AUDIT SISTEM INFORMASI

Risk Assessment dan Penentuan Scope Audit

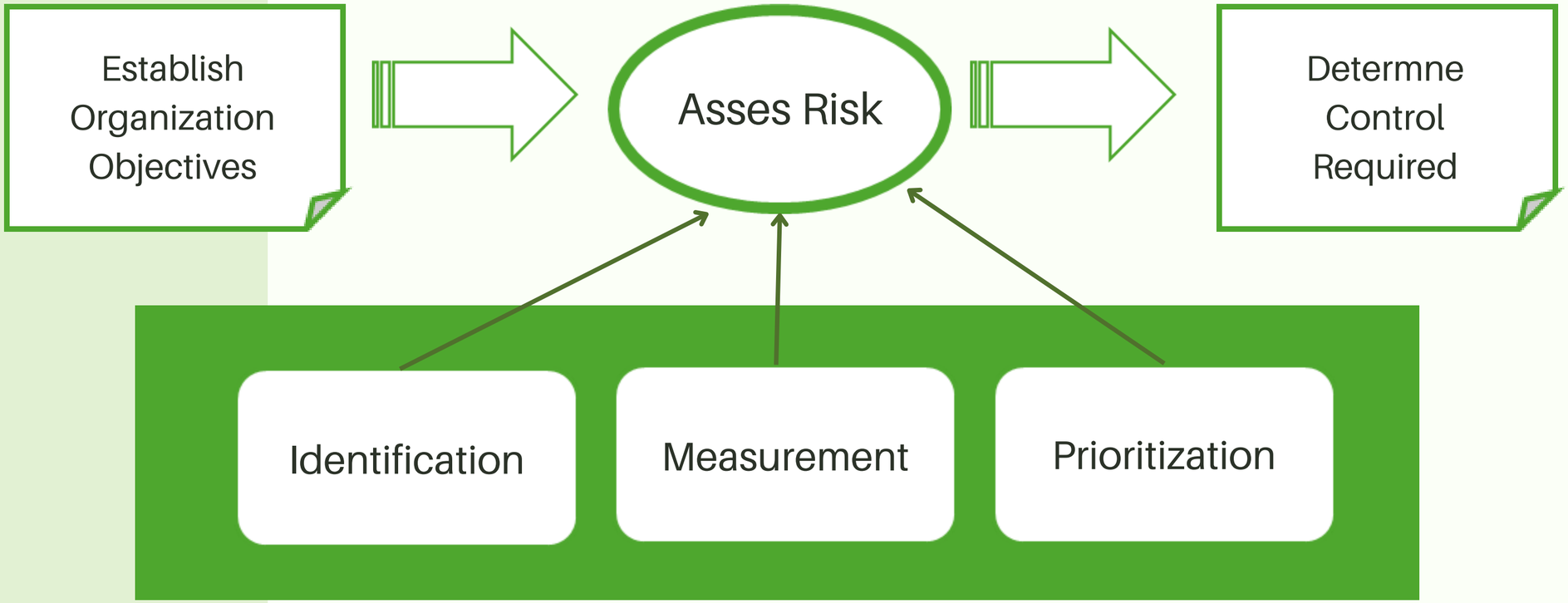
Oleh :
Siti Mukaromah, S.Kom., M.Kom.
Affifiana Prisyanti, S.Kom.M.Kom.

Risk Assessment

Menurut, ISACA (Information Systems Audit and Control Association), Risk Assessment adalah **proses identifikasi, evaluasi, dan pengukuran risiko yang mungkin mempengaruhi aset TI dan tujuan bisnis organisasi.**

Tujuan:
mengetahui ancaman terbesar, memprioritaskan area audit, mendukung keputusan

Hubungan Resiko dengan Perencanaan Audit



Hubungan Risk Assessment & Scope Audit

Risk assessment → membantu menentukan area kritikal seperti: ancaman, kerentanan, atau kelemahan kontrol.

Scope audit → fokus audit ke area risiko tinggi semakin tinggi risiko suatu area, semakin besar kemungkinan area tersebut dimasukkan dalam scope audit.

Hasil: audit lebih efektif, efisien, relevan

Tahapan *Risk Assessment*

Identifikasi Risiko →	ancaman (cyber attack, kegagalan sistem, kesalahan manusia, dll.)
Analisis Risiko →	dampak (impact) & kemungkinan (likelihood)
Evaluasi Risiko →	level risiko (rendah, sedang, tinggi)
Mitigasi Risiko →	kontrol pencegahan, deteksi, pemulihan

Metode Penilaian Risiko

- **Kualitatif → kate**gori (tinggi, sedang, rendah)
- **Kuantitatif →** nilai finansial/statistik
- **Hybrid →** kombinasi keduanya

Definisi Scope Audit

Scope audit = batasan & ruang lingkup area yang diperiksa auditor, yang terdiri dari: sistem, proses, aplikasi, infrastruktur yang diaudit

Infrastruktur TI: server, jaringan, firewall

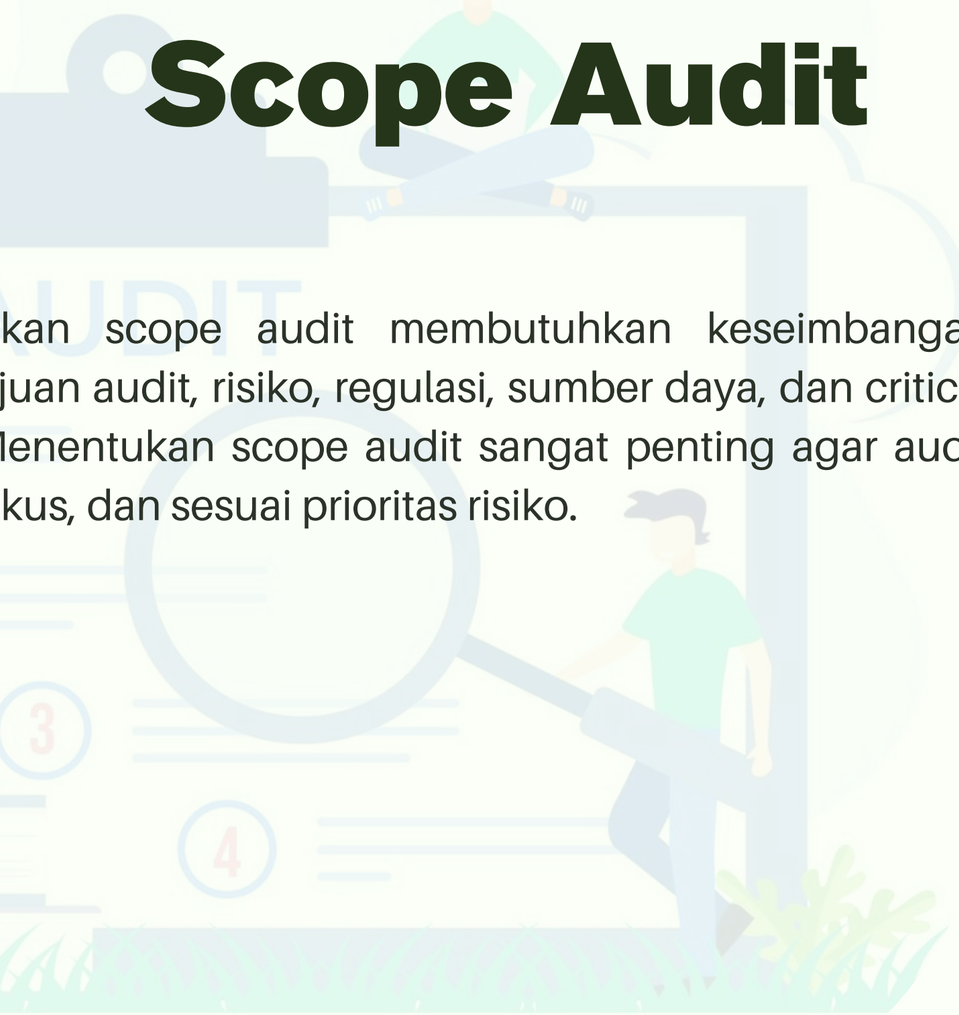
Aplikasi utama: ERP, HRIS, sistem keuangan

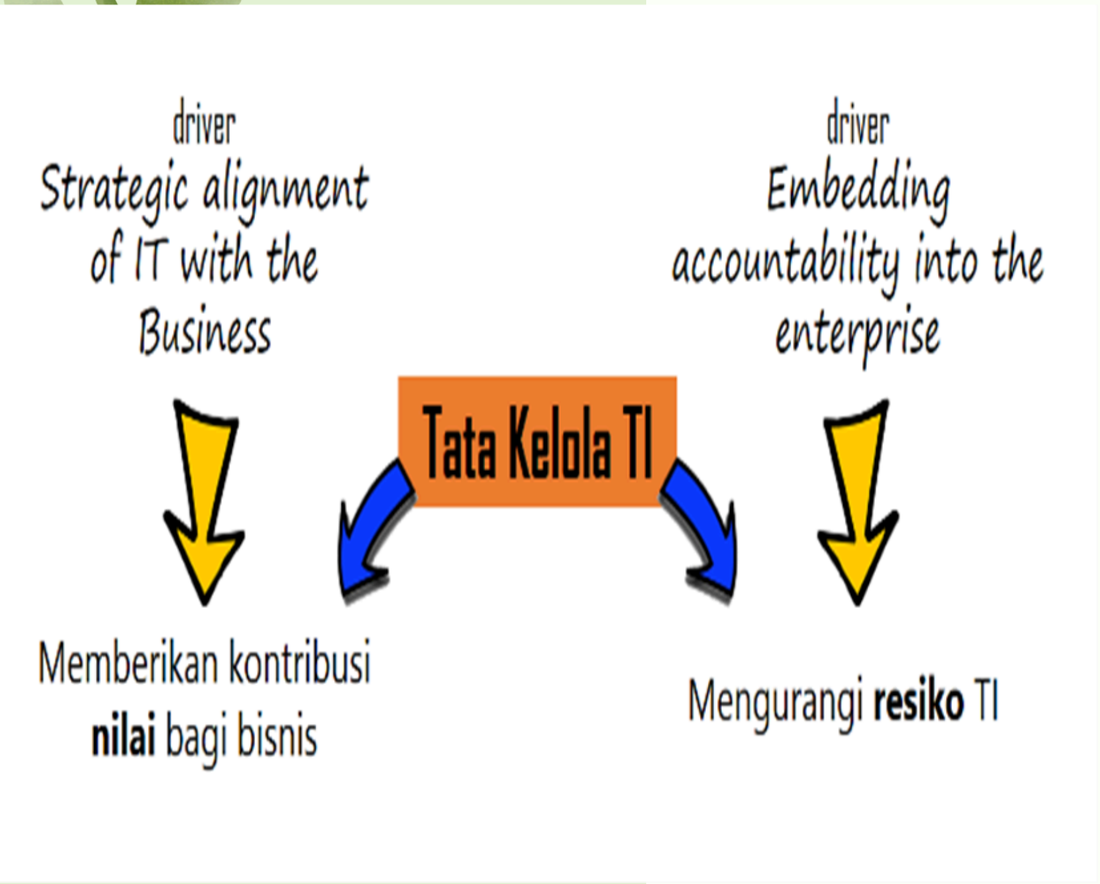
Proses bisnis: procurement, payroll, e-banking

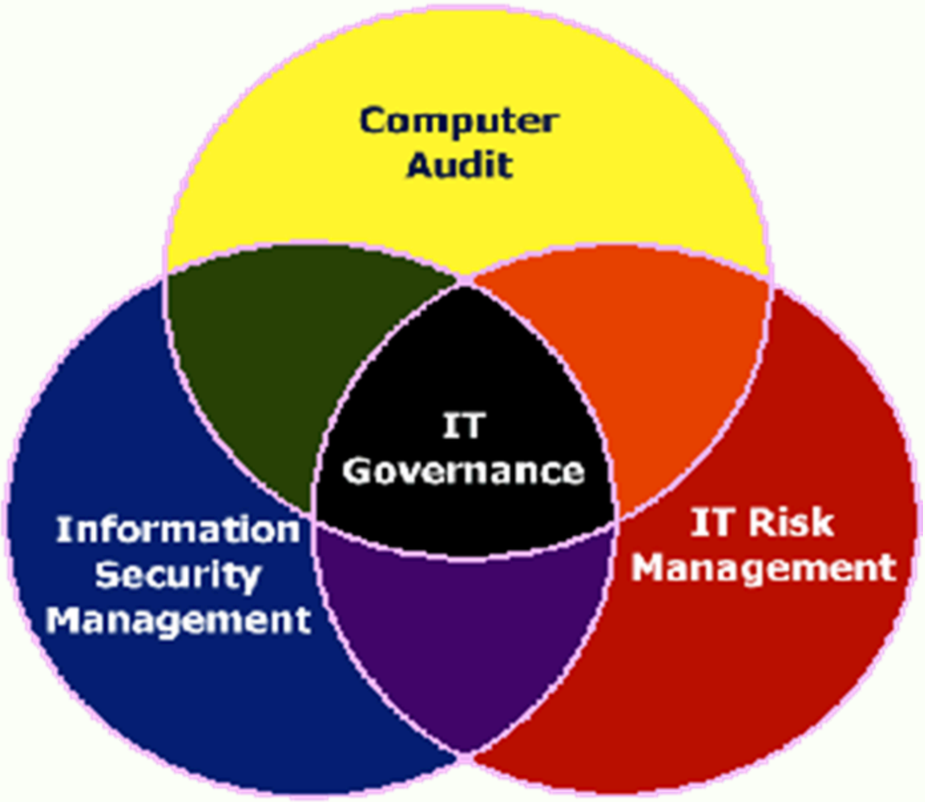
Faktor Penentu Scope Audit

- Tujuan bisnis & audit
- Hasil risk assessment (area risiko tinggi diprioritaskan)
- Regulasi & compliance
- Sumber daya auditor (waktu, biaya, SDM)
- Critical systems (sistem inti, aplikasi utama, data penting)

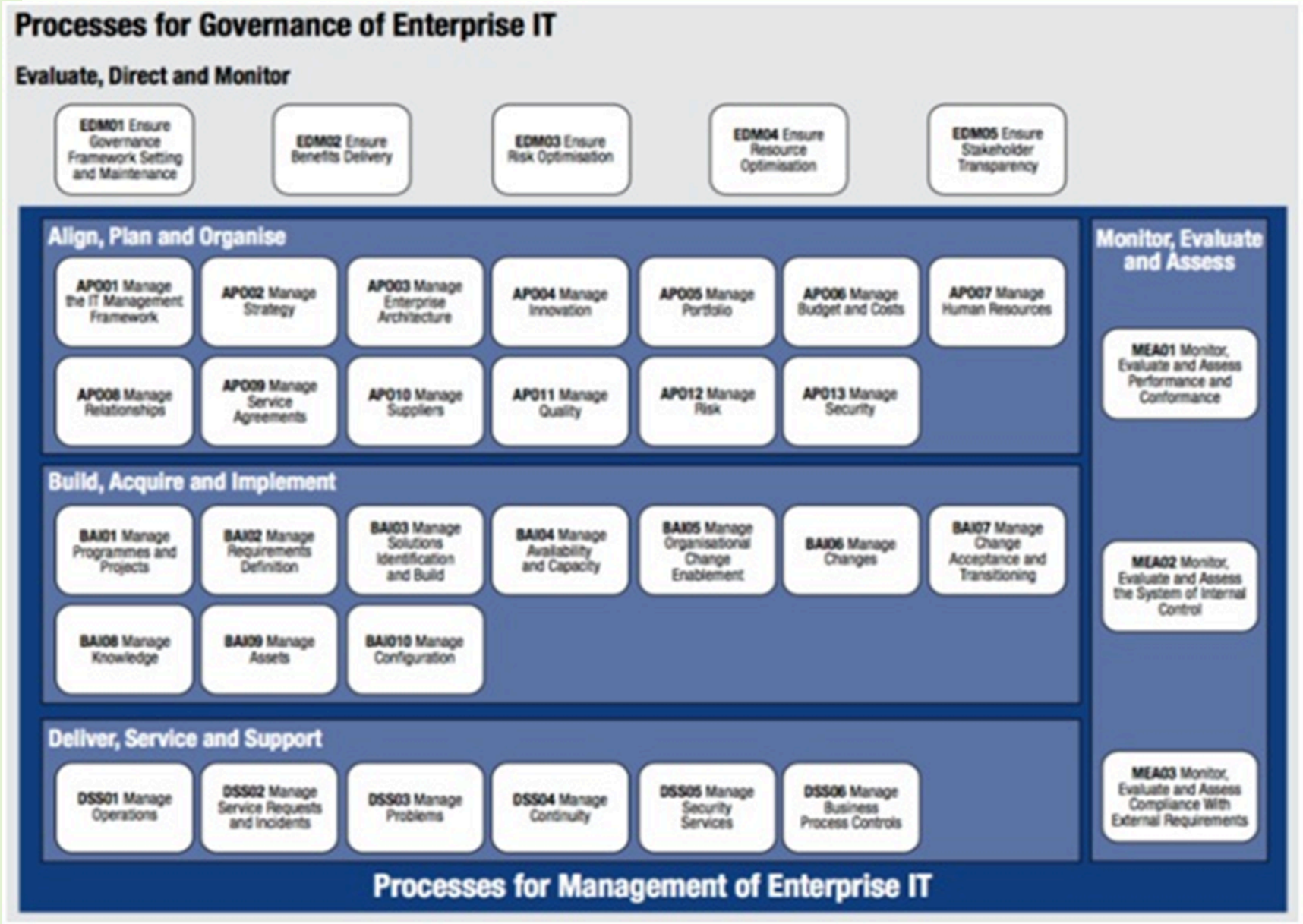
Menentukan scope audit membutuhkan keseimbangan antara tujuan audit, risiko, regulasi, sumber daya, dan critical system.Menentukan scope audit sangat penting agar audit efektif, fokus, dan sesuai prioritas risiko.



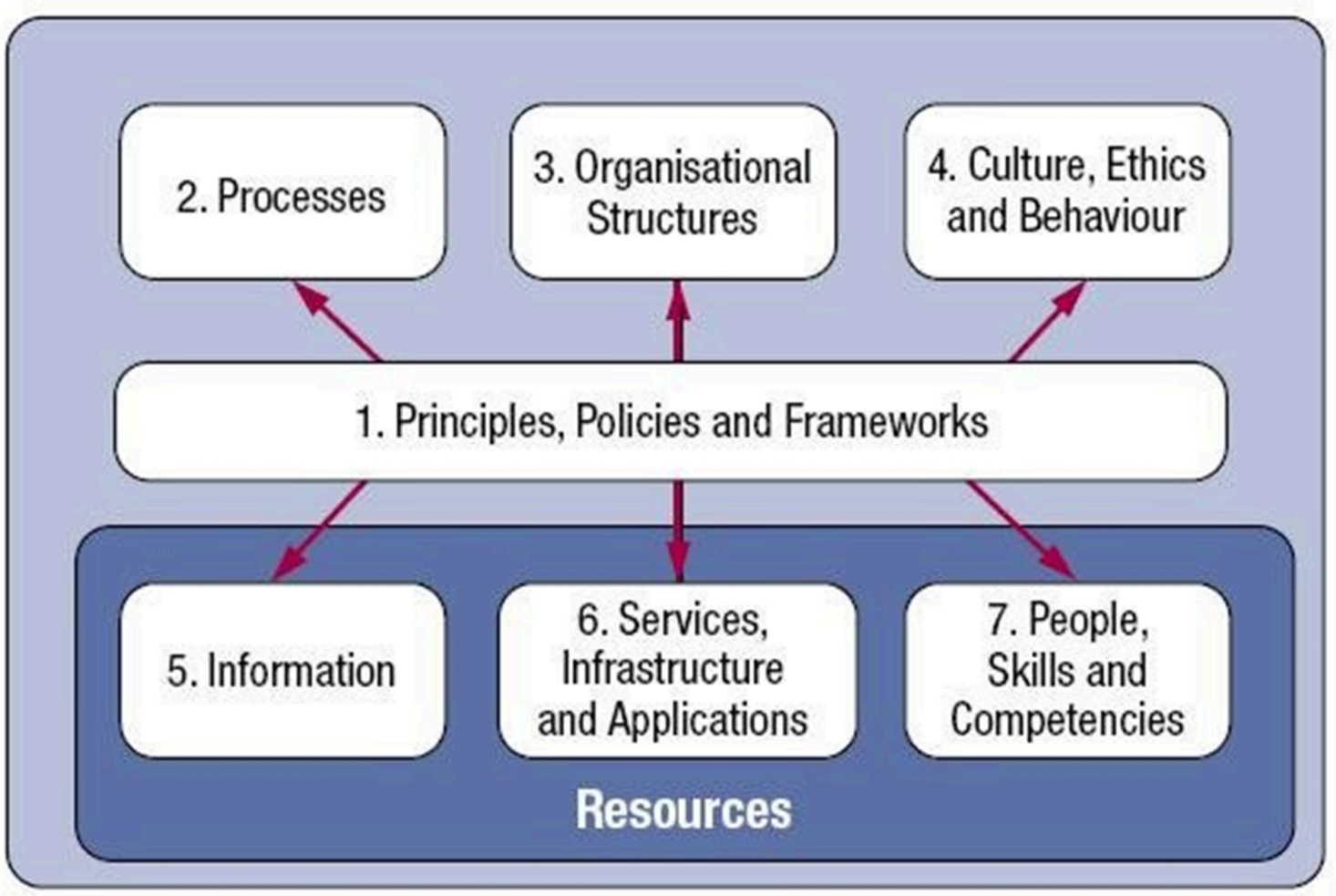

driver
Strategic alignment of IT with the Business
driver
Embedding accountability into the enterprise
Tata Kelola TI
Memberikan kontribusi **nilai** bagi bisnis
Mengurangi **resiko** TI


Computer Audit
IT Governance
Information Security Management
IT Risk Management

COBIT 5


Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI010 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

Seven enablers of COBIT



COBIT 5 dan Audit SI

- Audit sistem informasi lebih terkait dengan EDM – Evaluate, Direct, and Monitor.
- Fokusnya: governance dan monitoring TI untuk memastikan sistem informasi mendukung tujuan bisnis dan mematuhi regulasi.

- **EDM02 – Ensure Benefits Delivery → memastikan TI memberikan manfaat sesuai tujuan.e)**
- **EDM03 – Ensure Risk Optimization → memastikan risiko yang terkait TI diawasi dan dikendalikan.**

COBIT 5 dan Risk Assessment

Risk assessment lebih teknis dan operasional, biasanya masuk dalam domain APO – Align, Plan, and Organize.

APO12 – Manage Risk

- **Identifikasi risiko TI**
- **Analisis dan evaluasi risiko**
- **Penentuan mitigasi risiko**
- **Monitoring risiko secara berkelanjutan**

TERIMA KASIH

Studi Kasus

Sebuah perusahaan jasa keuangan menggunakan sistem informasi berbasis web untuk melayani nasabahnya, mulai dari pembukaan rekening, transaksi online, hingga laporan keuangan bulanan. Dalam proses audit internal, auditor menemukan beberapa temuan berikut:

- Tidak ada prosedur backup data harian yang terdokumentasi dengan baik.
- Beberapa akses administrator masih menggunakan password default.
- Laporan transaksi nasabah dapat diakses oleh staf yang tidak berhubungan langsung dengan bagian keuangan.
- Perusahaan belum melakukan penilaian risiko (risk assessment) secara formal terkait sistem informasi.

Pertanyaan

1. Identifikasi risiko-risiko utama yang dihadapi perusahaan dari kasus di atas.
2. Tentukan risiko mana yang termasuk high, medium, atau low risk, dan berikan alasan.
3. Sebagai auditor, langkah apa yang sebaiknya direkomendasikan untuk memperbaiki kondisi tersebut?
4. Metode penilaian apa yang digunakan untuk penentuan proses audit tersebut?
5. Jelaskan hubungan temuan tersebut dengan COBIT 5 domain terkait.

Aturan Pengumpulan Tugas

1. Tugas dijelaskan dengan cara penyampaian masing-masing individu dan dikumpulkan dalam bentuk video (sertakan referensi jurnal terkait di akhir video)
2. Tugas diupload di youtube atau media sosial masing-masing
3. Pengumpulan dalam bentuk link
4. Batas maksimum pengumpulan Jum'at, 2 Oktober 2025 jam 12.00 WIB melalui ilmu2.upnjatim.a.id