MODUL PERTEMUAN ONLINE
PROGRAM AUDIT SISTEM INFORMASI 2

A. RESIKO TERKAIT KOMPUTER DAN KONSEP DASAR AUDIT

1. Risiko Terkait Komputer

Semua hal melibatkan risiko dalam berbagai tingkatan. Risiko dikaitkan dengankemungkinan kejadian atau keadaan yang dapat merugikan dan mengancam pencapaian tujuan maupun sasaran organisasi. Risiko dapat dikurangi tetapi tidak dapat dihilangkan.

Menurut Suswinarno (2012) manajemen risiko adalah: “Suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman atau suatu rangkaian aktivitas manusia termasuk penilaian risiko, pengembangan strategi untuk mengelolanya dan mitigasi risiko dengan menggunakan pemberdayaan/pengelolaan sumber daya.”

Manajemen risiko berkaitan dengan menilai suatu produk, proses atau bisnis melalui:

a. Identikasi proses-proses
b. Identifikasi jenis risiko untuk setiap proses
c. Identifikasi kontrol untuk setiap proses
d. Evaluasi kecukupan sistem kontrol dalam mitigasi risiko
e. Menentukan kontrol utama terkait setiap proses
f. Menentukan efektifitas kontrol utama

Semua sistem informasi memiliki risiko, seperti bahaya-bahaya berikut:

- Fraud (Kecurangan/manipulasi)
- Business interruption (Gangguan bisnis)
- Errors (Sistem tidak berfungsi sebagaimana mestinya)
- Customer dissatisfaction (Ketidakpuasan konsumen)
- Poor public image(Citra yang buruk di mata masyarakat)
- Ineffective and inefficient use of resources (Penggunaan sumber daya yang tidak tepat dan pemborosan)

2. Jenis Resiko

Dari rumusan model risiko audit ada 4 (empat) jenis risiko audit. Masing-masing jenis risiko audit tersebut akan dijelaskan sebagai berikut:

a. **Planned Detection Risk (Risiko Penemuan yang Direncanakan)**
   Risiko bahwa bukti yang dikumpulkan dalam segmen gagal menemukan kekeliruan yang melampaui jumlah yang dapat ditolerir. Risiko deteksi Atau 'Detection Risk' (DR), adalah risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). Jadi DR ada dalam kendali auditor. Itu karena DR sepenuhnya ada pada kendali auditor, maka sudah pasti mereka harus berupaya untuk menekan risiko ini hingga ke tingkatakan yang paling minimal (tidak mungkin menghilangkan risiko ini sepenuhnya).

b. **Acceptable Audit Risk (Risiko Audit yang dapat diterima)**
   Ukuran atas tingkat kesediaan auditor untuk menerima kenyataan bahwa laporan keuangan mungkin masih mengandung salah saji yang material setelah audit selesai dilaksanakan serta suatu laporan audit wajar tanpa syarat telah diterbitkan.

c. **Inherent Risk (Risiko Bawaan atau Risiko Melekat)**
   Suatu ukuran yang dipergunakan oleh auditor dalam menilai adanya kemungkinan bahwa terdapat sejumlah salah saji yang material (kekeliruan atau kecurangan) dalam suatu segmen sebelum ia mempertimbangkan keefektifan dan pengendalian intern yang ada. Risiko inherent atau 'Inherent Risk' (IR) adalah risiko yang mungkin timbul akibat karakter bawaan dari suatu transaksi, bisa juga karena kompleksitas transaksi dan klas transaksi, atau kompleksitas perhitungan, aset yg mudah tercuri/digelapkan, ketiadaan informasi yang sifatnya obyektif. Sudah menjadi pemahaman publik bahwa inherent risk adalah diluar jangkauan auditor dalam melakukan pencegahan. Bahkan, juga diluar kendali pihak auditee sendiri. Jadi dengan kata lain, auditor hanya bisa menemukan tetapi tidak bisa melakukan apa-apa.

d. **Control Risk (Risiko Pengendalian)**
   Ukuran penetapan auditor akan kemungkinan adanya kekeliruan (salah saji) dalam segmen audit yang melampaui batas toleransi yang tidak terdeteksi atau tercegah oleh struktur pengendalian intern klien. Risiko pengendalian Atau 'Control Risk' (CR) adalah risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, tak tahu karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain—thus tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). Jadi CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau.

3. Efek dari Risiko

Efek Risiko dalam sistem informasi ditemui pada:

- Strategi (Strategic): risiko dimana sistem informasi tidak sesuai dengan tujuan organisasi dan tidak mendukung pencapaian misi.
- Operasi (Operations): risiko dimana sistem informasi menimbulkan beban yang terlalu besar bagi organisasi. Selain itu ketergantungan organisasi terhadap suatu sistem informasi berarti apabila sistem tersebut tidak tersedia selama waktu tertentu dapat menimbulkan risiko besar bagi operasional.
- Pelaporan (Reporting): risiko dimana sistem informasi tidak dapat diandalkan untuk menghasilkan informasi yang akurat, lengkap dan tepat waktu.
- Kepatuhan (Compliance): risiko dimana sistem informasi malah menimbulkan pelanggaran hukum dan regulasi yang merugikan bagi organisasi baik secara finansial maupun reputasi.

4. Bukti Audit

Bukti adalah informasi yang dimaksudkan untuk membuktikan atau mendukung suatu keyakinan.Bukti audit hendaknya memenuhi kriteria berikut:

- Cukup (Sufficient). Faktual, memadai dan meyakinkan dimana seseorang yang bijak akan mengambil kesimpulan yang sama dengan auditor.
- Kompeten(Competent). Handal dan merupakan Dapat diandalkan dan hasil terbaik dari penggunaan metode audit yang tepat.
- Relevan(Relevant). Mendukung temuan dan rekomendasi auditserta konsisten dengan tujuan audit.
- Berguna (Useful). Membantu organisasi dalam mencapai tujuannya.

5. Jenis Bukti Audit

a. Bukti Fisik (Physical evidence). Secara umum diperoleh dari hasil pengamatan terhadap orang, properti atau peristiwa bisa dalam bentuk foto, peta dan sebagainya. Bukti yang diperoleh dari hasil pengamatan haruslah didukung dengan contoh-contoh yang terdokumentasi atau bila tidak memungkinkan hendaknya didukung pengamatan lain yang menguatkan

b. Bukti Kesaksian (Testimonial evidence). Dapat berbentuk surat, pernyataan atau wawancara yang tidak bersifat konklusif karena merupakan pendapat seseorang. Bukti jenis ini hendaknya didukung dokumentasi selama memungkinkan.

c. Bukti Dokumen (Documentary evidence). Merupakan bukti yang paling lazim dalam audit bisa berupa surat, perjanjian, kontrak, perintah, memo dan berbagai jenis dokumen bisnis lain. Bukti jenis ini dapat juga diperoleh dari arsip komputer menggunakan alat dan teknik audit yang tepat. Sumber

dokumen akan menentukan tingkat kehandalan dan tingkat kepercayaan, tentunya kualitas proses kontrol internal ikut dipertimbangkan.

d. Bukti Analitis (Analytical evidence). Umumnya diperoleh dari hasil komputasi, perbandingan terhadap standar, operasi masa lalu atau operasi sejenis. Penggunaan perangkat komputer yang tepat sangat membantu auditor pada perolehan bukti jenis ini. Regulasi dan penalaran umum juga dapat menghasilkan bukti jenis ini.

6. Prosedur Bukti Audit

Auditor sangat bergantung pada pengumpulan bukti.Hal ini dilakukan melalui berbagai cara dan mengikuti Program Audit. Program Audit adalah serangkaian langkah-langkah yang rinci yang harus diikuti auditor untuk mendapatkan bukti yang tepat dan pada auditor sistem informasi hal ini berupa penggunaan teknik komputasi tertentu walaupun bisa juga bukan.

Program audit dibutuhkan untuk menciptakan audit yang efektif dan efisien. Menurut Jack J. Champlain(2003) selain itu masih memiliki dua keuntungan lain yaitu:

a. Membantu manajemen audit dalam perencanaan sumber daya, misal dapat dihitung berapa total jam yang dibutuhkan untuk melaksanakan audit berdasarkan waktu yang diharapkan untuk melaksanakan setiap langkah-langkah audit pada program audit.
b. Membantu konsistensi dalam pengujian pengendalian yang umum.

7. Tanggung Jawab terhadap Deteksi dan Pencegahan Kecurangan (Fraud)

Tanggung jawab terhadap deteksi dan pencegahan kecurangan termasuk kecurangan dalam sistem informasi merupakan tanggungjawab dari pengelola (operational management).Auditormemiliki peran dalam hal membantu pengelola menerapkan sistem kontrol dimana fraud kecil kemungkinan terjadi, tetapi apabila terjadi akan cepat dideteksi.

B. AUDIT Sistem Informasi

1. Definisi Audit Sistem Informasi

Audit memiliki beberapa definisi yang dinyatakan menurut beberapa ahli. Menurut Ikatan Akuntan Indonesia (IAI) pada PSAK (Pernyataan Standar Audit keuangan) menyebutkan bahwa Audit adalah suatu proses sistematik yang bertujuan untuk memperoleh dan mengevaluasi bukti yang dikumpulkan atas pernyataan atau asersi tentang aksi-aksi ekonomi, kejadian-kejadian dan melihat tingkat hubungan antara pernyataan atau asersi dan kenyataan, serta mengkomunikasikan hasilnya kepada yang berkepentingan.

Menurut Arens Loebbecke, Audit adalah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi termasuk dengan kriteria-kriteria yang telah ditetapkan.

Auditor merupakan pemeriksa, dimana terdapat dua jenis auditor yaitu internal daneksternal. Auditor internal ada di dalam organisasi itu sendiri misalkan divisi kepatuhan di perusahaan dan Inspektorat Jenderal pada instansi pemerintah. Auditor eksternal merupakan auditor yang berasal dari luar organisasi misalkan Kantor Akuntan Publikdan Badan Pemeriksa Keuangan. *Auditee* adalah pihak yang diperiksa. Pihak yang diperiksa ini adalah manajemen beserta personil lain pada organisasi.

Audit Sistem Informasi memiliki beberapa fokus tujuan, salah satunya adalah pada tata kelola TI atau *IT Governance*. Tata kelola TI adalah suatu cabang dari tata kelola perusahaan yang terfokus pada sistem teknologi informasi (TI) serta manajemen kinerja dan risikonya.

2. Jenis-Jenis Audit

Adapun Jenis-jenis audit sistem informasi yang lazim diketahui meliputi:

a. **Financial Audit,** adalah suatu review atas kelayakan penyajian laporan keuangan yang dibuat manajemen.
b. **Compliance Audit** (Audit Kepatuhan Tata Tertib Peraturan), adalah pemeriksaan terhadap tingkat kepatuhan para pelaksana opersional perusahaan dalam menjalakan setiap prosedur dan kebijaksanaan yang telah ditetapkan.
c. **Operational Audit,** adalah suatu pemeriksaan yang mencakup suatu hal atau operasi tertentu yang biasanya diluar juridiksi controller atau treasureer dalam suatu perusahaan/operasi
d. **Special Audit,** adalah pemeriksaan yang dilakukan apabila diketahui adanya indikasi kecurangan yang dilakukan oleh manajemen atau apabila pemeriksaan tersebut diluar dari pada golongan pemeriksaan keuangan, pemeriksaan opersional dan pemeriksaan kepatuhan
e. **Information System Audit,** adalah pemeriksaan sistem yang mengatur pengembangan, pengoperasian, pemeliharaan dan keamanan sistem aplikasi dalam lingkungan tertentu

Perbedaan audit sistem infromasi dengan audit keuangan yaitu fungsi audit keuangan mengevaluasi apakah suatu organisasi sudah mematuhi

standar akuntansi, sementara fungsi audit sistem informasi melakukan tinjauan atas desain pengendalian sistem informasi serta efektifitasnya.

Jenis-jenis audit Sistem Informasi dikelompokkan berdasarkan Luas Pemeriksaan, Bidang Pemeriksan dan Kelompok Pelaksana Audit (Auditor).

a. Jenis-jenis audit ditinjau dari luas pemeriksaan
   1) **Pemeriksaan Umum *(General Audit)***
      Merupakan suatu pemeriksaaan umum atas laporan keuangan yang dilakukan oleh Kantor Akuntan Publik (KAP) yang indipendent dengan tujuan dapat menilai sekaligus memberikan opini mengenai kewajaran laporan keuangan.
   2) **Pemeriksaan Khusus *(Special Audit)***
      Merupakan suatu pemeriksaan yang hanya terbatas hanya pada permintaan audit yang dilakukan oleh Kantor Akuntan Publik (KAP). Dengan memberikan opini
b. Jenis-jenis audit ditinjau dari bidang pemeriksaan
   1) **Audit Laporan Keuangan (*Financial Statement Audit)***
      Berkaitan dengan kegiatan mengumpulkan dan mengevaluasi bukti tentang laporan-laporan suatu entitas dengan tujuan memberikan pendapat (opini) tentang laporan tersebut apakah sesuai dengan kriteria yang ditetapkan sesuai prinsip-prinsip akuntansi yang berlaku umum.
   2) **Audit Operasional *(Management Audit)***
      Adalah jenis pemeriksaan terhadap kegiatan operasi suatu perusahaan. meliputi kebijakan akuntansi dan kebijakan operasional manajemen yang telah ditetapkan, dengan tujuan untuk mengetahui kegiatan operasi yang dilakukan berjalan secara efektif dan efisien.
   3) **Audit Ketaatan *(Compliance Audit)***
      Audit ketaatan berfungsi untuk menentukan sejauh mana perusahaan mentaati peraturan, kebijakan, peraturan pemerintah bahkan hukum yang harus dipatuhi oleh entitas yang di audit.
   4) **Audit Sistem Informasi**
      Yaitu pemeriksaan yang dilakukan Kantor Akuntan Publik (KAP) terhadap perusahaan yang melakukan proses data akuntansi, umumnya menggunakan system *Elektronik Data Processing*(EDP). Auditor harus memperhatikan hal-hal berikut :
      - Perlengkapan keamanan melindungi perlengkapan computer baik program, komunikasi, atau data dari akses yang tidak sah, modifikasi bahkan penghancuran.

- Pengembangan program yang dilakukan atas otorisasi khusus dan umum dari pihak manajemen perusahaan.
- Pemrosesan transaksi, file, laporan dan catatan computer dengan akurat dan lengkap.
- Data file laporan yang tersimpan di computer sangat dijaga kerahasiaanya.

5) **Audit Forensik**

Tujuan dilakukan audit forensic adalah sebagai upaya pencegahan terjadinya kecurangan (*fraud).* Hal yang dapat dilakukan audit forensik termasuk :

- Investigasi kriminal
- Indikasi kecurangan dalam bisnis atau karyawan
- Mengetahui kerugian suatu bisnis

6) **Audit Investigasi**Yang dimaksud audit investigasi adalah serangkaian kegiatan mengenali *(recorganized),*menidentifikasi *(Identify)* dan menguji *(examine)* fakta-fakta dan informasi yang ada guna mengungkap kejadian yang sebenarnya dalam rangka pembuktian demi mendukung proses hukum atas dugaan penyimpangan yang dapat merugikan keuangan suatu entitas (organisasi/perusahaan/negara/daerah).

7) **Audit Lingkungan**

Menurut (Kep. Men. LH 42/1994) audit lingkungan adalah proses manajemen yang meliputi evaluasi secara sistematik, tercatat (terdkumentasi), serta obyektif tentang bagaimana suatu kinerja manajemen organisasi yang bertujuan memfasilitasi kendali manajemen terhadap upaya pengendalian dampak lingkungan dan pemanfaatan kebijakan usaha terhadap perundang-undangan tentang pengelolaan lingkungan.

c. Jenis-jenis audit ditinjau dari kelompok pelaksana audit (auditor)

1) Auditor Internal

Mempunyai tugas membantu manajemen puncak *(top management)* dalam mengawasi asset *(saveguard of asset)* dan mengawasi kegiatan operasional perusahaan sehari-hari. bekerja untuk perusahaan yang mereka audit, oleh karena itu tugas auditor intern adalah mengaudit manajemen perusahaan termasuk *compliance* audit.

2) Auditor Ekstern

Bekerja untuk lembaga/kantor akuntan publik (pihak ke-3) yang statusnya diluar struktur perusahaan yang mereka audit dan bekerja

secara independent dan objektif. Umumnya auditor ekstern menghasilkan laporan *financial* audit.

3) **Auditor Pajak**
   Mempunyai tugas melakukan ketaatan wajib pajak yang diaudit menurut undang-undang perpajakan yang berlaku. Di Indonesia dilaksanakan oleh Direktorat Jendral Pajak (DJP) yang berada dibawah naungan Departemen Keuangan Republik Indonesia.
4) **Auditor Pemerintah**
   Adalah lembaga yang mempunyai tugas menilai kewajaran informasi laporan keuangan instansi pemerintah atas pelaksanaan program dan penggunaan asset milik pemerintah. Audit instansi pemerintah umumnya dilaksanakan oleh Badan Pemeriksa Keuangan (BPK) atau Badan Pemeriksa Keuangan dan Pembangunan (BPKP).

3. Hubungan Auditor dan Auditee

Hubungan auditor dengan auditee yaitu audit merupakan praktik manajemen yang lazim dilakukan terhadap organisasi manapun di dunia. Tetapi masih sering sekali terjadi bahwa auditee resisten terhadap pelaksanaan audit atau terhadap personil auditor. Auditee pada awalnya cenderung bereaksi negatif terhadap auditor, audit dipersepsikan sebagai usaha mencari-cari kesalahan belaka.Hal ini bisa diatasi dengan meningkatkan komunikasi antara dua pihak, auditee harus memahami standar atau aturan kerja yang melandasi pekerjaan auditor. Auditor juga harus memahami standar operasional dan aturan auditee. Auditee setidaknya harus memahami beberapa hal mendasar berikut:

- Definsi audit
- Definis temuan
- Atribut temuan
- Fungsi audit
- Jenis bukti
- Proses audit
- Jenis temuan

Auditor TI bertanggung jawab atas penilaian efisiensi tata kelola TI dengan tingkatan prosedur dalam pelaksanaannya. Auditor TI (dari dalam organisasi atau independen) dapat melakukan sejumlah peran kunci dalam Gary Hardy, “The Role of the IT Auditor in IT Governance” 1 (2009) :

- memulai program tata kelola TI: menjelaskan tata kelola TI dan nilainya pada manajemen

- menilai kondisi saat ini: memberikan masukan dan membantu memberikan penilaian kondisi yang sebenarnya
- merencanakan solusi tata kelola TI
- memantau inisiatif tata kelola TI
- membantu membuat bisnis tata kelola TI, seperti : memberikan input objektif dan konstruktif, mendorong penilaian diri, dan memberikan keyakinan kepada manajemen bahwa tata kelola bekerja secara efektif.

Karakteristik audit mencakup tiga ciri dasar sebagai berikut (Pusat Pendidikan Dan Pelatihan Pengawasan Badan Pengawasan Keuangan dan Pembangunan, 2009):

- Auditing merupakan suatu proses penilaian.
- Penilaian tersebut dilakukan terhadap informasi, kondisi, operasi, dan/atau pengendalian.
- Penilaian harus dilakukan secara objektif oleh pihak yang kompeten dan independen.

Organisasi sektor publik dalam hal ini pemerintahan, mendapatkan amanah dan kepercayaan dari masyarakat untuk menggunakan sumber daya publik. Oleh karenanya, dituntut pengelolaan sumber daya tersebut secara akuntabel dan transparan. Selanjutnya untuk meningkatkan pengelolaan tersebut diperlukan audit pada sektor publik. Secara umum tidak ada perbedaan mendasar antara audit sektor publik dan privat. Namun diperlukan perhatian khusus, karena karakteristik manajemen sektor publik berkaitan erat dengan kebijakan dan pertimbangan politik serta ketentuan perundang-undangan.

Berdasarkan UU No. 15 tahun 2004 terdapat tiga jenis audit menurut tujuan pelaksanaan audit, yaitu: audit keuangan, audit kinerja dan audit dengan tujuan tertentu.

- Audit keuangan adalah untuk menentukan apakah informasi keuangan telah akurat dan dapat diandalkan (sesuai Standar Akuntansi Pemerintahan/SAP), serta untuk memberikan opini kewajaran atas penyajian laporan keuangan.
- Audit kinerja adalah pemeriksaan atas pengelolaan keuangan negara yang terdiri atas pemeriksaan aspek ekonomi dan efisiensi serta pemeriksaan aspek efektivitas. Dalam melakukan audit kinerja, auditor juga menguji kepatuhan terhadap ketentuan perundang-undangan serta pengendalian intern. Audit kinerja menghasilkan temuan, simpulan, dan rekomendasi. Menentukan: keandalan informasi kinerja, tingkat

ketaatan, pemenuhan standar mutu operasi, efisiensi, ekonomis, dan efektivitas.

- Audit dengan tujuan tertentu adalah pemeriksaan yang tidak termasuk dalam pemeriksaan keuangan dan pemeriksaan kinerja/audit operasional. Sesuai dengan definisinya, jenis audit ini dapat berupa semua jenis audit, selain audit keuangan dan audit operasional. Jenis audit ini termasuk di antaranya audit ketaatan dan audit investigatif. Audit ketaatan bertujuan untuk menentukan apakah peraturan ekstern serta kebijakan dan prosedur intern telah dipenuhi. Audit investigatif bertujuan untuk menentukan apakah kecurangan/ penyimpangan benar terjadi.

Di dalamnya, belum diatur secara khusus mengenai audit yang difokuskan pada manajemen kinerja dan risiko dalam sistem pengelolaan Teknologi Informasi (TI) di instansi pemerintah. Kemudian untuk menunjang hal tersebut, diperlukan metodologi audit yang tujuannya berbeda dengan metode pada audit keuangan, audit kinerja dan audit dengan tujuan tertentu.

Dikarenakan audit memegang peranan penting sebagai salah satu bentuk pengawasan pada instansi pemerintah, maka perlu dipertimbangkan agar pemerintah Indonesia membuat pedoman audit yang memiliki tujuan khusus dalam pemeriksaan tata kelola TI di instansi pemerintah. Tujuannya adalah melakukan penilaian atas tata kelola TI dengan tingkatan prosedur dalam pelaksanaannya, serta memberikan masukan dan solusi pada instansi pemerintah agar tata kelola TI bekerja secara efektif dan efisien. Untuk itulah diusulkan sebuah metodologi audit tata kelola TI di instansi pemerintah Indonesia, yang diharapkan dapat memberikan manfaat dan dijadikan sebagai pedoman dalam audit tata kelola TI.

4. Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi pada tata kelola TI diantaranya adalah:

a. **Meningkatkan pengamanan aset**

Asset (aktiva) yang berhubungan dengan instalasi sistem informasi mencakup: perangkat keras, perangkat lunak, fasilitas, manusia, *file* data, dokumentasi sistem, dan peralatan pendukung lainnya. Sama halnya dngan aktiva – aktiva lainnya, maka aktiva ini juga perlu dilindungi dengan memasang pengendalian internal. Perangkat keras bisa rusak karena unsur kejahatan ataupun sebab-sebab lain. Perangkat lunak dan isi *file* data dapat dicuri. Peralatan pendukung

dapat dihancurkan atau digunakan untuk tujuan yang tidak diotorisasi. Karena konsentrasi aktiva tersebut berada pada lokasi pusat sistem informasi, maka pengamanannya pun menjadi perhatian dan tujuan yang sangat penting.

b. **Menjaga integritas data**
   Integritas data merupakan konsep dasar audit sistem informasi. Integritas data berarti data memiliki atribut: kelengkapan (*completeness*), sehat dan jujur (*soundness*), kemurnian (*purity*), ketelitian (*veracity*). Tanpa menjaga integritas data, organisasi tidak dapat memperlihatkan potret dirinya dengan benar akibatnya, keputusan maupun langkah-langkah penting di organisasi salah sasaran karena tidak didukung dengan data yang benar.

c. **Meningkatkan efektivitas system**
   Sistem informasi dikatakan efektif hanya jika sistem tersebut dapat mencapai tujuannya. Untuk menilai efektivitas sistem, auditor sistem informasi harus tahu mengenai kebutuhan pengguna sistem atau pihak-pihak pembuat keputusan yang terkait dengan layanan sistem tersebut. Selanjutnya, untuk menilai apakah sistem menghasilkan laporan / informasi yang bermanfaat bagi penggunanya, auditor perlu mengetahui karakteristik user berikut proses pengambilan keputusannya.

d. **Mengingkatkan efisiensi sumber daya**
   Suatu sistem sebagai fasilitas pemrosesan informasi dikatakan efisien jika ia menggunakan sumber daya seminimal mungkin untuk menghasilkan *output* yang dibutuhkan. Efisiensi sistem pengolahan data menjadi penting apabila tidak ada lagi kapasitas sistem yang menganggur.

Audit sistem informasi pada tata kelola TI yang sering dilakukan adalah menggunakan kerangka kerja COBIT. Contoh penerapannya dapat disimak pada paper Setia Wardani dan Mita Puspita Sari dari Fakultas Teknik Universitas PGRI Yogyakarta (UPY) tahun 2014 dengan judul *"Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT Dengan Model Maturity Level".*

5. Sasaran Audit Sistem Informasi
Untuk mengulas, menilai dan melaporkan :

a. Kelayakan, kecukupan dan penerapan standar operasi sistem informasi.
b. Kelayakan, kecukupan dan penerapan standar pengembangan sistem.
c. Tingkat kepatuhan terhadap standar organisasi.

d. Keamanan terhadap investasi sistem informasi organisasi.
e. Kecukupan pengaturan kontingensi.
f. Kelengkapan dan ketepatan informasi yang diproses oleh computer.
g. Apakah semua sumber daya komputer telah digunakan secara optimal.
h. Kelayakan sistem aplikasi yang dikembangkan.

6. Fungsi Audit Sistem Informasi

Fungsi audit sistem informasi dan fungsi audit umum terdapat berbagai pandangan berbeda. Pandangan yang pertama yang biasanya diyakini oleh auditor sistem informasi sendiri bahwa setiap audit terhadap pengendalian yang melibatkan komputer hendaknya dilakukan oleh auditor sistem informasi professional.

Pandangan yang berlawanan meyakini auditor sistem informasi dan auditor umum haruslah terintegrasi seutuhnya. Diantara kedua pandangan tadi masih ada pandangan lain yang lebih banyak diyakini secara umum. Bahwa ada keuntungan pada beberapa area audit yang melibatkan review terhadap sistem komputer apabila dilakukan oleh auditor umum yang memahami sistem informasi.

Audit sistem informasi dapat juga dipandang sebagai fungsi pendukung terhadap keseluruhan fungsi audit internal dan mungkin melibatkan pengembangan alat/metode komputasi audit, membantu auditor non sistem informasi bahkan pelatihan terhadap auditor non sistem informasi.

Auditor sistem informasi bisa juga dilibatkan dalam pengembangan prosedur pengendalian untuk penggunaan komputer pada lingkungan internal dengan memastikan hasil penelitian sistem informasi yang lebih modern dan teknik audit sistem informasi diterapkan.

C. AUDIT TATA KELOLA TI

Tata Kelola TI adalah suatu cabang dari tata kelola perusahaan yang terfokus pada Sistem/Teknologi informasi serta manajemen Kinerja dan risikonya. Tata kelola TI adalah struktur kebijakan atau prosedur dan kumpulan proses yang bertujuan untuk memastikan kesesuaian penerapan TI dengan dukungannya terhadap pencapaian tujuan institusi, dengan cara mengoptimalkan keuntungan dan kesempatan yang ditawarkan TI, mengendalikan penggunaan terhadap sumber daya TI dan mengelola resiko-resiko terkait TI.

Tata kelola TI merupakan suatu proses pengendalian manajemen organisasi terhadap sumber daya TI/sistem informasi yang dibeli, yang mencakup mulai dari sumber daya komputer (software, brainware,

database dan sebagainya) hingga ke Teknologi Informasi dan Jaringan LAN/Internet.

IT Governance terdiri dari struktur organisasi, kepemimpinan, dan proses yang memastikan IT dapat mendukung strategi dan tujuan organisasi. Ada 5 komponen dari IT Governance yaitu Struktur Organisasi dan Governance, Kepemimpinan dan Dukungan Eksekutif, Perencanaan strategis dan opresional, Penyampaian Service dan pengukuran, Organisasi IT dan Manajemen Resiko.

Kerangka tata kelola TI salah satunya adalah COBIT terdiri atas beberapa arahan/pedoman, yakni:

1. Control Objectives, Terdiri atas 4 tujuan pengendalian tingkat-tinggi (high-level control objectives) yang terbagi dalam 4 domain, yaitu : Planning & Organization , Acquisition & Implementation , Delivery & Support , dan Monitoring & Evaluation.
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 :
    - Sejauh mana TI harus bergerak atau digunakan, dan apakah biaya TI yang dikeluarkan sesuai dengan manfaat yang dihasilkannya.
    - Apa saja indikator untuk suatu kinerja yang bagus.
    - Apa saja faktor atau kondisi yang harus diciptakan agar dapat mencapai sukses (critical success factors).
    - Apa saja risiko-risiko yang timbul, apabila kita tidak mencapai sasaran yang ditentukan.
    - Bagaimana dengan perusahaan lainnya, apa yang mereka lakukan.
    - Bagaimana mengukur keberhasilan dan bagaimana pula membandingkannya.

Audit *IT Governance* membutuhkan pengetahuan yang lebih dibandingkan audit Sistem Informasi biasa karena auditor TI harus mengevaluasi sejauh mana TI mendukung strategi bisnis. Audit tata kelola TI memiliki tujuan khusus untuk memeriksa pengelolaan sumber daya TI, apakah dapat mendukung dan sejalan dengan strategi bisnis. Metode yang dihasilkan dapat dijadikan sebagai salah satu acuan auditor

pemerintah dalam mengevaluasi risiko yang terkait dengan audit tata kelola TI.

Audit sistem informasi umumnya digunakan untuk menjelaskan perbedaan jenis aktivitas yang terkait dengan komputer. Seperti untuk menjelaskan pengkajian ulang proses dan evaluasi pengendalian internal dalam sebuah sistem pemrosesan data elektronik. Sementara audit *IT Governance* mencakup lingkup yang lebih luas, bertujuan untuk memeriksa apakah tata kelola sumber daya TI (termasuk di dalamnya manajemen organisasi dan pimpinan) dapat mendukung dan sejalan dengan strategi bisnis.

Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia:

- mengalokasikan sumber daya TI sesuai dengan prioritas bisnis
- melaksanakan pengendalian dengan memadai yang memungkinkan identifikasi infrastruktur TI lebih terpenuhi
- mempertahankan investasi yang layak dalam pengembangan staf, pengembangan pendidikan dan pelatihan operasional TI.

Dalam audit tata kelola TI dikenal 3 jenis audit meliputi:

1. **System Audit,** Audit terhadap sistem terdokumentasi untuk memastikan sudah memenuhi standar nasional atau internasional
2. **Compliance Audit,** Untuk menguji efektifitas implementasi dari kebijakan, prosedur, kontrol dan unsur hukum yang lain
3. **Product / Service Audit,** Untuk menguji suatu produk atau layanan telah sesuai seperti spesifikasi yang telah ditentukan dan cocok digunakan

DAFTAR PUSTAKA

1. Cascarino,Richard.2007.Auditor’s Guide to Information Systems Auditing.Wiley: New Jersey.
2. Champlain, J, Jack.2003.Auditing Information Systems Second Edition.Wiley: New Jersey.
3. Indrajit, R.E. 2016. Konsep Dasar Tata Kelola Teknologi Informasi. The Preinexus Indonesia.
4. ITGI. 2005. IT Governance A Framework for Performance and Compliance: Board briefing on IT governance. www.itgi.org
5. Setiawan, H. & Mustofa, H. 2013. Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia. *IPTEK-KOM*, Vol. 15 No. 1 Juni 2013: 1-15
6. Suswinarno, 2012. Aman dari Risiko dalam Pengadaan Barang/Jasa Pemerintah. Visimedia: Jakarta