Audit Sistem Informasi (DMHC2)

Oleh :Tim Dosen MK Pengantar Audit SI

Pengertian Audit IS,

- Proses **pengumpulan dan evaluasi bukti-bukti** untuk menentukan apakah sistem komputer yang digunakan telah dapat [1]:
  - melindungi aset milik organisasi,
  - mampu menjaga integritas data,
  - membantu pencapaian tujuan organisasi secara efektif,
  - menggunakan sumber daya yang dimiliki secara efisien.
- Audit SI ialah **proses mengumpulkan dan mengevaluasi fakta** untuk memutuskan **apakah sistem komputer** yang merupakan aset bagi perusahaan **terlindungi**, **integritas data terpelihara**, **sesuai dengan tujuan organisasi** untuk **mencapai efektifitas dan efisiensi dalam penggunaan sumber daya** [2]
- Audit SI/TI merupakan **upaya menilai apakah proses IT sudah dilakukan dengan baik** untuk **mendukung tujuan organisasi** dengan **melakukan pengendalian dari outcome yang dihasilkan**. [3]

Pengertian Audit IS,

Audit Sistem Informasi adalah sebuah **proses yang sistematis** dalam **mengumpulkan dan mengevaluasi bukti-bukti** untuk **menentukan** bahwa sebuah **sistem informasi** yang digunakan oleh **organisasi** telah dapat **mencapai tujuannya**, antara lain: [4]

- Pengamanan atas aktiva (asset).
- Pemeliharaan atas integritas data.
- Peningkatan Efektifitas

Pentingnya Audit IS

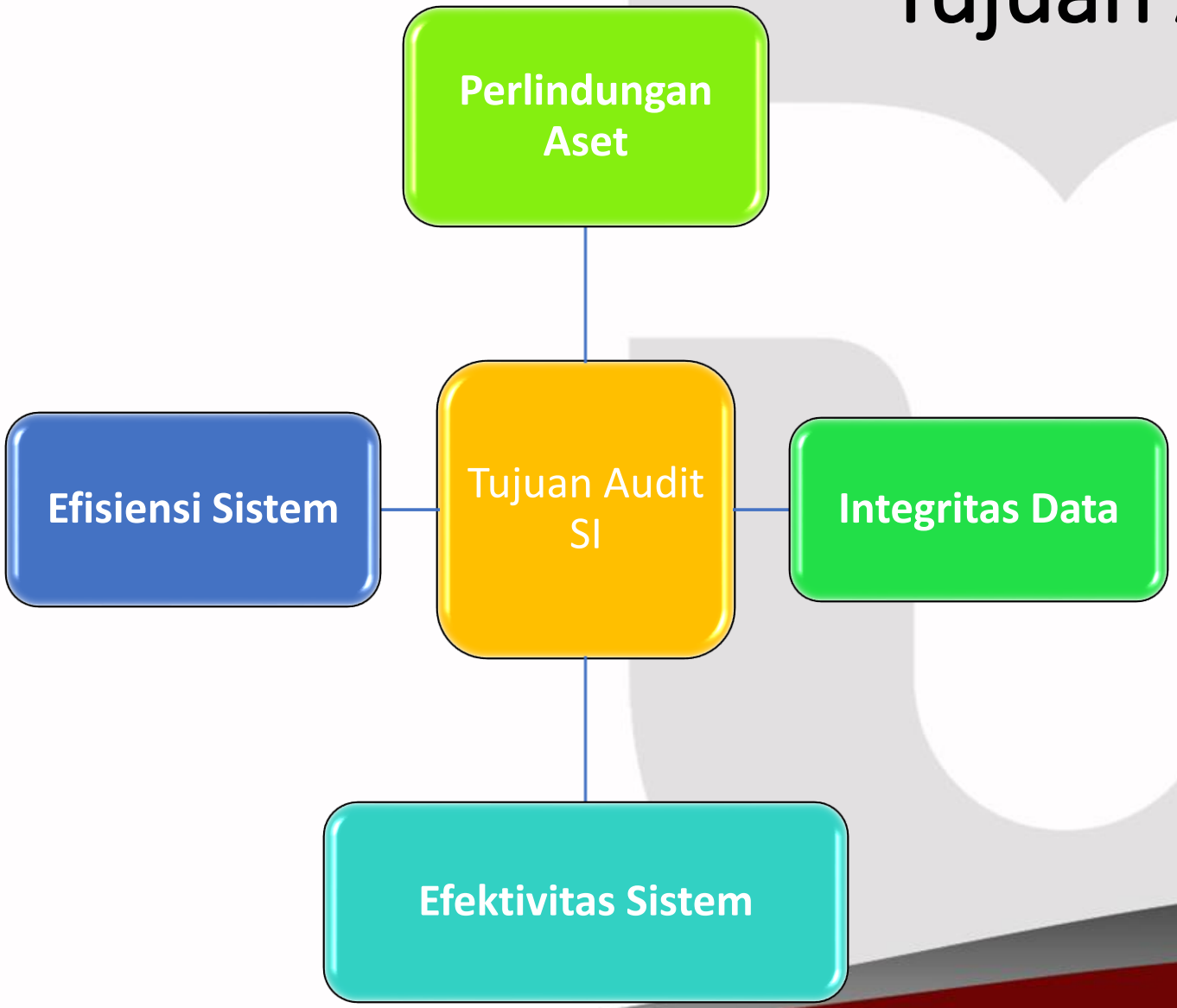
Audit Sistem Informasi merupakan hal yang penting bagi sebuah organisasi untuk dapat menghindari:

- Kerugian akibat kehilangan data
- Kerugian akibat kesalahan pemrosesan computer
- Pengambilan keputusan yang salah akibat informasi yang salah
- Kerugian karena penyalahgunaan komputer (Computer Abused)
- Nilai hardware, software dan personil sistem informasi
- Pemeliharaan kerahasiaan informasi

Penyalahgunaan komputer

Tipe	Jenis
• Hacking • Virus • Illegal Physical Access • Abuse of Privileges	• Destruction of asset (perusakan aset) • Theft of asset (pencurian aset) • Modification of asset (modifikasi aset) • Privacy violation (pelanggaran privasi) • Disruption of Operations (pengacauan operasi) • Unauthorized use of asset (penyalahgunaan otorisasi aset) • Physical harm to personnel (kejahatan fisik terhadap personal)

Tujuan Audit SI [2]



Tujuan Audit SI [2]

- **Perlindungan Aset**
  - Aset SI didalam organisasi adalah HW, SW, fasilitas, user (konwledge), file data, dokumentasi sistem dan persediaan barang. Sebaiknya semua aset harus dilindungi oleh sistem pengendalian internal.
- **Integritas Data**
  - Integritas data ialah konsep dasar didalam audit SI. Jika integritas data tidak dipelihara, maka organisasi tidak akan mendapatkan represntasi data yang benar untuk suatu aktifitas, akibatnya organisasi tidak dapat berkompetisi dan data tidak dapat digunakan untuk pengabilan keputusan yang valid.
- **Efektivitas Sistem**
  - Audit sering dilakukan setelah sistem berjalan untuk beberapa waktu. Manajemen membutuhkan hasil efektivitas untuk mengambil keputusan apakah system informasi terus dijalankan atau dihentikan sementara untuk proses modifikasi.
- **Efisiensi Sistem**
  - Efisiensi SI dilakukan dengan cara menggunakan sumber daya minimum untuk menyelesaikan suatu tujuan objek. Variasi sumber daya terdiri dari mesin, waktu, peripheral, S/W sistem dan pekerja.

Tujuan dari perlindungan aset, integritas data, efektivitas sistem dan efisiensi sistem dapat dicapat dengan baik jika **manajemen organisasi meningkatkan sistem pengendalian internalnya**.

Aspek Audit SI

Jika melihat tujuan Audit Sistem Informasi pada bagian sebelumnya maka terdapat dua aspek utama, yaitu:

- **Conformance** (Kesesuaian)
  - Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kesesuaian, yaitu : Confidentiality (Kerahasiaan), Integrity (**Integritas**), Availability (Ketersediaan) dan Compliance (Kepatuhan).
- **Performance** (Kinerja)
  - Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kinerja, yaitu : Effectiveness (**Efektifitas**), Efficiency (**Efisiensi**), Reliability (Kehandalan).
- Audit SI dimaksudkan untuk memberikan informasi kepada manajemen puncak agar manajemen mempunyai "*a clear assessment*" terhadap sistem informasi yang diimplementasikan pada organisasi tersebut.
  - Misalnya, bahwa *aplikasi* yang ada telah dianalisis dan didesain dengan baik, telah diimplementasikan dengan *security features* yang memadai.

Ruang Lingkup Audit SI [4]

- Mengidentifikasi sistem yang ada
- Memahami seberapa besar sistem informasi mendukung kebutuhan strategis organisasi dan operasional organisasi
- Mengetahui pada bidang atau area mana, fungsi, kegiatan atau *business processes* yang didukung dengan sistem informasi.
- Menganalisis tingkat pentingnya data/informasi yang dihasilkan oleh sistem dalam rangka mendukung kebutuhan para pemakainya.
- Mengetahui keterkaitan antara data, sistem pengolahan dan transfer informasi.
- Mengidentifikasi apakah ada kesenjangan (*gap*) antara sistem dengan kebutuhan.
- Membuat peta (*map*) dari *information flows* yang ada.

Metodologi Audit SI [5]

- Dalam pelaksanaanya, auditor TI mengumpulkan bukti-bukti yang memadai melalui berbagai teknik termasuk survey, wawancara, observasi dan review dokumentasi.
- Satu hal yang unik, bukti-bukti audit yang diambil oleh auditor biasanya mencakup pula bukti elektronis. Biasanya, auditor TI menerapkan teknik audit berbantuan computer, disebut juga dengan CAAT (Computer Aided Auditing Technique).
- Teknik ini digunakan untuk menganalisa data, misalnya saja data transaksi penjualan, pembelian, transaksi aktivitas persediaan, aktivitas nasabah, dan lain-lain.

Tahapan Audit SI [5]

Tahapan audit mencakup beberapa aktivitas yaitu perencanaan, pemeriksaan lapangan, pelaporan dan tindak lanjut.

1. **Perencanaan (*Planning*)**
   - Tahap perencanaan ini yang akan dilakukan adalah menentukan ruang lingkup (scope), objek yang akan diaudit, standard evaluasi dari hasil audit dan komunikasi dengan managen pada organisasi yang bersangkutan dengan menganalisa visi, misi, sasaran dan tujuan objek yang diteliti serta strategi, kebijakan-kebijakan yang terkait dengan pengolahan investigasi
   - Perencanaan meliputi beberapa aktivitas utama, yaitu:
     - Penetapan ruang lingkup dan tujuan audit
     - Pengorganisasian tim audit
     - Pemahaman mengenai operasi bisnis klien
     - Kaji ulang hasil audit sebelumnya
     - Penyiapan program audit

Tahapan Audit SI [5]

2. Pemeriksaan Lapangan (*Field Work*)

- Pengumpulan informasi yang dilakukan dengan cara mengumpulkan data dengan pihak-pihak yang terkait.
- Metode pengumpulan data yaitu: wawancara, quesioner ataupun melakukan survey ke lokasi penelitian.

3. Pelaporan (*Reporting*)

- Setelah proses pengumpulan data, maka akan didapat data yang akan diproses untuk dihitung berdasarkan perhitungan *maturity level*.
- Pada tahap ini yang akan dilakukan memberikan informasi berupa hasil-hasil dari audit.
- Perhitungan maturity level dilakukan mengacu pada hasil wawancara, survey dan rekapitulasi hasil penyebaran quesioner.
- Berdasarkan hasil maturity level yang mencerminkan kinerja saat ini (*current maturity level*) dan kinerja standard atau ideal yang diharapkan akan menjadi acuan untuk selanjutnya dilakukan analisis kesenjangan (*gap*).

Tahapan Audit SI [5]

4. Tindak Lanjut (*Follow Up*)

- Tahap ini yang dilakukan adalah memberikan laporan hasil audit berupa rekomendasi tindakan perbaikan kepada pihak managemen objek yang diteliti
- Wewenang perbaikan menjadi tanggung jawab managemen objek yang diteliti apakah akan diterapkan atau hanya menjadi acuhan untuk perbaikan dimasa yang akan datang.

Siapa Yang Melakukan Audit[5]

Tergantung Tujuan Audit

1. Internal Audit (first party audit)
   - Dilakukan oleh atau atas nama organisasi itu sendiri
   - Biasanya untuk management review atau tujuan internal perusahaan
2. Lembaga independen di luar organisasi
   - Second party audit : Dilakukan oleh pihak yang memiliki kepentingan thd perusahaan
   - Third party audit : Dilakukan oleh pihak independen dari luar perusahaan. Misalnya untuk sertifikasi (ISO 9001, BS7799 dll).

Siapa Yang Di Audit[5]

- Management
- IT Manager
- IT Specialist (network, database, system analyst, programmer, dll.)
- User

- Contoh : Audit Sistem Informasi Akademik TEL-U
  - Management : Rektor, Warek, Dekan, Dir Akademik
  - IT Manager : Dir Sisfo, Manager Aplikasi
  - IT Spesialist : Programmer
  - User : Dosen, Mahasiswa, User di Unit

Tugas Auditor SI[5]

Tugas Auditor

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

Yang dilakukan

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

Output kegiatan Audit oleh Auditor SI[5]

Hasil akhir adalah berupa laporan yang berisi:

- Ruang Lingkup audit
- Metodologi
- Temuan-temuan
- Ketidaksesuaian (sifat ketidaksesuaian, bukti2 pendukung, syarat yg tdk dipenuhi, lokasi, tingkat ketidaksesuaian)
- Kesimpulan (tingkat kesesuaian dengan kriteria audit, efektifitas implementasi, pemeliharaan dan pengembangan sistem manajemen, rekomendasi)

Kompetensi Auditor SI[5]

Audit Skill

- Sampling, komunikasi, melakukan interview, mengajukan pertanyaan, mencatat

Generic knowledge

- Pengetahuan mengenai prinsip2 audit, prosedur dan teknik, sistem manajemen dan dokumen2 referensi, organisasi, peraturan2 yang berlaku

Specific knowledge

- Background IT/IS, bisnis, specialist technical skill, pengalaman audit sistem manajemen, perundangan

Prinsip Seorang Auditor SI[5]

- **Ethical conduct**
  - Berdasar pada profesionalisme, kejujuran, integritas, kerahasiaan dan kebijaksanaan
- **Fair Presentation**
  - Kewajiban melaporkan secara jujur dan akurat
- **Due professional care**
  - Implementasi dari kesungguhan dan pertimbangan yang diberikan
- **Independence**
- **Evidence-base approach**

Peluang Profesi Auditor SI[5]

- Ketergantungan terhadap sistem informasi semakin besar sehingga muncul kebutuhan untuk melakukan audit SI
- Auditor SI yang sekarang banyak yang berasal bukan dari bidang IT
- Banyak permasalahan (bisnis) dalam pengelolaan IT

Referensi

[1]. https://www.academia.edu/4742018/Audit_Sistem_Informasi_Apa_itu_Audit_Sistem_Informasi_Teknologi_Informasi

[2] http://www.pendidikanmu.com/2015/05/pengertian-audit-sistem-informasi.html

[3] ITGI. 2007. IT Assurance Guide: Using Cobit. IT Governance Institute 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA

[4] Buku Fraud & Auditing, 2014

[5] https://simponi.mdp.ac.id/materi201120121/SI308/051041/SI308

https://www.youtube.com/watch?v=wypvhcq4N-0


raibh
Dziękuję
Go
Obrigado
je
Misaotra
Takk
Thank
you
Merci
Þakka
Grazie
dankie
Dankewol
Obrigada
fyri
baie
Dank
Mulţumesc
Teşekkür
agat
ederim
Gratias
dekem
Paldies
Köszönöm
Gracias
Kiitos
Tak
Gràcies
Tack
Sipas
Mahalo
maith
Danke
Hvala
þér