

AUDIT IT adalah proses sistematis mengumpulkan dan mengevaluasi bukti untuk menemukan secara independen dan obyektif, apakah suatu sistem informasi telah dapat melindungi aset, menjaga integritas data dan memungkinkan tujuan organisasi tercapai secara efektif dengan menggunakan sumber daya secara efisien dan **mematuhi peraturan yang berlaku**.

TUJUAN AUDIT TI :

- Mengamankan** Asset
- Menjaga **Integritas** data
- Menjaga **efektivitas** dan **efisiensi** sistem

TARGET AUDIT :

- AVAILABILITY** (Ketersediaan informasi)
- CONFIDENTIALITY** (Kerahasiaan informasi)
- INTEGRITY** (Keakuratan dan ketepatan waktu)
- RELIABILITY** (Keandalan)

KEUNTUNGAN AUDIT :

- Menilai **keefektifitas** aktivitas dokumentasi dalam organisasi
- Memonitor **kesesuaian** dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
- Mengukur** tingkat keefektifitas dari sistem
- Mengidentifikasi kelemahan** di sistem yang mungkin mengabaikan ketidaksesuaian di masa datang
- Menyediakan** informasi untuk proses peningkatan
- Mengingatn **saling memahami** antar departemen dan antar individu
- Melaporkan** hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen

ALASAN DIPERLUKANNYA AUDIT :

- Agar tidak terjadi **kerugian kehilangan** data
- Agar tidak terjadi **kesalahan pengambilan keputusan**
- Resiko **kebocoran** data
- Penyalahgunaan** komputer
- Kerugian** kesalahan dalam proses perhitungan
- Tingginya nilai **investasi** hardware dan software

FUNGSI AUDIT (DALAM IT)

a. System and Application Audit

Audit terhadap sistem terdokumentasi untuk memastikan sudah **memenuhi standar** nasional atau internasional

b. Compliance Audit

Untuk **menguji efektivitas** implementasi dari kebijakan prosedur, kontrol dan unsur hukum yang lain

c. Product / Service Audit

Untuk **menguji** suatu produk atau layanan telah sesuai seperti spesifikasi yang telah ditentukan dan cocok digunakan

d. Information Processing Facilitis

Audit terhadap **fasilitas** yang disediakan oleh organisasi. Contoh : Hardware.

e. System Development

Audit **kesesuaian** antara pengembangan sistem dengan perencanaan.

f. Management of IT and Enterprise Architecture

Audit kesesuaian sistem terhadap **struktur dan prosedur** yg ada.

g. Client/Server Telecommunication and Intranet / Extranet

Audit pada tingkat **pengendalian** proses komunikasi data.

JENIS AUDIT (SECARA UMUM)

- Compliance / Kepatuhan terhadap aturan yang berlaku
- Kinerja
- Kecurangan
- Sertifikasi

JENIS AUDIT TEKNOLOGI INFORMASI :

- Pendekatan umum pada audit SI,
- Audit aplikasi SI,
- Audit pengembangan SI
- Audit pusat layanan komputer

KONSEP AUDIT SISTEM INFORMASI YAITU :

- Audit melalui komputer (Audit through the computer)**
Pengujian terhadap proses dan sistemnya, biasa dg whitebox.
- Audit menggunakan komputer (Audit around the computer).**
Hanya memeriksa dari sisi user pada level input dan output
- Audit dengan komputer (**Audit with computer**).

IT AUDIT AREA :

- Planning** (Perencanaan)
- Organization and Management** (Pengelolaan)
- Policies and Procedures** (Peraturan yang berlaku)
- Security** (Keamanan)
- Regulation dan Standar** (Kebijakan dan SOP)

CAKUPAN AUDIT :

- Organizational Audit
- Internal Control Audit
- Information Technology Audit
- Information System Audit
- Security Control Audit

KOMPONEN YANG DIAUDIT :

- Business Process and Services
- Interface
- Application
- Databases
- Server Platform
- Network Infrastructure

PIHAK YANG DIAUDIT :

- Management
- IT Manager
- IT Specialist (network, database, analis, programmer,dll)
- User

AUDITOR IT

PRINSIP-PRINSIP SEORANG AUDITOR :

- Ethical conduct** (berdasarkan profesionalisme, kejujuran, integritas, kerahasiaan dan kebijakan)
- Fair Presentation** (kewajiban melaporkan secara jujur dan akurat
- Due profesional care** (implementasi dari kesungguhan dan pertimbangan yang diberikan)
- Independence**
- Evidence-base approach** (pendekatan berdasarkan fakta)

TUGAS DARI AUDITOR IT :

- Memastikan sisi-sisi penerapan IT memiliki kontrol yang diperlukan
- Memastikan kontrol tersebut diterapkan dengan baik sesuai yang diharapkan

YANG DILAKUKAN OLEH SEORANG AUDITOR IT :

- Persiapan
- Review Dokumen
- Persiapan kegiatan on-site audit
- Melakukan kegiatan on-site audit
- Persiapan, persetujuan dan distribusi laporan audit
- Follow Up Audit

TAHAPAN AUDIT TI :

- Perencanaan (**Planning**)
- Review Pendahuluan (**Studying and Evaluation Controls**)
- Pengujian (**Testing and Evaluating Controls**)
- Pengendalian
- Pelaporan (**Reporting**)
- Tindak Lanjut (**Follow Up**)

HASIL OUTPUT KEGIATAN AUDIT :

- Ruang Lingkup Audit
- Mekanisme Audit
- Temuan-temuan
- Ketidakesuaian
- Kesimpulan

JENIS BUKTI AUDIT :

- Bukti Fisik (Physical evidence).**
Secara umum diperoleh dari hasil pengamatan terhadap orang, properti atau peristiwa tertentu, bisa dalam bentuk foto, peta dan sebagainya.
- Bukti Kesalahan (testimonial evidence).**
Dapat berbentuk surat, pernyataan atau wawancara yang tidak bersifat konklusif karena merupakan pendapat seseorang.
- Bukti Dokumen (Documentary evidence).**
Merupakan bukti yang paling lazim dalam audit bisa berupa surat, perjanjian kontrak, perintah, memo dan berbagai jenis dokumen bisnis lainnya.
- Bukti Analitis (Analytical evidence).**
Hasil dari komputasi, perbandingan standar operasi di masa lalu atau operasi sejenisnya.

RISIKO DALAM SISTEM INFORMASI :

- Fraud** (kecurangan/manipulasi)
- Business Interruption** (ketidakamanan)
- Errors** (Kesalahan)
- Customer Dissatisfaction** (Kekecewaan pelanggan)
- Poor Public Image** (Citra buruk)
- Ineffective and inefficient use of Resource**

KARAKTERISTIK sistem yang baik meliputi atribut sebagai berikut :

- Accuracy (**Keakuratan**)
- Completeness (**Kelengkapan**)
- Economy (**Ekonomis**)
- Reliability (**Kehandalan**)
- Relevance (**Keterkaitan**)
- Simplicity (**Kesederhanaan / Mudah dimengerti**)
- Timeliness (**Ketepatan waktu**)
- Verifiability (**Dapat diverifikasi**)

PERATURAN DAN STANDAR YANG BIASA DIGUNAKAN :

COBIT
ISO /IEC 17799 dan BS7799
ISO 9000

STANDAR yang dapat diaplikasikan untuk audit IT terdiri dari 11 standar, yaitu

- S1 **Audit Charter** (Dokumen formal)
- S2 **Audit Independent** (Jujur dan tidak mudah dipengaruhi)
- S3 **Audit Profesional Ethic and Standard** (Berkode etik)
- S4 **Professional Competence** (Berkompetensi Profesional)
- S5 **Planning** (Adanya Perencanaan)
- S6 **Performance of Audit Work** (Berkinerja)
- S7 **Reporting** (Adanya Pelaporan)
- S8 **Follow Up Activity** (Adanya Tindak Lanjut)
- S9 **Irregularities and Irregular Act** (Tidak Menyimpang)
- S10 **IT Governance** (Adanya Tata Kelola TI)

S11 Use of Risk Assessment in Audit Planning (Penanganan Risiko)

KPI DAN KGI

KPI (Key Performance Indicator) mendefinisikan pengukuran yang menentukan seberapa baik proses teknologi informasi dilakukan. KPI mengukur tujuan aktivitas yang merupakan tindakan yang harus diambil untuk proses untuk mencapai proses yang efektif

KGI (Key Goal Indicator) mendefinisikan pengukuran yang menginformasikan kepada manajemen apakah suatu proses teknologi informasi telah mencapai kebutuhan bisnisnya,
- Ketersediaan informasi yang diperlukan
- Ketiadaan integritas dan risiko kerahasiaan
- Efisiensi biaya proses dan operasi
- Konfirmasi keandalan, efektifitas dan kepatuhan.

CAAT (COMPUTER ASSISTED AUDIT TOOLS)

Merupakan metode perolehan informasi, analisis program dan prosedur termasuk aplikasi yang mengatur, menggabungkan, mengekstrak dan menganalisis informasi.

ISACA (INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION)

Sebuah organisasi internasional yang berfokus pada tata kelola sistem informasi.

Sertifikasi profesional yang dikeluarkan ISACA diantaranya :

- Certified Information System Auditor (**CISA**)
- Certified Information Security Manager (**CISM**)
- Certified In the Governance of Enterprise IT (**CGEIT**)
- Control Objective for Information & Related Technology (**COBIT**) 5

FRAMEWORK COBIT

COBIT dibuat oleh **ISACA**, kemudian **dikembangkan** oleh **ITGI**. COBIT berfokus pada **Audit, Control** dan **Security Issues**.

KOMPONEN :

Executive, Summary, Framework, Control Objective, Audit Guidelines, Management Guideline, Control Practice.

Lingkup COBIT (4 Domain)

PERENCANAAN DAN ORGANISASI:

- pendefinisian framework manajemen TI
- Perencanaan strategis dan taktis
- Kebijakan prosedur dan instruksi kerja
- Manajemen Program, Manajemen Portofolio dan Manajemen proyek
- Pemantauan Kinerja

PENGADAAN DAN PENGEMBANGAN :

- SDLC
- Manajemen Proyek
- Pengadaan Barang dan Jasa

PENGANTARAN DAN DUKUNGAN:

- Manajemen Operasi
- Manajemen Layanan
- Manajemen Perubahan
- Disaster Recovery
- Manajemen Aset dan Konfigurasi

PENGAWASAN DAN EVALUASI:

- Kepatuhan dan Kesesuaian
- Manajemen Risiko TI
- Quality Assurance