Audit Sistem Informasi

Minggu 4

Ice Breaking: Audit Detective

- Tujuan: Melatih mahasiswa berpikir cepat tentang risiko & fokus audit.
- Format: Kelompok (4–5 kelompok).

Kasus 1

Sebuah bank sering kehilangan data transaksi nasabah, namun manajemen mengklaim sistem backup selalu berjalan.

Pertanyaan: Bagian mana yang harus diaudit terlebih dahulu? (*hint: kaitkan dengan MK yang telah dipelajari*)

Jawaban:

Proses backup & recovery data, termasuk validasi log dan kontrol akses.

(apakah prosedur dijalankan, diuji, dan sesuai kebijakan).

Tambahan yang bisa diperiksa: disaster recovery plan & integrity check.

COBIT Reference:

Cobit 4.1

- DS4 – Ensure Continuous Service
- DS11 – Manage Data

Cobit 5 & Cobit 2019

- DSS04 – Manage Continuity (kelangsungan layanan & backup)
- DSS01 – Manage Operations (operasional harian, termasuk log & monitoring)

ISO/IEC 27001:2022 Annex A

- A.5.28 Backup
- A.5.12 Data retention
- A.5.15 Access control

Kasus 2

Perusahaan retail online mengalami serangan siber berulang, tetapi tim TI mengaku firewall sudah aktif.

Pertanyaan: Fokus audit utama apa?

Jawaban:

Audit keamanan jaringan & konfigurasi firewall, termasuk uji penetrasi (penetration testing).

Serangan berulang menunjukkan kontrol keamanan jaringan mungkin lemah (misconfig, update patching, IDS/IPS tidak berjalan).

COBIT Reference:

Cobit 4.1

- DS5 – Ensure Systems Security

Cobit 5 & Cobit 2019

- DSS05 – Manage Security Services
- BAI09 – Manage Assets (termasuk konfigurasi perangkat keamanan)

ISO/IEC 27001:2022 Annex A

- A.8.16 Network security
- A.8.23 Configuration management
- A.8.28 Vulnerability management

Kasus 3

Sistem ERP baru dibeli, tetapi karyawan banyak yang mengeluh sulit digunakan dan produktivitas menurun.

Pertanyaan: Apa yang harus diaudit?

Jawaban:

Audit kesesuaian sistem (usability & user training) + evaluasi strategic alignment.

Yang diperiksa:

- Usability (apakah antarmuka sesuai kebutuhan user).
- User training & change management.
- Strategic alignment → masih bisa diperdebatkan, tapi relevan karena ERP seharusnya mendukung proses bisnis.

COBIT Reference:

Cobit 4.1

- PO7 – Manage IT Human Resources
- AI7 – Install & Accredit Solutions

Cobit 5 & Cobit 2019

- APO07 – Manage Human Resources (skill & training)
- BAI08 – Manage Knowledge (transfer pengetahuan pengguna)
- APO02 – Manage Strategy (kesesuaian strategi bisnis dan SI/TI)

ISO/IEC 27001:2022 Annex A

- A.6.3 Security awareness & training
- A.5.9 Inventory of assets
- A.5.1 Information security policies

Kasus 4

Perusahaan klaim uptime server 99,9%, namun laporan bulanan menunjukkan sering terjadi downtime.

Pertanyaan: Audit diarahkan ke mana?

Jawaban:

Audit SLA & kinerja infrastruktur (performance measurement), uptime report, dan reliability infrastruktur.

COBIT Reference:

Cobit 4.1

- DS3 – Manage Performance & Capacity
- ME1 – Monitor & Evaluate IT Performance

Cobit 5 & Cobit 2019

- MEA01 – Monitor, Evaluate & Assess Performance and Conformance
- DSS01 – Manage Operations (availability & monitoring)

ISO/IEC 27001:2022 Annex A

- A.5.17 Information security continuity
- A.8.14 Capacity management
- A.5.36 Performance monitoring

Kasus 5 (opsional)

Startup menghabiskan anggaran besar untuk aplikasi mobile, tetapi jumlah pengguna sangat rendah.

Pertanyaan: Bagian mana yang diaudit?

Jawaban:

Audit value delivery & efektivitas investasi TI.

--> apakah investasi TI memberikan manfaat bisnis (IT Value Delivery / Benefit Realization).

COBIT Reference:

Cobit 4.1

- PO5 – Manage the IT Investment
- ME1 – Monitor & Evaluate IT Performance

Cobit 5 & Cobit 2019

- EDM02 – Ensure Benefits Delivery
- APO05 – Manage Portfolio (manajemen investasi SI/TI)

ISO/IEC 27001:2022 Annex A

- A.5.1 Information security policies
- (jika app berbasis cloud → A.5.37 Cloud services security)

Studi kasus diatas tidak eksklusif hanya bisa dijawab dengan COBIT.

COBIT (5/2019) → memberi kerangka governance & manajemen TI/SI. Lebih ke arah strategis: bagaimana IT selaras dengan bisnis, value delivery, manajemen risiko, dan kontrol pada level proses.

ISO/IEC 27001 → memberi kerangka kontrol keamanan informasi (Annex A). Lebih ke arah operasional & teknis: apa kontrol spesifik yang harus ada untuk melindungi aset informasi, misalnya backup, firewall, pelatihan user, dll.

Kedua framework bisa dipakai untuk menjawab kasus yang sama, hanya dari perspektif yang berbeda:

COBIT → menjawab “apakah proses governance & manajemen sudah tepat?”

ISO 27001 → menjawab “apakah kontrol keamanan yang spesifik sudah diterapkan & efektif?”

Mapping Singkat

COBIT 4.1

- PO (Plan & Organise)
- AI (Acquire & Implement)
- DS (Deliver & Support)
- ME (Monitor & Evaluate)

COBIT 5 / COBIT 2019

- APO (Align, Plan & Organise)
- BAI (Build, Acquire & Implement)
- DSS (Deliver, Service & Support)
- MEA (Monitor, Evaluate & Assess)
- EDM (Evaluate, Direct & Monitor) (domain governance baru)