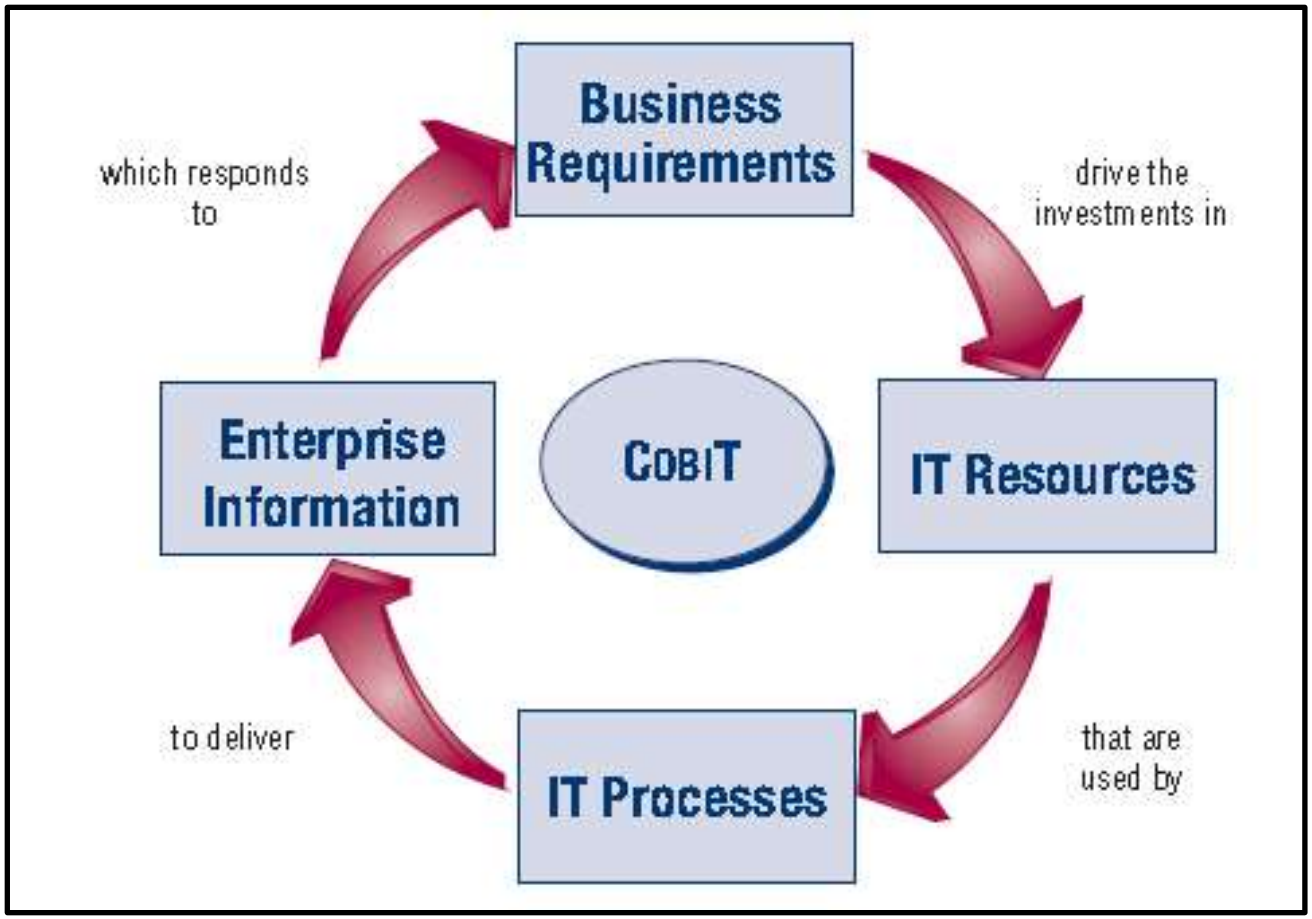
COBIT 5: Now One Complete Business Framework

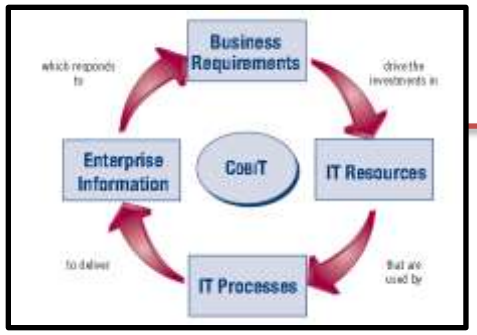
Information Systems Audit and Control Association®



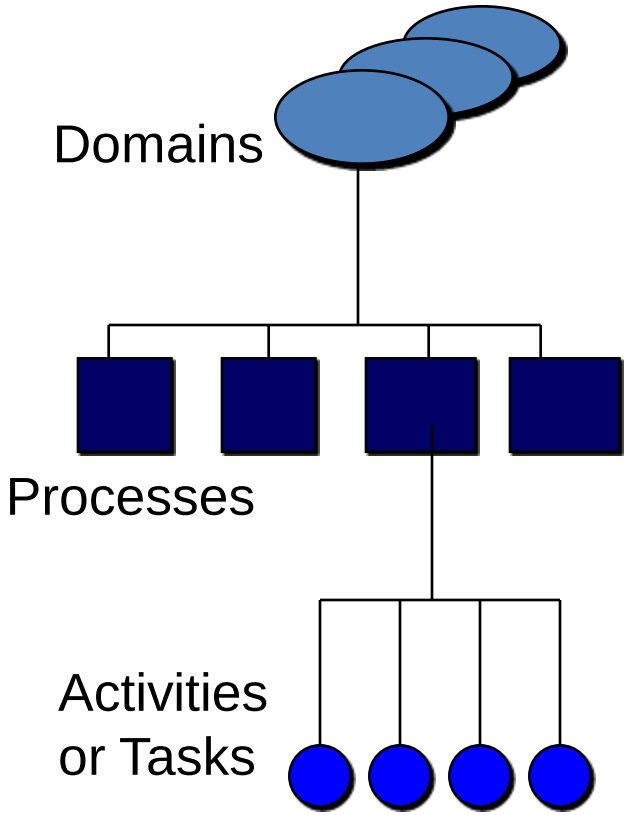
COBIT 4.1

CobiT 4.1 Basic Principle





Process Orientation



Pengelompokan proses, sering bersesuaian juga dengan domain tanggung-jawab organisasi.

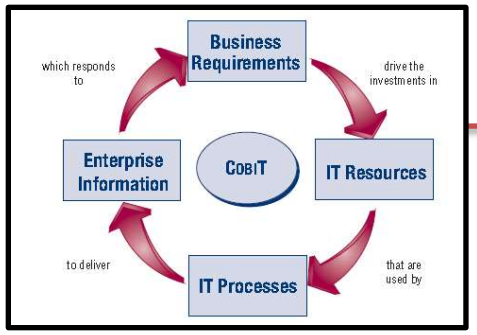
Contoh: Plan & Organize, Acquire & Implement, Deliver & Support, Monitor & Evaluate

Kelompok aktifitas-aktifitas sejenis

Contoh: Incident Management, Problem Management, IT Strategy Plan, Change Management, dst.

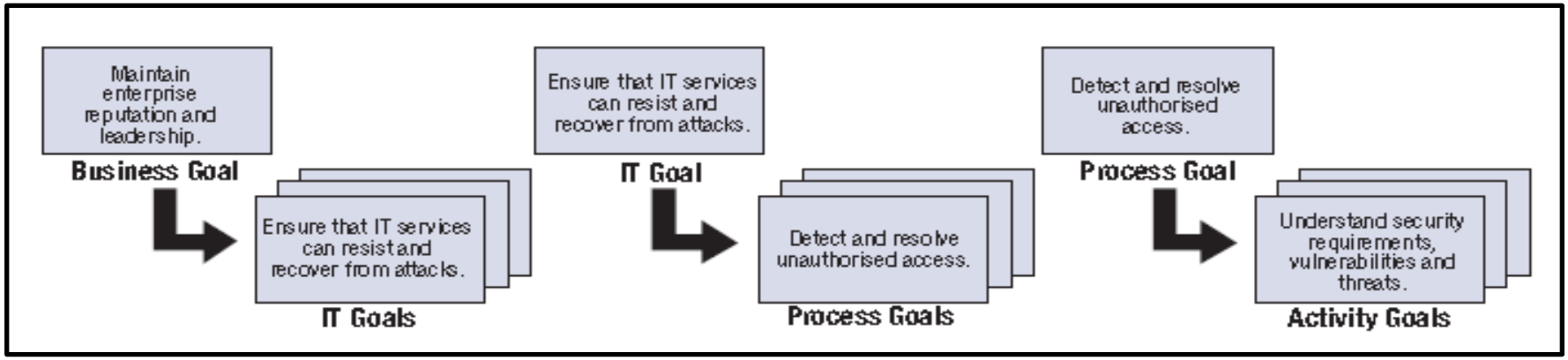
Aksi-aksi yang dibutuhkan untuk mencapai sebuah hasil terukur

Contoh: record new problem, propose solution, analisis, monitor solution, dst.

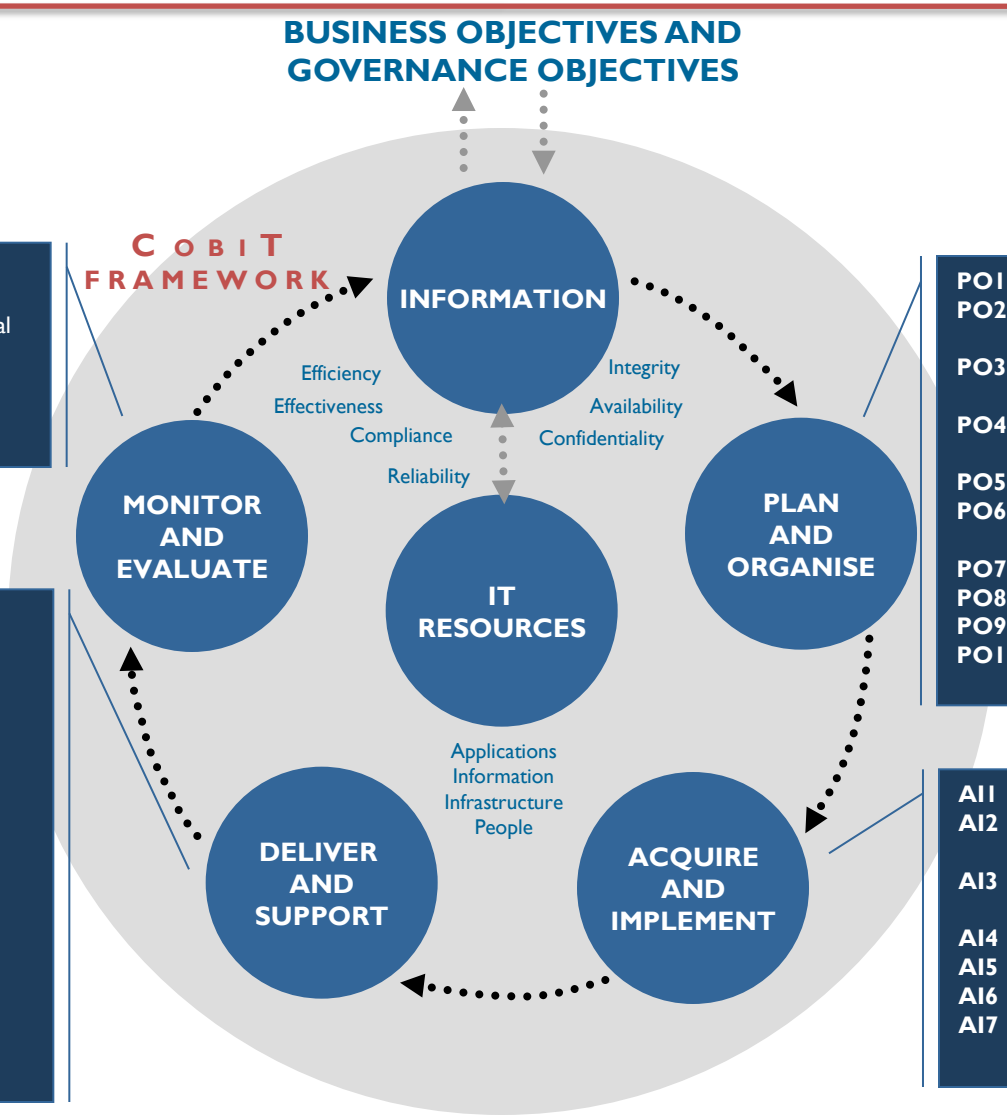


Business-IT Aligment in CobiT 4.1

Business Goal → IT Goal → Process Goal → Activity Goal



The COBIT 4.1 Framework



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

Control dan IT Control Objective

Information Systems Audit and Control Association®

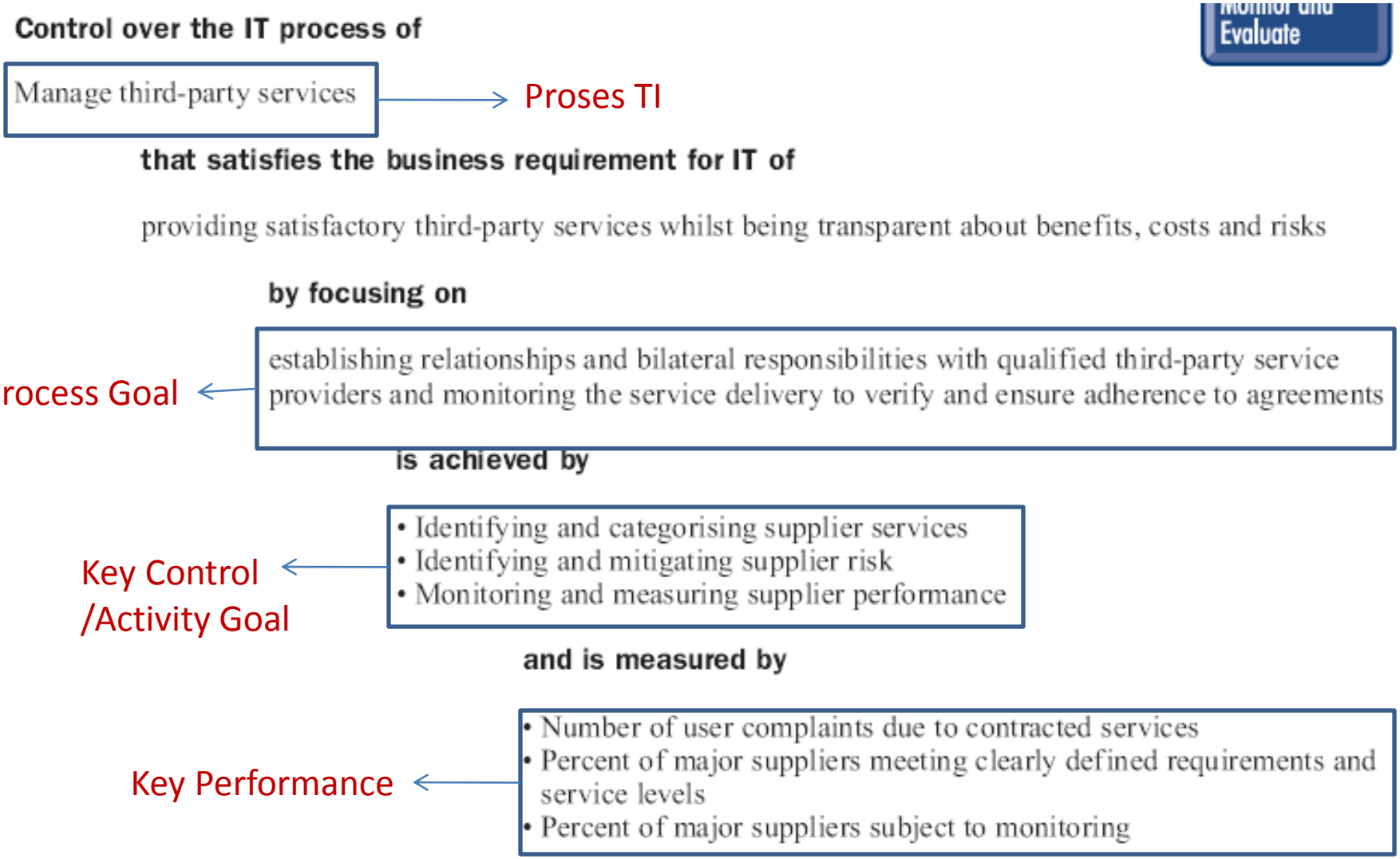
Definisi kontrol

"Kebijakan, Prosedur, Praktik-praktik dan struktur organisasi yang dirancang untuk memberikan kepastian yang memadaii serta kejadian yang tidak diinginkan akan dapat dicegah, dideteksi atau diperbaiki.

Definisi IT Control Objective

Pernyataan atas hasil yang diharapkan atau tujuan yang akan dituju dengan menerapkan kontrol pada suatu aktifitas TI tertentu.

Contoh: DS2 Waterfall



Contoh: DS2 Management Guidelines

DS2 Manage Third-party Services

From	Inputs
PO1	IT sourcing strategy
PO8	Acquisition standards
AI5	Contractual arrangements, third-party relationship management requirements
DS1	SLAs, contract review report
DS4	Disaster service requirements, including roles and responsibilities

Outputs	To
Process performance reports	ME1
Supplier catalogue	AI5
Supplier risks	PO9

Hasil dari Proses ini menjadi input untuk proses mana?

Dari mana saja Input Proses ini?

RACI Chart

Functions

Aktifitas apa yang terdapat dalam proses ini? Siapa yang bertanggung-jawab?

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Identify and categorise third-party service relationships.				I	C	R	C	R	A/R	C	C
Define and document supplier management processes.		C		A	I	R	I	R	R	C	C
Establish supplier evaluation and selection policies and procedures.		C		A	C	C		C	R	C	C
Identify, assess and mitigate supplier risks.		I		A		R		R	R	C	C
Monitor supplier service delivery.				R	A	R		R	R	C	C
Evaluate long-term goals of the service relationship for all stakeholders.	C	C	C	A/R	C	C	C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Control Practices

Petunjuk detail untuk setiap Control Objectives?

Contoh: **DS2- Manage Third-party Services**

Control Objectives:

DS2.1 Identification of All Supplier Relationship

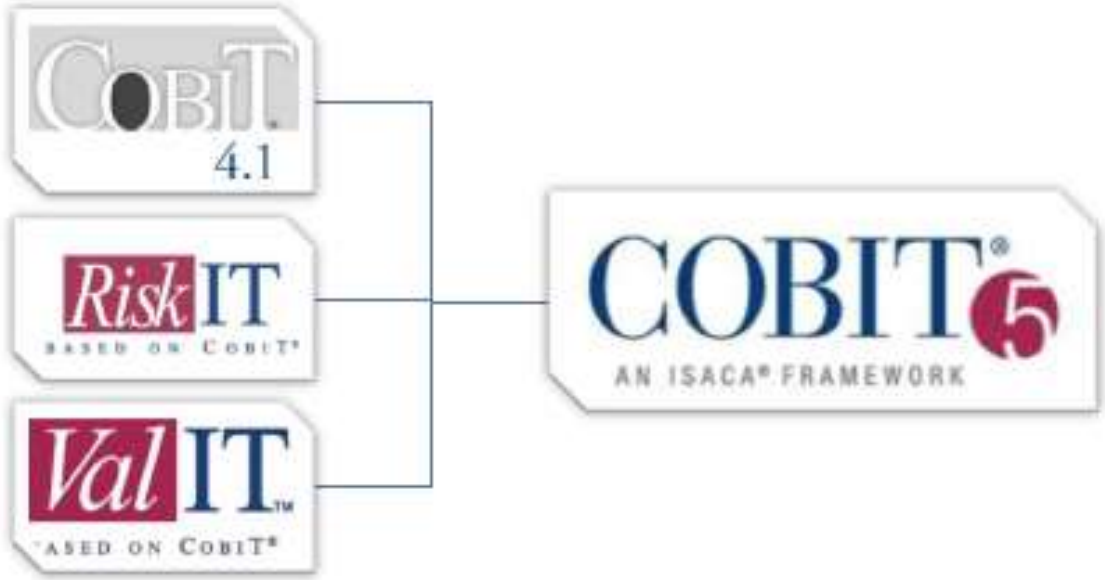
Identify all supplier services, and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.

Control Practices:

1. Define and regularly review criteria to identify and categorise all supplier relationships according to supplier type, significance and criticality of service. The list should include a category describing vendors as preferred, non-preferred or not recommended.
2. Establish and maintain a detailed register of suppliers, including name, scope, purpose of the service, expected deliverables, service objectives and key contact details.

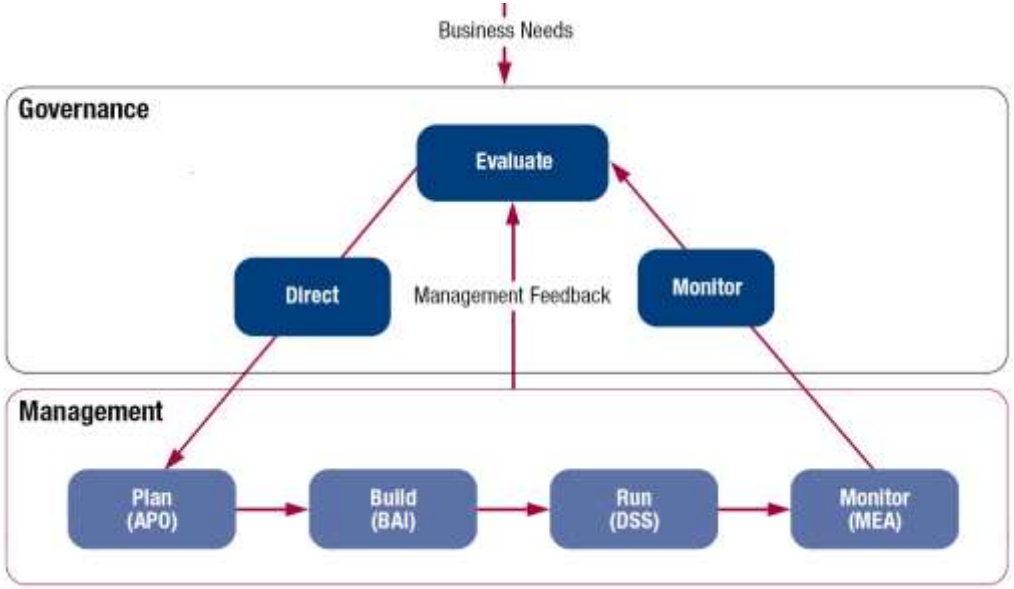
CobiT 5

- CobiT 5 dibangun dari COBIT 4.1 (ditambah Val IT dan Risk IT), sehingga memungkinkan organisasi yang telah menggunakan versi sebelumnya dapat bermigrasi ke CobiT 5
- COBIT 5 menjelaskan proses-proses di tingkatan manajemen dan mengintegrasikan COBIT 4.1 dengan konten dari Val IT dan Risk IT menjasi sebuah model referensi proses.



COBIT 5: The Governance and Management of Enterprise IT Framework

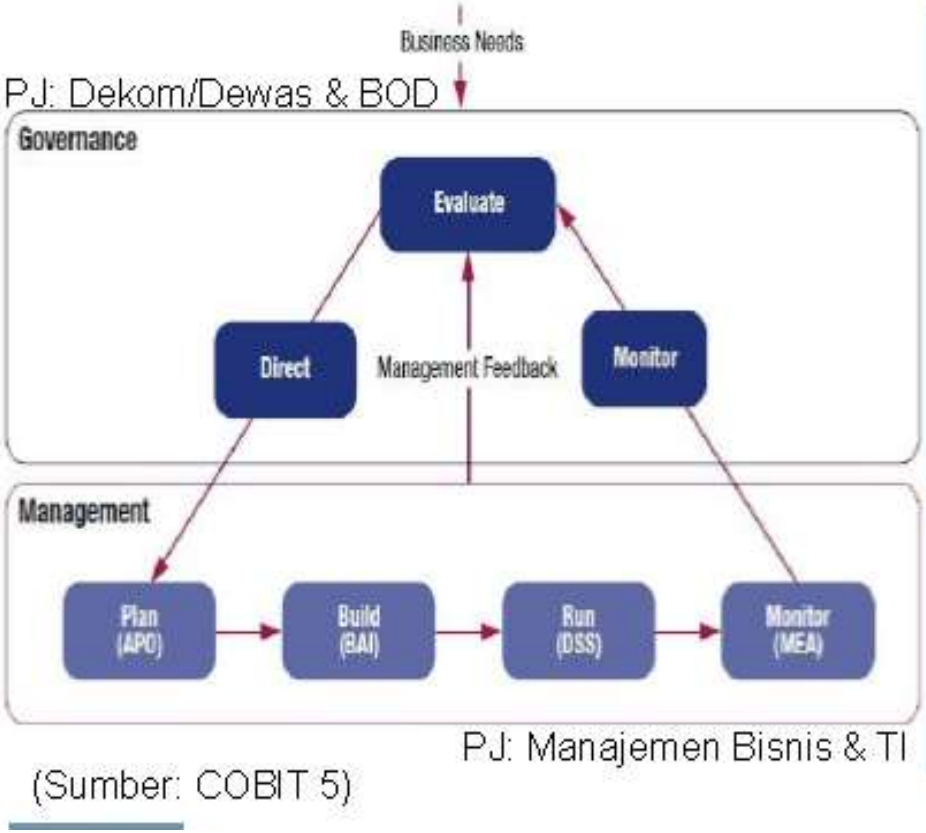
- **Tata Kelola** memastikan bahwa obyektif organisasi tercapai dengan meng-**Evaluasi** kebutuhan stakeholder, kondisi dan opsi-opsinya; menetapkan arahan (**Direction**) melalui prioritasi dan pengambilan keputusan; serta me-**Monitor** kinerja, kepatuhan dan progress atas direksi dan tujuan yang disepakati (**EDM**).



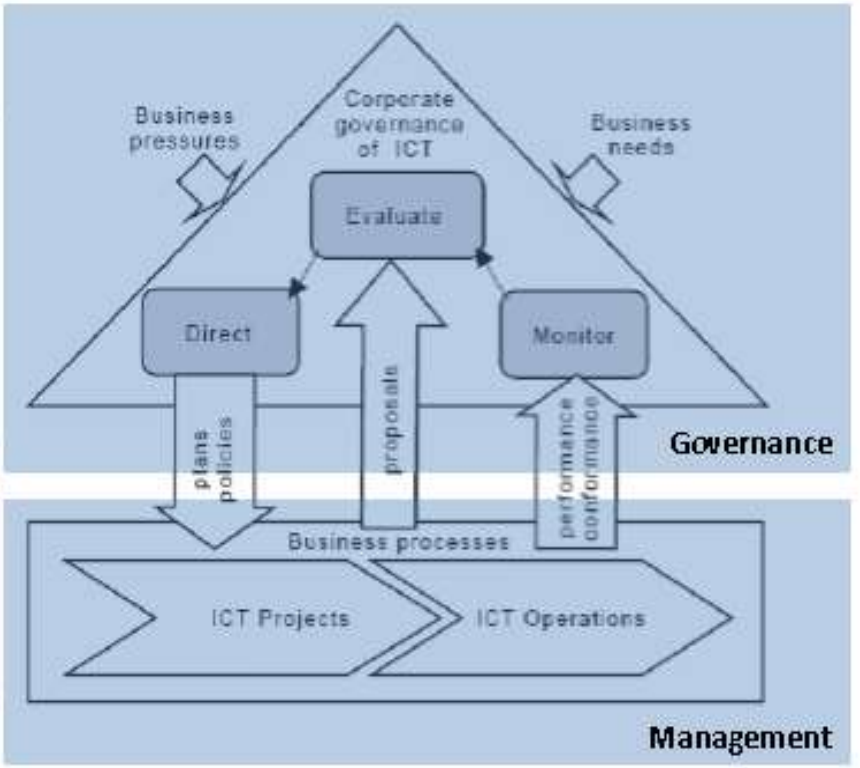
- **Manajemen** merencanakan (**Plans**), membangun (**Builds**), menjalankan (**Runs**) dan me-**Monitor** aktifitas dalam menyelaraskan dengan arahan yang ditetapkan oleh lembaga *governance* untnuk mencapai tujuan organisasi **(PBRM).**

COBIT 5 dan ISO 38500

Walau tidak disebutkan secara eksplisit, pendekatan COBIT 5 mengadopsi pendekatan ISO 38500



(Sumber: COBIT 5)



Sumber: ISO 38500

Stakeholder Value

- Memberikan *value* pada para stakeholders menuntut **tata kelola** dan **manajemen** yang baik atas aset-aset IT.
- Board, eksekutif dan manajemen harus memperlakukan **IT sebagaimana bagian bisnis** lainnya.
- **Tuntutan kepatuhan** legal, regulasi dan perjanjian atas penggunaan IT terus meningkat dan mengancam *value* ini jika dilanggar.
- **COBIT 5: framework komprehensif untuk membantu organisasi meraih tujuannya dan memberikan *value* melalui tata kelola dan manajemen TI organisasi yang efektif.**

The COBIT 5 Framework

CobiT 5 → Membantu organisasi **menciptakan value optimal** dari IT

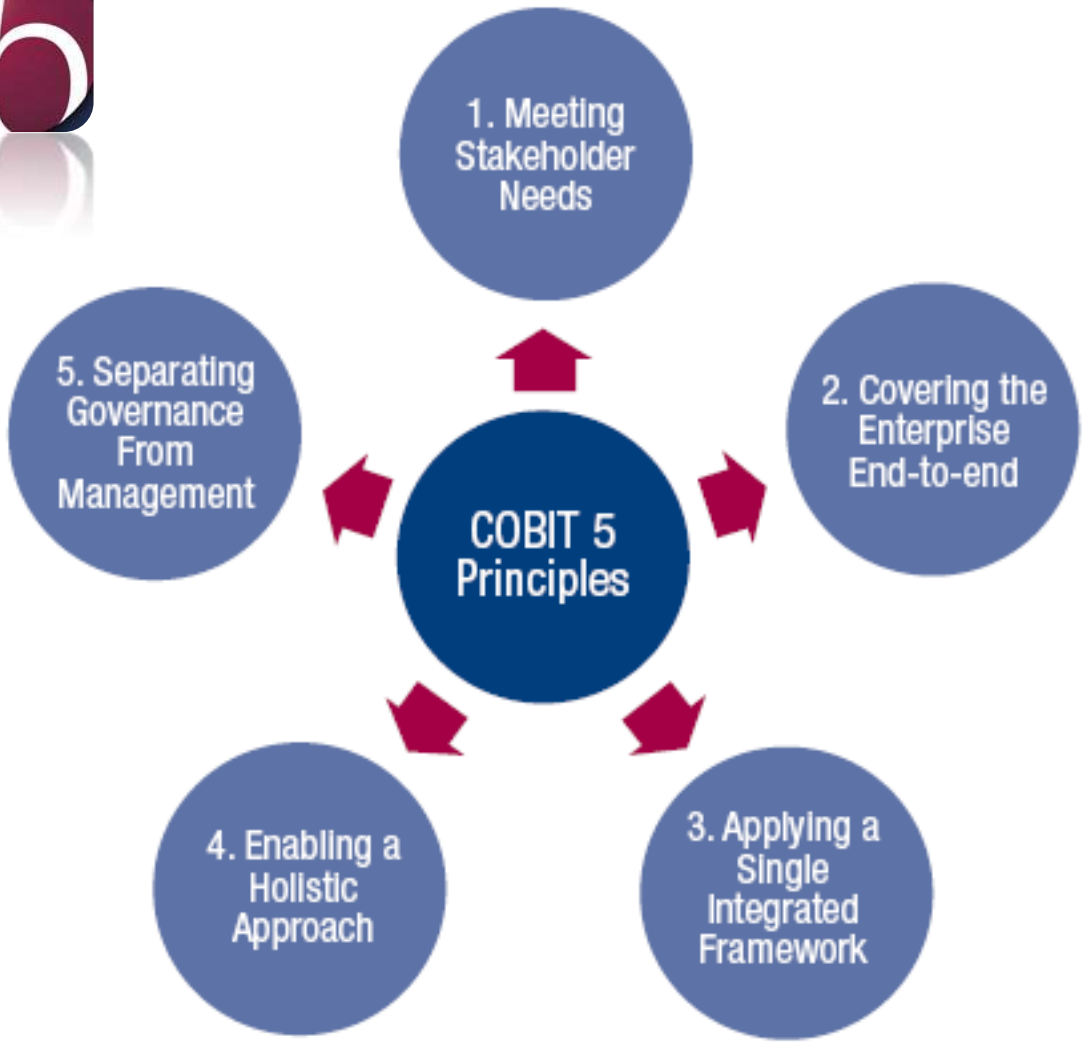
Dengan menjaga keseimbangan antara

- Realisasi manfaat
- Optimasi risiko
- Optimasi Penggunaan resource

CobiT 5 → Memungkinkan **tata kelola** dan **manajemen** dalam konteks organisasi yang holistik terhadap informasi dan teknologi yang terkait

CobiT 5 → Mengandung **prinsip-prinsip** dan **enabler** yang bersifat **generik** dan dapat digunakan **untuk berbagai ukuran organisasi**, baik komersial, non-profit maupun sektor publik.

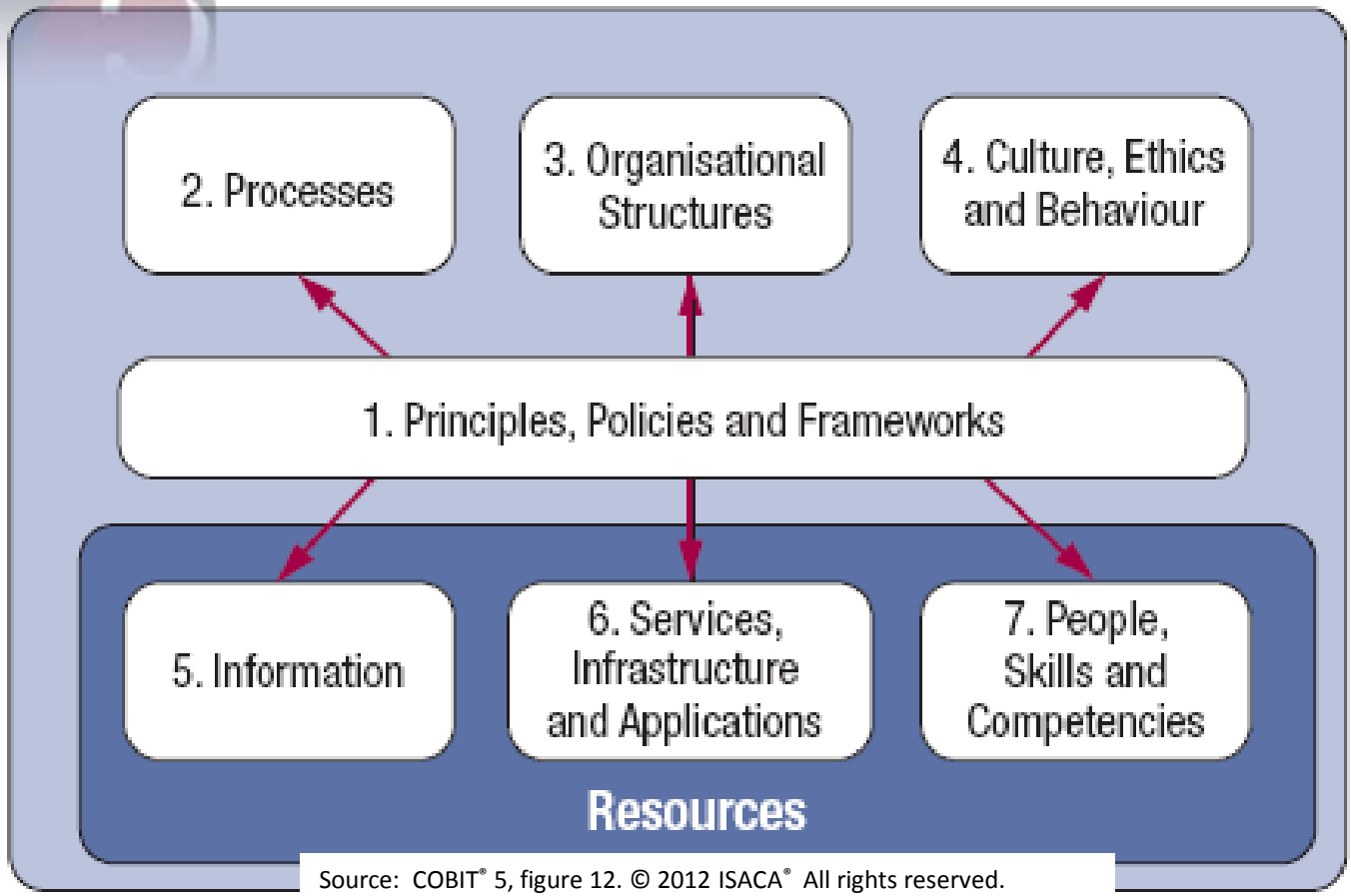
COBIT 5 Principles



Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

COBIT 5 Enablers

Faktor-faktor yang, secara individual dan kolektif, mempengaruhi apakah sesuatu akan berjalan atau tidak dalam tata kelola dan manajemen TI organisasi



Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

Area Perubahan

- Berikut ini adalah perubahan mendasar pada COBIT 5 dan bagaimana dampaknya pada implementasi/peningkatan GEIT:
  1. New GEIT Principles
  2. Increased Focus on Enablers
  3. New Process Reference Model
  4. New and Modified Processes
  5. Practices and Activities
  6. Goals and Metrics
  7. Inputs and Outputs
  8. RACI Charts
  9. Process Capability Maturity Models and Assessments

Regulasi Nasional Terkait

Regulasi Nasional Terkait

GCG:

- Kepmen BUMN No. Kep-117/M-MBU/2002 tentang penerapan praktik GCG di BUMN
- Permen BUMN No. PER-01/MBU/2011 tentang penerapan tata kelola perusahaan yang baik (GCG) pada BUMN

IT Governance:

- Permen Kominfo 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola TIK Nasional
- PBI No 9/15/PBI/2007 tentang Manajemen Risiko TI untuk Bank Umum
- Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik dari Kominfo 2011
- **Permen BUMN PER-02/MBU/2013 tentang Panduan Penyusunan Pengelolaan Tata Kelola TI BUMN**
- Pedoman Tata Kerja SKK Migas Kementerian ESDM KEP-0008/SKO0000/2013/SO tentang Pengelolaan TIK pada Kontraktor Kontrak Kerja Sama (KKKS)

Permen Kominfo No.41/2007:

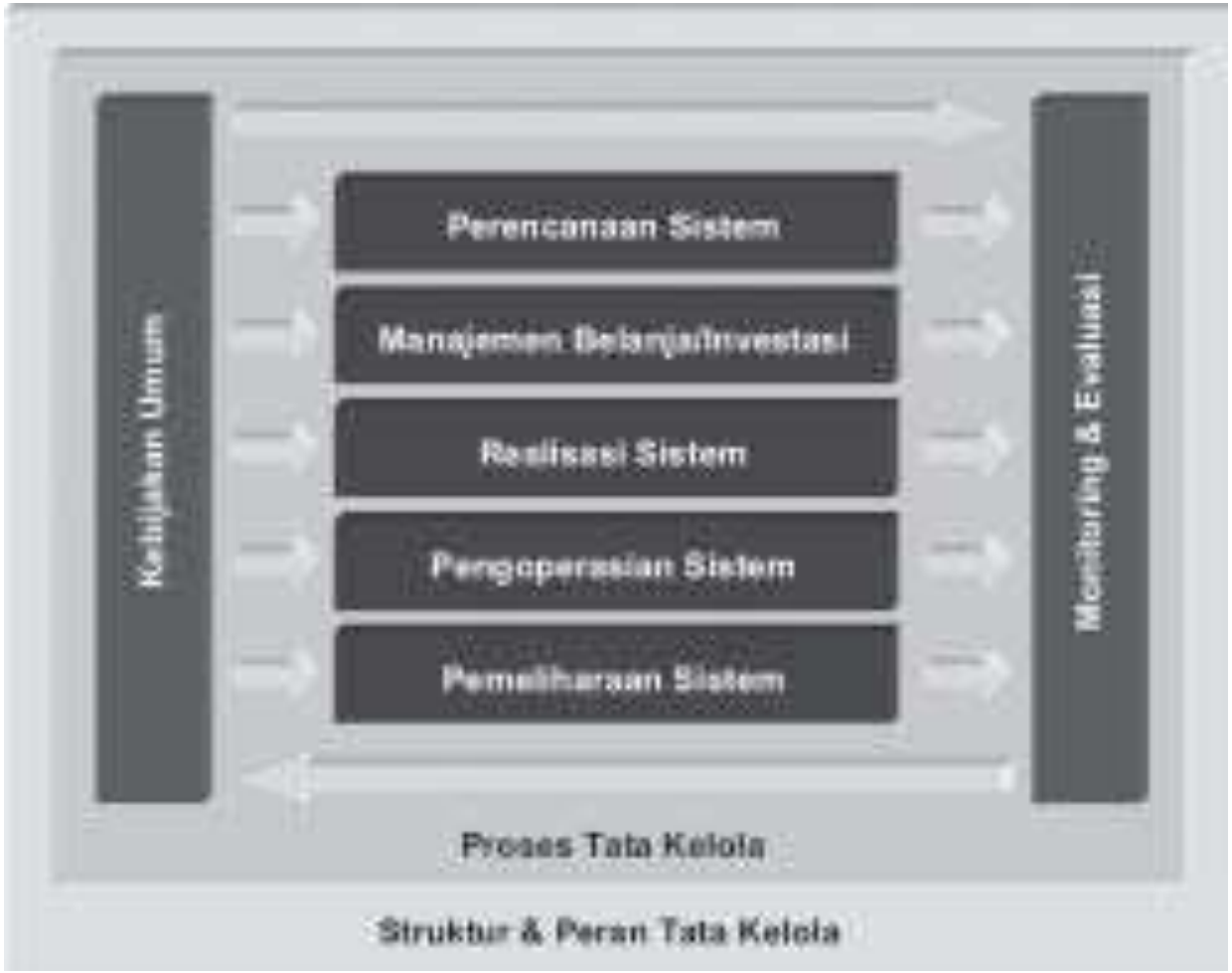
Panduan Umum Tata Kelola TIK Nasional

Prinsip Dasar Tata Kelola TIK Nasional:

- **Prinsip 1** – Perencanaan TIK yang sinergis dan konvergen di level internal institusi dan nasional
- **Prinsip 2** – Penetapan kepemimpinan dan tanggung jawab TIK yang jelas di level internal institusi dan nasional
- **Prinsip 3** – Pengembangan dan/atau akuisi TIK secara valid
- **Prinsip 4** – Memastikan operasi TIK berjalan dengan baik, kapan pun dibutuhkan
- **Prinsip 5** – Memastikan terjadinya perbaikan berkesinambungan (*continuous improvement*) dengan memperhatikan faktor manajemen perubahan organisasi dan sumber daya manusia

Permen Kominfo No.41/2007:

Panduan Umum Tata Kelola TIK Nasional (lanjutan)



Model Tata Kelola TIK Nasional, terdiri atas 2 bagian:

1. Struktur & Peran Tata Kelola
2. Proses Tata Kelola

Kepmen BUMN Kep-117/M-MBU/2002:

Penerapan Praktik GCG pada BUMN

- *Corporate governance* adalah suatu **proses** dan **struktur** yang digunakan oleh organ BUMN untuk **meningkatkan keberhasilan usaha** dan **akuntabilitas perusahaan** guna mewujudkan **nilai pemegang saham** dalam jangka panjang dengan tetap memperhatikan **kepentingan *stakeholder*** lainnya, berlandaskan peraturan perundangan dan nilai-nilai etika.
- Prinsip-prinsip GCG:
  - Transparansi
  - Kemandirian (profesional, tanpa tekanan yang tidak semestinya)
  - Akuntabilitas (kejelasan fungi, peran dan tanggung-jawab)
  - Pertanggung-jawaban (kepatuhan terhadap regulasi)
  - Kewajaran (keadilan dan kesetaraan pemenuhan hak stakeholder)

Permen BUMN Per-01/MBU/2011:

Penerapan GCG pada BUMN

- GCG: prinsip-prinsip yang mendasari suatu **proses** dan **mekanisme** pengelolaan perusahaan **berlandaskan peraturan perundang-undangan** dan **etika berusaha**

Bagian Kedua
Kewajiban BUMN Menerapkan GCG

Pasal 2

(1) BUMN wajib menerapkan GCG secara konsisten dan berkelanjutan dengan berpedoman pada Peraturan Menteri ini dengan tetap memperhatikan ketentuan, dan norma yang berlaku serta anggaran dasar BUMN.

(2) Dalam rangka penerapan GCG sebagaimana dimaksud pada ayat (1), Direksi menyusun GCG manual yang diantaranya dapat memuat *board* manual, manajemen risiko manual, sistem pengendalian intern, sistem pengawasan intern, mekanisme pelaporan atas dugaan penyimpangan pada BUMN yang bersangkutan, tata kelola teknologi informasi, dan pedoman perilaku etika (*code of conduct*).

- Prinsip-Prinsip GCG masih sama dengan Kepmen sebelumnya (Kepmen BUMN Kep-117/M-MBU/2002)

Permen BUMN Per-01/MBU/2011:

Penerapan GCG pada BUMN

Bagian Ketujuh
Sistem Pengendalian Intern (*Internal Control System*)

Pasal 26

(1) Direksi harus menetapkan suatu sistem pengendalian intern yang efektif untuk mengamankan investasi dan aset perusahaan.

(2) Sistem pengendalian intern sebagaimana dimaksud pada ayat (1), antara lain mencakup hal-hal sebagai berikut:

a. Lingkungan pengendalian intern dalam perusahaan yang dilaksanakan dengan disiplin dan terstruktur, yang terdiri dari:
   1) integritas, nilai etika dan kompetensi karyawan;
   2) filosofi dan gaya manajemen;
   3) cara yang ditempuh manajemen dalam melaksanakan kewenangan dan tanggung jawabnya;
   4) pengorganisasian dan pengembangan sumber daya manusia; dan
   5) perhatian dan arahan yang dilakukan oleh Direksi.

b. pengkajian terhadap pengelolaan risiko usaha (*risk assessment*), yaitu suatu proses untuk mengidentifikasi, menganalisis, menilai pengelolaan risiko yang relevan.

c. aktivitas pengendalian, yaitu tindakan-tindakan yang dilakukan dalam suatu proses pengendalian terhadap kegiatan perusahaan pada setiap tingkat dan unit dalam struktur organisasi BUMN, antara lain mengenai kewenangan, otorisasi, verifikasi, rekonsiliasi, penilaian atas prestasi kerja, pembagian tugas, dan keamanan terhadap aset perusahaan.

d. sistem informasi dan komunikasi, yaitu suatu proses penyajian laporan mengenai kegiatan operasional, finansial, serta ketaatan dan kepatuhan terhadap ketentuan peraturan perundang-undangan oleh BUMN.

Permen BUMN Per-01/MBU/2011:

Penerapan GCG pada BUMN

Bagian Kedelapan
Pengawasan Intern

Pasal 28

(1) Direksi wajib menyelenggarakan pengawasan intern.

(2) Pengawasan intern sebagaimana dimaksud pada ayat (1) dilakukan, dengan:

a. membentuk Satuan Pengawasan Intern; dan

b. membuat Piagam Pengawasan Intern.

(3) Satuan Pengawasan Intern sebagaimana dimaksud pada ayat (2) huruf a, dipimpin oleh seorang kepala yang diangkat dan diberhentikan oleh Direktur Utama berdasarkan mekanisme internal perusahaan dengan persetujuan Dewan Komisaris/Dewan Pengawas.

(4) Fungsi pengawasan intern sebagaimana dimaksud pada ayat (1), adalah:

a. Evaluasi atas efektifitas pelaksanaan pengendalian intern, manajemen risiko, dan proses tata kelola perusahaan, sesuai dengan peraturan perundang-undangan dan kebijakan perusahaan;

b. Pemeriksaan dan penilaian atas efisiensi dan efektifitas di bidang keuangan, operasional, sumber daya manusia, teknologi informasi, dan kegiatan lainnya;

(5) Direksi wajib menyampaikan laporan pelaksanaan fungsi pengawasan intern secara periodik kepada Dewan Komisaris/Dewan Pengawas.

(6) Direksi wajib menjaga dan mengevaluasi kualitas fungsi pengawasan intern di perusahaan.

Permen BUMN Per-01/MBU/2011:

Penerapan GCG pada BUMN

Bagian Kesepuluh
Tatakelola Teknologi Informasi

Pasal 30

(1) Direksi dapat menetapkan tatakelola teknologi informasi yang efektif.

(2) Direksi wajib menyampaikan laporan pelaksanaan tata kelola teknologi informasi secara periodik kepada Dewan Komisaris/Dewan Pengawas.

(3) Direksi wajib menjaga dan mengevaluasi kualitas fungsi tatakelola teknologi informasi di perusahaan.

Permen BUMN No. PER-02/MBU/2013

PANDUAN PENYUSUNAN PENGELOLAAN TEKNOLOGI INFORMASI BADAN USAHA MILIK NEGARA

Latar Belakang

- Potensi *value* dari TI sangat besar bagi BUMN jika dikembangkan secara terarah dan terukur
- Bahwa agar terarah, terukur dan sesuai GCG maka pengembangan TI di BUMN perlu:
  - Menerapkan sistem **Tata Kelola TI**
  - Menyusun **Master Plan TI**
  - Dikembangkan secara **bersinergi sesama BUMN**

Tanggung-Jawab Tata Kelola dan Master Plan TI

- Penyusunan dan penetapan Tata Kelola TI adalah tanggung-jawab Direksi (Pasal 2 ayat 2)

> (2) Tata kelola teknologi informasi sebagaimana dimaksud pada ayat (1), disusun dan ditetapkan oleh Direksi dengan mengacu pada Lampiran I Peraturan Menteri ini.

- Berkaitan dengan Master Plan, Direksi bertanggung-jawab untuk:
  - Penyusunan dan penetapan Master Plan TI (Pasal 3 ayat 2)
  - Monitoring keberjalanan Master Plan TI (Pasal 3 ayat 5)
  - Laporan berkala, kaji ulang dan pemeliharaan master plan TI (Ps. 3 ayat 6 & 7)

> (2) Master plan teknologi informasi sebagaimana dimaksud pada ayat (1), disusun dan ditetapkan oleh Direksi dengan mengacu pada Lampiran II Peraturan Menteri ini.

> (5) Direksi wajib melakukan monitoring dan evaluasi pelaksanaan master plan teknologi informasi secara berkala dan setiap tahun untuk mengetahui keberhasilan pencapaian pelaksanaan, hasil, dan tujuan master plan teknologi informasi.
>
> (6) Hasil monitoring dan evaluasi berkala menjadi bagian dari Laporan Manajemen BUMN yang disampaikan kepada RUPS/Menteri setiap triwulan dan hasil evaluasi tahunan.
>
> (7) Direksi dapat melakukan pengkajian ulang dan melakukan perubahan master plan teknologi informasi yang telah ditetapkan apabila diperlukan untuk mengantisipasi perubahan bisnis dan perkembangan teknologi informasi.

Sinergi TI BUMN

- Setiap BUMN mengutamakan sinergi antar BUMN dalam pemanfaatan dan pengembangan teknologi informasi.
- Sinergi antar BUMN sebagaimana dimaksud ayat (1) diutamakan **membawa TKDN (Tingkat Kandungan Dalam Negeri) terbesar**.
- Sinergi teknologi informasi mengacu pada Lampiran III Peraturan Menteri ini.
- Sinergi teknologi informasi dapat dilakukan pada bidang keuangan, pemasaran, produksi, distribusi, penelitian, pengadaan, SDM, dan teknologi informasi.
- Pelaksanaan sinergi teknologi informasi dilakukan berdasarkan azas manfaat yang berlandaskan pada prinsip-prinsip *Good Corporate Governance*

Implementasi Sinergi TI BUMN

Pendekatan Rantai Nilai

- Misalnya: sinergi membangun aplikasi supply chain antara BUMN Pupuk dengan BUMN Perkebunan

Pendekatan Industri

- Misalnya: sinergi membangun aplikasi GIS untuk BUMN Pertambangan atau Perkebunan

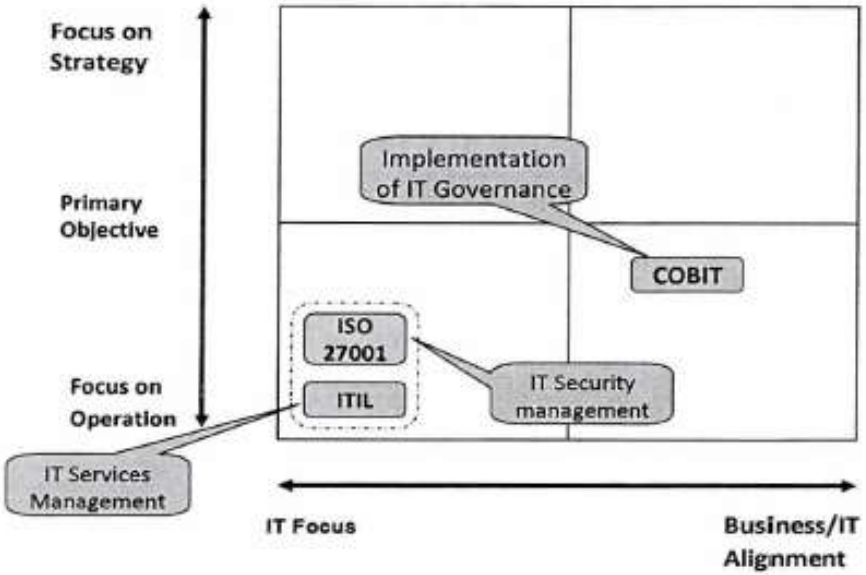
Pendekatan Lintas Sektoral

- Misalnya: sinergi BUMN Telekomunikasi atau IT dengan BUMN lainnya untuk membangun sistem komunikasi atau IT.

Pendekatan Fungsional/Kompetensi

- Misalnya: sinergi BUMN Perbankan dengan BUMN lainnya untuk e-Payment

- Tata kelola TI bagian integral dari Enterprise Governance agar dapat **menjamin pemanfaatan** dari implementasi TI.



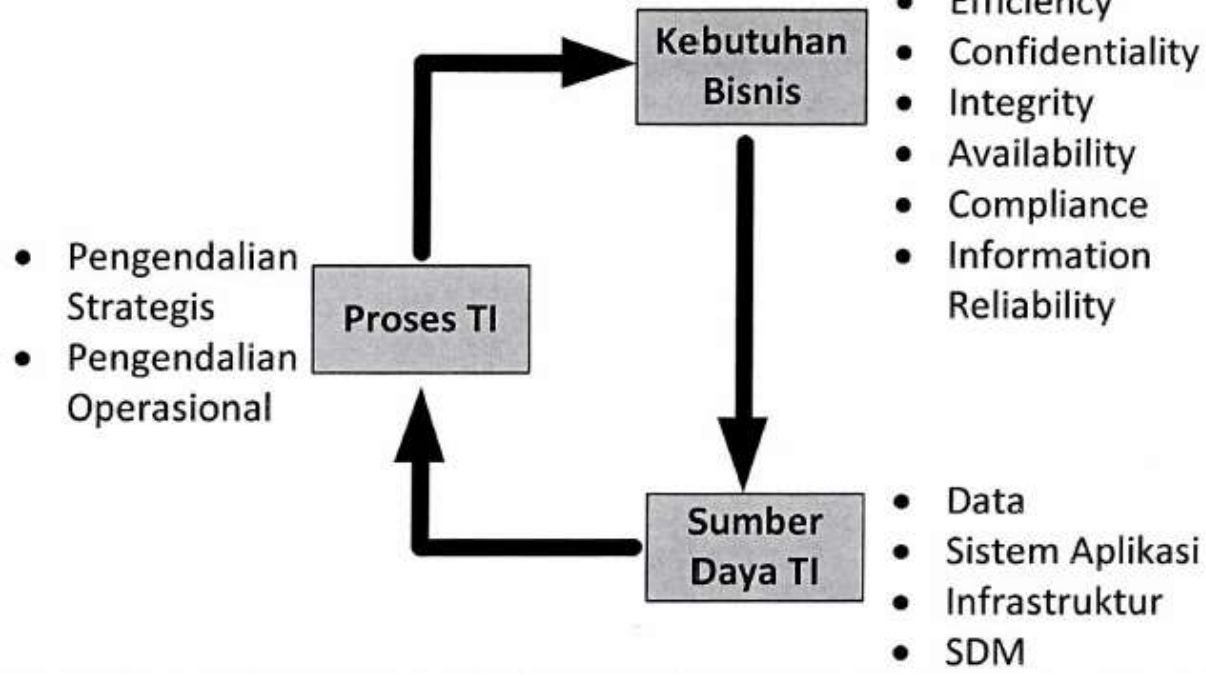
- Penerapan Tata Kelola TI **sangat membutuhkan standard yang sudah diterima secara luas dan teruji**.
- Standard yang disebutkan dalam Permen ini:
  - CobiT
  - ITIL
  - ISO 27001
  - TOGAF
  - PMBOK

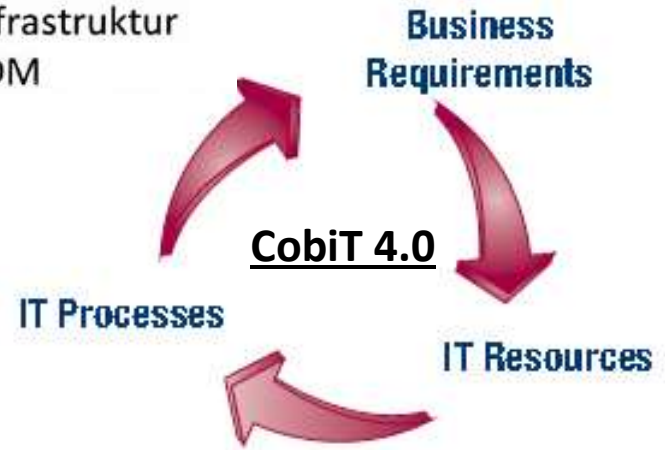
Tujuan dan Sasaran

- Tujuan:
  - Terwujudnya pelaksanaan tata kelola TI yang baik dengan penerapan pola **standardisasi** kerangka pengelolaan TI pada setiap BUMN untuk dapat mendukung penerapan GCG secara komprehensif
- Sasaran:
  - Setiap BUMN diwajibkan memiliki **Kebijakan Tata kelola TI dan *Master Plan TI***
  - **Kepatuhan pada HAKI** akan lisensi *software* atau menggunakan alternatif aplikasi *open source.*
  - **Target *maturity level*** dari Tata Kelola TI BUMN mencapai level 3 dalam 5 tahun kedepan
  - Penyediaan sumber daya TI harus dapat memaksimalkan program **sinergi BUMN**.

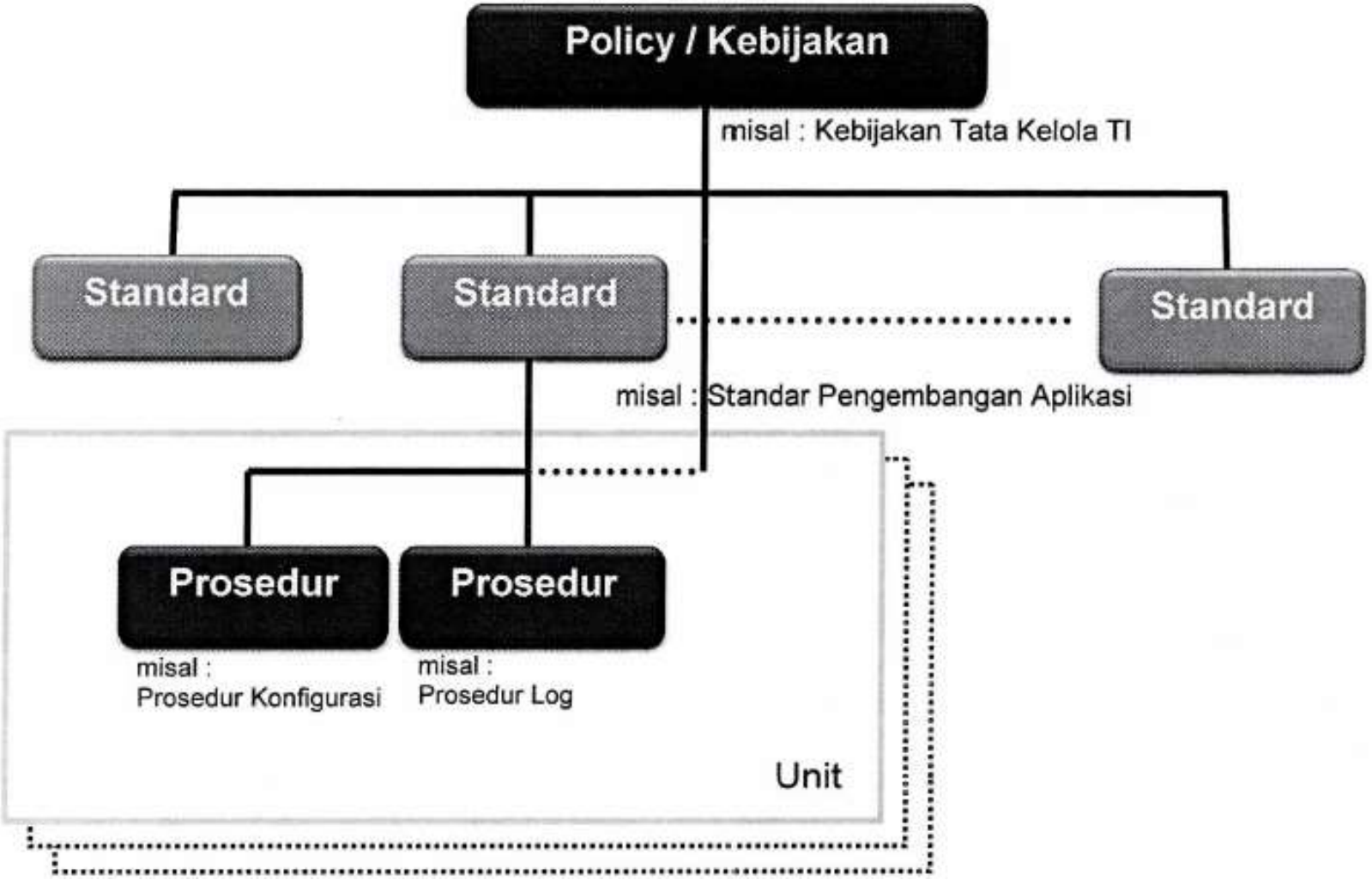
Framework Tata Kelola TI

Permen BUMN PER-02/MBU/2013

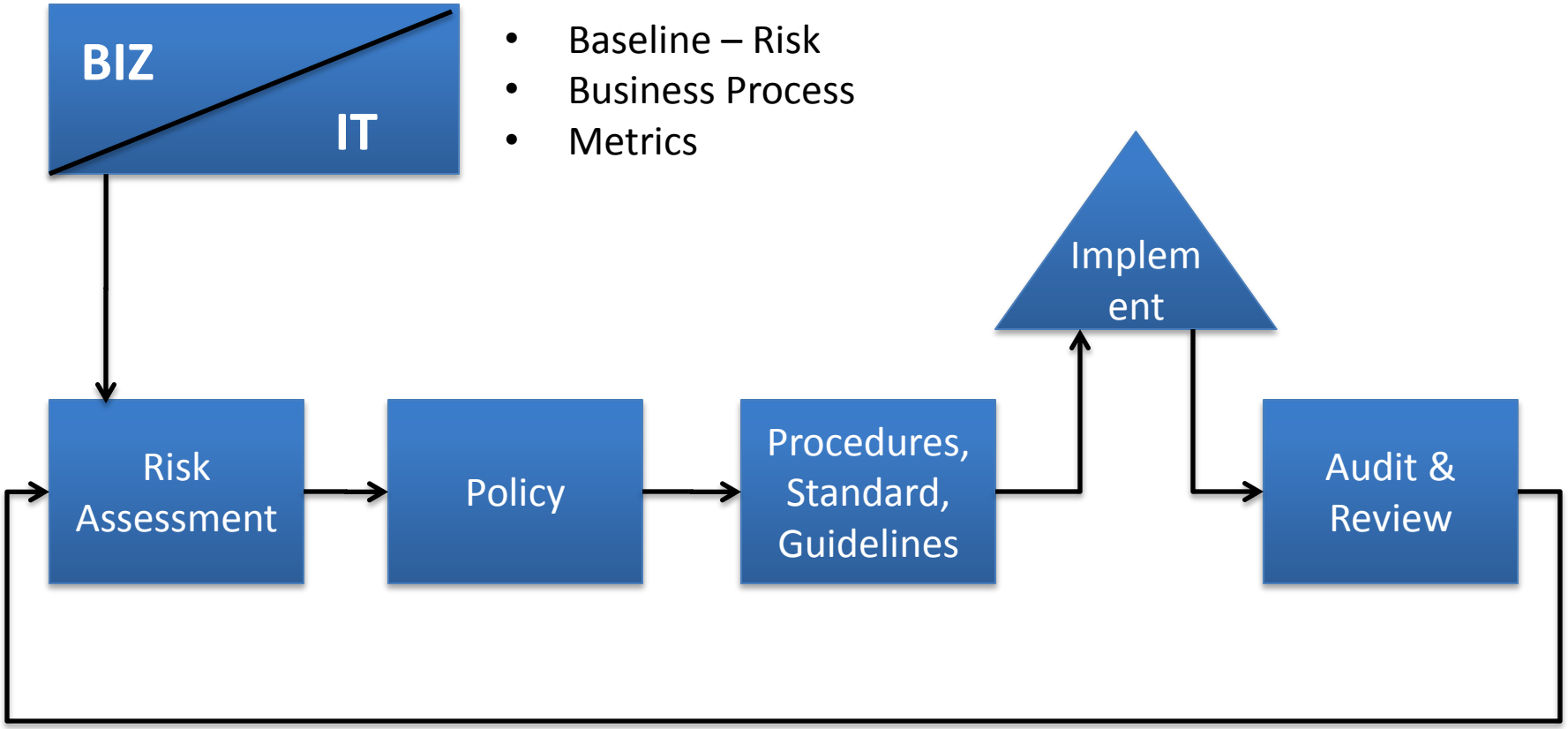




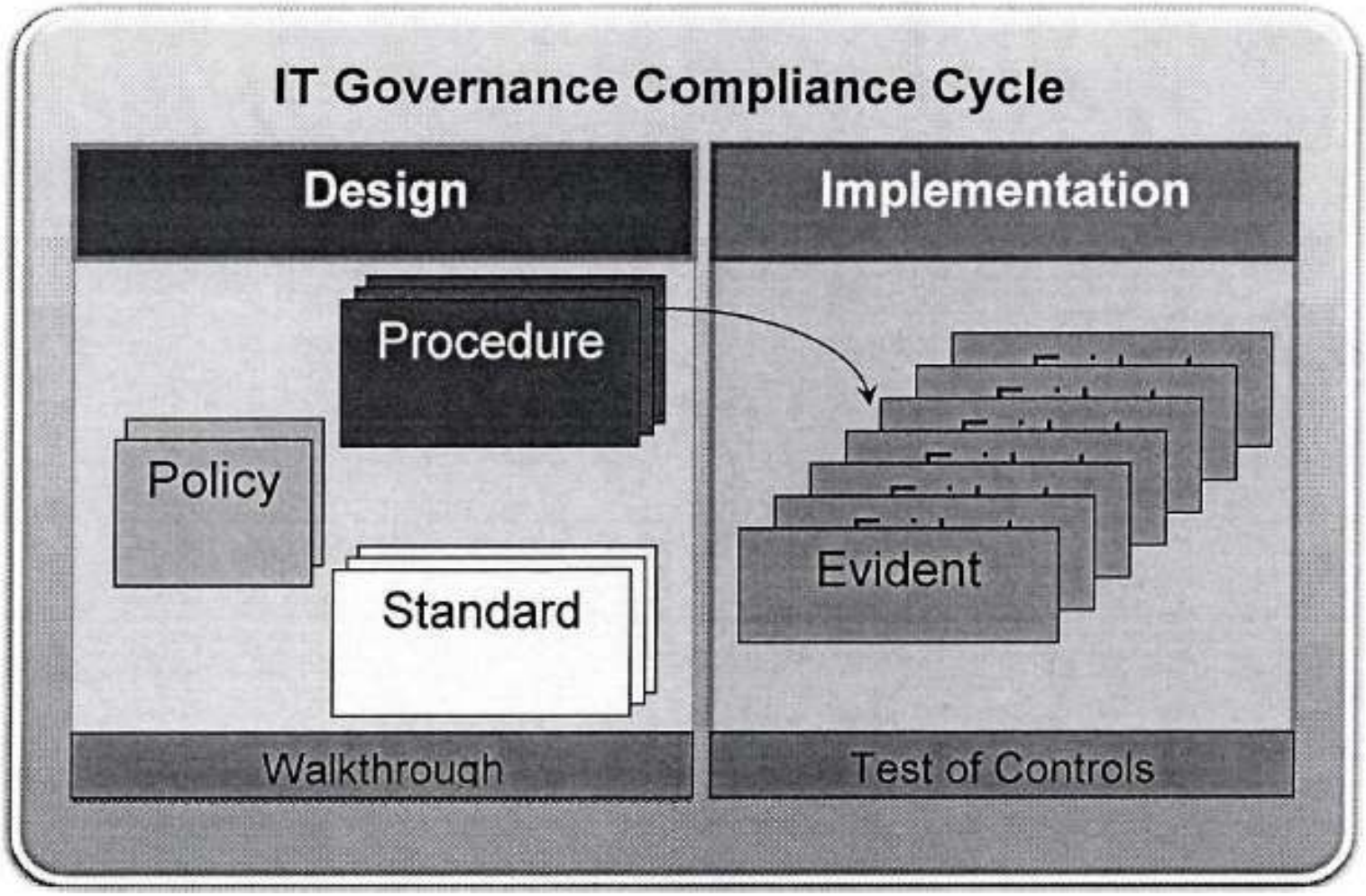
Arsitektur Kebijakan Tata Kelola TI



Siklus Kebijakan Tata Kelola TI



Siklus Audit Kepatuhan Tata Kelola TI



Proses Tata Kelola TI

Strategis

- Penetapan Peran TI
- Perencanaan TI
- Proses dan Organisasi TI
- Pengelolaan Sumber Daya TI
- Pengelolaan Investasi TI
- Pengelolaan Risiko TI
- Pengelolaan Proyek
- Penanganan Kebutuhan dan Identifikasi Solusi

Operasional

- Pengelolaan Layanan TI
- Pengelolaan Sekuriti
- Pengelolaan Layanan Pihak ketiga
- Pengelolaan Operasional
- Pengelolaan Mutu
- Knowledge Transfer
- Pengelolaan Data Monitor dan Evaluasi Kinerja TI
- Monitor dan Evaluasi Pengendalian Internal TI
- Pengelolaan Kepatuhan Regulasi Eksternal

1.1. Penetapan Peran TI Perusahaan

- Definisi
  - Pernyataan kebijakan yang ditetapkan untuk menentukan peran TI dalam perusahaan.
- Tujuan
  - Untuk menempatkan fungsi TI sesuai dengan peran yang telah ditentukan. Hal ini akan berkaitan dengan tugas, wewenang, dan tanggung jawab TI dalam perusahaan.
- Ruang Lingkup
  - Penetapan peran TI perusahaan didefinisikan berdasarkan tujuan strategis diimplementasikannya TI dan *IT Value di perusahaan terkait.*
- Deliverable
  - Pernyataan kebijakan peran TI bagi perusahaan

1.2. Perencanaan TI

- Definisi
  - Kebijakan yang mengatur tata kelola perencanaan TI dalam suatu perusahaan sesuai dengan peran TI dalam perusahaan tersebut.
- Tujuan
  - Agar perencanaan TI selaras dengan perencanaan dan tujuan bisnis perusahaan. Setiap BUMN diwajibkan untuk memiliki *Master Plan* TI yang berjangka waktu dan di review secara periodik
- Ruang Lingkup
  - Teknologi Informasi perlu dinyatakan secara jelas untuk menjamin keselarasan bisnis dengan TI, sesuai dengan peran TI dalam perusahaan.
- Deliverable
  - Visi & Misi TI perusahaan, *Master Plan TI, & (jika diperlukan) Fundamental Technical Plan(FTP)* yang berisikan standar teknologi yang akan digunakan dalam implementasi TI perusahaan

1.3 Kerangka Kerja Proses dan Organisasi TI

- Definisi
  - Kebijakan yang mengatur tata kelola proses TI perusahaan serta kebutuhan organisasi pendukungnya.
- Tujuan
  - Agar proses utama TI perusahaan dapat dijalankan dan selaras dengan peran TI perusahaan, serta tersedianya organisasi pendukung proses tersebut
- Ruang Lingkup
  - Meliputi struktur proses, *ownership, performance measurement & compliance.*
- Deliverable
  - Tatanan proses pengelolaan TI perusahaan yang dilengkapi dengan tugas dan tanggung jawabnya, serta bentuk organisasi (termasuk organisasi *ad hoc) TI pendukung proses TI* yang telah didefinisikan.

1.4. Pengelolaan Investasi TI

- Definisi
  - Kebijakan yang mengatur tata kelola investasi TI perusahaan dimana pada kebijakan ini harus dipastikan bahwa setiap investasi TI harus terkait dengan inisiatif bisnis perusahaan.
- Tujuan
  - Agar setiap investasi TI selaras dengan strategi bisnis perusahaan.
- Ruang Lingkup
  - Pengelolaan investasi TI Perusahaan merupakan bagian dari proses pengembangan, operasi, dan pemeliharaan sistem informasi yang harus dilaksanakan dalam kerangka *Master Plan TI*
- Deliverable
  - *Roadmap* atau rencana investasi yang dituangkan dalam *master plan* dan pengelolaan Rencana Kegiatan dan Anggaran Perusahaan (RKAP) bidang TI.

1.5 Pengelolaan Sumber Daya TI

- Definisi
  - Kebijakan yang mengatur tatanan pengelolaan seluruh sumber daya TI yang berupa SDM, data/informasi, aplikasi dan infrastruktur.
- Tujuan
  - Agar seluruh proses pengelolaan sumber daya TI dapat dikelola sesuai dengan aturan-aturan yang dipersyaratkan sehingga dapat menghasilkan produk TI yang dapat dipercaya, efektif dan efisien
- Ruang Lingkup
  - Kebijakan pengelolaan sumber daya TI meliputi kebijakan-kebijakan yang mengatur SDM, Data/Informasi, Aplikasi, Infrastruktur, tata kelola pengadaan sumber daya TI
- Deliverable
  - Standard dan prosedur yang mengatur tata cara penyediaan dan pengelolaan sumber daya TI, yang antara lain berupa : standard pengembangan aplkasi *(Software Development Life CycleISDLC),* standard teknologi infrastruktur TI, prosedur akusisi aplikasi, data dan infrastruktur, dan prosedur terkait lainnya.

1.6 Pengelolaan Risiko TI

- Definisi
  - Kebijakan yang mengatur pengelolaan risiko akibat diimplementasikannya TI dalam pencapaian sasaran bisnis perusahaan.
- Tujuan
  - Agar risiko-risiko akibat diimplementasi-kannya TI atau tidak beroperasinya TI sebagai pendukung bisnis dapat diidentifikasi dan dilakukan mitigasi yang tepat
- Ruang Lingkup
  - Meliputi pengaturan proses identifikasi risiko TI dalam suatu asesmen / penilaian risiko *(risk assessment), dampak* potensialnya terhadap bisnis dan tujuan perusahaan serta rencana mitigasinya yang merupakan tanggapan dari hasil identifikasi risiko
- Deliverable
  - Standard atau prosedur kerangka kerja pengelolaan risiko TI yang terintegrasi dengan kerangka kerja pengelolaan risiko perusahaan

2.1 Pengelolaan Layanan TI

- Definisi
  - Kebijakan yang mengatur tata kelola layanan TI yang bertujuan agar proses layanan TI dapat teridentifikasi dan didefinisikan dengan baik untuk mencapai kinerja TI yang diharapkan dan kelangsungan layanan TI perusahaan
- Ruang Lingkup
  - Meliputi antara lain proses -proses Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement
- Deliverables
  - Prosedur atau standard yang mengatur secara lebih detail proses yang diperlukan dalam menyelenggarakan layanan TI. *Best practice* yang dapat digunakan sebagai referensi dalam penyusunan prosedur atau standar proses ini adalah *IT Infrastructure Library (ITIL)* dengan penyesuaian yang diperlukan

2.2 Pengelolaan Sekuriti TI

- Definisi
  - Kebijakan yang mengatur tata kelola sekuriti TI dalam perusahaan.
- Tujuan
  - Untuk menjaga kerahasiaan *(confidentiality),* integritas *(integrity),* dan ketersediaan (*availability*) informasi perusahaan
- Ruang Lingkup
  - Meliputi aspek-aspek tentang pendefinisian aturan sekuriti TI, yang meliputi rencana sekuriti TI, klasifikasi aset TI, prosedur sekuriti, monitoring, pendeteksian, pelaporan, penyelesaian *vulnerabilities* & insiden sekuriti, serta rencana kesinambungan bisnis perusahaan atau *Business Continuity Plan (BCP).*
- Deliverable
  - Pendefinisian secara lebih detail untuk kebijakan ini dapat dituangkan dalam suatu prosedur atau standard sekuriti TI yang pada umumnya mengadopsi proses *Information Security Management System (ISMS*) yang berbasis ISO 27000 disesuaikan dengan kebutuhan perusahaan.Salah satu standar atau *guideline* sekuriti yang umum digunakan adalah kebijakan *acceptable use of IT* assets seperti bagaimana penggunaan *email* perusahaan, laptop perusahaan, jaringan internal perusahaan, dan hal lain yang perlu diatur pemakaiannya.

2.3 Pengelolaan Layanan Pihak Ketiga

- Definisi
  - Kebijakan yang mengatur tata kelola layanan TI yang dilakukan oleh pihak ketiga *(outsourcing).*
- Tujuan
  - Untuk menjamin bahwa layanan yang dijalankan oleh pihak ketiga *(suppliers, vendors, & partners)* memenuhi kebutuhan bisnis perusahaan dan juga meminimalkan risiko bisnis jika pihak ketiga tidak dapat memenuhi kewajibannya dalam memberikan layanan TI
- Ruang Lingkup
  - Meliputi pendefinisian tugas, tanggung jawab, dan ekspektasi dalam perjanjian dengan pihak ketiga, pendefinisan proses *reviewing* dan monitoring perjanjian pihak ketiga, pengelolaan risiko layanan TI oleh pihak ketiga. identifikasi hubungan pihak ketiga, *supplier relationship management, supplier risk management,* dan *supplier performance monitoring*
- Deliverable
  - Dapat berupa pembuatan kontrak dengan pihak ketiga berdasarkan *template* kontrak yang dibuat berdasarkan persyaratan yang berlaku dalam kebijakan ini, prosedur pengelolaan hubungan kemitraan dengan pihak ketiga, prosedur pengelolaan risiko untuk layanan pihak ketiga, dan prosedur pemantauan kinerja pihak ketiga.

2.4. Monitor dan Evaluasi Kinerja TI

- Definisi
  - Kebijakan yang mengatur pengelolaan indikator kinerja TI hingga level korporat dan sistematika pelaporan kinerja serta tindak lanjut yang diperlukan jika terjadi deviasi
- Tujuan
  - untuk memastikan bahwa seluruh kinerja TI sesuai dengan arahan dan kebijakan yang berlaku
- Ruang Lingkup
  - meliputi pengaturan pendekatan dan metoda monitoring kinerja TI, pendefinisian dan cara pengumpulan data, proses asesmen kinerja TI, proses pelaporan kinerja TI secara periodik, dan proses perencanaan remediasi akibat deviasi hasil asesmen kinerja TI
- Deliverable
  - Dapat dituangkan dalam prosedur pengukuran kinerja yang didefinisikan dalam KPI *(Key Performance Indikator)* unit, prosedur tata cara pengumpulan data kinerja TI, prosedur proses pelaksanaan asesmen kinerja TI, prosedur pelaporan kinerja TI, dan prosedur tata cara remediasi deviasi kinerja TI

2.5 Monitor & Evaluasi Pengendalian Internal

- Definisi
  - Kebijakan monitor dan evaluasi pengendalian internal *(internal control*) adalah kebijakan yang diperlukan.
- Tujuan
  - Untuk memberikan jaminan mengenai operasi TI yang efektif dan efisien dan kepatuhannya terhadap kebijakan dan aturan yang berlaku
- Ruang Lingkup
  - Kebijakan ini mengatur proses monitoring dan pelaporan pengecualian kontrol *(control exception*), pengelolaan asesmen dan basil dari *control self assessment (CSA*), mengelola proses remediasi, dan review pihak ketiga
- Deliverable
  - Dapat dituangkan dalam pendefinisian pengendalian internal yang akan diterapkan dalam layanan TI, prosedur pelaporan pengecualian kontrol, prosedur asesmen dan *control self assessment,* prosedur tata cara remediasi, dan prosedur tata cara mengevaluasi pihak ketiga.

2.6 Pengelolaan Compliance External Regulation

- Definisi
  - Kebijakan pengelolaan *compliance external regulation* adalah kebijakan yang mengatur proses identifikasi kebutuhan *compliance* dan proses evaluasi untuk menjamin *compliance* terhadap aturan yang berlaku.
- Tujuan
  - Untuk memastikan bahwa persyaratan aturan atau hukum yang berlaku telah dipatuhi.
- Ruang Lingkup
  - Mengatur proses identifikasi persyaratan *compliance,* mengoptimalkan dan mengevaluasi tanggapan terhadap hasil audit, memastikan tingkat kepatuhan, dan menyusun laporan yang terintegrasi dengan bisnis.
- Deliverable
  - Implementasi kebijakan ini dapat dituangkan dalam pendefinisian kebutuhan persyaratan *compliance* terhadap aturan tertentu (misal Sarbanes-Oxley, Basel II, PCI, Peraturan Bank Indonesia no.9/15/PBI/2007, prosedur pengelolaan *review* terhadap audit eksternal dan prosedur penyusunan laporan yang terintegrasi dengan laporan bisnis.

Komponen Master Plan TI

- Konteks Bisnis
  - Konteks Bisnis
    - Definisi
    - Tujuan
    - Kegiatan
    - Dokumen pendukung konteks bisnis
  - Kebutuhan Bisnis
    - Definisi
    - Tujuan
    - Kegiatan
    - Dokumen pendukung
- Kajian TI
  - Asesmen TI pada saat ini
  - Tren Industri TI dan Best Practice
  - Arah Strategi TI

Komponen Master Plan TI (2)

- Portofolio Proyek
  - Identifikasi Arsitektur/Strategi Aplikasi
  - Strategi Pengembangan Infrastrukut
  - Target Model Proses
  - Penetapan portofolio proyek dan pendanaan
- Roadmap
  - Roadmap
  - Menyusun business case
  - Perencanaan TI yang berkesinmbungan

Komponen Master Plan TI (3)

- Tata Kelola TI
  - Definisi
    - Suatu wewenang & tanggung jawab dari komisaris, direktur dan manager TI terkait dengan upaya TI menunjang strategi & tujuan organisasi, yang memanfaatkan mekanisme struktural, mekanisme komunikasi dan proses-proses tertentu.
  - Tujuan:
    - Membangun tata kelola, pengawasan, pengendalian, pemantauan dan audit pengembangan / implementasi MPTI
  - Kegiatan:
    - Menyusun tata kelola pengembangan / implementasi TI
    - Menyusun cara pengawasan dan pengendalian pengembangan / implementasi TI
    - Menyusun cara pemantauan, audit proses pengembangan / implementasi TI
  - Dokumen Pendukung
    - Tata kelola pengembangan / implementasi TI
    - Cara pengawasan dan pengendalian pengembangan / implementasi TI
    - Cara pemantauan, audit proses pengembangan / implementasi TI
  - Alat Bantu:
    - *Risk and Value Analysis*
    - *Prior Value Analysis*
    - *Dependencies Analysis*
    - *COBIT*
- Penutup

A. Kebijakan Strategis

No	Kebijakan	Pelaksanaan (Tidak Ada, Kadang Ada, Selalu Ada)	Bukti Dokumentasi	Komunikasi / Sosialisasi (Ya / Tidak)
1	Penetapan Peran TI Perusahaan		Statement (IT Support / IT Enabler) dalam dokumen strategi perusahaan (RJPP)	
			KPI/ Key Performance Indicator atau BSC/ Balanced Scorecard	
2	Perencanaan TI Perusahaan		IT Strategic BSC (1 tahun, 3-5 tahun)	
			IT Roadmap	
			Master Plan TI	
3	Kerangka Kerja Proses dan Organisasi TI		IT Steering Committee	
			Pengelolaan IT Policy	
			IT Operation & Development (procedure)	

No	Kebijakan	Pelaksanaan (Tidak Ada, Kadang Ada, Selalu Ada)	Bukti Dokumentasi	Komunikasi / Sosialisasi (Ya / Tidak)
4	Pengelolaan Sumber Daya TI		Prosedur Pengelolaan SDM (Kompetensi / Jobdesc, Rumpun Jabatan / Struktur, Pelatihan) Prosedur Pengelolaan Data / Informasi Prosedur Pengelolaan HW / SW Prosedur Pengelolaan Infrastruktur (DC, Network, dll)	
5	Pengelolaan Investasi TI		RKAP, RJPP IT Alignment BSC Horizontal Alignment Prosedur Pengelolaan Pengadaan Investasi TI	
6	Pengelolaan Risiko TI		Prosedur Risk Assessment DRP DRC	

B. Kebijakan Operasional

No	Kebijakan	Pelaksanaan (Tidak Ada, Kadang Ada, Selalu Ada)	Bukti Dokumentasi	Komunikasi / Sosialisasi (Ya / Tidak)
1	Pengelolaan Layanan TI		Prosedur Helpdesk Prosedur atau Standard Layanan TI (system manual) Implementasi ITIL	
2	Pengelolaan Sekuriti		Standard atau Guideline sekuriti yang umum digunakan dan acceptable use of IT assets seperti penggunaan email, atau PC/Laptop perusahaan. Prosedur keamanan jaringan internal perusahaan dan hal lain yang perlu diatur pemakaiannya.	
3	Pengelolaan Layanan Pihak Ketiga		Pengelolaan Perjanjian dan Kontrak Tersedianya template kontrak untuk pengelolaan kontrak yang lebih profesional Laporan evaluasi dan monitoring perjanjian ke pihak ketiga	

No	Kebijakan	Pelaksanaan (Tidak Ada, Kadang Ada, Selalu Ada)	Bukti Dokumentasi	Komunikasi / Sosialisasi (Ya / Tidak)
4	Monitor dan Evaluasi Kinerja TI		Prosedur pengukuran dan pelaporan kinerja TI prosedur untuk monitor dan evaluasi kinerja (KPI)	
5	Monitor dan Evaluasi Pengendalian Internal		Dokumen checklist tata kelola TI Prosedur asesmen tata kelola TI dan evaluasi pihak ketiga	
6	Pengelolaan Compliance External Regulation		Standard regulasi eksternal (checklist) asesmen terhadap external compliance yang dicapai	