Jelaskan berdasarkan pendapat anda, mengapa kita harus melakukan Audit TI ?

dan sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini

Dampak dan Pentingnya Audit SI bagi Perusahaan atau Organisasi

Perkembangan teknologi telah mengakibatkan perubahan pengolahan data yang dilakukan perusahaan dari sistem manual menjadi secara mekanis, elektromekanis, dan selanjutnya ke sistem elektronik atau komputerisasi. Peralihan ke sistem yang terkomputerisasi memungkinkan data yang kompleks dapat diproses dengan cepat dan teliti, guna menghasilkan suatu informasi. Dalam mendukung aktivitas sebuah organisasi, informasi menjadi bagian yang sangat penting baik untuk perkembangan organisasi maupun membaca persaingan pasar. Dalam hal proses data menjadi suatu informasi merupakan sebuah kegiatan dalam organisasi yang bersifat repetitif sehingga harus dilaksanakan secara sistematis dan otomatis.

Dengan demikian, sangat diperlukan adanya pengelolaan yang baik dalam sistem yang mendukung proses pengolahan data tersebut. Dalam sebuah organisasi tata kelola sistem dilakukan dengan melakukan audit. Menurut Juliandarini (2013) Audit sistem informasi (Information Systems (IS) audit atau Information technology (IT) audit) adalah bentuk pengawasan dan pengendalian dari infrastruktur sistem informasi secara menyeluruh.Menurut Romney (2004) audit sistem informasi merupakan tinjauan pengendalian umum dan aplikasi untuk menilai pemenuhan kebijakan dan prosedur pengendalian internal serta keefektivitasannya untuk menjaga asset.

Sehingga menurut uraian teori diatas, maka penulis dapat simpulkan bahwa audit sistem informasi adalah suatu proses pengumpulan dan pengevaluasian bahan bukti audit untuk menentukan apakah sistem komputer perusahaan telah menggunakan asset sistem informasi secara tepat dan mampu mendukung pengamanan asset tersebut memelihara kebenaran dan integritas data dalam mencapai tujuan perusahaan yang efektif dan efisien.

Menurut Weber (1999) terdapat beberapa alasan mendasar mengapa organisasi perlu melakukan audit sebagai evaluasi dan pengendalian terhadap sistem yang digunakan oleh organisasi :

1. Pencegahan terhadap biaya organisasi untuk data yang hilang

Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan backup yang memadai terhadap file data, sehingga kehilangan file dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat file tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu.

2. Pengambilan keputusan yang tidak sesuai

Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang – orang yang berkepentingan di suatu organisasi.

3. Penyalahgunaan computer

Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi.

4. Nilai dari perangkat keras komputer, perangkat lunak dan personel

Disamping data, hardware dan software serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi hardware perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan hardware baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika software rusak akan mengganggu jalannya operasional dan bila software dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional.

5. Biaya yang tinggi untuk kerusakan computer

Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data error mengakibatkan jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer.

6. Kerahasiaan

Banyak data tentang diri pribadi yang saat ini dapat diperoleh dengan cepat, dengan adanya komputerisasi kependudukan maka data mengenai seseorang dapat segera diketahui termasuk hal – hal pribadi.

7. Pengontrolan penggunaan computer

Teknologi adalah hal yang alami, tidak ada teknologi yang baik atau buruk. Pengguna teknologi tersebut yang dapat menentukan apakah teknologi itu akan menjadi baik atau malah menimbulkan gangguan. Banyak keputusan yang harus diambil untuk mengetahui apakah komputer digunakan untuk suatu hal yang baik atau buruk.

Menurut Weber (1999) terdapat empat tujuan utama mengapa perlu dilakukannya audit sistem informasi yaitu:

(1) Mengamankan asset

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.

(2) 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.

(3) Menjaga 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.

(4) Mencapai 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.

Ancaman-ancaman atas Prinsip Dasar Etika Audit

- **Kepentingan diri *(self-interest*)**

Kepentingan Diri adalah wujud sifat yang lebih mengutamakan kepentingan pribadi atau keluarga dibandingkan dengan kepentingan publik yang lebih luas. Contoh langsung Ancaman Kepentingan Diri untuk akuntan publik, antara lain:

Kepentingan keuangan dalam perusaahan klien, atau kepentingan keuangan bersama pada suatu perusaah klien.

Kekhawatiran berlebiahan bila kehilangan suatu klien.

Contoh langsung Ancaman Kepentingan Diri untuk akuntan bisnis, antara lain:

Perjanjian kompensasi insentif.

Penggunaan harta perusahaan yang tidak tepat.

Tekanan komersial dari pihak di luar perusahaan

- **Review diri (*Self-review*)**

Ancaman yang disebabkan oleh ketidaktepatan akuntan dalam mengevaluasi hasil pertimbangan. Contoh Ancaman Review Diri untuk akuntan publik antara lain:

Temuan kesalahan material saat dilakukan evaluasi ulang.

Pelaporan operasi sistem keuangan setelah terlibat dalam perancangan dan implementasi sistem tersebut.

Contoh Ancaman Review Diri untuk akuntan bisnis, yaitu keputusan bisnis atau data yang sedang ditinjau oleh akuntan frofesional yang sama yang membuat keputusan bisnis atau penyiapan data tersebut.

- **Advokasi (*Advocacy*)**

Ancaman Advokasi dapat timbul bila akuntan profesional endukung suatu posisi atau pendapat sampai titik dimana objektivitas dapat dikompromikan. Contoh langsung ancaman untuk akuntan publik antara lain :

Mempromosikan saham perusahaan publik dari klien, dimana perusahaan tersebut merupakan klien audit.

Bertindak sebagai pengacara (penasihat hukum) untuk klien penjaminan dalam suatu litigasi atau perkara perselisihan dengan pihak ketiga.

- **Kekerabatan (*Familiarity*)**

Ancaman kekerabatan timbul dari kedekatan hubungan sehingga akuntan profesional menjadi terlalu bersimpati terhadap kepentingan orang lain yang mempunyai hubungan dekat dengan akuntan tersebut. Contoh langsung Ancaman Kekerabatan untuk akuntan publik, antara lain:

Anggota tim mempunyai hubungan keluarga dekat dengan seorang direktur atau pejabat perusahaan klien.

Anggota tim mempunyai hubungan keluarga dekat dengan seorang karyawan klien yang memiliki jabatan yang berpengaruh langsung dan segnifikan terhadap pokok dari penugasan.

Contoh langsung Ancaman Kekerabatan untuk akuntan bisnis, antara lain:

Hubungan yang lama dengan rekan bisnis yang mempunyai pengaruh pada keputusan bisnis.

Penerimaan hadiah atau perlakuan khusus, kecuali nilainya tidak segnifikan.

- **Intimidasi (*Intimidation*)**

Ancaman Intimidasi dapat timbul jika akuntan profesional dihalang untuk bertindak objektif, baik secara nyata maupun dipersepsikan. Contoh Ancaman Intimidasi untuk Akuntan Publik, antara lain:

Diancam dipecat atau diganti dalam hubungannya dengan penugasan klien.

Diancam dengan tuntutan hukum.

Ditekan secara tidak wajar untuk mengurangi ruang lingkup pekerjaan dengan maksud untuk mengurangi fee.

Mengapa kita harus melakukan Audit TI?

Dalam mendukung aktivitas sebuah organisasi, informasi menjadi bagian yang sangat penting baik untuk perkembangan organisasi maupun membaca persaingan pasar. Dalam hal proses data menjadi suatu informasi merupakan sebuah kegiatan dalam organisasi yang bersifat repetitif sehingga harus dilaksanakan secara sistematis dan otomatis.

Dengan demikian, sangat diperlukan adanya pengelolaan yang baik dalam sistem yang mendukung proses pengolahan data tersebut. Dalam sebuah organisasi tata kelola sistem dilakukan dengan melakukan audit. Menurut Juliandarini (2013) Audit sistem informasi (Information Systems (IS) audit atau Information technology (IT) audit) adalah bentuk pengawasan dan pengendalian dari infrastruktur sistem informasi secara menyeluruh.Menurut Romney (2004) audit sistem informasi merupakan tinjauan pengendalian umum dan aplikasi untuk menilai pemenuhan kebijakan dan prosedur pengendalian internal serta keefektivitasannya untuk menjaga asset.

5 jenis ancaman yang melatarbelakangi perlunya Audit TI

Macam ancaman	**Contoh**
Bencana alam	Gempa bumi, banjir, kebakaran, perang.
Kesalahan manusia	Kesalahan pemasukan data. Kesalahan penghapusan data. Kesalahan operator(salah memberi label pada pita magnetik.
Kegagalan perangkat lunak dan perangkat keras	Gangguan listrik. Kegagalan peralatan. Kegagalan fungsi perangkat lunak.
Kecurangan dan kejahatan komputer	Penyelewengan aktivitas. Penyalagunaan kartu kredit. Sabotase. Pengaksesan oleh orang lain yang tidak berhak
Program yang jahat/usil	Virus, cacing, bom waktu dll.

1.) jelaskan berdasarkan pendapat anda, mengapa kita harus melakukan Audit IT...?

Diera sekarang ini teknologi telah mengakibatkan perubahan pengolahan data yang dilakukan perusahaan dari sistem manual menjadi secara mekanis, elektromekanis, dan selanjutnya ke sistem elektronik atau komputerisasi. Peralihan ke sistem yang terkomputerisasi memungkinkan data yang kompleks dapat diproses dengan cepat dan teliti, guna menghasilkan suatu informasi. Dalam mendukung aktivitas sebuah organisasi, informasi menjadi bagian yang sangat penting baik untuk perkembangan organisasi maupun membaca persaingan pasar. Dalam hal proses data menjadi suatu informasi merupakan sebuah kegiatan dalam organisasi yang bersifat repetitif sehingga harus dilaksanakan secara sistematis dan otomatis.

Maka dari itu, sangat diperlukan adanya pengelolaan yang baik dalam sistem yang mendukung proses pengolahan data tersebut. Dalam sebuah organisasi tata kelola sistem dilakukan dengan melakukan audit. Menurut Juliandarini (2013) Audit sistem informasi (Information Systems (IS) audit atau Information technology (IT) audit) adalah bentuk pengawasan dan pengendalian dari infrastruktur sistem informasi secara menyeluruh.Menurut Romney (2004) audit sistem informasi merupakan tinjauan pengendalian umum dan aplikasi untuk menilai pemenuhan kebijakan dan prosedur pengendalian internal serta keefektivitasannya untuk menjaga *asset.*

Sehingga menurut uraian teori diatas, dapat saya simpulkan bahwa audit sistem informasi adalah suatu proses pengumpulan dan pengevaluasian bahan bukti audit untuk menentukan apakah sistem komputer perusahaan telah menggunakan *asset* sistem informasi secara tepat dan mampu mendukung pengamanan *asset* tersebut memelihara kebenaran dan integritas data dalam mencapai tujuan perusahaan yang efektif dan efisien. merupakan konsep dasar audit sistem informasi. Dari alasan dan tujuan tersebut sangat jelas bahwa penting bagi sebuah organisasi untuk melakukan audit sistem informasi guna melihat kembali apakah sistem yang berjalansudah tepat dan terpenting sistem mampu untuk mendukung tercapainya tujuan organisasi

2.) 5 jenis ancaman yang melatarbelakangi perlunya Audit IT dalam suatu organisasi saat ini:

1. Bencana Alam : Misalnya, Bnjir, Kebakaran, Tsunami dan sebagainya.

2. Kesalahan User/Manusia : kurangnya sosialisasi terhadap sistem yang berjalan sehingga dapat membingungkan user dalam menimput data, serta kurangan peraturan dari sebuah organisai.

3. kesalahan sistem : Rentannya kerusakan/eror, penyalahgunaan sistem yang berjalan serta kurangnya pemeliharaan perangkat keras.

4. kejahatan dan kecurangan komputer : ilegal accsess, dengan senganja mengakses sistem secara tidaak sah ke sebuah sistem komputer, serta memalsukan data-data penting di sebuah organisai

5. Perangkat Lunak Jahat/perusak : Misalnya seorang pengembang dengan sengaja menanamkan sebuat back-door, VIRUS,Trojan,Spyware dan virus berbahaya lainya.

Bencana alam	Gempa bumi, banjir, kebakaran, perang dan lain-lain

1. mengapa kita harus melakukan Audit TI

Integritas data merupakan konsep dasar audit sistem informasi. ... Dari alasan dan tujuan tersebut sangat jelas bahwa penting bagi sebuah organisasi untuk melakukan audit sistem informasi guna melihat kembali apakah sistem yang berjalansudah tepat dan terpenting sistem mampu untuk mendukung tercapainya tujuan organisasi

2. 5 jenis ancaman yang melatarbelakangi perlunya Audit TI

Macam ancaman	**Contoh**
Bencana alam	Gempa bumi, banjir, kebakaran, perang.
Kesalahan manusia	Kesalahan pemasukan data. Kesalahan penghapusan data. Kesalahan operator(salah memberi label pada pita magnetik.
Kegagalan perangkat lunak dan perangkat keras	Gangguan listrik. Kegagalan peralatan. Kegagalan fungsi perangkat lunak.
Kecurangan dan kejahatan komputer	Penyelewengan aktivitas. Penyalagunaan kartu kredit. Sabotase. Pengaksesan oleh orang lain yang tidak berhak
Program yang jahat/usil	Virus, cacing, bom waktu dll.

IT AUDIT (TASK 1)

1. mengapa kita harus melakukan Audit TI dan sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini?

Karna didalam suatu organisasi pasti sangat membutuhkan sebuah pengawasan dan pengendalian dari setiap infrastruktur sistem informasi yang ada, baik dalam menilai efektivitas dari infrastruktur sistem informasi tersebut dan juga untuk mendukung kinerja suatu organisasi sehingga dapat mencapai tujuannya.

Berikut 5 jenis ancamannya :

a. Pencegahan terhadap biaya organisasi untuk data yang hilang

b. Pengambilan keputusan yang tidak sesuai

c. Penyalahgunaan computer

d. Pengontrolan penggunaan komputer

e. Nilai dari perangkat keras komputer, perangkat lunak dan personel

Mengapa kita harus melakukan Audit TI ?

Saat ini perusahaan dan organisasi banyak menghabiskan dana untuk investasi dibidang IT. Manfaat IT dalam peningkatan layanan dan proses kerja sebuah organisasi sangat terasa.

Dengan investasi yang cukup besar organisasi perlu memastikan kehandalan dan keamanan dari sistem IT yang akan digunakan. Sistem IT juga harus mampu memenui kebutuhan proses kerja, mampu mengurangi resiko data di sabotasi, kehilangan data, gangguan layanan dan manajemen yang buruk dari sistem IT

Sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini

1. Kehilangan Data

Data merupakan aset teknologi informasi yang sangat kritikal bagi kelangsungan operasional perusahaan.

2. Kesalahan pengambilan keputusan

Sebuah keputusa pada umumnya diambil berdasarkan data dan informasi yang tersedia.

3 Penyalahgunaan komputer

Rsiko kemungkinan penyalahgunaan teknologi yang dapat mengakibatkat kerugian yang bahkan tidak terbayangkan.

4. Nilai investasi

Sebagian investasi dalam teknologi informasi memerlukan dana yang tidak sedikit dan cenderung sulit dikendalikan

5. Aspek privasi

Banyak data dan informasi yang brsifat pribadi tersimpan dalam sistem komputer, seperti misalnya apabila kita mempunyai kartu kredit, maka data tanggal lahir, tempat tinggal, pekerjaan dan lainnya yang terkadang merupakan informasi pribadi akan tersimpan dalam sistem komputer penyedia kartu kredit.

TUGAS IT AUDIT

NAMA : FIDO RIZKI

NIM : 182420060

PERTANYAAN

1. Jelaskan berdasrkan pendapat anda, mengapa kita harus melakukan Audit TI ?
2. Sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini !

JAWAB

1. Audit TI adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. dan dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis. Pada mulanya istilah ini dikenal dengan audit pemrosesan data elektronik, dan sekarang audit TI secara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan itu. Istilah lain dari audit teknologi informasi adalah audit komputer yang banyak dipakai untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya. Maka dari itu, audit TI haruslah dilakukan untuk menjaga keamanan sistem informasi sebagai asset organisasi, untuk mempertahankan integritas informasi yang disimpan dan diolah dan tentu saja untuk meningkatkan keefektifan penggunaan teknologi informasi serta mendukung efisiensi dalam organisasi.

2.Jenis kejahatan atau ancaman (threats) yang dikelompokkan dalam beberapa bentuk antara lain :

- · **Unauthorized Access to Computer System and Service**

Pada kejahatan ini dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia

- · **Illegal Contents**

Kejahatan ini merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum

- · **Data Forgery**

Kejahatan ini merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless document melalui Internet.

- · **Cyber Espionage**

Kejahatan ini merupakan kejahatan yang memanfaatkan jaringan Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (data base) tersimpan dalam suatu sistem yang computerized (tersambung dalam jaringan komputer)

- · **Offense against Intellectual Property**

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh, peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya

Nama : Fitrianto Puja Kesuma NIM : 182420082 terdapat beberapa alasan mendasar mengapa organisasi perlu melakukan audit sebagai evaluasi dan pengendalian terhadap sistem yang digunakan oleh organisasi : 1. Pencegahan terhadap biaya organisasi untuk data yang hilang Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan backup yang memadai terhadap file data, sehingga kehilangan file dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat file tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu. 2. Pengambilan keputusan yang tidak sesuai Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang – orang yang berkepentingan di suatu organisasi. 3. Penyalahgunaan komputer Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi. 4. Nilai dari perangkat keras komputer, perangkat lunak dan personel Disamping data, hardware dan software serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi hardware perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan hardware baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika software rusak akan mengganggu jalannya operasional dan bila software dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional. 5. Biaya yang tinggi untuk kerusakan komputer Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data error mengakibatkan jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer. 6. Kerahasiaan Banyak data tentang diri pribadi yang saat ini dapat diperoleh dengan cepat, dengan adanya komputerisasi kependudukan maka data mengenai seseorang dapat segera diketahui termasuk hal – hal pribadi. 7. Pengontrolan penggunaan komputer Teknologi adalah hal yang alami, tidak ada teknologi yang baik atau buruk. Pengguna teknologi tersebut yang dapat menentukan apakah teknologi itu akan menjadi baik atau malah menimbulkan gangguan. Banyak keputusan yang harus diambil untuk mengetahui apakah komputer digunakan untuk suatu hal yang baik atau buruk.

1. Mengapa kita harus melakukan Audit TI Untuk mengumpulkan dan mengavaluasi fakta untuk memutuskan apakah sistem komputer yang merupakan aset perusahaan terlindungi, integritas data terpelihara, sesuai dengan tujuan organisasi untuk mencapai efektifitas dan efisiensi dalam penggunaan sumber daya. 2. 5 jenis ancaman yang melatarbelakangi perlunya Audit TI 1. Kredensial yang lemah Kredensial atau kata sandi yang lemah menjadi salah satu penyebab data breach dapat terjadi. Kata sandi dibuat dengan tujuan untuk mengamankan sistem. Namun sayangnya masih banyak yang menggunakan kata sandi dengan frasa sederhana seperti Password1 atau 123456. Jika hacker dapat menemukan kata sandi yang Anda gunakan, mereka dapat dengan mudah masuk ke dalam sistem dan mengakses data-data sensitif di dalamnya. Oleh karena itu, penting bagi perusahaan untuk selalu menggunakan kata sandi yang kuat dan secara regular memperbaruinya. 2. Adanya kerentanan di dalam aplikasi Sebagian besar hacker akan melakukan sejumlah serangan ketika mereka menemukan kerentanan dalam sebuah sistem. Itulah sebabnya, penting bagi perusahaan untuk melakukan penetration testing secara rutin. Penetration testing dapat membantu perusahaan untuk menemukan celah keamanan agar bisa segera ditambal atau diperbaiki. 3. Malware Malware (malicious software) merupakan suatu program atau file berbahaya yang dibuat dengan tujuan jahat. Peretas dapat menyebarluaskan malware ketika sistem memiliki kerentanan keamanan. Mereka juga dapat menanamkan malware ketika karyawan Anda secara tidak sadar mengklik tautan berbahaya yang dikirim melalui email. Berbagai serangan malware ini biasanya digunakan oleh peretas untuk menghilangkan langkah otentikasi yang digunakan untuk melindungi sistem. 4. Orang dalam yang berbahaya Selain karena faktor kesalahan teknis, data breach juga dapat terjadi karena faktor kesengajaan. Beberapa karyawan Anda mungkin memiliki akses untuk melihat data sensitif perusahaan. Terkadang karena iming-iming imbalan berupa uang, karyawan dapat menyalahgunakannya dan memberikan akses tersebut kepada peretas. Jika peretas berhasil membujuk karyawan Anda, mereka dapat mengakses data dengan mudah tanpa harus mengekploitasi sistem untuk menemukan celah keamanan.

Nama : Hendri

Nim : 182420098

1. Pencegahan terhadap biaya organisasi untuk data yang hilang

Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan *backup* yang memadai terhadap *file* data, sehingga kehilangan *file* dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat *file* tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu.

2. Pengambilan keputusan yang tidak sesuai

Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang – orang yang berkepentingan di suatu organisasi.

3. Penyalahgunaan komputer

Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi.

4. Nilai dari perangkat keras komputer, perangkat lunak dan personel

Disamping data, *hardware* dan *software* serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi *hardware* perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan *hardware* baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika *software* rusak akan mengganggu jalannya operasional dan bila *software* dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional.

5. Biaya yang tinggi untuk kerusakan komputer

Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data *error* mengakibatkan jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer.

6. Kerahasiaan

Banyak data tentang diri pribadi yang saat ini dapat diperoleh dengan cepat, dengan adanya komputerisasi kependudukan maka data mengenai seseorang dapat segera diketahui termasuk hal – hal pribadi.

7. Pengontrolan penggunaan komputer

Teknologi adalah hal yang alami, tidak ada teknologi yang baik atau buruk. Pengguna teknologi tersebut yang dapat menentukan apakah teknologi itu akan menjadi baik atau malah menimbulkan gangguan. Banyak keputusan yang harus diambil untuk mengetahui apakah komputer digunakan untuk suatu hal yang baik atau buruk.

5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi

1. **Kepentingan diri *(self-interest*)**
2. **Review diri (*Self-review*)**
3. **Advokasi (*Advocacy*)**
4. **Kekerabatan (*Familiarity*)**
5. **Intimidasi (*Intimidation*)**

Pemenuhan kebutuhan akan sistem informasi bagi semua jenis organisasi menyebabkan perkembangan sistem informasi yang begitu pesat. Semakin signifikannya peran TI dalam mendukung pencapaian tujuan organisasi tentu saja harus dibarengi dengan pengendalian TI yang memadai. Tanpa adanya tata kelola TI yang memadai, sistem informasi (sebagai kesatuan sumber daya informasi) yang dimiliki organisasi dapat menjadi bumerang yang justru menghambat pencapaian tujuan organisasi.

Bukan hanya kehidupan manusia sebagai individu, tetapi organisasi modern pun bergantung pada dukungan TI untuk dapat beroperasi dengan efektif dan efisien setiap harinya. Berbagai proses komunikasi bisnis, pengolahan informasi transaksi, bahkan pengambilan keputusan-keputusan penting membutuhkan dukungan TI yang cukup.

Pemanfaatan Teknologi Informasi sebagai pendukung pencapaian tujuan dan sasaran organisasi harus diimbangi dengan keefektifan dan efisiensi pengelolaannya. Maka dari itu, audit TI haruslah dilakukan untuk menjaga keamanan sistem informasi sebagai asset organisasi, untuk mempertahankan integritas informasi yang disimpan dan diolah dan tentu saja untuk meningkatkan keefektifan penggunaan teknologi informasi serta mendukung efisiensi dalam organisasi.

Auditing TI muncul seiring dengan pesatnya teknologi informasi. Dimana peranan computer dalam proses auditing sangat penting. Bahkan sekarang ini mulai dari input, proses, dan output telah banyak yang menggunakan komputer atau sudah tidak manual lagi.

Audit TI adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit TI ini dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis. Pada mulanya istilah ini dikenal dengan audit pemrosesan data elektronik, dan sekarang audit TI secara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan itu. Istilah lain dari audit teknologi informasi adalah audit komputer yang banyak dipakai untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya.

Adapun beberapa ancaman yang terjadi pada sistem informasi sehingga diperlukannya IT Audit adalah sebgai berikut :

1. Kejahatan yang dilakukan dengan menyusup kedalam sistem jaringan komputer tanpa sepengetahuan dari pemilik sistem jaringan komputer. Contohnya : seorang pelaku kejahatan atau hacker melakukan sabotase terhadap informasi yang sangat penting atau mencuri informasi yang sangat penting dan rahasia.
2. Kejahatan dengan memasukkan data atau berupa informasi ke jaringan internet tentang sesuatu yang tidak benar dan melanggar ketentuan hukum. Contohnya pemuatan berita atau informasi yang tidak benar seperti memuat video pornografi, memuat informasi yang sangat rahasia seperti rahasi negara, dll
3. Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan pada dokumen melalu internet.
4. Kejahatan dengan memanfaatkan jaringan internet untuk melakukan mata-mata terhadap pihak yang menjadi sasaran, dengan memasuki sistem jaringan komputer pihak yang menjadi sasarannya.
5. Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau pengahncuran terhadap data atau sistem jaringan komputer. Misalnya menyusupkan virus komputer dimana data yang terkena virus tidak dapat digunakan lagi.

Nama : Indri Endang Lestari

Nim : 182420046

Task 1 : Why we need IT Audit?

Jelaskan berdasarkan pendapat anda, mengapa kita harus melakukan Audit TI ?

Jawab :

Karena IT Audit dapat memastikan bahwa mekanisme sistem informasi yang berjalan di suatu organisasi, tetap berada di koridor integritas. Dengan investasi yang cukup besar, suatu organisasi perlu memastikan kehandalan dan keamanan dari sistem IT yang akan digunakan. Sistem IT juga harus mampu memenuhi kebutuhan proses kerja, mampu mengurangi resiko data di sabotasi, kehilangan data, gangguan layanan dan manajemen yang buruk dari sistem IT.

dan sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini

jawab :

1. Akses ke jaringan oleh orang yang tidak berwenang(Access to the network by unauthorized persons)
2. Kehilangan daya listrik (Loss of electricity)
3. Pengungkapan kata sandi(Disclosure of passwords)
4. Akses tidak sah ke sistem informasi(Unauthorized access to the information system)
5. Mengorbankan informasi rahasia (Compromising confidential information)

Nama : M. RISKI QISTHANO

Kelas : 18R2

NIM : 182420040

Alasan kenapa kita butuh IT Audit ?

Jawaban :

Integritas data merupakan konsep dasar audit sistem informasi.Dari alasan dan tujuan tersebut sangat jelas bahwa penting bagi sebuah organisasi untuk melakukan audit sistem informasi guna melihat kembali apakah sistem yang berjalansudah tepat dan terpenting sistem mampu untuk mendukung tercapainya tujuan organisasi.

Threats

1. Boms
2. Thief
3. User Error
4. Breach of contractual relations
5. Social Engginers

Vurnability

Threat	Threat Source	Vulnerability	Impact VS LikeliHood	Risk
Bomb Threats	Ekternal, Rival	Inadequate control of physical access, Inadequate security awareness	5 x 1	Very Low (5)
Thieft	Internal, Ekternal	Inadequate control of physical access, Inadequate security awareness	5 x 5	Very High (25)
User Error	Pegawai	Inadequate training of employees	2 x 5	Medium (10)
Breach Of Contractual Relations	Organisasi	Incomplete specification for software development	5 x 2	Medium (10)

Social Enggineering	Cracker, Hacker	Unprotected public network connections	5 x 5	Very High (25)

SOAL

1. Jelaskan berdasarkan pendapat anda, mengapa kita harus melakukan Audit TI dan sebutkan 5 jenis ancaman yang melatar belakangi perlunya Audit TI dalam suatu organisasi pada saat ini ?

Jawaban

Mengapa kita harus melakukan Audit TI ? Pendapat saya untuk meninjau dan mengevaluasi beberapa faktor, seperti Ketersediaan, Keamanan dan kelengkapan dari Sistem Informasi yang digunakan oleh organisasi tersebut. audit sistem informasi merupakan tinjauan pengendalian umum dan aplikasi untuk menilai pemenuhan kebijakan dan prosedur pengendalian internal serta keefektivitasannya untuk menjaga *asset*.

terdapat tujuan utama mengapa perlu dilakukannya audit sistem informasi yaitu:

1. Pencegahan terhadap biaya organisasi untuk data yang hilang

Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan *backup* yang memadai terhadap *file* data, sehingga kehilangan *file* dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat *file* tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu.

2. Pengambilan keputusan yang tidak sesuai

Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang – orang yang berkepentingan di suatu organisasi.

3. Penyalahgunaan komputer

Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi.

4. Nilai dari perangkat keras komputer, perangkat lunak dan personel

Disamping data, *hardware* dan *software* serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi *hardware* perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan *hardware* baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika *software* rusak akan mengganggu jalannya operasional dan bila *software* dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional.

5. Biaya yang tinggi untuk kerusakan komputer

Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data *error* mengakibatkan jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer.

6. Kerahasiaan

Banyak data tentang diri pribadi yang saat ini dapat diperoleh dengan cepat, dengan adanya komputerisasi kependudukan maka data mengenai seseorang dapat segera diketahui termasuk hal – hal pribadi.

7. Pengontrolan penggunaan komputer

Teknologi adalah hal yang alami, tidak ada teknologi yang baik atau buruk. Pengguna teknologi tersebut yang dapat menentukan apakah teknologi itu akan menjadi baik atau malah menimbulkan gangguan. Banyak keputusan yang harus diambil untuk mengetahui apakah komputer digunakan untuk suatu hal yang baik atau buruk.

Soal

Lima jenis ancaman yang melatar belakangi perlunya Audit TI dalam suatu organisasi pada saat ini ?

1. Kejahatan dengan memanfaatkan jaringan internet untuk melakukan mata-mata terhadap pihak yang menjadi sasaran, dengan memasuki sistem jaringan komputer pihak yang menjadi sasarannya.
2. Kejahatan yang dilakukan dengan menyusup kedalam sistem jaringan komputer tanpa sepengetahuan dari pemilik sistem jaringan komputer. Contohnya : seorang pelaku kejahatan atau hacker melakukan sabotase terhadap informasi yang sangat penting atau mencuri informasi yang sangat penting dan rahasia.
3. Kejahatan dengan memasukkan data atau berupa informasi ke jaringan internet tentang sesuatu yang tidak benar dan melanggar ketentuan hukum. Contohnya pemuatan berita atau informasi yang tidak benar seperti memuat video pornografi, memuat informasi yang sangat rahasia seperti rahasi negara, dll
4. Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau pengahncuran terhadap data atau sistem jaringan komputer. Misalnya menyusupkan virus komputer dimana data yang terkena virus tidak dapat digunakan lagi.
5. Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan pada dokumen melalu internet.

Cakupan atau area yang terlibat dalam proses Audit Teknologi Informasi ini terdiri dari:

1. Organizational IT Audits (Management Control over IT)

Teknologi informasi sering dilibatkan penerapannya dalam area manajerial bisnis organisasi. Hal ini dapat terlihat dari segala bentuk keputusan yang diambil melalui kewenangan dan tanggung jawab dari masing-masing pihak manajemen. Salah satu contoh yang sering digunakan adalah KMS (Knowledge Management System), ES (Expert System). Jenis teknologi informasi tersebut digunakan untuk membantu pihak manajemen mengambil alternatif dan keputusan yang tepat yang dijadikan sebagai bentuk strategi bisnis yang nantinya akan diimplementasikan dalam proses bisnis organisasi.

2. Technical IT Audits (Infrastructure, Data Centers, Data Communication)

Proses audit TI ini sering dilakukan di departemen atau area fungsional bagian IT organisasi karena departemen tersebut berperan dalam memberikan pengetahuan dan pengalaman bagi sumebr daya manusia organisasi yang menggunakan TI tersebut. Selain itu, departemen IT juga bertanggung jawab terhadap komponen hardware maupun software yang dimiliki organisasi serta memastikan tingkat keamanan informasi yang sudah disimpan dalam database organisasi sehingga kerahasiaan tetap terjaga dalam organisasi dan pihak eksternal tidak mengetahui informasi penting tersebut.

3. Application IT Audits (Business/ Financial/ Operational)

Audit TI dilakukan dalam masing-masing area operasional maupun keseluruhan departemen fungsional organisasi dimulai dari cara penggunaan TI oleh masing-masing user/ pengguna sistem yang berlaku sebagai karyawan organisasi. Selain itu, berbagai bentuk aplikasi yang sering digunakan organisasi dalam meningkatkan pendapatan sehingga pengukuran nilai finansial bertambah, nilai bisnis dan strategi yang akan diimplementasikan juga berhasil dilakukan dengan dukungan TI, daya jual atau proses bisnis sebagai aktivitas operasional organisasi berjalan secara efektif dan efisien.

4. Development/ Implementation IT Audits (Specification/ Requirements, Design, Development, and Postimplementation Phases)

Proses audit TI ini juga dilakukan dalam area ini dimana organisasi melakukan evaluasi terhadap teknologi informasi yang terlibat selama proses pengembangan produk-produk tertentu organisasi (seperti: produk dan layanan yang dijual ke pihak eksternal organisasi, komponen hardware maupun software yang dikembangkan lebih lanjut untuk mengikuti trend, dan aspek-aspek lainnya. Proses audit ini juga sering dilakukan dalam ruang lingkup proyek sehingga menghasilkan produk TI yang tetap terjaga kualitasnya dan menggunakan prinsip meminimalisasikan biaya tetapi memaksimalisasikan keuntungan/ profit.

5. Compliances IT Audits

Proses audit TI yang dilakukan dalam setiap area organisasi harus mampu memeuhi standard-standard audit TI yang sudah berskala internasional. Baik pihak internal maupun pihak eksternal organisasi harus mampu mengikuti trend yang ditawarkan lewat standard tersebut yang kemudian diselaraskan kembali dengan kebijakan organisasi terkait peran dan tanggung jawab terhadap TI. Saat ini banyak standard yang dikeluarkan untuk audit TI tersebut, seperti COBIT, ITIL, dan lain-lain untuk memastikan bahwa teknologi informasi yang diterapkan sudah memadai dan layak untuk digunakan atau dikembangkan lebih lanjut atau tidak.

-

Kesimpulan

Dalam suatu perusahaan perlu dilakukan audit sistem informasi untuk meninjau dan mengevaluasi pengendalian internal yang melindungi sistem tersebut. Dalam audit sistem informasi terdapat 3 pengendalian yaitu pengendalian internal, pengendalian umum dan pengendalian aplikasi. Untuk memastikan pengendalian lingkungan dalam keadaan stabil dan di kelola dengan baik perlu dilakukannya pengendalian umum. Pengendalian umum berperan penting untuk membantu agar kegiatan komputerisasi yang digunakan oleh perusahaan tersebut seperti aplikasi dan sistem informasi dapat berjalan dengan baik dan terjaga integritas serta keamanannya

Menurut saya, perlu dilakukan audit TI didalam suatu organisasi dikarenakan besarnya resiko yang dihadapi suatu organisasi yang berkaitan dengan penggunaan TI. Resiko tersebut seperti kehilangan data, kesalahan dalam pengambilan keputusan, privasi, penyalahgunaan akses komputer dan lain sebagainya. Audit TI merupakan bentuk pengawasan dan pengendalian dari infrastruktur TI secara menyeluruh. Audit TI ini dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis di dalam suatu organisasi tersebut.

Selain itu ada beberapa ancaman yang melatarbelakangi perlunya audit TI dalam suatu organisasi yakni sebagai berikut:
1. Kejahatan yang dilakukan dengan menyusup kedalam sistem jaringan komputer tanpa sepengetahuan dari pemilik sistem jaringan komputer. Contohnya : seorang pelaku kejahatan atau hacker melakukan sabotase terhadap informasi yang sangat penting atau mencuri informasi yang sangat penting dan rahasia.
2. Kejahatan dengan memasukkan data atau berupa informasi ke jaringan internet tentang sesuatu yang tidak benar dan melanggar ketentuan hukum. Contohnya pemuatan berita atau informasi yang tidak benar seperti memuat video pornografi, memuat informasi yang sangat rahasia seperti rahasi negara, dll
3. Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan pada dokumen melalu internet.
4. Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap data atau sistem jaringan komputer. Misalnya menyusupkan virus komputer dimana data yang terkena virus tidak dapat digunakan lagi.
5. Kejahatan dengan memanfaatkan jaringan internet untuk melakukan mata-mata terhadap pihak yang menjadi sasaran, dengan memasuki sistem jaringan komputer pihak yang menjadi sasarannya.

Menurut pendapat saya mengapa kita harus melakukan IT Audit, Audit sistem informasi / IT Audit adalah suatu proses pengumpulan dan pengevaluasian bahan bukti audit untuk menentukan apakah sistem komputer perusahaan telah menggunakan *asset* sistem informasi secara tepat dan mampu mendukung pengamanan *asset* tersebut memelihara kebenaran dan integritas data dalam mencapai tujuan perusahaan yang efektif dan efisien.

Terdapat beberapa alasan mendasar dan **melatarbelakangi mengapa organisasi perlu melakukan audit** sebagai evaluasi dan pengendalian terhadap sistem yang digunakan oleh organisasi :

1. Pencegahan terhadap biaya organisasi untuk data yang hilang

Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan *backup* yang memadai terhadap *file* data, sehingga kehilangan *file* dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat *file* tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu.

2. Pengambilan keputusan yang tidak sesuai

Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang – orang yang berkepentingan di suatu organisasi.

3. Penyalahgunaan komputer

Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi.

4. Nilai dari perangkat keras komputer, perangkat lunak dan personel

Disamping data, *hardware* dan *software* serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi *hardware* perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan *hardware* baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika *software* rusak akan mengganggu jalannya operasional dan bila *software* dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional.

5. Biaya yang tinggi untuk kerusakan komputer

Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data *error* mengakibatkan jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer.

6. Kerahasiaan

Banyak data tentang diri pribadi yang saat ini dapat diperoleh dengan cepat, dengan adanya komputerisasi kependudukan maka data mengenai seseorang dapat segera diketahui termasuk hal – hal pribadi.

7. Pengontrolan penggunaan komputer

Teknologi adalah hal yang alami, tidak ada teknologi yang baik atau buruk. Pengguna teknologi tersebut yang dapat menentukan apakah teknologi itu akan menjadi baik atau malah menimbulkan gangguan. Banyak keputusan yang harus diambil untuk mengetahui apakah komputer digunakan untuk suatu hal yang baik atau buruk.

Jawab :

Perkembangan teknologi telah mengakibatkan perubahan pengolahan data yang dilakukan perusahaan dari sistem manual menjadi secara mekanis, elektromekanis, dan selanjutnya ke sistem elektronik atau komputerisasi. Peralihan ke sistem yang terkomputerisasi memungkinkan data yang kompleks dapat diproses dengan cepat dan teliti, guna menghasilkan suatu informasi. Dalam mendukung aktivitas sebuah organisasi, informasi menjadi bagian yang sangat penting baik untuk perkembangan organisasi maupun membaca persaingan pasar. Dalam hal proses data menjadi suatu informasi merupakan sebuah kegiatan dalam organisasi yang bersifat repetitif sehingga harus dilaksanakan secara sistematis dan otomatis.

Dengan demikian, sangat diperlukan adanya pengelolaan yang baik dalam sistem yang mendukung proses pengolahan data tersebut. Dalam sebuah organisasi tata kelola IT dilakukan dengan melakukan audit. Audit IT adalah suatu proses pengumpulan dan pengevaluasian bahan bukti audit untuk menentukan apakah sistem komputer perusahaan telah menggunakan asset sistem informasi secara tepat dan mampu mendukung pengamanan asset tersebut memelihara kebenaran dan integritas data dalam mencapai tujuan perusahaan yang efektif dan efisien.

Terdapat beberapa alasan mendasar mengapa organisasi perlu melakukan audit sebagai evaluasi dan pengendalian terhadap sistem yang digunakan oleh organisasi :

1. **1. Pencegahan terhadap biaya organisasi untuk data yang hilang**

Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan backup yang memadai terhadap file data, sehingga kehilangan file dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat file tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu.

1. **2. Pengambilan keputusan yang tidak sesuai**

Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang-orang yang berkepentingan di suatu organisasi.

1. **3. Penyalahgunaan komputer**

Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi.

1. **4. Nilai dari perangkat keras komputer, perangkat lunak dan personel**

Disamping data, hardware dan software serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi hardware perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan hardware baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika software rusak akan mengganggu jalannya operasional dan bila software dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional.

1. **5. Biaya yang tinggi untuk kerusakan komputer**

Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data error mengakibatkan jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer.

1. **6. Kerahasiaan**

Banyak data tentang diri pribadi yang saat ini dapat diperoleh dengan cepat, dengan adanya komputerisasi kependudukan maka data mengenai seseorang dapat segera diketahui termasuk hal-hal pribadi.

1. **7. Pengontrolan penggunaan komputer**

Teknologi adalah hal yang alami, tidak ada teknologi yang baik atau buruk. Pengguna teknologi tersebut yang dapat menentukan apakah teknologi itu akan menjadi baik atau malah menimbulkan gangguan. Banyak keputusan yang harus diambil untuk mengetahui apakah komputer digunakan untuk suatu hal yang baik atau buruk.

Sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini.

Jawab :

1. Malware : ancaman yang secara umum dapat mencuri data dan dapat menggunakan/ mengambil alih akun pengguna dan sistem. Malware dapat berupa : virus yang menduplikasi kode program dirinya sendiri untuk merusak sistem, worm yang menduplikasi diri hingga memenuhi sistem induk dengan hal yang tidak berguna, rootkit yang membuka remote akses secara diam-diam, backdoor yang membuka jalan remote akses untuk memanipulasi sistem, dan trojan yang dapat menyembunyikan diri dalam melihat atau mencuri informasi.
2. Spyware : ancaman yang dapat mendapatkan informasi melalui jejak aktifitas pengguna sistem seperti trackware ataupun dalam bentuk aplikasi mata-mata.
3. Riskware : berupa penyalahgunaan perangkat monitoring yang dilakukan oleh pihak yang tidak sah dengan tujuan mencari celah keamanan sistem. Riskware dapat berupa monitoring tool, hack tool, keylogger dan lain-lain.
4. Ancaman fisik yang dapat berpotensi mengganggu berjalannya bisnis organisasi seperti adanya bencana alam, kerusuhan termasuk ancaman fisik pada kurir yang mengantarkan backup menuju tempat aman.
5. Ancaman Internal dan Eksternal, Ancaman internal bukan hanya mencakup karyawan perusahaan, tetapi juga pekerja temporer, konsultan, kontraktor, bahkan mitra bisnis perusahaan tersebut. Ancaman internal diperkirakan menghasilkan kerusakan yang secara potensi lebih serius jika dibandingkan denga ancaman eksternal, dikarenakan pengetahuan anccaman internal yang lebih mendalam akan sistem tersebut. Ancaman eksternal misalnya perusahaan lain yang memiliki produk yang sama dengan produk perusahaan atau disebut juga pesaing usaha.

PENTINGNYA DILAKUKAN AUDIT SISTEM INFORMASI DAN ANCAMANNYA :

Hal tersebut dilakukan karena pada saat ini teknologi semakin berkembang, sehingga dapat memudahkan penggunanya untuk melakukan segala aktifitas. Salah satunya adalah melakukan Audit SI. Karena dengan menggunakan teknologi komputerisasi data yang diolah akan menjadi lebih baik lagi hasilnya. Beberapa alasan mengapa Audit SI penting untuk dilakukan adalah sebagai berikut :

1. Kerugian akibat kehilangan data
Informasi berasal dari suatu data yang diolah dan memiliki manfa'at bagi penggunanya. Oleh karena itu, data adalah suatu aset yang penting bagi suatu perusahaan atau organisasi. Informasi dari suatu data akan menjadi gambaran dari kondisi di masa lalu, sekarang, dan masa yang akan datang. Jika informasi dari data tersebut hilang, maka akan menyebabkan suatu kesalahan yang fatal.

2. Kesalahan dalam pengambilan keputusan
Saat ini masih banyak instansi yang menggunakan perangkat lunak dalam mengambil keputusan. Namun, resiko yang ditimbulkan bisa saja bukan lagi membahayakan sistem, tetapi juga dapat membahayakan nyawa seseorang seperti dalam penggunaan DSS (Sistem Penunjang Keputusan) dalam bidang kedokteran. Tingkat akurasi dan pentingnya suatu data tergantung kepada jenis keputusan yang akan diambil.

3. Kerugian yang disebabkan oleh kesalahan pemrosesan komputer
Banyak organisasi atau perusahaan yang telah menggunakan komputer sebagai sarana untuk meningkatkan kualitas pekerjaan mereka. Mulai dari hal yang sederhana, pernghitungan bunga dalam jumlah besar, dan juga navigasi pesawat terbang atau peluru kendali. Kerugian tersebut dapat pula berupa kebocoran data dan dapat menimbulkan dampak yang akan merugikan bagi suatu perusahaan atau organisasi seperti kehilangan klien, pelanggan, perhitungan matematis yang sulit dipercaya, dan juga dapat menggangu kelangsungan hidup perusahaan.

4. Penggunaan komputer yang di salah gunakan
Tingginya tingkat penyalahgunaan komputer menjadi salah satu alasan mengapa audit sistem informasi diperlukan. Banyak sekali pihak yang tidak bertanggungjawab dapat melakukan kejahatan komputer seperti Hacker, Cracker dan Virus.

a) *Hacker* : Merupakan seseorang yang dengan sengaja masuk ke dalam suatu sistem tanpa izin. Mereka melakukan hal tersebut biasanya hanya untuk membuat dirinya sendiri atau kelompoknya bangga karena telah berhasil menembus sistem keamanan dari suatu perusahaan atau organisasi, tanpa ada maksud untuk merusak atau mengambil sesuatu atas apa yang telah dilakukan.

b) *Cracker* : Cracker memasuki suatu sistem yang memiliki tujuan untuk mengambil keuntungan sebanyak-banyaknya seperti mengubah, merusak, atau bahkan menghancurkan sistem tersebut.

c) *Virus* : Merupakan sebuah program komputer yang melekatkan diri dan menjalankan dirinya sendiri pada suatu data. Virus meriplikasi dirinya sendiri secara aktif dan mengganggu atau merusak suatu sistem operasi, data, dan bahkan mengacaukan sistem.

Kejahatan komputer juga dapat dilakukan oleh karyawan yang merasa tidak puas dengan kebijaksanaan perusahaan, baik yang masih bekerja, sudah berhenti, keluar, diberhentikan dari perusahaan tersebut dan bahkan yang pindah bekerja ke perusahaan lain. Dan hal tersebut dilakukan untuk memperoleh keuntungan atau manfaat dalam bersaing. Oleh karena itu audit sangat diperlukan dan terdapat dua hal utama yang harus diperhatikan pada saat melakukan audit atau pemrosesan data elektronik seperti pengumpulan bukti dan evaluasi bukti.

5. Kesalahan pada proses perhitungan
Sistem Informasi sering digunakan untuk melakukan proses menghitung yang rumit karena memiliki kemampuan untuk mengolah data secara tepat dan akurat, namun juga menimbulkan resiko kesalahan. Tanpa adanya pengembangan sistem yang baik, tentu saja dapat terjadi kesalahan menghitung dan yang lebih buruk adalah sistem yang baru yang sudah dibuat akan sulit di deteksi tanpa ada proses audit yang dilakukan.

6. Nilai investasi yang tinggi untuk perangkat keras dan perangkat lunak komputer
Investasi yang dikeluarkan suatu perusahaan tentu sangat besar dan sulit untuk mengukur manfaat yang dapat diberikan oleh suatu sistem atau teknologi informasi.

Nama : RAJU SEPTA WIJAYA

Nim : 182420094

Kelas : MTIK319 B

1. Mengapa Kita harus Melakukan IT Audit ?

jawaban :

Menurut pendapat saya bahwa penting meakukan IT Audit bagi sebuah Organisasi untuk melakukan audit sistem informasi guna melhat kembali apakah sistem yang berjalan sudah tepat dan terpentng sistem mampu untuk mendukung tercapainya tujun organisasi.

2. 5 jenis ancaman yang melatarbelakangi perlunya IT Audit.

jawaban :

1. Bencana Alam / Natural disaster seperti : gempa bumi, banjir, kebakaran dll

2. Kegagalan sistem / System Failure : Kegagalan perangkat lunak dan kegagalan perangkat keras (Kegagalan peralatan, kegagalan fungsi perangkat lunak dan perangkat keras) solusi dengan kualitas perangkat yang baik mengurangi kelemahan ini.

3. yang tidak disengaja / accidental humans adalah tidak sengaja melakukan sesuatu yang membuat sistem bermaslah seperti : salah pemasukan data, salah penghapusan data.

4. Melicious Humans / manusia yang berbahaya adalah orang yang sengaja melakukan kegiatan yang bertujuan melicious seperti : Kecurangan dan kejahatan komputer.

- Impersonation : Mencuri credit card untuk kepentingan mereka
- Interception : classical concept hacking, mencuri data
- Interferers : seseorang yang merusak bisnis anda tanpa merusak system,tidak mencuri informasi, misalnya orang mencuri komputer, membuat system down

5. Program yang jahat / Usil (Virus, Malware, trojan dll)

Audit TI pada suatu organisasi sangat penting dan perlu dilakukan guna melihat kembali apakah sistem yang berjalan sudah tepat dan terpenting sistem mampu untuk mendukung tercapainya tujuan organisasi. Selain itu, audit TI perlu dilakukan agar dapat mengevaluasi sistem untuk menjaga keamanan data organisasi dan menilai resiko untuk menjaga aset berharga serta dapat menetapkan metode untuk meminimalkan resiko tersebut.

5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini.

1) Pencegahan terhadap biaya organisasi untuk data yang hilang

Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan *backup* yang memadai terhadap *file* data, sehingga kehilangan *file* dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat *file* tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu.

2) Pengambilan keputusan yang tidak sesuai

Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang-orang yang berkepentingan di suatu organisasi.

3) Penyalahgunaan komputer

Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi.

4) Nilai dari perangkat keras komputer, perangkat lunak dan personel

Disamping data, *hardware* dan *software* serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi *hardware* perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan *hardware* baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika *software* rusak akan mengganggu jalannya operasional dan bila *software* dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional.

5) Biaya yang tinggi untuk kerusakan komputer

Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data *error* mengakibatkan jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer.

Audit IT diperlukan untuk mengetahui celah dalam suatu keamanan teknologi informasi, sehingga kita dapat terlepas dari permasalahan/ancaman yang dapat mengakibatkan resiko-reisko dari suatu celah keamanan tersebut

5 Acanaman yang melatarbelakangi perlunya audit IT

1. Akses ke data rahasia
2. Akses yang tidak sah ke komputer departemen
3. Pemakaian password
4. Serangan virus
5. Open ports

Task 1 : Why we need IT Audit?

Jelaskan berdasarkan pendapat anda, mengapa kita harus melakukan Audit TI ?

Jawab :

Perkembangan teknologi telah mengakibatkan perubahan pengolahan data yang dilakukan perusahaan dari sistem manual menjadi secara mekanis, elektromekanis, dan selanjutnya ke sistem elektronik atau komputerisasi. Peralihan ke sistem yang terkomputerisasi memungkinkan data yang kompleks dapat diproses dengan cepat dan teliti, guna menghasilkan suatu informasi. Dalam mendukung aktivitas sebuah organisasi, informasi menjadi bagian yang sangat penting baik untuk perkembangan organisasi maupun membaca persaingan pasar. Dalam hal proses data menjadi suatu informasi merupakan sebuah kegiatan dalam organisasi yang bersifat repetitif sehingga harus dilaksanakan secara sistematis dan otomatis.

Dengan demikian, sangat diperlukan adanya pengelolaan yang baik dalam sistem yang mendukung proses pengolahan data tersebut. Dalam sebuah organisasi tata kelola IT dilakukan dengan melakukan audit. Audit IT adalah suatu proses pengumpulan dan pengevaluasian bahan bukti audit untuk menentukan apakah sistem komputer perusahaan telah menggunakan asset sistem informasi secara tepat dan mampu mendukung pengamanan asset tersebut memelihara kebenaran dan integritas data dalam mencapai tujuan perusahaan yang efektif dan efisien.

Terdapat beberapa alasan mendasar mengapa organisasi perlu melakukan audit sebagai evaluasi dan pengendalian terhadap sistem yang digunakan oleh organisasi :

1. **1. Pencegahan terhadap biaya organisasi untuk data yang hilang**

Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan backup yang memadai terhadap file data, sehingga kehilangan file dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat file tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu.

1. **2. Pengambilan keputusan yang tidak sesuai**

Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang-orang yang berkepentingan di suatu organisasi.

1. **3. Penyalahgunaan komputer**

Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi.

1. **4. Nilai dari perangkat keras komputer, perangkat lunak dan personel**

Disamping data, hardware dan software serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi hardware perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan hardware baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika software rusak akan mengganggu jalannya operasional dan bila software dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional.

1. **5. Biaya yang tinggi untuk kerusakan komputer**

Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data error mengakibatkan

jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer.

1. **6. Kerahasiaan**

Banyak data tentang diri pribadi yang saat ini dapat diperoleh dengan cepat, dengan adanya komputerisasi kependudukan maka data mengenai seseorang dapat segera diketahui termasuk hal-hal pribadi.

1. **7. Pengontrolan penggunaan komputer**

Teknologi adalah hal yang alami, tidak ada teknologi yang baik atau buruk. Pengguna teknologi tersebut yang dapat menentukan apakah teknologi itu akan menjadi baik atau malah menimbulkan gangguan. Banyak keputusan yang harus diambil untuk mengetahui apakah komputer digunakan untuk suatu hal yang baik atau buruk.

Sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini.

Jawab :

1. Malware : ancaman yang secara umum dapat mencuri data dan dapat menggunakan/ mengambil alih akun pengguna dan sistem. Malware dapat berupa : virus yang menduplikasi kode program dirinya sendiri untuk merusak sistem, worm yang menduplikasi diri hingga memenuhi sistem induk dengan hal yang tidak berguna, rootkit yang membuka remote akses secara diam-diam, backdoor yang membuka jalan remote akses untuk memanipulasi sistem, dan trojan yang dapat menyembunyikan diri dalam melihat atau mencuri informasi.
2. Spyware : ancaman yang dapat mendapatkan informasi melalui jejak aktifitas pengguna sistem seperti trackware ataupun dalam bentuk aplikasi mata-mata.
3. Riskware : berupa penyalahgunaan perangkat monitoring yang dilakukan oleh pihak yang tidak sah dengan tujuan mencari celah keamanan sistem. Riskware dapat berupa monitoring tool, hack tool, keylogger dan lain-lain.
4. Ancaman fisik yang dapat berpotensi mengganggu berjalannya bisnis organisasi seperti adanya bencana alam, kerusuhan termasuk ancaman fisik pada kurir yang mengantarkan backup menuju tempat aman.
5. Ancaman Internal dan Eksternal, Ancaman internal bukan hanya mencakup karyawan perusahaan, tetapi juga pekerja temporer, konsultan, kontraktor, bahkan mitra bisnis perusahaan tersebut. Ancaman internal diperkirakan menghasilkan kerusakan yang secara potensi lebih serius jika dibandingkan denga ancaman eksternal, dikarenakan pengetahuan anccaman internal yang lebih mendalam akan sistem tersebut. Ancaman eksternal misalnya perusahaan lain yang memiliki produk yang sama dengan produk perusahaan atau disebut juga pesaing usaha.

Menurut pendapat saya, audit TI harus dilaksanakan untuk melihat kembali apakah sistem yg berjalan sudah tepat dan apakah sistem mampu untuk mendukung tercapainya tujuan organisasi, seperti:

- untuk mengamankan aset yang berhubungan dengan instalasi sistem informasi mencakup perangkat keras, perangkat lunak, fasilitas, manusia, file data, dokumntasi sistem dan internal. seperti perangkat keras bisa rusak karena unsur kejahatan ataupun sebab lainnya. perangkat lunak dan isi file yang dicuri. dll

- menjaga integritas data yang merupakan konsep dasar audit sistem informasi. integritas data berarti data memiliki atribut: kelengkapan, sehat dan jujur, kemurnian dan ketelitian. tanpa menjaga integritas data , keputusan maupun langkah penting organisasi menjadi salah sasaran karena tidak didukung dengan data yang benar

-menjaga efektivitas sistem, sistem informasi dikatakan efektif hanya jika sistem tersebut dapat mencapai tujuannya untuk menilai efektivitas sistem, auditor sistem informasi harus tahu mengenai kebutuhan pengguna sistem.

- mencapai efisiensi sumber daya, sistem sebagai fasilitas pemrosesan informasi dikatakan efisien jika ia menggunakan sumber daya seminimal mungkin untuk menghasilkan output yang dibutuhkan.

lima jenis ancaman yang melatarbelakangi perlunya AUDIT TI dalam organisasi adalah:

a. bencana alam/natural disaster seperti gempa, banjir, kebakaran dll

b. kegagalan sistem (system failure), seperti kegagalan fungsi software dan hardware solusinya dengan mengurangi kelemahan perangkat.

c. manusia yang tidak disengaja Accidental humans sperti tidak sengaja menghapus data, salam pemasukan data.

d. malicious human/manusia yang berbahaya, sengaja melakukan kegiatan yang bertujuan malicious. seperti mencuri data, seseorang yang merusak bisnis anda tanpa merusak sistem seperti mencuri komputer, membuat system down.

e. program jahat/usil seperti virus, malware trojan dll

Menurut saya, kita/organisasi harus melakukan Audit TI/Sistem informasi tersebuat adalah karna kita/organisasi tersebut harus meminimalisir kemungkinan-kemungkinan yang tidak di inginkan seperti kehilangan data, kesalahan dalam pengambilan keputusan, penyalah gunaan komputer. Dll.

5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi :

1. Kehilangan data
2. Kesalahan dalam pengambilan keputusan
3. Penyalagunaan komputer
4. Kesalahan pengoporasian komputer
5. Nilai investasi

Mengapa kita harus melakukan Audit TI?

Perkembangan teknologi telah mengakibatkan perubahan pengolahan data yang dilakukan perusahaan dari sistem manual menjadi secara mekanis, elektromekanis, dan selanjutnya ke sistem elektronik atau komputerisasi. Peralihan ke sistem yang terkomputerisasi memungkinkan data yang kompleks dapat diproses dengan cepat dan teliti, guna menghasilkan suatu informasi. Dalam mendukung aktivitas sebuah organisasi, informasi menjadi bagian yang sangat penting baik untuk perkembangan organisasi maupun membaca persaingan pasar. Dalam hal proses data menjadi suatu informasi merupakan sebuah kegiatan dalam organisasi yang bersifat repetitif sehingga harus dilaksanakan secara sistematis dan otomatis.

Dengan demikian, sangat diperlukan adanya pengelolaan yang baik dalam sistem yang mendukung proses pengolahan data tersebut. Dalam sebuah organisasi tata kelola sistem dilakukan dengan melakukan audit. Menurut Juliandarini (2013) Audit sistem informasi (Information Systems (IS) audit atau Information technology (IT) audit) adalah bentuk pengawasan dan pengendalian dari infrastruktur sistem informasi secara menyeluruh.Menurut Romney (2004) audit sistem informasi merupakan tinjauan pengendalian umum dan aplikasi untuk menilai pemenuhan kebijakan dan prosedur pengendalian internal serta keefektivitasannya untuk menjaga asset.

Sehingga menurut uraian teori diatas, maka penulis dapat simpulkan bahwa audit sistem informasi adalah suatu proses pengumpulan dan pengevaluasian bahan bukti audit untuk menentukan apakah sistem komputer perusahaan telah menggunakan asset sistem informasi secara tepat dan mampu mendukung pengamanan asset tersebut memelihara kebenaran dan integritas data dalam mencapai tujuan perusahaan yang efektif dan efisien.

Menurut Weber (1999) terdapat beberapa alasan mendasar mengapa organisasi perlu melakukan audit sebagai evaluasi dan pengendalian terhadap sistem yang digunakan oleh organisasi :

1. Pencegahan terhadap biaya organisasi untuk data yang hilang

Kehilangan data dapat terjadi karena ketidakmampuan pengendalian terhadap pemakaian komputer. Kelalaian dengan tidak menyediakan backup yang memadai terhadap file data, sehingga kehilangan file dapat terjadi karena program komputer yang rusak, adanya sabotase, atau kerusakan normal yang membuat file tersebut tidak dapat diperbaiki sehingga akhirnya membuat kelanjutan operasional organisasi menjadi terganggu.

2. Pengambilan keputusan yang tidak sesuai

Membuat keputusan yang berkualitas tergantung pada kualitas data yang akurat dan kualitas dari proses pengambilan keputusan itu sendiri. Pentingnya data yang akurat bergantung kepada jenis keputusan yang akan dibuat oleh orang – orang yang berkepentingan di suatu organisasi.

3. Penyalahgunaan komputer

Penyalahgunaan komputer memberikan pengaruh kuat terhadap pengembangan EDP audit maka untuk dapat memahami EDP audit diperlukan pemahaman yang baik terhadap beberapa kasus penyalahgunaan komputer yang pernah terjadi.

4. Nilai dari perangkat keras komputer, perangkat lunak dan personel

Disamping data, hardware dan software serta personel komputer juga merupakan sumber daya yang kritikal bagi suatu organisasi, walaupun investasi hardware perusahaan sudah dilindungi oleh asuransi, tetapi kehilangan hardware baik terjadi karena kesengajaan maupun ketidaksengajaan dapat mengakibatkan gangguan. Jika software rusak akan mengganggu jalannya operasional dan bila software dicuri maka informasi yang rahasia dapat dijual kepada kompetitor. Personel adalah sumber daya yang paling berharga, mereka harus dididik dengan baik agar menjadi tenaga handal dibidang komputer yang profesional.

5. Biaya yang tinggi untuk kerusakan komputer

Saat ini pemakaian komputer sudah sangat meluas dan dilakukan juga terhadap fungsi kritis pada kehidupan kita. Kesalahan yang terjadi pada komputer memberikan implikasi yang luar biasa, sebagai contoh data error mengakibatkan jatuhnya pesawat di Antartika yang menyebabkan 257 orang meninggal atau seseorang divonis masuk penjara karena kesalahan data di komputer.

6. Kerahasiaan

Banyak data tentang diri pribadi yang saat ini dapat diperoleh dengan cepat, dengan adanya komputerisasi kependudukan maka data mengenai seseorang dapat segera diketahui termasuk hal – hal pribadi.

7. Pengontrolan penggunaan komputer

Teknologi adalah hal yang alami, tidak ada teknologi yang baik atau buruk. Pengguna teknologi tersebut yang dapat menentukan apakah teknologi itu akan menjadi baik atau malah menimbulkan gangguan. Banyak keputusan yang harus diambil untuk mengetahui apakah komputer digunakan untuk suatu hal yang baik atau buruk.

Menurut Weber (1999) terdapat empat tujuan utama mengapa perlu dilakukannya audit sistem informasi yaitu:

(1) Mengamankan asset

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.

(2) 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.

(3) Menjaga efektivitas sistem

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.

(4) Mencapai 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.

Dari alasan dan tujuan tersebut sangat jelas bahwa penting bagi sebuah organisasi untuk melakukan audit sistem informasi guna melihat kembali apakah sistem yang berjalansudah tepat dan terpenting sistem mampu untuk mendukung tercapainya tujuan organisasi.

Terlihat mudah namun percaya atau tidak penulis menemukan masih banyak organisasi yang belum dengan secara konsisten melakukan audit serta evaluasi terhadap sistem yang digunakan meskipun secara sadar bahwa investasi yang ditanamkan tidak dalam jumlah yang kecil, namun ironisnya yang justru terjadi adalah audit dan evaluasi baru mulai

secara rutin dilakukan setelah organisasi merasakan resiko dan baru mulai mencari tahu penyebabnya.

Sedari dini, mulailah untuk dengan seksama melakukan penilaian terhadap sistem yang digunakan agar tujuan awal investasi tidak menjadi sia – sia.

5 jenis ancaman yang melatarbelakangi perlunya audit TI?

Secara khusus, audit internal membawa manfaat dalam bentuk:

1. Objektivitas
Pelaksana audit internal atau auditor wajib memberikan pendapat yang objektif mengenai aspek yang sedang diamati. Oleh karena itu, pelaksana audit internal harus berasal dari luar departemen yang bersangkutan dan tidak boleh memiliki kewajiban atau tanggung jawab kerja di tempat tersebut. Dengan begitu, pelaksana audit internal akan mampu bersikap independen dan tidak bias dalam melakukan proses audit untuk kebaikan perusahaan itu sendiri.

2. Menunjukkan diri sebagai perusahaan yang taat hukum
Proses audit internal merupakan salah satu peraturan yang wajib dijalankan oleh setiap perusahaan. Keberlangsungan proses ini akan menjadi salah satu cara untuk memastikan bahwa setiap aspek dari perusahaan telah sesuai dengan peraturan yang ada. Audit internal juga merupakan bentuk persiapan perusahaan sebelum dilakukannya audit eksternal. Sebuah perusahaan yang telah lulus proses audit internal dan juga eksternal akan memiliki nilai lebih di mata klien dan konsumen.

3. Perlindungan terhadap aset perusahaan
Salah satu cara untuk melindungi aset perusahaan yang ada adalah dengan mengenali risiko yang dapat membahayakan tersebut, terutama risiko yang berasal dari dalam lingkungan perusahaan. Audit internal akan membantu pihak manajemen untuk menemukan permasalahan yang ada serta mengambil tindakan pencegahan dan perbaikan lebih lanjut. Selain mengidentifikasi masalah dan risiko, proses audit internal juga akan mendokumentasikan semua langkah yang diambil untuk meringankan tingkat risiko yang dihadapi, sebagai catatan evaluasi di masa yang akan datang.

4. Peningkatan efisiensi dan produktivitas perusahaan
Ada kalanya, kondisi yang terjadi di lapangan tidak sesuai dengan prosedur dan kebijakan yang telah ditetapkan sebelumnya. Proses audit internal menjadi salah satu cara untuk memastikan kesesuaian antara SOP dengan kondisi di lapangan. Proses ini juga akan membuktikan apakah SOP yang ada merupakan prosedur yang tepat dalam menghadapi risiko yang dihadapi perusahaan. Proses audit internal akan menghasilkan rekomendasi yang ditujukan untuk perbaikan aspek-aspek yang masih memiliki kekurangan.

5. Mengidentifikasi tingkat kesuksesan sistem kontrol yang ada
Setiap perusahaan pastinya telah memiliki sistem kontrol tersendiri. Hal yang menjadi pertanyaan adalah seberapa besar tingkat kesuksesan sistem kontrol tersebut? Proses internal audit akan mengidentifikasi tingkat kesuksesan sistem kontrol ini. Apabila masih ditemukan kekurangan, informasi dari hasil audit ini nantinya akan dipergunakan untuk mengembangkan strategi baru yang lebih sesuai dengan kondisi di lapangan.

Nama : Yuniarti Denita Sari

Kelas : MTI 2019 REGULER B / IT AUDIT

Kita harus melakukan audit TI karena audit TI berkaitan dengan proses menghimpun kebutuhan teknologi informasi dan mengevaluasi infrastruktur IT. Audit IT memastikan bahwa mekanisme sistem informasi yang berjalan, tetap berada di koridor integritas. Hal ini terjadi sebab mekanisme sistem informasi sangat terkait dengan perekonomian secara global. Semuanya menjadi sangat berkaitan satu dengan lainnya, sangat berbeda dengan sebelumnya ketika belum ada sistem terintegrasi. Contoh yang paling terlihat adalah operasional infrastruktur elektronik serta e-commerce atau sistem yang terintegrasi. Layanan ini memproses layanan kebutuhan data di seluruh dunia. Kondisi tersebut memaksa adanya kontrol dan audit TI yang luar biasa. Jika ada satu saja kesalahan yang tidak terdeteksi, bisa berakibat fatal terhadap proses bisnis dan layanan yang dijanjikan.

Lima jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini yaitu :

1. Bencana alam / natural disaster, contohnya : gempa bu,i, banjir, kebakaran, dan lain-lain.
2. Kegagalan sistem / system failure, contohnya : teknologi ketinggalan zaman, kabel putus (kegagalan peralatan, kegagalan perangkat keras dan lunak), mati lampu, dan lain-lain.
3. Manusia (tindakan yang tidak disengaja / accidental human), contohnya : pegawai baru yang sudah diberi tugas untuk melakukan entry data dan tidak di training terlebih dahulu, anggota tubuh yang menyenggol perangkat hardware / keras secara tidak sengaja.
4. Manusia yanng berbahaya (memiliki niat tidak baik) / malicious human, contohnya : mecuri data orang lain untuk mendapatkan keuntungan bagi diri sendiri, melakukan hacking, merusak system agar tidak dapat dipakai oleh orang lain.
5. Program yang dapat digunakan untuk melakukan kejahatan, contohnya : virus (malware, trojan, dan lain-lain).

Nama : Zena Lusi

Nim : 182420095

Kelas : MTIK319 B

1. Mengapa Kita harus Melakukan IT Audit ?

jawaban :

Menurut pendapat saya bahwa penting meakukan IT Audit bagi sebuah Organisasi untuk melakukan audit sistem informasi guna melhat kembali apakah sistem yang berjalan sudah tepat dan terpentng sistem mampu untuk mendukung tercapainya tujun organisasi.

2. 5 jenis ancaman yang melatarbelakangi perlunya IT Audit.

jawaban :

1. Bencana Alam / Natural disaster seperti : gempa bumi, banjir, kebakaran dll

2. Kegagalan sistem / System Failure : Kegagalan perangkat lunak dan kegagalan perangkat keras (Kegagalan peralatan, kegagalan fungsi perangkat lunak dan perangkat keras) solusi dengan kualitas perangkat yang baik mengurangi kelemahan ini.

3. yang tidak disengaja / accidental humans adalah tidak sengaja melakukan sesuatu yang membuat sistem bermaslah seperti : salah pemasukan data, salah penghapusan data.

4. Melicious Humans / manusia yang berbahaya adalah orang yang sengaja melakukan kegiatan yang bertujuan melicious seperti : Kecurangan dan kejahatan komputer.

- Impersonation : Mencuri credit card untuk kepentingan mereka
- Interception : classical concept hacking, mencuri data
- Interferers : seseorang yang merusak bisnis anda tanpa merusak system,tidak mencuri informasi, misalnya orang mencuri komputer, membuat system down

5. Program yang jahat / Usil (Virus, Malware, trojan dll)

Audit TI harus di lakukan untuk mengevaluasi apakah pengendalian dan prosedur yang diterapkan telah dilakuakan dengan baik atau tidak. selaian itu audit IT harus dilakukan untuk beberapa hal, diantaranya yaitu :

1. Mendeteksi agar komputer tidak dikelola secara kurang terarah.

2. Mendeteksi resiko kehilangan data.

3. Mendeteksi resiko pengambilan keputusan yang salah akibat informasi hasil proses sistem komputerisasi salah/lambat/tidak lengkap.

4. Menjaga aset perusahaan karena nilai hardware, software dan personil yang lazimnya tinggi.

5. Mendeteksi resiko error komputer.

6. Mendeteksi resiko penyalahgunaan komputer (fraud).

7. Menjaga kerahasiaan

8. Meningkatkan pengendalian evolusi penggunaan komputer

5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi yaitu :

1. Bencana alam **:** Gempa bumi, banjir, kebakaran, perang.

2. Kesalahan manusia : Kesalahan pemasukan data. Kesalahan penghapusan data. Kesalahan operator(salah memberi label pada pita magnetik.

3. Kegagalan perangkat lunak dan perangkat keras : Gangguan listrik. Kegagalan peralatan. Kegagalan fungsi perangkat lunak.

4. Kecurangan dan kejahatan komputer : Penyelewengan aktivitas. Penyalagunaan kartu kredit. Sabotase. Pengaksesan oleh orang lain yang tidak berhak

5. Program yang jahat/usil : Virus, cacing, bom waktu dll.

Mengapa kita harus melakukan Audit TI?

Hal ini karena risiko yang dihadapi oleh perusahaan sangat besar sehingga sangat penting untuk memastikan bahwa teknologi informasi yang ada maupun yang akan dipakai mengikuti perkembangan jaman teknologi agar dapat berjalan secara efektif dan efisien.

Sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini.

1. Data Forgery, memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless document melalui internet.
2. Bencana Alam
3. Manusia yang tidak disengaja / Accidental Human
4. Malicious Human
5. Kegagalan System

1. mengapa kita harus melakukan Audit TI ?

karena pada saat ini teknologi semakin berkembang, sehingga dapat memudahkan penggunanya untuk melakukan segala aktifitas. Salah satunya adalah melakukan Audit SI. Karena dengan menggunakan teknologi komputerisasi data yang diolah akan menjadi lebih baik lagi hasilnya.

2. sebutkan 5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini.

beberapa alasan mendasar mengapa organisasi perlu melakukan audit TI sebagai evaluasi dan pengendalian terhadap sistem yang digunakan oleh organisasi :

1. Pencegahan terhadap biaya organisasi untuk data yang hilang
2. Pengambilan keputusan yang tidak sesuai
3. Penyalahgunaan komputer
4. Nilai dari perangkat keras komputer, perangkat lunak dan personel
5. Biaya yang tinggi untuk kerusakan komputer

Banyak perusahaan, terlepas dari ukuran atau ruang lingkup operasinya, telah menyadari pentingnya menggunakan teknologi informasi untuk tetap mampu bersaing menuju revolusi industry 4.0. Perusahaan telah mengakui banyak manfaat yang dibawa IT untuk operasional perusahaan mereka. Selain itu juga, perusahaan harus menyadari pentingnya memastikan sistem IT dapat diandalkan, aman, dan kebal terhadap serangan komputer. Keamanan ini untuk memastikan kerahasiaan *(Confidentiality)*, integritas *(Integrity),* dan ketersediaan data *(Availability).* Melindungi informasi ini adalah bagian utama dari keamanan informasi. Kerahasiaan data berarti melindungi informasi dari pengungkapan kepada pihak yang tidak berwenang. Integritas data mengacu pada perlindungan informasi agar tidak dimodifikasi oleh pihak yang tidak berwenang. Ketersediaan informasi mengacu pada memastikan orang yang diberi wewenang memiliki akses ke informasi saat dan ketika dibutuhkan. Kunci untuk memastikan ketersediaan data adalah *back up* data. Oleh karena itu, audit sistem informasi akan memastikan bahwa data organisasi disimpan secara rahasia, kemudian integritas data dipastikan aman dan data tersedia setiap saat untuk pengguna yang berwenang. Tujuan audit termasuk mencari tahu apakah ada kelebihan, ketidakefisienan, dan pemborosan dalam penggunaan dan pengelolaan sistem IT. Audit dilakukan untuk meyakinkan para pemangku kepentingan bahwa sistem IT yang ada adalah nilai dari uang yang diinvestasikan untuk system IT itu sendiri.

Singkatnya, audit sistem informasi penting karena memberikan jaminan bahwa sistem IT dilindungi secara memadai, memberikan informasi yang dapat diandalkan kepada pengguna, dan dikelola dengan baik untuk mencapai manfaat yang diharapkan. Ini juga mengurangi resiko gangguan data, kehilangan atau kebocoran data, gangguan layanan dan manajemen sistem TI yang buruk.

5 jenis ancaman yang melatarbelakangi perlunya Audit TI dalam suatu organisasi pada saat ini :

1. Ancaman kehilangan dan pencurian data
2. Ancaman dari internal organisasi terhadap penyalahgunaan wewenang
3. Ancaman kerugian besar yang ditimbulkan oleh rusaknya perangkat
4. Ancaman malfungsi sumber daya
5. Ancaman dari bencana alam