INSTITUT TEKNOLOGI PLN

Teknik Kontrol dan Audit Sistem Informasi

Oleh

Esa Firmansyah M

Menara PLN Jl.Lingkar luar barat, Duri Kosambi
website: ften.itpln.ac.id

Learning Objectives

Agar mahasiswa mampu melakukan proses pengumpulan data dan pengevaluasian bukti-bukti untuk menentukan :
1. apakah suatu sistem aplikasi dan komponen pendukungnya telah menetapkan dan menerapkan sistem pengendalian internal yang memadai
2. Semua aktivitas dilindungi dengan baik serta terjaminnya integritas data, keandalan
3. prosesnya dilakukan secara efektif dan efisien.

Sistem Penilaian dan Materi Kuliah

Sistem Penilaian

Kuis	30%
UTS	25%
UAS	25%
Project	20%
	--------- +
Total	100%

Kehadiran minimal 80%

Semua Bahan mengacu kepada buku :
CISA Review Manual 27th Edition

Materi Perkuliahan

1. Penjelasan Silabus dan Overview dari Audit Sistem Informasi.
2. Proses Audit Sistem Informasi.
3. Tata kelola Teknologi Informasi.
4. Siklus Hidup Pengembangan Aplikasi.
5. Layanan TI dan Infrastruktur.
6. Perlindungan Aset Informasi.
7. Teknik pemilihan sampling dan analisanya.
8. Computer Assisted Audit Tools (CAAT): Generalized Audit software serta pengenalan tools ACL.
9. Data Manipulation dan Data Analysis menggunakan CAAT dan Excel.
10. Case Study: Audit Sistem Operasi.
11. Case Study: Audit Jaringan.
12. Case Study: Audit Aplikasi dan Basis Data.
13. Case Study: Audit Pengembangan Sistem.
14. Trend dalam IS/IT Audit dan Review Jurnal.

INSTITUT TEKNOLOGI PLN

PERTEMUAN KE- 1

Proses Audit

Apa itu Audit SI ?

Information system auditing is the formal evaluation of information systems to ensure they comply with relevant laws, regulations, governance frameworks, and the strategic objectives of an organization

Financial Auditing

Focus Area:

This type of audit primarily assesses the financial health and performance of an organization.

Information System Auditing

Scope:

Concentrates on the evaluation of systems, processes, and procedures related to information technology.

Purpose

Core Focus Areas:

The primary aim of an information system audit is to guarantee system security. This encompasses three critical aspects of data management:

Confidentiality: Ensuring that sensitive information is accessible only to authorized individuals.

Integrity: Safeguarding the accuracy and completeness of data.

Availability: Making sure that data and systems are accessible when needed.

Importance of Information System Auditing

Certification and Compliance

Regulatory Significance:

Conducting information system audits is essential for organizations seeking certifications such as ISO 27000 or PCIDSS. These certifications are crucial for meeting regulatory and compliance standards that govern business operations.

Audits provide a mechanism for validating the claims made by management to stakeholders, thus ensuring that the organization is fulfilling its regulatory and operational responsibilities

Internal vs. External Audits

Internal Audits:

Conducted by teams within the organization to assess internal controls and processes.

External Audits:

Performed by independent thirdparty auditors to provide an objective assessment of the organization’s systems and compliance.

Qualified Professionals

Audit Authority:

Information system auditors are certified professionals who possess the skills to assess, plan, and implement audit missions effectively.

Team Composition

Diverse Skill Sets:

Audits are executed by a multidisciplinary team that combines various skills to identify potential risks and control measures.

Avoiding Conflicts of Interest

Maintaining Objectivity:

Auditors must refrain from auditing their own work or undertaking operational roles to preserve the integrity of the audit process.

Audit Process and Practices

Scope of Audit

Comprehensive Review:

Audits involve examining various elements such as systems, processes, change management, access controls, human resources processes, and compliance with security standards.

Conflict of Interest

Transparency in Auditing:

Auditors are required to avoid conflicts by not reviewing areas where they have previously been involved and must openly communicate any potential conflicts that may arise.

Business Objectives and Strategy

Strategic Alignment:

Auditors must have a clear understanding of the organization's mission and strategic objectives to effectively assess compliance and the overall status of information systems.

These enriched takeaways provide a thorough understanding of the essential components, significance, and practices related to information system auditing, highlighting its role in ensuring organizational integrity and compliance.

Audit Siklus

Source: ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016

Dilakukan dengan :

1. memegang prinsip Kode Etik Auditor
2. Memahami proses bisnis
3. Komunikasi yang baik dengan para auditee

Audit Planning

Figure 1.2—Steps to Perform Audit Planning

- Gain an understanding of the organization's mission, objectives, purpose and processes, which include information and processing requirements such as availability, integrity, security, and business technology and information confidentiality.
- Gain an understanding of the organization's governance structure and practices related to the audit objectives.
- Understand changes in the business environment of the auditee.
- Review prior work papers.
- Identify stated contents such as policies, standards and required guidelines, procedures, and organization structure.
- Perform a risk analysis to help in designing the audit plan.
- Set the audit scope and audit objectives.
- Develop the audit approach or audit strategy.
- Assign personnel resources to the audit.
- Address engagement logistics.

Audit Planning