



COBIT

(Control Objectives for Information and Related Technology)

Jurusan Sistem Informasi
Fakultas Ilmu Komputer dan Teknologi Informasi

PTA 2024/2025



Manajemen Kontrol Keamanan

- ❑ Mampu memberikan gambaran Konsep audit IT dengan penerapan COBIT
- ❑ Memahami Konsep dan kerangka COBIT
- ❑ Memahami dan menerapkan COBIT dalam audit IT
- ❑ Konsep dasar COBIT
- ❑ Ruang Lingkup COBIT
- ❑ Kerangka Kerja COBIT
- ❑ Domain COBIT




Tujuan

Materi



Konsep Dasar COBIT



ISACA (Information Systems Audit and Control Association)



ISACA → Organisasi dalam tata kelola teknologi informasi → Audit IT dan standar penjamin IT

ISACA → Keamanan informasi → Dasar dari audit sistem informasi dan pengendalian





COBIT (Control Objectives for Information and Related Technology)



- ❑ Framework → mengelola teknologi informasi
- ❑ COBIT → IT Governance Institute dan ISACA
- ❑ Manajemen → menyeimbangkan antara risiko dan investasi dalam lingkup IT yang tidak dapat di prediksi
- ❑ Auditor → Mendukung dan memperkuat opini yang dihasilkan




COBIT (Control Objectives for Information and Related Technology)



COBIT dibuat oleh ISACA (Information Systems Audit and Control Association)
→ IT Governance Institute

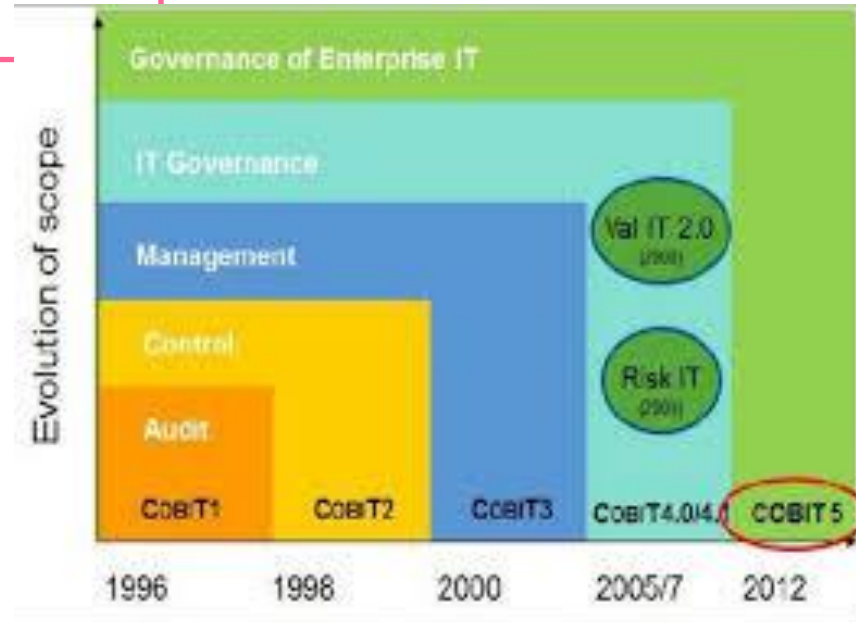
COBIT berfokus pada audit, control and security issues



COBIT dirancang sebagai alat penguasaan IT → membantu pemahaman dan manage resiko, manfaat dan evaluasi IT

COBIT (Control Objectives for Information and Related Technology)

COBIT Framework → standar kontrol terhadap TI dengan kerangka kerja dan kontrol TI → audit SI





Kriteria Informasi COBIT

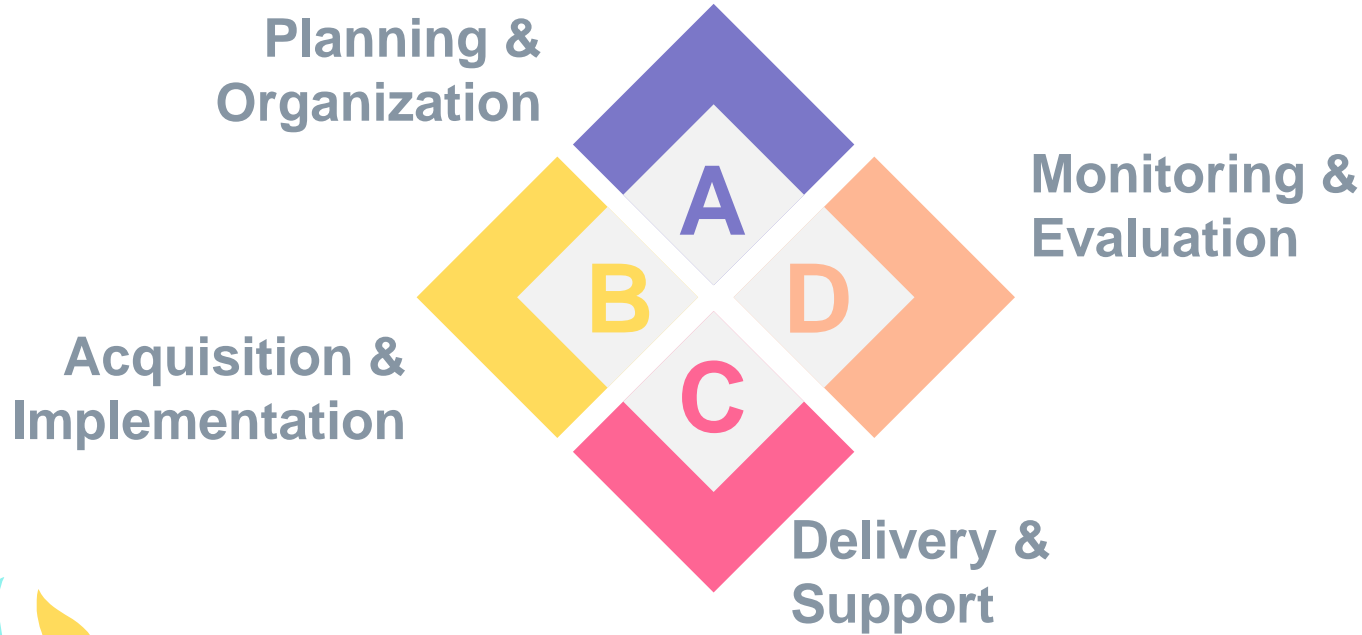


- ☐ Efektifitas (Effectiveness)
 - ☐ Efisiensi (Efficiency)
 - ☐ Kerahasiaan (Confidentiality)
 - ☐ Integritas (Integrity)
 - ☐ Ketersediaan (Availability)
 - ☐ Kepatuhan (Compliance)
 - ☐ Keandalan (Reliability)
- 
- 



Ruang Lingkup dan Kerangka COBIT

Lingkup COBIT (4 Domain dalam COBIT)

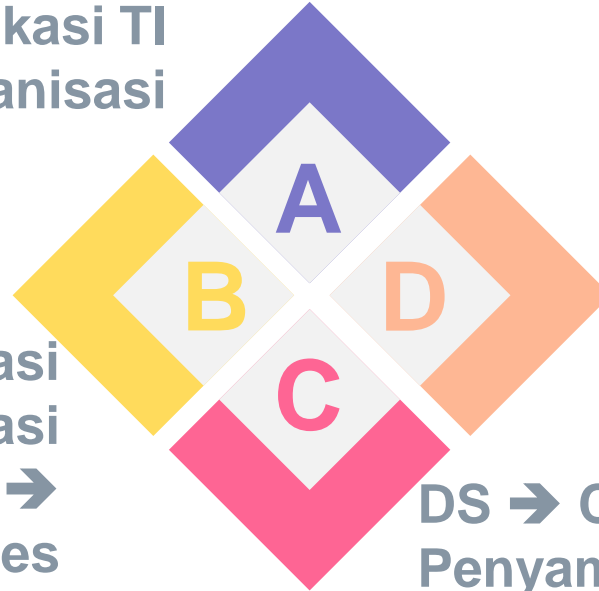


Lingkup COBIT

(4 Domain dalam COBIT)

PO → Cakupan : strategi
taktik dan identifikasi TI
→ Tujuan organisasi

AI → Cakupan : Realisasi
strategi TI, identifikasi
dan pengembangan TI →
Bisnis Proses



ME → Cakupan :
Manajemen kinerja,
pemantauan control dan
pelaksanaan

DS → Cakupan :
Penyampaian jasa
(penyediaan layanan dan
manajemen keuangan)

COBIT Frameworks

COBIT Framework

How do they relate?

IT
Resources



IT
Processes



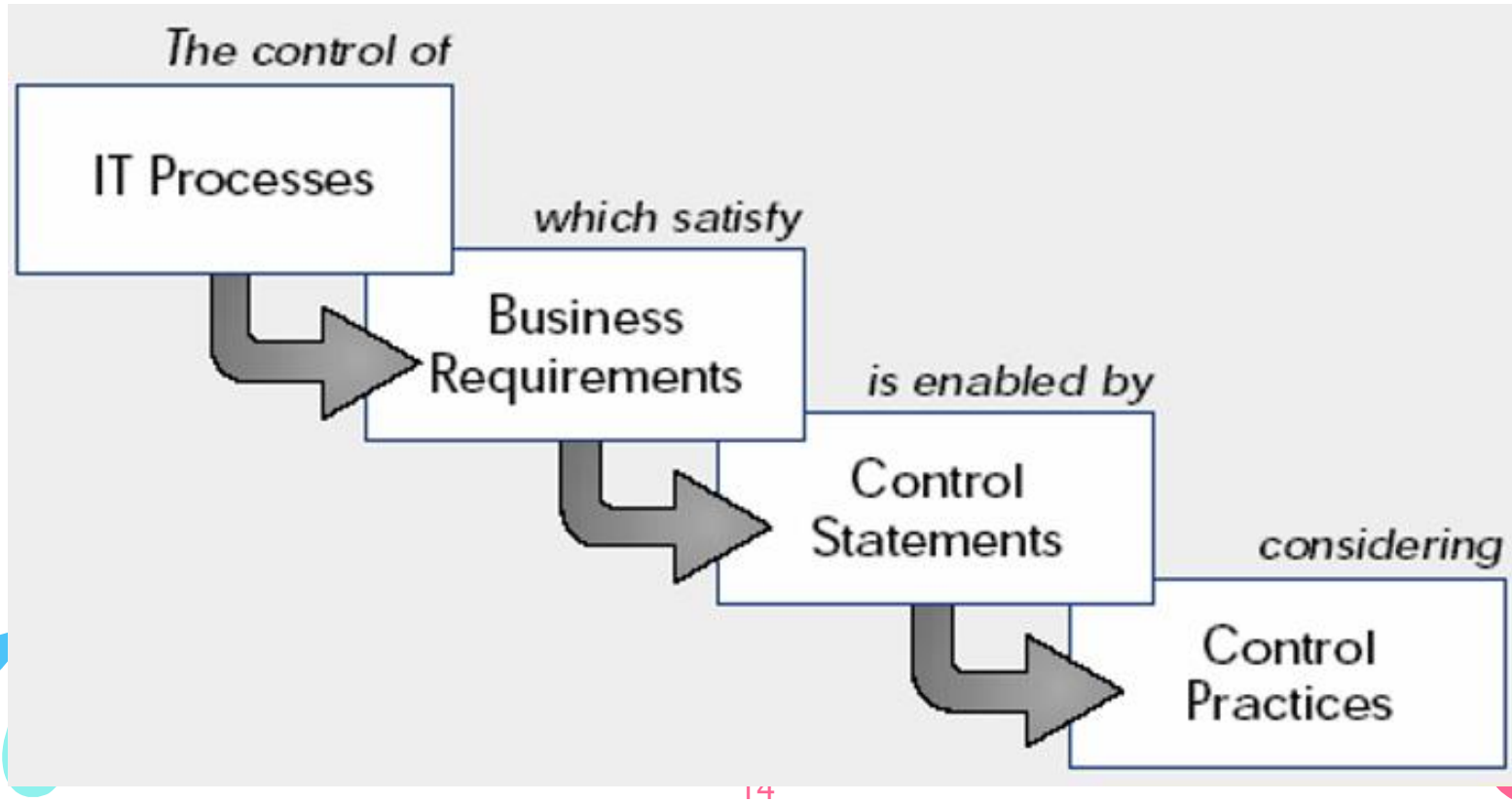
Business
Requirements

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

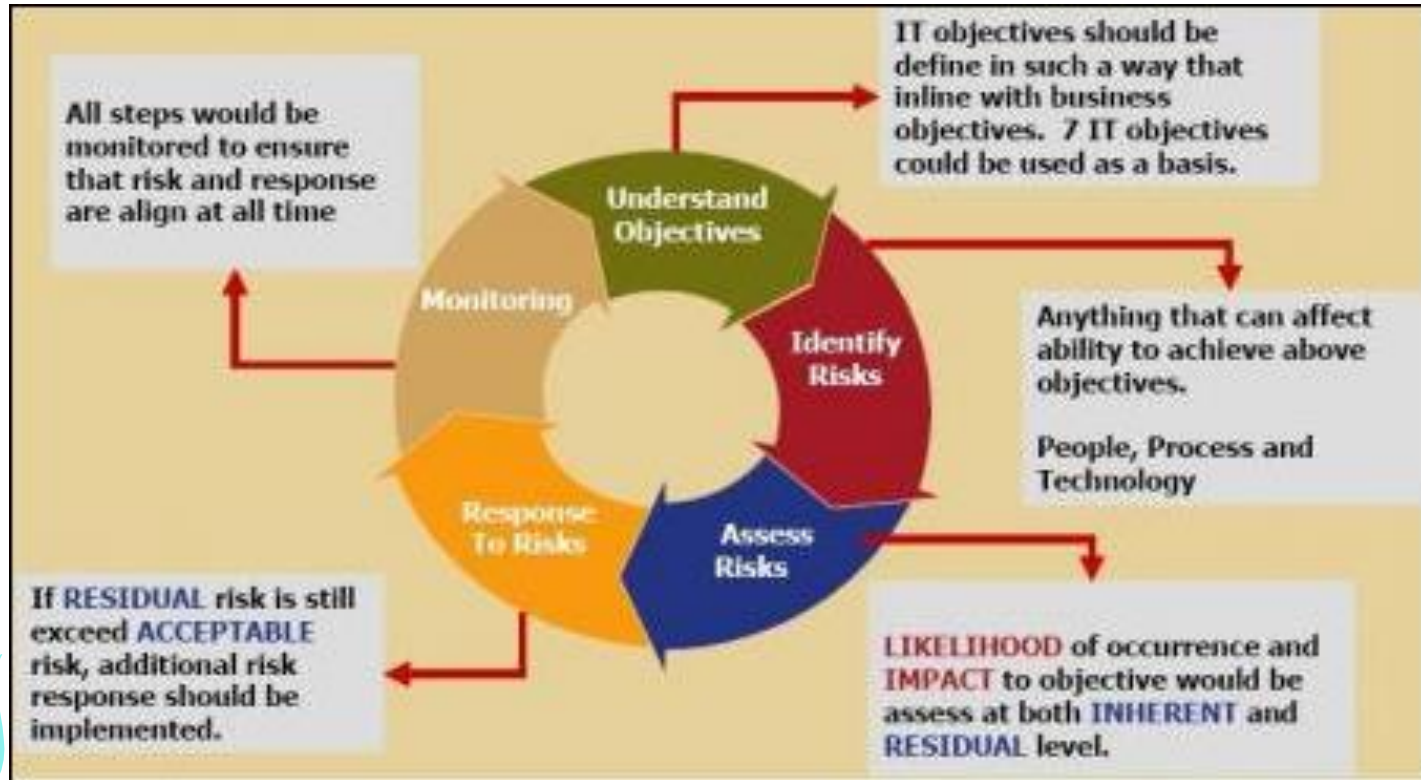
- Plan and Organise
(Perencanaan & Org.)
- Acquire and Implement
(Pengadaan & Implementasi)
- Deliver and Support
(Pengantaran & dukungan)
- Monitor and Evaluate
(Pengawasan & Evaluasi)

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

Pola Pikir COBIT



IT Risk Management Framework COBIT





Framework IT Manajemen Resiko



Penetapan Objektif

Kriteria informasi dari COBIT → dasar dalam mengidentifikasi objektif TI. Kriteria informasi COBIT (Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance dan Reliability)

Identifikasi Resiko

Proses untuk mengetahui resiko → Sumber (manusia, proses dan teknologi, internal, eksternal, bencana, ketidakpastia, kesempatan)

Penilaian Resiko

Proses untuk menilai seberapa besar resiko terjadi dan dampak dari resiko



Penilaian Resiko

Level	Business Impacts	Likelihood
0	Kerusakan yang hampir tidak signifikan	Hampir mustahil terjadi
1	Kerusakan kecil	Jarang terjadi
2	Kerusakan yang signifikan tetapi dapat ditolerir	Mungkin terjadi
3	Kerusakan besar	Sering terjadi
4	Kerusakan yang dapat mengancam kelangsungan bisnis	Sangat sering terjadi

Objectives	Events
Effectiveness and Efficiency	Manajemen yang buruk (perencanaan dan kebijakan)
	Sistem (Hardware, software dan teknologi).
	Kemampuan TI dan non-TI.
	Manajemen proses (desain dan eksekusi)
Confidentiality	Manajemen Keamanan (kebijakan dan prosedur).
	Sistem (Hardware, software teknologi dan jaringan).
	Kesadaran pengguna
	Hacker dan virus
Integrity and Reliability	Desain sistem (input, proses, output)
	Hacker dan pelanggar akses
	Prosedur pemberian otoritas yang buruk.
Availability	Desain system dan jaringan
	Kegagalan hardware
	Sabotase dari luar
	Virus dan serangan
	Tidak ada BCP, backup dan recovery
Compliance	Tidak sadar atau tidak mengerti terhadap aturan dan regulasi
	Tidak ada monitoring

Identifikasi Resiko



Framework IT Manajemen Resiko





Respon Resiko

Menerapkan control objektif yang sesuai dalam melakukan manajemen resiko → 34 Control Objectives.

Monitor Resiko

Setiap langkah dimonitor untuk menjamin bahwa resiko dan respon berjalan sepanjang waktu.





Domain COBIT



Control Domain Planning & Organisation



Planning & Organisation

PO1

Define a strategic IT plan

PO2

Define the information architecture

PO3

Determine technological direction

PO4

Define the IT organization and relationships

PO5

Manage the IT investment

PO6

Communicate management aims and direction

PO7

Manage human resource

PO8

Ensure compliance with external requirements

PO9

Assess risks

PO10

Manage projects

PO11

Manage quality





Control Domain Acquisition & Implementation



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



Control Domain Delivery & Support

● Delivery & Support

DS1

Define and manage service levels

DS2

Manage third-party services

DS3

Manage performance and capacity

DS4

Ensure continuous service

DS5

Ensure system security

DS6

Identify and allocate costs

DS7

Educate and train users

DS8

Assists and advise customers

DS9

Manage the configuration

DS10

Manage problems and incidents

DS11

Manage data

DS12

Manage facilities

DS13



Manage operations



Control Domain Monitoring



Monitoring	M1	Monitor the processes
	M2	Assess internal control adequacy
	M3	Obtain independent assurance
	M4	Provider for independent audit





CobiT Framework (Plan and Organise)



Topics :

1. Strategi dan taktik
2. Merencanakan visi
3. Organisasi dan infrastruktur

Questions :

1. Apakah IT dan strategi bisnis sudah ditetapkan ?
2. Apakah perusahaan sudah menggunakan secara maksimum sumber dayanya ?
3. Apakah semua orang di dalam organisasi sudah memahami sasaran IT ?
4. Apakah resiko IT sudah dipahami & diatur ?
5. Apakah mutu system IT sudah sesuai dengan kebutuhan bisnis ?



CobiT Framework (Acquire and Implement)



Topics :

1. IT solutions
2. Perubahandan dan Pemeliharaan
Pemeliharaan



Questions :

1. Apakah proyek baru dapat dapat memberikan solusi terhadap kebutuhan bisnis?
2. Apakah proyek baru dapat selesai tepat waktu dan sesuai anggaran?
3. Apakah sistem kerja yg baru bisa diterapkandgn dgn baik?
4. Apakah perubahan yg dibuat tdk merepotkan kegiatan bisnis yg berjalan?



CobiT Framework (Deliver and Support)



Topics :

1. **Layanan pengantaran & dukungan**
2. **Dukungan proses penyusunan**



Questions :

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



CobiT Framework (Monitor and Evaluate)



Topics :

1. Penilaian over time, jaminan pengiriman
2. Sistem pengendalian manajemen kesalahan
3. Pengukuran pekerjaan

Questions :

1. Dapatkah IT mendeteksi suatu permasalahan sebelum semuanya terlambat?
2. Apakah jaminan kemandirian yg diperlukan dpt memastikan bidang2 kritis bisa beroperasi sesuai dgn yg diharapkan?





Skala Maturity Framework COBIT



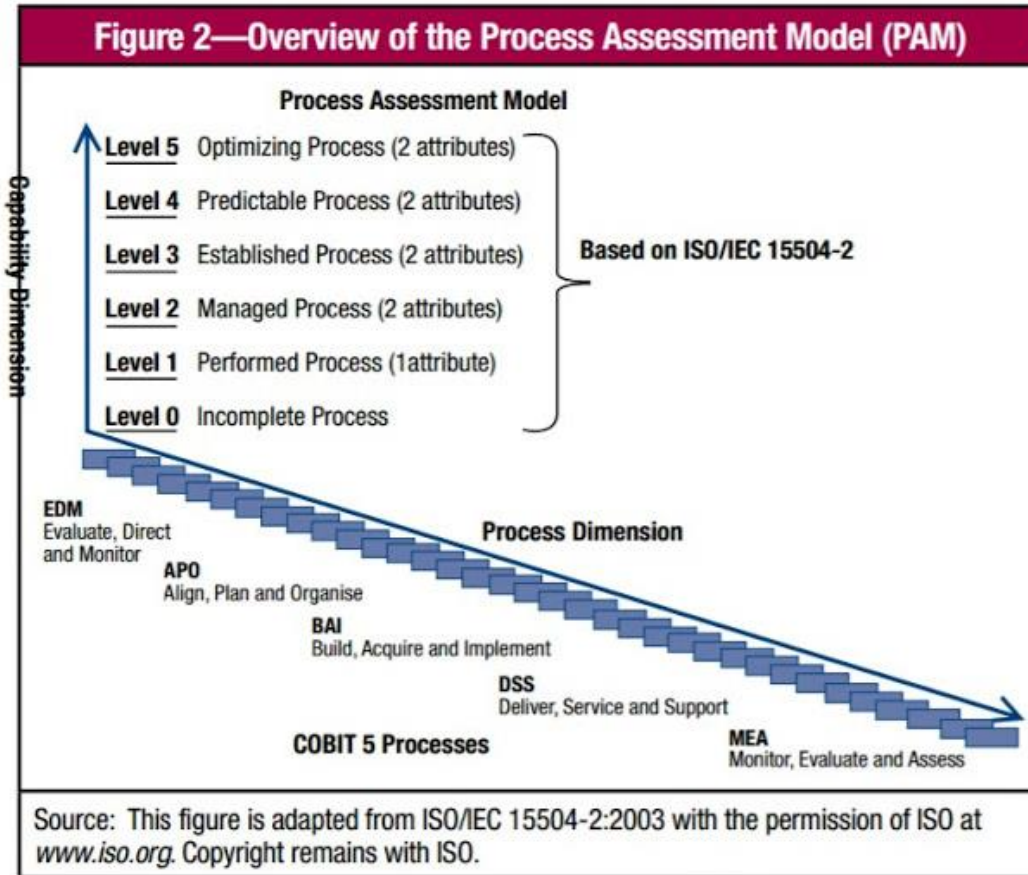
Maturity Model → Metode untuk mengukur level pengembangan manajemen proses → untuk mengukur kapabilitas manajemen dalam COBIT Framework

Maturity Model digunakan untuk memetakan :

- 1. Status pengelolaan TI perusahaan pada saat itu.**
- 2. Status standart industri dalam bidang TI saat ini (sebagai pembandingan)**
- 3. Status standart internasional dalam bidang TI saat ini (sebagai pembandingan)**
- 4. Strategi pengelolaan TI perusahaan (ekspetasi perusahaan terhadap posisi pengelolaan TI perusahaan)**




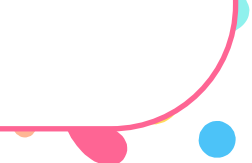
COBIT Maturity Model





Tingkat Skala Maturity (6 Level)





- Skala 0 (Non-existent) → Perusahaan tidak menyadari perlunya perencanaan strategis dalam TI.
 - Skala 1 (Initial Level) → Perusahaan mulai menyadari pentingnya membuat perencanaan strategis TI.
 - Skala 2 (Repeatable Level) → Perusahaan telah menetapkan prosedur untuk dipatuhi human.
- 
- 



Tingkat Skala Maturity (6 Level)



- Skala 3 (Defined Level) → Proses telah didokumentasikan dan dilakukan sesuai metode pengembangan.
 - Skala 4 (Managed Level) → Proses komputerisasi telah dimonitor dan dievaluasi.
 - Skala 5 (Optimized Level) → Best Practices, Otomatisasi sistem sudah terencana dengan metode
- 
- 

34 Domain Proses COBIT, Skor dan Tingkat Maturity

Plan and Organize

NO	KODE PROSES	SKOR	TINGKAT MATURITY
1	PO1 Menetapkan rencana Strategis TI	3	Define
2	PO2 Menetapkan arsitektur sistem informasi	0	Non-Existent
3	PO3 Menetapkan arah teknologi	3	Define
4	PO4 Menetapkan proses TI, organisasi dan hubungannya	3	Define
5	PO5 Mengatur investasi TI	3	Define
6	PO6 Mengkomunikasikan tujuan dan arahan manajemen	4	Manage
7	PO7 Mengelola sumberdaya manusia	4	Manage
8	PO8 Mengatur kualitas	3	Define
9	PO9 Menilai dan mengatur resiko TI	0	Non-Existent
10	PO10 Mengatur Proyek	0	Non-Existent
	Rata-rata Domain PO	2.3	Repeatable

34 Domain Proses COBIT, Skor dan Tingkat Maturity

Acquire and Implement

NO	KODEPROSES	SKOR	TINGKAT MATURITY
1	AI1 Identifikasi solusi-solusi otomatis	0	Non-Existent
2	AI2 Mendapatkan dan memelihara perangkat lunak aplikasi	3	Define
3	AI3 Mendapatkan dan memelihara infrastruktur teknologi	3	Define
4	AI4 Menjalankan operasi dan menggunakannya	3	Define
5	AI5 Pengadaan sumber daya TI	3	Define
6	AI6 Mengelola perubahan	0	Non-Existent
7	AI7 Instalasi dan akreditasi solusi serta perubahan	0	Non-Existent
	Rata-rata Domain AI	1.7	Repeatable

34 Domain Proses COBIT, Skor dan Tingkat Maturity

Delivery and Support

NO	KODE PROSES	SKOR	TINGKAT MATURITY
1	DS1 Menetapkan dan mengatur tingkat layanan	0	Non-Existent
2	DS2 Pengaturan layanan dengan pihak ketiga	3	Define
3	DS3 Mengatur kinerja dan kapasitas	0	Non-Existent
4	DS4 Memastikan ketersediaan layanan	3	Define
5	DS5 Memastikan keamanan sistem	3	Define
6	DS6 Identifikasi dan biaya tambahan	0	Non-Existent
7	DS7 Mendidik dan melatih user	3	Define
8	DS8 Mengelola bantuan layanan dan insiden	0	Non-Existent
9	DS9 Mengatur konfigurasi	0	Non-Existent
10	DS10 Mengelola masalah	0	Non-Existent
11	DS11 Mengelola data	3	Define
12	DS12 Mengelola fasilitas	3	Define
13	DS13 Mengelola operasi	3	Define
	Rata-rata Domain DS	1.6	Repeatable

34 Domain Proses COBIT, Skor dan Tingkat Maturity

Monitor and Evaluate

NO	KODE PROSES	SKOR	TINGKAT MATURITY
1	ME1 Monitor dan Evaluasi Kinerja TI	3	Define
2	ME2 Monitor dan Evaluasi Pengendalian Internal	3	Define
3	ME3 Mendapatkan jaminan independent	0	Non-Existent
4	ME4 Penyediaan untuk tatakelola TI	3	Define
	Rata-rata Domain ME	2.3	Repeatable



Thanks!

Any questions?

