

MODUL PRAKTIKUM
MATA KULIAH
AUDIT SISTEM INFORMASI



PERCOBAAN IV

PRODI S1 SISTEM INFORMASI
JURUSAN TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS TADULAKO
TAHUN
2025

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat saat ini membawa dampak signifikan terhadap hampir semua sektor kehidupan, termasuk di bidang pendidikan. Sistem informasi digunakan untuk mendukung berbagai proses operasional dan pengambilan keputusan yang lebih efektif. Namun, seiring dengan meningkatnya ketergantungan terhadap teknologi, risiko yang berkaitan dengan sistem informasi juga semakin kompleks. Risiko-risiko tersebut dapat mencakup gangguan operasional, kerugian finansial, hingga ancaman terhadap keamanan data. Dalam konteks ini, audit sistem informasi berfungsi sebagai sarana untuk menilai keandalan dan efektivitas sistem informasi, serta untuk memastikan bahwa sistem tersebut dapat mendukung pencapaian tujuan organisasi dengan baik. Namun, proses audit seringkali dihadapkan pada tantangan, seperti ketidaktahuan mengenai potensi risiko yang ada dan kurangnya pengetahuan dalam penanganan masalah teknis yang terkait dengan sistem informasi.

Latar belakang tidak akan berubah dari modul 1-akhir, jadi buatlah sehalaman full untuk latar belakangnya

1.2 Tujuan

1.2.1 Pengenalan Audit SI: Analisis Risiko

1.2.2 Kerangka Audit SI: Framework, Risk Analysis, dan Audit Planning

1.2.3 Audit Keamanan SI: Penerapan Teknik Audit Dalam Pemeriksaan Autentikasi Dan Enkripsi

1.2.4 Audit Sistem Informasi: Pelaporan Hasil dan Evaluasi Kepatuhan

1. Menyusun laporan audit sistem informasi secara sistematis dan profesional.

2. Melakukan evaluasi kepatuhan (compliance evaluation) terhadap kebijakan dan standar industri seperti COBIT dan ISO/IEC 27001.
3. Mengidentifikasi temuan audit serta menyusun rekomendasi perbaikan yang relevan dan aplikatif.
4. Menyajikan hasil audit dalam bentuk laporan yang dapat digunakan oleh manajemen organisasi.

1.3 Alat dan Bahan

1.3.1 Pengenalan Audit SI: Analisis Resiko

1.3.2 Kerangka Audit SI: Framework, Risk Analysis, dan Audit Planning

1.3.3 Audit Keamanan SI: Penerapan Teknik Audit dalam Pemeriksaan Autentikasi dan Enkripsi

1.3.4 Audit Sistem Informasi: Pelaporan Hasil dan Evaluasi Kepatuhan

1. PC/Laptop
2. *Microsoft Word*
3. *Microsoft Excel*
4. Modul Praktikum

BAB II

LANDASAN TEORI

2.1 Teori Dasar

2.1.1 Pengenalan Audit SI: Analisis Resiko

2.1.2 Kerangka Kerja Audit SI: Framework, Risk Analysis, dan Audit Planning

2.1.3 Audit Keamanan SI: Penerapan Teknik Audit dalam Pemeriksaan Autentikasi dan Enkripsi

2.1.4 Audit Sistem Informasi: Pelaporan Hasil dan Evaluasi Kepatuhan

1. Pelaporan Audit Sistem Informasi

Pelaporan audit sistem informasi adalah tahap akhir dalam proses audit sistem informasi yang bertujuan untuk menyampaikan hasil audit secara formal kepada manajemen atau pihak terkait.

Laporan audit memiliki fungsi untuk mengkomunikasikan temuan audit, yaitu kelemahan atau ketidaksesuaian dalam sistem. Menyediakan bukti objektif atas hasil pemeriksaan. Memberikan rekomendasi perbaikan terhadap kontrol atau kebijakan TI.

Struktur umum laporan audit:




- a. Halaman judul
- b. Ringkasan eksekutif
- c. Latar belakang audit
- d. Tujuan dan ruang lingkup
- e. Metodologi audit
- f. Temuan audit
- g. Evaluasi kepatuhan
- h. Rekomendasi perbaikan
- i. Kesimpulan dan tindak lanjut

2. Evaluasi Kepatuhan (Compliance Evaluation)

Evaluasi kepatuhan adalah proses untuk menilai sejauh mana sistem informasi mematuhi standar atau kebijakan yang berlaku, baik internal maupun eksternal.

Framework yang umum digunakan seperti, COBIT (Control Objectives for Information and Related Technology) berfokus pada tata kelola TI dan pengendalian proses bisnis. ISO/IEC 27001 berfokus pada sistem manajemen keamanan informasi (Information Security Management System / ISMS).

Langkah-langkah evaluasi kepatuhan:

- a. Menentukan standar atau kontrol yang akan dievaluasi.
 - b. Membandingkan kondisi aktual sistem dengan standar tersebut.
 - c. Memberikan status penilaian:
 - 1)  *Compliant*
 - 2)  *Partially Compliant*
 - 3)  *Non-Compliant*
 - d. Memberikan rekomendasi untuk peningkatan kepatuhan.
- ## 3. Hubungan Pelaporan dan Evaluasi Kepatuhan

Evaluasi kepatuhan merupakan bagian penting dari pelaporan audit, karena menunjukkan apakah sistem telah memenuhi standar yang diacu. Temuan dari evaluasi kepatuhan digunakan untuk menyusun bagian temuan audit dan *rekomendasi perbaikan* dalam laporan akhir.

BAB III

PROSEDUR KERJA

3.1 Langkah Kerja

3.1.1 Pengenalan Audit SI: Analisis Resiko

3.1.2 Kerangka Kerja Audit SI: Framework, Risk Analysis, dan Audit Planning

3.1.3 Audit Keamanan SI: Penerapan Teknik Audit dalam Pemeriksaan Autentikasi dan Enkripsi

3.1.4 Audit Sistem Informasi: Pelaporan Hasil dan Evaluasi Kepatuhan




1. Persiapan

- a. Siapkan hasil audit dari pertemuan sebelumnya (misalnya audit keamanan sebuah sistem).
- b. Tentukan framework yang akan digunakan (COBIT atau ISO 27001).
- c. Siapkan template laporan audit dan tabel evaluasi kepatuhan.

2. Evaluasi Kepatuhan

- a. Buat tabel compliance checklist dengan kolom berikut:

No	Kontrol/Domain	Deskripsi Standar	Kondisi Saat Ini	Status	Rekomendasi
1					

- b. Isi tabel berdasarkan hasil audit yang telah dilakukan:
 - 1) Bandingkan kondisi sistem dengan kontrol pada COBIT / ISO 27001.
 - 2) Tentukan status kepatuhan:
 - a)  *Compliant* → sesuai standar
 - b)  *Partially Compliant* → sebagian sesuai
 - c)  *Non-Compliant* → belum sesuai sama sekali
 - 3) Tuliskan rekomendasi perbaikan untuk setiap poin yang tidak sesuai.

3. Penyusunan Laporan Audit

- a. Buat dokumen laporan dengan struktur berikut:
 - 1) Halaman Judul
 - 2) Ringkasan Eksekutif
 - 3) Latar Belakang & Tujuan Audit
 - 4) Metodologi Audit
 - 5) Temuan Audit
 - 6) Hasil Evaluasi Kepatuhan (sertakan tabel compliance)
 - 7) Rekomendasi Perbaikan
 - 8) Kesimpulan dan Tindak Lanjut
- b. Gunakan hasil dari tabel kepatuhan dan temuan audit untuk memperkuat bagian rekomendasi.
- c. Pastikan laporan disusun dengan bahasa profesional dan objektif.

4. Presentasi Singkat

- a. Setiap kelompok mempresentasikan hasil laporan audit (maksimal 10 menit).
- b. Asisten dan rekan mahasiswa memberikan umpan balik atas struktur laporan dan rekomendasi yang diajukan.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Hasil dan Pembahasan

4.1.1 Pengenalan Audit SI: Analisis Resiko



4.1.2 Kerangka Kerja Audit SI: Framework, Risk Analysis, dan Audit Planning

4.1.3 Audit Keamanan SI: Penerapan Teknik Audit dalam Pemeriksaan Autentikasi dan Enkripsi

4.1.4 Audit Sistem Informasi: Pelaporan Hasil dan Evaluasi Kepatuhan

1. Laporan audit sistem informasi lengkap yang mencakup temuan audit, evaluasi kepatuhan, dan rekomendasi perbaikan.
2. Tabel compliance checklist yang menunjukkan tingkat kepatuhan sistem terhadap standar acuan.

Contoh:

No	Kontrol / Domain	Kondisi Saat Ini	Status	Rekomendasi
1	ISO 27001 A.9.2.1 – User Access Management	Akun admin ganda tanpa pembatasan peran	 Non-compliant	Terapkan pembatasan hak akses berdasarkan role
2	COBIT DSS05 Ensure System Security	Firewall aktif dan IDS tersedia	 Compliant	Lanjutkan monitoring berkala

BAB V

PENUTUP

5.1 Kesimpulan

5.1.1 Pengenalan Audit SI: Analisis Resiko

5.1.2 Kerangka Kerja Audit SI: Framework, Risk Analysis, dan Audit Planning

5.1.3 Audit Keamanan SI: Penerapan Teknik Audit dalam Pemeriksaan Autentikasi dan Enkripsi

5.1.4 Audit Sistem Informasi: Pelaporan Hasil dan Evaluasi Kepatuhan

Seperti biasa dibuat minimal 5 baris (1paragraf)

DAFTAR PUSTAKA

Minimal 3 sumber dakpus