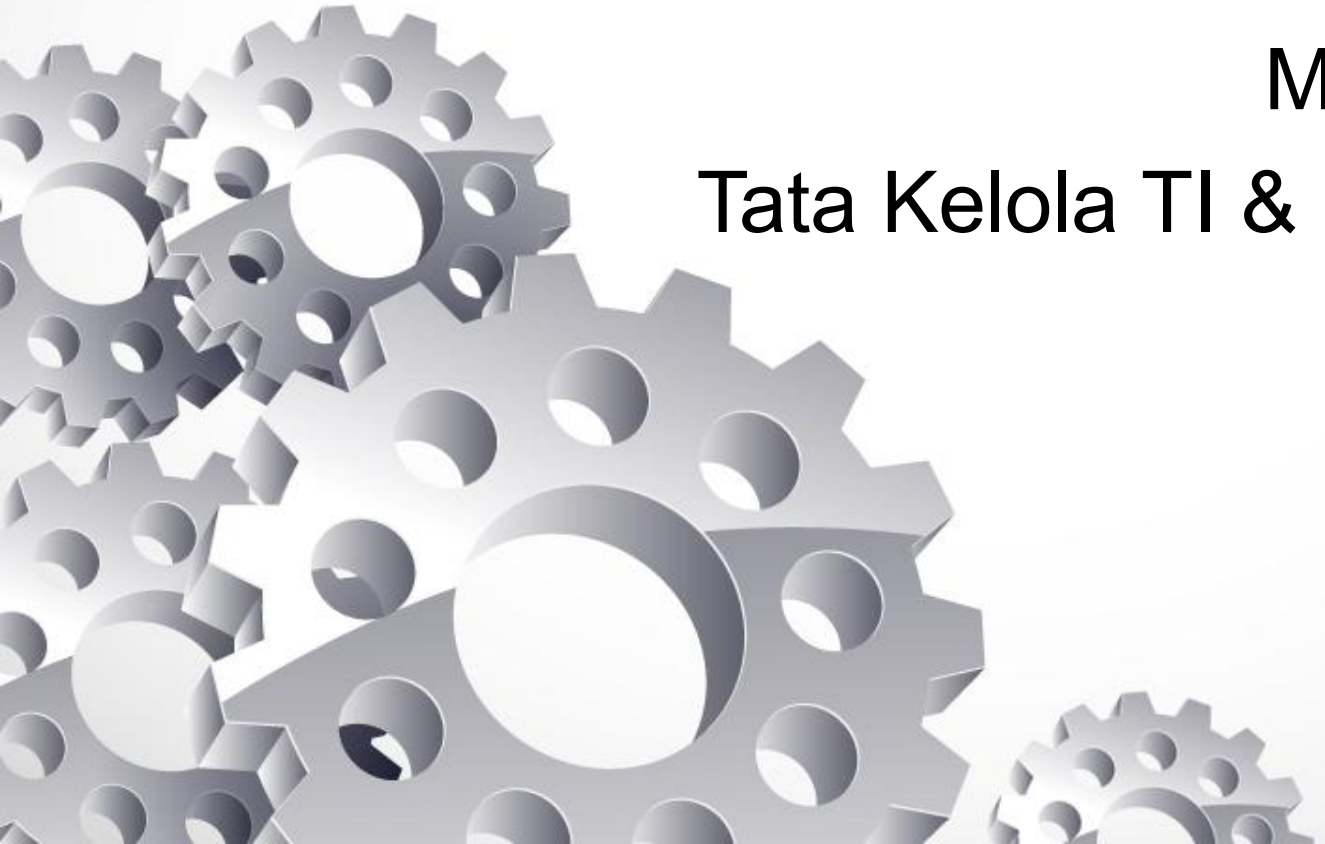
# Audit Sistem Informasi

## Minggu ke-4:
## Tata Kelola TI & Risiko SI/TI



# Pengantar

- Tata kelola TI = mekanisme untuk memastikan penggunaan TI mendukung strategi & tujuan organisasi
- Risiko SI/TI = potensi kerugian akibat kegagalan sistem, penyalahgunaan, atau pengelolaan TI yang buruk

# Elemen Utama Tata Kelola TI

1. Strategic Alignment
2. Value Delivery
3. Risk Management
4. Resource Management
5. Performance Measurement

# 1. Strategic Alignment

- Menyelaraskan strategi TI dengan strategi bisnis
- Contoh: investasi ERP mendukung efisiensi rantai pasok

# 2. Value Delivery

- Memastikan TI memberikan manfaat nyata (efisiensi, inovasi, keunggulan kompetitif)
- Contoh: sistem e-commerce meningkatkan penjualan 20%

# 3. Risk Management

- Mengidentifikasi, menilai, dan mengendalikan risiko TI
- Contoh: mitigasi risiko serangan siber dengan firewall & audit berkala

# 4. Resource Management

- Optimalisasi penggunaan SDM TI, aplikasi, infrastruktur, data
- Contoh: cloud computing untuk efisiensi kapasitas server

# 5. Performance Measurement

- Mengukur kinerja TI menggunakan KPI, SLA, atau balanced scorecard
- Contoh: target uptime sistem 99,9% per tahun

# Governance & Risiko SI/TI

- Governance baik → risiko terkelola → TI mendukung bisnis
- Governance lemah → risiko tinggi → kerugian finansial & reputasi
- Contoh kasus: gagal proyek TI → cost overrun → reputasi jatuh

# Proses Audit SI

1. Memahami Program Audit
2. Melaksanakan Audit Khusus
3. Penilaian Risiko Audit
4. Menentukan Audit Dimungkinkan
5. Melakukan Audit
6. Mengumpulkan Bukti Audit
7. Pengujian Bukti Audit
8. Melaporkan Temuan
9. Tindak Lanjut (Closing Meeting)

# 1. Memahami Program Audit

- Audit program = rencana menyeluruh audit SI
- Berisi ruang lingkup, tujuan, metodologi, jadwal
- Contoh: Audit ERP di perusahaan manufaktur

# 2. Melaksanakan Audit Khusus

- Audit spesifik sesuai isu tertentu
- Fokus: keamanan, kepatuhan, kinerja
- Contoh: Audit kepatuhan POJK (Peraturan Otoritas Jasa Keuangan) pada bank

# 3. Penilaian Risiko Audit

- Identifikasi risiko → analisis → prioritas
- Contoh: Risiko terbesar = kehilangan data pelanggan
- Fokus audit: backup & enkripsi data

# 4. Menentukan Audit Dimungkinkan

- Menilai ketersediaan data, SDM, akses
- Audit bisa ditunda jika bukti tidak tersedia
- Contoh: Vendor cloud tidak beri akses log penuh

# 5. Melakukan Audit

- Eksekusi audit sesuai rencana
- Teknik: pemeriksaan dokumen, wawancara, observasi, uji sistem
- Contoh: Audit kinerja server vs SLA

# 6. Mengumpulkan Bukti Audit

- Bukti: dokumentasi, log sistem, wawancara, observasi
- Contoh: Log login user tunjukkan 3 percobaan akses ilegal

# 7. Pengujian Bukti Audit

- Uji keandalan bukti (valid, akurat, lengkap)
- Metode: compliance testing & substantive testing
- Contoh: Cek 30 sampel transaksi → tidak ada manipulasi

# 8. Melaporkan Temuan

- Laporan berisi temuan, risiko, rekomendasi
- Contoh: Audit ERP → kelemahan kontrol akses
- Rekomendasi: role-based access

# 9. Tindak Lanjut (Closing Meeting)

- Diskusi dengan manajemen
- Sepakati tindakan korektif
- Contoh: tambah firewall + training keamanan siber

# Studi Kasus Mini

Perusahaan e-commerce sering downtime saat promo besar

→ Lakukan audit infrastruktur TI

# Studi Kasus: Langkah Audit

1. Program audit → infrastruktur TI
2. Audit khusus → kapasitas server
3. Risiko utama → kehilangan penjualan
4. Audit dimungkinkan → data log tersedia
5. Melakukan audit → review konfigurasi & load balancing

# Studi Kasus: Bukti & Laporan

6. Bukti: log downtime 12 jam/bulan
7. Uji: simulasi traffic tinggi
8. Laporan: sistem tidak siap, perlu upgrade cloud

# Studi Kasus: Closing Meeting

9. Closing meeting → migrasi ke cloud elastis

→ TI lebih siap hadapi lonjakan traffic


thank you