PELAKSANAAN KONTROL DAN AUDIT SISTEM INFORMASI PADA ORGANISASI

Radiant Victor Imbar
Jurusan Sistem Informasi
Fakultas Teknologi Informasi Universitas Kristen Maranatha
Jl. Prof. drg. Suria Sumantri No. 65, Bandung 40164
Email: radiant.vi@itmaranatha.org

Abstract

Information system auditing is a function that has been developed to assess whether computer systems safeguard assets, maintain data integrity, and allow the goals of an organization to be achived effectively and efficiently. As a result, the need to maintain the integrity data processed by computers now seems to pervade our lives. We have concerns about the privacy of data we exchange with organizations such as tax department and credit granting institutions. Information systems auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently.
This paper will explain about how to conduct information system audit in organization and some risk that might happen during an information system audit.

Keyword : Information system, audit, organization

1. Pendahuluan.

Audit sistem informasi adalah fungsi dari organisasi yang mengevaluasi keamanan aset, integritas data, efektifitas dan efisiensi sistem dalam sistem informasi berbasis komputer. Kebutuhan audit ini disebabkan oleh beberapa faktor yaitu :

1. Kemungkinan kehilangan data.
2. Kemungkinan kesalahan penempatan sumber daya akibat kesalahan pengambilan keputusan yang diakibatkan karena kesalahan pemrosesan data.
3. Kemungkinan komputer rusak karena tidak terkontrol
4. Harga komputer hardware, software sangat mahal
5. Biaya yang tinggi apabila ada error pada komputer
6. Kebutuhan privacy dari organisasi/seseorang.
7. Kebutuhan untuk mengontrol penggunaan komputer.

Para auditor sistem informasi secara khusus berkonsentrasi pada evaluasi kehandalan atau efektifitas pengendalian / kontrol sistem. Kontrol adalah sebuah sistem untuk mencegah, mendeteksi atau memperbaiki situasi yang tidak teratur.

Terdapat tiga aspek penting yang berkaitan dengan definisi kontrol di atas, yaitu :

a. kontrol adalah sebuah sistem, dengan kata lain kontrol terdiri atas sekumpulan komponen-komponen yang saling berhubungan dan bekerja sama untuk mencapai tujuan yang sama.
b. Fokus dari kontrol adalah situasi yang tidak teratur, dimana keadaan ini bisa terjadi jika ada masukan yang tidak semestinya masuk ke dalam sistem.

c. Kontrol digunakan untuk mencegah, mendeteksi dan memperbaiki situasi yang tidak teratur, sebagai contoh :
    a. *Preventive control* : instruksi yang diletakkan pada dokumen untuk mencegah kesalahan pemasukan data
    b. *Detective control* : Kontrol yang diletakkan pada program yang berfungsi mendeteksi kesalahan pemasukan data
    c. *Corrective control* : program yang dibuat khusus untuk memperbaiki kesalahan pada data yang mungkin timbul akibat gangguan pada jaringan, komputer ataupun kesalahan user.

Secara umum, fungsi dari kontrol adalah untuk menekan kerugian yang mungkin timbul akibat kejadian yang tidak diharapkan yang mungkin terjadi pada sebuah sistem.

Tugas auditor adalah untuk menetapkan apakah kontrol sudah berjalan sesuai dengan yang diharapkan untuk mencegah terjadinya situasi yang tidak diharapkan. Auditor harus dapat memastikan bahwa setidaknya ada satu buah kontrol yang dapat menangani resiko bila resiko tersebut benar-benar terjadi.

2. Langkah – langkah audit sistem informasi.

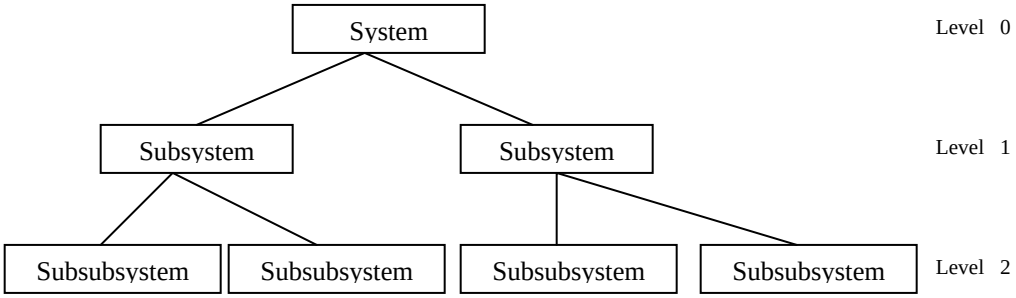
Proses audit sistem informasi adalah proses yang berkaitan langsung dengan kompleksitas. Terkadang auditor harus menyelesaikan tugasnya dalam sistem yang sangat banyak dan kompleks. Karena kompleksitas merupakan akar permasalahan dari setiap problem yang dihadapai oleh para profesional, maka para ilmuwan telah berusaha untuk membuat panduan untuk mengurangi kompleksitas tersebut, yaitu :

a. Memecah sebuah sistem yang besar menjadi beberapa subsistem untuk dievaluasi secara terpisah
b. Menentukan kehandalan setiap subsistem dan pengaruh setiap subsistem terhadap kehandalan sistem secara keseluruhan

2.1 Faktorisasi Subsistem (Subsystem Factoring)

Langkah pertama dalam memahami sebuah sistem yang besar adalah dengan memecahnya menjadi beberapa subsistem. Subsistem adalah komponen dari sistem yang dapat melakukan beberapa fungsi dasar yang diperlukan oleh sistem. Subsistem adalah komponen lojik dari sebuah sistem, bukan komponen fisik. Dengan kata lain, subsistem tidak dapat dilihat secara nyata.

Proses dekomposisi sistem menjadi subsistem disebut dengan factoring. Factoring merupakan sebuah proses pengulangan yang akan berhenti jika subsistem yang dihasilkan sudah cukup kecil dan auditor dapat dengan mudah mengevaluasinya. Sistem yang akan dievaluasi dapat dijabarkan sebagai sebuah level structure dari subsistem, di mana setiap subsistem melakukan fungsi yang dibutuhkan oleh subsistem diatasnya.



Gambar 1. Tingkatan Struktur Sistem dan Subsistem

Untuk memahami proses factoring, kita membutuhkan dasar untuk mengidentifikasi subsistem itu sendiri. Yang pertama sudah terlebih dahulu dijelaskan, yaitu untuk memahami sebuah subsistem harus dipahami dahulu fungsi yang dikerjakan oleh subsistem tersebut. Auditor harus dapat menemukan fungsi utama yang dikerjakan oleh subsistem tersebut dan perannya terhadap tujuan umum dari sistem diatasnya.

Selain fungsi, teori sistem mengindikasikan dua panduan lain yang harus dipakai dalam mengidentifikasi dan menggambarkan subsistem:

a. setiap subsistem sebaiknya terpisah dari subsistem lainnya. Tujuannya adalah agar auditor dapat menganalisa setiap subsistem secara terpisah dari subsistem yang lain, dengan kata lain setiap subsistem tidak tergantung dari subsistem yang lain pada level yang sama.
b. Pada bagian internal setiap subsistem, harus terdapat kohesif yang cukup tinggi. Setiap aktivitas yang dilakukan oleh subsistem harus bertujuan untuk menyelesaikan fungsi yang dimiliki oleh subsistem tersebut.

Dari sudut pandang audit, subsistem akan sulit untuk dimengerti dan kehandalannya sulit diukur kecuali jika subsistem tersebut tidak saling berpasangan (*loosely coupled*) dan secara internal derajat kohesifnya cukup tinggi.

Terdapat dua cara untuk melakukan dekomposisi subsistem (*factoring*) :

a. Berdasarkan *managerial function*, yang harus dilakukan untuk memastikan bahwa pengembangan, implementasi, operasi dan perawatan dari sistem informasi dilaksanakan dengan cara yang sudah direncanakan dan terkontrol. Managerial system function memungkinkan penyediaan infrastruktur yang stabil dimana sistem informasi dapat dibuat, dioperasikan dan dirawat untuk keperluan harian. Beberapa jenis management subsystem telah diidentifikasi hubungannya dengan struktur organisasi dan kegiatan utama yang dilakukan oleh fungsi sistem informasi

b. Berdasarkan *apllication function* yang diperlukan untuk menyelesaikan pemrosesan informasi yang dapat dipercaya. Proses ini berkaitan dengan pendekatan “siklus” yang telah digunakan oleh auditor untuk melaksanakan audit. Sistem informasi yang mendukung organisasi adalah yang pertama dikelompokkan kedalam siklus. Siklus dapat berbeda-beda tergantung dari industri yang diambil oleh organisasi tersebut, tetapi terdapat siklus umum yang terdapat dalam perusahaan komersial atau manufaktur, yaitu:

a. *Sales* dan *collections*
b. *Payroll* dan *personnel*
c. Acquisitions dan *payment*
d. Conversion, *inventory* dan *warehousing*
e. Treasury

Setiap siklus difaktorkan menjadi satu atau lebih sistem aplikasi. Sistem aplikasi kemudian difaktorkan menjadi subsistem.

2.2 Penilaian Keandalan Subsistem *(Assesing Subsystem Reliability)*

Setelah kita mengidentifikasi level terendah dari subsistem, kita kemudian dapat mengevaluasi kehandalan dari dari kontrol. Diawali pada subsistem level terendah, kita mencoba mengidentifikasi semua kejadian yang mungkin terjadi dalam subsistem ini, baik kejadian yang diharapkan dan kejadian yang tidak diharapkan. Fokus utama auditor tentunya pada terjadinya situasi yang tidak diharapkan.

Sebagai dasar dari identifikasi semua kejadian pada management subsistem, kita fokuskan pada fungsi utama yang dijalankan oleh setiap subsistem. Kita sadari bagaimana setiap fungsi harus dijalankan kemudian mengevaluasi seberapa baik subsistem bekerja untuk mendukung sistem secara keseluruhan.

Aspek penting dalam mengidentifikasi kejadian yang diharapkan dan tidak diharapkan pada subsistem manajemen adalah keputusan bagaimana fungsi tertentu harus dilaksanakan dalam sebuah subsistem. Setelah dilakukan penelitian yang cukup pada manajemen sistem informasi, jelas terlihat bahwa manajemen sistem informasi yang harus dilaksanakan pada sebuah organisasi tergantung dari permasalahan yang dihadapi oleh perusahaan tersebut.

Sebagai dasar dari proses identifikasi kejadian yang diharapkan dan yang tidak diharapkan pada subsistem aplikasi, kita memfokuskan pada transaksi yang dapat terjadi sebagai masukan pada subsistem. Semua kejadian pada sistem aplikasi harus mucul dari transaksi. Sistem aplikasi pada mulanya akan berganti status (sebuah kejadian terjadi) pada saat transaksi menerima sebuah input.

Untuk mengidentifikasi semua kejadian yang mungkin terjadi dalam sistem aplikasi sebagai akibat dari transaksi, kita harus memahami bagaimana sistem bekerja dalam memproses sebuah transaksi. Auditor harus menggunakan teknik *walk-through* untuk menyelesaikan tugas ini. Mencari transaksi yang umum, komponen yang terlibat di dalam sistem yang ikut memproses transaksi, kemudian berusaha untuk memahami setiap langkah yang dieksekusi oleh komponen. Mereka juga berusaha menemukan kesalahan yang mungkin terjadi pada saat proses eksekusi berlangsung.

Proses pemantauan ini biasanya memakan banyak biaya, sehingga auditor terkadang memfokuskan diri pada *class of transaction*, di mana beberapa transaksi yang memiliki kesamaan proses dikelompokkan menjadi satu kelompok. Dengan cara ini, auditor memfokuskan diri pada transaksi yang dianggap sebagai transaksi utama dari sudut pandang auditor. Kelemahan dari cara ini adalah tidak semua kejadian yang mungkin terjadi dapat diidentifikasi. Auditor harus dapat memprediksikan semua transaksi dan kejadian yang dinilai penting, agar jangan sampai ada kejadian penting yang terlewat.

Ketika semua kejadian/event utama dalam sistem aplikasi sudah diidentifikasi, auditor harus mengevaluasi apakah kontrol telah berada ditempatnyadan bekerja dengan baik untuk menangani setiap masalah yang tidak diharapkan. Sesuai dengan itu, para auditor mengumpulkan bukti nyata pada kontrol yang ada untuk menentukan apakah kerugian yang ditimulkan oleh setiap kejadian yang tidak diharapkan dapat ditekan ke level yang bisa diterima.

Pada saat melakukan evaluasi untuk level sistem yang lebih tinggi, kita akan menemui kontrol baru untuk tiga alasan :

a. Kontrol pada sistem level rendah dapat rusak / berjalan tidak sbagaimana mestinya. Recall, sebuah kontrol adalah sebuah sistem itu sendiri, dan kontrol dapat tidak dipercaya, sama seperti sistem pada umumnya. Kontrol di level yang lebih tinggi dapat dipakai untuk mengantisipasi jika kontrol di level bawah tidak mampu menangani masalah.
b. Akan lebih murah jika mengimplementasikan kontrol pada level yang lebih tinggi. Misalnya jika karyawan bagian entri sudah sangat terlatih, maka tidak diperlukan pengecekan ganda untuk sebuah pekerjaan.
c. Beberapa kejadian tidak menunjukkan resiko kecuali berada di dalam level yang lebih tinggi.

Secara jelas, proses menggabungkan subsistem ke level yang lebih tinggi dapat menjadi persoalan yang cukup besar. Kesalahan yang terjadi pada suatu level dapat terakumulasi pada level di atasnya, sehingga auditor harus berhati-hati dalam membuat keputusan kelayakan sebuah sistem, terlebih pada saat melangkah dari subsistem level bawah ke subsistem di atasnya.

3. Resiko – resiko audit.

Audit sistem informasi berkaitan dengan empat hal yaitu: penjagaan aset, integritas data, efektivitas sistem dan efisiensi sistem. Untuk memperkirakan apakah suatu organisasi mencapai sasaran yang telah ditetapkan sebelumnya, maka auditor mengumpulkan informasi yang berkaitan dengan empat hal di atas. Pada saat pengumpulan informasi, ada kemungkinan bahwa auditor gagal untuk menemukan kerugian material yang riil maupun potensial atau kesalahan akuntansi. Resiko dari kegagalan auditor untuk menemukan kerugian material ataupun kesalahan akuntansi disebut sebagai *audit risk*.

Sebagai dasar untuk penentuan seberapa besar tingkat *audit risk* yang diinginkan, para auditor profesional telah mengadopsi sebuah model penentuan *audit risk* untuk fungsi audit eksternal:

DAR = IR x CR x DR

Pada model ini, *DAR (Desired Audit Risk)* adalah tingkat *audit risk* yang diinginkan. *IR (Inherent Risk)* merupakan kerugian material atau kesalahan akuntansi yang terdapat dalam beberapa bagian yang diaudit, sebelum realibilitas kontrol internal dipertimbangkan. *CR (Control Risk)* menggambarkan kemungkinan bahwa kontrol internal dalam beberapa bagian yang diaudit tidak dapat mencegah, mendeteksi atau memperbaiki kerugian material atau kesalahan akuntansi yang muncul. *DR (Detection Risk)* menggambarkan prosedur-prosedur audit yang digunakan dalam beberapa bagian yang diaudit akan gagal untuk mendeteksi kerugian material ataupun kesalahan akuntansi.

Untuk menerapkan model yang akan dipakai, pertama-tama auditor menentukan besarnya *desired audit risk*. Auditor eksternal mempertimbangkan

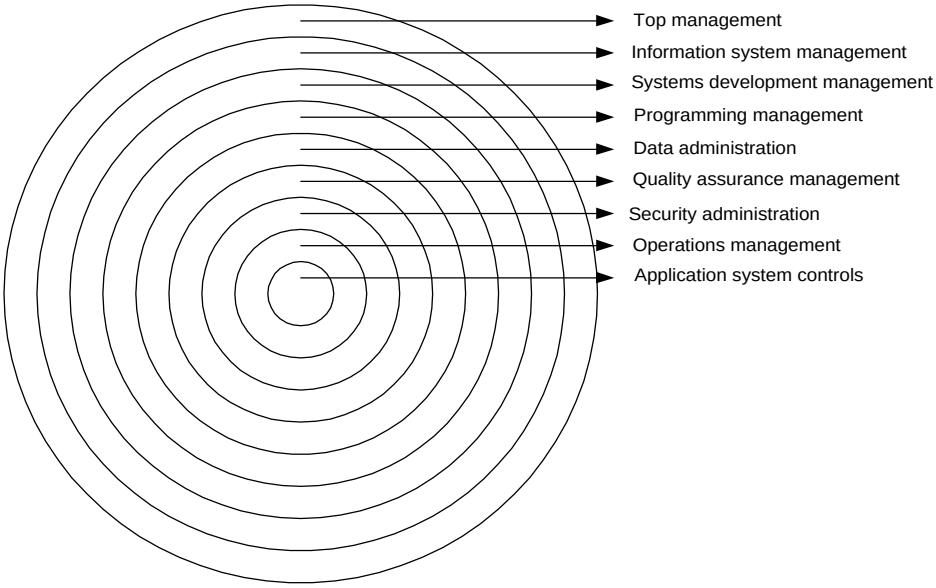
beberapa faktor seperti ketergantungan perusahaan pada pihak luar untuk menentukan kebijakan finansial dan kemungkinan-kemungkinan perusahaan akan mengalami kesulitan keuangan setelah proses audit. Selain mempertimbangkan faktor-faktor di atas, auditor internal juga memperkirakan dampak jangka pendek dan panjang yang dapat terjadi, apabila mereka gagal untuk mendeteksi kerugian material riil maupun potensial yang disebabkan dari kegiatan yang kurang efektif dan efisien pada perusahaan.

Berikutnya auditor menentukan besarnya *inherent risk*. Biasanya auditor memperkirakan faktor-faktor umum pada perusahaan (misalnya: apakah perusahaan tersebut berkembang dengan pesat?), pada bidang industri apa perusahaan tersebut bergerak (misalnya: apakah industri tersebut selalu mengalami perubahan dalam waktu yang singkat?), karakteristik manajemen perusahaan (misalnya: apakah manajemen perusahaan bersifat agresif dan otokrasi?), dan hal-hal yang berhubungan dengan akuntansi dan audit (misalnya: apakah kebiasaan-kebiasaan akuntansi yang digunakan oleh perusahaan?). Kemudian auditor mempertimbangkan *inherent risk* yang berhubungan dengan bagian-bagian yang berbeda seperti: kegiatan perusahaan, sistem aplikasi, dan kebijakan-kebijakan akuntansi. Untuk setiap bagian, auditor mempertimbangkan faktor-faktor sebagai berikut:

- Sistem finansial
  Merupakan sistem-sistem yang biasanya menyediakan kontrol finansial dari aset-aset utama sebuah perusahaan, misalnya: penerimaan uang dan distribusinya, daftar gaji, rekening-rekening perusahaan yang biasanya mempunyai *inherent risk* yang lebih tinggi karena merupakan sasaran dari penipuan dan penggelapan.
- Sistem strategi
  Merupakan sistem-sistem yang menyediakan strategi kompetitif suatu perusahaan, misalnya: sistem yang menunjukkan rahasia-rahasia perdagangan, hak paten suatu perusahaan, biasanya mempunyai *inherent risk* yang tinggi karena merupakan sasaran dari kegiatan spionase industri kompetitor.
- Sistem operasional kritis
  Merupakan sistem-sistem yang dapat melumpuhkan sebuah perusahaan apabila mengalami kegagalan, misalnya: sistem perlindungan konsumen atau sistem kontrol produksi, biasanya mempunyai *inherent risk* yang tinggi.
- Sistem teknologi terkini
  Merupakan sistem-sistem yang menggunakan teknologi maju, seringkali mempunyai *inherent risk* yang tinggi karena bersifat kompleks dan perusahaan tidak memiliki pengalaman yang cukup.

Untuk memperkirakan besarnya *control risk* yang berhubungan dengan bagian yang diaudit, auditor mempertimbangkan realibilitas dari manajemen dan kontrol aplikasi. Biasanya auditor mengidentifikasi dan mengevaluasi kontrol pada subsistem manajemen terlebih dahulu, subsistem manajemen merupakan kontrol dasar sebuah perusahaan karena mencakup seluruh sistem aplikasi. Oleh karena itu ketiadaan sebuah kontrol manajemen merupakan masalah serius untuk auditor. Pada konsepnya kontrol manajemen merupakan lapisan-lapisan yang berbentuk seperti irisan bawang, untuk memperluas lapisan yang lebih luar, lapisan yang lebih dalam sebaiknya merupakan lapisan yang utuh. Seringkali akan menjadi lebih

efisien apabila auditor mengevaluasi kontrol manajemen sebelum kontrol aplikasi. Setelah auditor mengevaluasi kontrol manajemen, auditor tidak perlu untuk memeriksa lagi secara lebih detail, karena kontrol manajemen merupakan fungsi dari seluruh aplikasi. Sebagai contoh, apabila auditor menemukan bahwa perusahaan yang diaudit mempunyai standar dokumentasi yang berkualitas tinggi, maka auditor tidak perlu lagi untuk melihat kembali dokumentasi untuk setiap sistem aplikasi.



Gambar 2: Manajemen Kontrol sebagai Lapisan Berlapis dari Aplikasi Kontrol

Berikutnya auditor menghitung besarnya *detection risk* yang harus dicapai untuk memperoleh *desired audit risk*. Kemudian mereka akan mendesain prosedur pengumpulan informasi yang bertujuan untuk mencapai *detection risk* tersebut. Untuk memperkirakan berapa besarnya detection risk yang mungkin dicapai dengan prosedur audit, auditor harus mempunyai pemahaman yang baik tentang bagaimana prosedur tersebut mendeteksi kerugian material atau kesalahan akuntansi yang muncul. Lebih jauh lagi, auditor harus mengevaluasi bagaimana prosedur tersebut diterapkan.

Pada akhirnya kita dapat merangkum bahwa seluruh poin dalam *audit risk* model adalah usaha audit seharusnya difokuskan pada dimana mereka akan menerima bayaran yang paling tinggi. Pada kebanyakan kasus, auditor tidak dapat mengumpulkan informasi yang diinginkan, mereka harus ahli dalam menerapkan prosedur audit dan mengintepretasikan informasi yang diperoleh.

4. Jenis – jenis prosedur audit.

Ketika auditor eksternal mengumpulkan informasi untuk menentukan apakah telah terjadi kerugian material atau kesalahan informasi finansial telah terjadi, mereka menggunakan lima tipe prosedur:

1. Prosedur untuk memperoleh pengertian dari kontrol
   Penyelidikan, inspeksi dan observasi dapat digunakan untuk memperoleh pengertian dari kontrol yang sudah ada, seberapa baik desainnya dan apakah telah diterapkan dengan baik pula.

2. Pengujian terhadap kontrol
   Penyelidikan, inspeksi, observasi dan pengujian prosedur-prosedur kontrol dapat digunakan untuk mengevaluasi apakah kontrol telah beroperasi secara efektif.
3. Pengujian nyata terhadap detail transaksi
   Pengujian ini didesain untuk menemukan kesalahan keuangan atau transaksi-transaksi yang tidak wajar yang akan mempengaruhi kebijakan finansial perusahaan.
4. Pengujian nyata terhadap detail neraca keuangan
   Pengujian ini terfokus pada bagian akhir dari buku besar.
5. Prosedur peninjauan ulang secara analitis
   Pengujian ini terfokus pada keterhubungan antara data yang dimiliki dengan kenyataan yang ada dilapangan.

Auditor juga dapat menggunakan beberapa tipe prosedur yang mirip jika mereka memperhatikan faktor efektivitas dan efisiensi dari operasional perusahaan, seringkali urutan prosedur pengujian dilakukan dari yang berbiaya rendah ke yang berbiaya tinggi, yaitu: prosedur peninjauan ulang secara analitis, prosedur untuk memperoleh pengertian dari kontrol, pengujian terhadap kontrol, pengujian nyata terhadap detail trransaksi dan pengujian nyata terhadap detail neraca keuangan. Pada saat tertentu, urutan tersebut dijalankan secara terbalik ketika kita mempertimbangkan reabilitas dan isi informasi yang disediakan oleh prosedur audit yang berbeda. Prosedur pengujian dilakukan dari yang berbiaya rendah ke tinggi mempunyai harapan bahwa informasi yang diperoleh akan mendeteksi kerugian material yang terjadi atau yang akan terjadi. Jika hasil ini yang terjadi, auditor dapat merubah kebiasaan, waktu dan penghematan biaya dari pengujian yang dilakukan.

Kesimpulan

Para auditor sistem informasi secara khusus berkonsentrasi pada evaluasi kehandalan atau efektifitas pengendalian / kontrol sistem. Kontrol adalah sebuah sistem untuk mencegah, mendeteksi atau memperbaiki situasi yang tidak teratur. Proses audit sistem informasi adalah proses yang berkaitan langsung dengan kompleksitas. Terkadang auditor harus menyelesaikan tugasnya dalam sistem yang sangat banyak dan kompleks. Karena kompleksitas merupakan akar permasalahan dari setiap problem yang dihadapai oleh para profesional, maka para ilmuwan telah berusaha untuk membuat panduan untuk mengurangi kompleksitas tersebut, yaitu :

a. Memecah sebuah sistem yang besar menjadi beberapa subsistem untuk dievaluasi secara terpisah
b. Menentukan kehandalan setiap subsistem dan pengaruh setiap subsistem terhadap kehandalan sistem secara keseluruhan

Ada 5 langkah yang perlu dilakukan untuk audit sistem informasi yaitu :

1. Auditor harus merencanakan audit.
2. Auditor harus mengetes kontrol.
3. Auditor harus mengetes transaksi.
4. Auditor harus mengetes output dari sistem.
5. Auditor harus melakukan review terhadap hasil audit agar hasil audit dapat dipertanggungjawabkan.

Daftar Pustaka

Weber R. (1999). Information System Audit and Control. Pearson Education.

Cangemi M.P. (1994). Managing the Audit Function : A Corporate Audit Department Procedures Guide. John Wiley & Son.