

PERTEMUAN VI

AUDIT TEKNOLOGI INFORMASI

6.1 Pengertian

Audit Teknologi Informasi seringkali diistilahkan Audit Sistem Informasi. menurut Ron Weber (1999), Audit sistem informasi adalah proses pengumpulan dan penilaian bukti - bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien. Berdasarkan definisi tersebut, dapat disimpulkan bahwa tujuan audit teknologi informasi adalah sebagai berikut :

1. Mengamankan aset
2. Menjaga integritas data
3. Menjaga efektivitas sistem
4. Mencapai efisiensi sumberdaya

6.2 Pendekatan Audit SI

Pesatnya perkembangan dunia komputer, diikuti dengan peningkatan pengetahuan auditor, ternyata mengundang dua perlakuan berbeda terhadap komputer, yaitu :

- (1) Komputer dipergunakan sebagai alat bantu auditor dalam melaksanakan audit, misalnya untuk mengambil contoh transaksi, memproses data akuntansi, mencetak surat konfirmasi piutang dan sebagainya.
- (2) Komputer dijadikan sebagai target audit, karena data di-*entry* ke komputer dan hasilnya dianalisa untuk menilai kehandalan pemrosesan dan keakuratan program komputer.

Dengan berjalannya evolusi tersebut, maka muncullah pendekatan audit sistem informasi yang dapat dikategorikan ke dalam tiga kelompok, yaitu :

a. Audit Melalui Komputer (*Audit through the Computer*)

Dalam audit ini masukan, keluaran dan pemrosesan diperiksa. Auditor mengkaji logika program, menguji data, dan mengendalikan pemrosesan serta pemrosesan ulang. Fokus perhatian Auditor langsung pada operasi pemrosesan didalam sistem komputer.

Keunggulan pendekatan audit melalui komputer adalah :

- a. Auditor memperoleh kemampuan yang besar dan efektif dalam melakukan pengujian terhadap sistem komputer.
- b. Auditor akan merasa lebih yakin terhadap kebenaran hasil kerjanya.
- c. Auditor dapat menilai kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan.

Kelemahan : Memerlukan biaya yang besar dan tenaga ahli yang terampil mengingat pendekatan ini demikian kompleksnya.

b. Audit Dengan Komputer (*Audit with the Computer*).

Pemeriksaan dilakukan dengan menggunakan gabungan dari data klien, peranti lunak Auditor, dan peranti keras klien serta Auditor. Penggunaan komputer dan software audit khusus oleh Auditor dimaksudkan untuk otomatisasi prosedur pelaksanaan audit

software audit yang digunakan dapat digolongkan menjadi dua golongan :

- 1) Perangkat lunak audit terspesialisasi (SAS/ specialized audit software). SAS merupakan satu atau lebih program khusus yang dirancang oleh auditor agar sesuai dengan situasi audit tertentu. Software audit ini jarang digunakan karena penyiapannya memakan waktu dan biayanya mahal, dan diperlukan keahlian auditor dibidang komputer. Cara penanggulangannya dapat dengan menggunakan program yang relevan dengan tujuan audit yang saat itu digunakan oleh perusahaan.
- 2) Perangkat lunak audit tergeneralisasi (GAS/ generalized audit software). Perangkat lunak audit yang digeneralisasi terdiri dari seperangkat program komputer yang secara bersama melaksanakan bermacam fungsi pemrosesan data atau manipulasi data. GAS dikembalikan oleh kantor akuntan untuk berbagai tugas audit dan dapat digunakan pada berbagai perusahaan.

Keunggulan rogram-program yang digeneralisasi :

- a) program ini dikembangkan sedemikian rupa sehingga memudahkan pelatihan bagi staf auditor dalam menggunakan program, tidak perlu memiliki pengetahuan dalam pemrograman.
- b) dapat diterapkan pada lingkup tugas-tugas yang lebih besar tanpa harus mengeluarkan biaya atau mengalami kesulitan dalam mengembangkan program.

Kelemahannya adalah biaya pengembangan pada awalnya besar, dan kecepatan pengolahan relatif kurang efisien

6.3 Tahapan Audit Sistem Informasi

Menurut Ron Weber dalam bukunya *Information Systems Control and Audit* halaman 47-55, terdapat 5 (lima) langkah atau tahapan audit sistem informasi yaitu :

1. Perencanaan Audit (*Planning the Audits*)
2. Pengetesan Kendali (*Tests of Controls*)
3. Pengetesan Transaksi (*Tests of Transactions*)
4. Pengetesan Keseimbangan atau Keseluruhan Hasil (*Tests of Balances or Overall Results*)
5. Pengakhiran (penyelesaian) Audit (*Completion of the Audit*)

Sedangkan menurut Gallegos Cs. dalam bukunya *Audit and Control of Information Systems* (chapter 10), tahapan audit sistem informasi mencakup aktivitas :

1. Perencanaan (*Planning*) kegiatan perencanaan untuk melaksanakan audit
2. Pemeriksaan Lapangan (*Fieldwork*). kegiatan pemeriksaan dan evaluasi sistem yang dilaksanakan di lapangan
3. Pelaporan (*Reporting*). kegiatan pelaporan hasil-hasil yang diperoleh dari *fieldwork*
4. Tindak Lanjut (*Follow Up*). tindakan lebih lanjut yang dilaksanakan oleh pihak manajemen berkaitan dengan laporan hasil pemeriksaan.

6.4 COBIT (Control Objectives for Information and Related Technology)

Untuk praktek pengamanan teknologi informasi serta pengendaliannya ada standar yang berlaku internasional Standar itu adalah **COBIT** (*Control Objectives for Information and Related Technology*) yang mempunyai beberapa tahapan mulai dari perencanaan, penerapan sampai dengan kontrol teknologi informasi.

COBIT dikembangkan oleh IT Governance Institute, yang merupakan bagian dari *Information Systems Audit and Control Association (ISACA)*. COBIT memberikan arahan (*guidelines*) yang berorientasi pada bisnis, dan karena itu *business process owners* dan manajer, termasuk juga auditor dan user, diharapkan dapat memanfaatkan guidelines ini dengan sebaik-baiknya.

Menurut Campbell dalam hirarki COBIT terdapat 4 domain COBIT yang terbagi menjadi 34 proses dan 318 control objectives, serta 1547 control practitices. Dalam setiap domain dan proses di dalamnya tersedia pula panduan manajemen, panduan audit, dan ringkasan bagi pihak eksekutif

Adapun kerangka kerja COBIT secara keseluruhan terdiri atas arahan sebagai berikut :

1. **Control Objectives:** Terdiri atas 4 tujuan pengendalian tingkat-tinggi (*high-level control objectives*) yang tercermin dalam 4 domain, yaitu: *planning & organization* , *acquisition & implementation* , *delivery & support* , dan *monitoring* .
2. **Audit Guidelines :** Berisi sebanyak 318 tujuan-tujuan pengendalian yang bersifat rinci (*detailed control objectives*) untuk membantu para auditor dalam memberikan *management assurance* dan/atau saran perbaikan.
3. **Management Guidelines:** Berisi arahan, baik secara umum maupun spesifik, mengenai apa saja yang mesti dilakukan, terutama agar dapat menjawab pertanyaan – pertanyaan berikut:
 1. Sejauh mana Anda (TI) harus bergerak, dan apakah biaya TI yang dikeluarkan sesuai dengan manfaat yang dihasilkannya.
 2. Apa saja indikator untuk suatu kinerja yang bagus?
 3. Apa saja faktor atau kondisi yang harus diciptakan agar dapat mencapai sukses (*critical success factors*)?
 4. Apa saja risiko-risiko yang timbul, apabila kita tidak mencapai sasaran yang ditentukan?
 5. Bagaimana dengan perusahaan lainnya – apa yang mereka lakukan?
 6. Bagaimana Anda mengukur keberhasilan dan bagaimana pula membandingkannya.