sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.

jelaskan dengan adanya contoh kasus yang terkait

jangan lupa tambahkan referensi

Nama : Mezi Puspayani

NIM : 182420120

Kelas : MTI20B

Tugas 1.

sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.

jelaskan dengan adanya contoh kasus yang terkait

jangan lupa tambahkan referensi

Jawab :

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya “scope creep” (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan.

Contohnya :

Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (*IT Governance*) (Herawan, 2012).

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (*Information System and Control Association*) dan ITGI (*IT Governance Institute*) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.(Wibowo, 2008).

Nama : **Miftahul Fallah**
Nim : **182420132**
Kelas : **MTI. 20A**
DosenPengasuh : **Dr Widya Cholil , S.Kom., M.I.T.**
Mata Kuliah : **IT Audit**

Soal

Sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.
Jelaskan dengan adanya contoh kasus yang terkait
Jangan lupa tambahkan referensi

Jawaban

***information technology (IT) audit atau information systems (IS) audit*)** adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi 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 teknologi informasi** 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.

A. Salah satu jenis yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit adalah risiko audit dalam penerapan sistem informasi di perusahaan.

RESIKO DALAM PENERAPAN SISTEM INFORMASI DI PERUSAHAAN

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan. Di lain pihak, seiring makin meluasnya implementasi sistem informasi maka kesadaran akan perlunya dilakukan review atas pengembangan suatu sistem informasi semakin meningkat. Kesadaran ini muncul karena munculnya berbagai kasus yang terkait dengan gagalnya sistem informasi, sehingga memberikan akibat yang sangat mempengaruhi kinerja organisasi.

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya "scope creep" (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah **CISA® (Certified Information Systems Auditor)** yang dikeluarkan oleh **ISACA (Information Systems Audit and Control Association).** **Audit sistem informasi** dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contohnya :

Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (*IT Governance*) (Herawan, 2012).

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu

diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (*Information System and Control Association*) dan ITGI (*IT Governance Institute*) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.(Wibowo, 2008).

Referensi

Fanani, M. F. (2012, September 24). *Implementasi COBIT Di PT PERTAMINA*. Retrieved November 27, 2012, from http://www.slideshare.net: http://www.slideshare.net/fananifaiz/cobit-pertamina#btnNext

Herawan, R. (2012, April 4). *Implementasi COBIT pada PT Transindo*. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/

Meidyanto, Riky (2009, Juni 19). *Audit Sistem Informasi dengan Menggunakan COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 27, 2012, from http://krikkrikx.blog.binusian.org: http://www.krikkrikx.blog.binusian.org/files/2009/06/untuk-blog221.doc

Susanto, Erdi (2012, November). *Kerangka Kerja COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 28, 2012, from http://erdi-susanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobit-control-objectives.html

Wibowo, M. P. (2008, Agustus 9). *Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective For Information And Related Technology): Studi Kasus Di Perpustakaan Universitas Indonesia*. Retrieved November 27, 2012, from http://sangprabu.multiply.com: http://sangprabu.multiply.com/journal/item/27

Wikipedia. *COBIT*. Retrieved November 27, 2012, from http://www.wikipedia.org: http://en.wikipedia.org/wiki/COBIT

Sumber : https://sis.binus.ac.id/2015/07/01/resiko-dalam-penerapan-sistem-informasi-di-perusahaan/

Nama : **Moh Fajri Al Amin**
Nim : **182420121**
Kelas : **MTI. 20A**
DosenPengasuh : **Dr Widya Cholil , S.Kom., M.I.T.**
Mata Kuliah : **IT Audit**

Soal

Sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.
Jelaskan dengan adanya contoh kasus yang terkait
Jangan lupa tambahkan referensi!

Jawab:

***Information Technology (IT) audit atau information systems (IS) audit*)** adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi 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 teknologi informasi** 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 menurut Ron Webber (Dekan Fakultas Teknologi Informasi, Monash University) dalam bukunya *Information System Controls and Audit* (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Sebagai contoh berikut adalah contoh kasus yang berkaitan dengan IT audit:

Kejahatan Di Dunia Perbankan

JAKARTA – Masyarakat resah melihat kasus pembobolan dana nasabah di bank yang intensitasnya meningkat sejak awal 2011. Kasus-kasus yang terjadi dalam rentang waktu berdekatan ini pun berdampak pada makin kurangnya kepercayaan publik terhadap perbankan.

Dengan begitu, pengamat perbankan Mirza Adityaswara mengatakan, masyarakat akan lebih berhati-hati menggunakan layanan perbankan setelah mencuatnya kasus-kasus yang terjadi. “Masyarakat yang semula kurang awas, akan lebih waspada,” katanya, Ahad (2/5).

Mirza berpendapat sistem perbankan yang ada saat ini memang belum sempurna. Ini, jelas dia, bukan hanya terlihat dari sisi pegawai bank, melainkan juga nasabah. “Jangan tergoda melakukan penyelewengan,” katanya.

Tony Prasetyantono, pengamat perbankan, mengatakan berkurangnya kepercayaan publik pasti akan terjadi menyusul berbagai kasus tersebut. Namun, nasabah belum sampai pada satu tindakan menarik uangnya besar-besaran. Karena, jelas Tony, nasabah tidak memiliki pilihan lain yang lebih baik untuk menempatkan uangnya.

Sejauh ini, ujar Tony, bank masih dinilai sebagai tempat terbaik menyimpan aset. “Apalagi yang bersifat likuid, seperti rekening giro dan tabungan,” katanya. “Namun, nasabah akan lebih se-lektif memilih bank.”

Nasabah, lanjut dia, juga akan lebih memantau rekeningnya agar luput dari pembobolan. Tony menilai, kejahatan perbankan yang terjadi belakangan lebih mengarah pada kesalahan kolektif. Penyebabnya, ia menjelaskan, muncul dari sisi perbankan, nasabah, Bank Indonesia, maupun aturan hukumnya.

Tony mencontohkan, bank kerap menyembunyikan penyimpangan karena takut reputasinya rusak, sedangkan nasabah tidak aktif memantau rekening miliknya. Sementara, BI memiliki keterbatasan dalam memantau banyaknya perbankan yang ada di Tanah Air. “Hukuman terhadap pelaku fra ud juga ku-rang maksimal sehingga kurang menimbulkan efek jera,” jelasnya.

Saat ini. Direktorat Kriminal Khusus (Ditkrimsus) Polda Metro Jaya sedang menangani sembilan kasus perbankan sejak Januari 2011. Bulan lalu, dana deposito milik PT Elnusa Rp 111 miliar di Bank Mega dicairkan tanpa seizin manajemen perusahaan tersebut dengan pelaku melibatkan orang dalam bank. Sebelumnya, simpanan nasabah prioritas Citibank dibobol oleh karyawan bank asing tersebut yang bernama Inong Malinda alias Malinda Dee.

Kepala Bidang Humas Polda Metro Jaya Kombes Baharudin Djafar mengatakan, kasus pembobolan bank tak ha-nya terjadi di bank swasta. Menurutnya, akhir pekan lalu, bank milik negara pun tak luput dari jarahan oknum pegawainya yang nakal. Dari sembilan kasus perbankan itu, polisi berhasil menangkap 30 tersangkanya.

Kasat Fiskal, Moneter, dan Devisa Ditkrimsus Polda Metro Jaya AKBP Arismunandar menambahkan, kasus pembobolan dana perbankan biasanya melibatkan orang dalam bank. Sementara itu, Corporate Secretary BSB, Evi Yulia Kurniawati, mengatakan pihaknya menjalankan tata tertib sesuai standar dan memperketat kontrol internal agar terhindar dari kejahatan perbankan.

Saran-saran agar kejahatan serupa tidak terulang:

- Dalam kasus diatas sebaiknya para nasabah harus lebih berhati-hati dan sebaiknya pihak perbankan memberikan penyuluhan kepada para nasabah.

- Selain itu dunia perbankan wajib melakukan edukasi kepada nasabah tentang masalah yang sering terjadi. Edukasi tersebut diberikan setidaknya bagi nasabah baru dalammenggunakan fasilitas perbankan.
- Melakukan perbaikan atas lemahnya sisem keamanan jaringan.
- saatnya otoritas mengurus sistemik real, karena kalau bank saja tidak dipercaya masyarakat krisis akan berlanjut ke masalah krisis perbankan seperti yang ditakutkan sekarang ini.
- Memperkuat infrastruktur perbankan.

Referensi:

Fanani, M. F. (2012, September 24). *Implementasi COBIT Di PT PERTAMINA*. Retrieved November 27, 2012, from http://www.slideshare.net: http://www.slideshare.net/fananifaiz/cobit-pertamina#btnNext

Herawan, R. (2012, April 4). *Implementasi COBIT pada PT Transindo*. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/

Meidyanto, Riky (2009, Juni 19). *Audit Sistem Informasi dengan Menggunakan COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 27, 2012, from http://krikkrikx.blog.binusian.org: http://www.krikkrikx.blog.binusian.org/files/2009/06/untuk-blog221.doc

Susanto, Erdi (2012, November). *Kerangka Kerja COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 28, 2012, from http://erdi-susanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobit-control-objectives.html

Wibowo, M. P. (2008, Agustus 9). *Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective For Information And Related Technology): Studi Kasus Di Perpustakaan Universitas Indonesia*. Retrieved November 27, 2012, from http://sangprabu.multiply.com: http://sangprabu.multiply.com/journal/item/27

Wikipedia. *COBIT*. Retrieved November 27, 2012, from http://www.wikipedia.org: http://en.wikipedia.org/wiki/COBIT

https://dendyoktavianto23.wordpress.com/2017/10/09/studi-kasus-audit-teknologi-informasi/

NAMA : MOH. RENDY SEPTIYAN

NIM : 182420103

MATA KULIAH : IT AUDIT

Jenis resiko yang menjadi factor utama sehingga perlu adanya IT Audit atau IS Audit

a. Kehilangan data
b. Kesalahan pengambilan keputusan
c. Penyalagunaan computer
d. Nilai investasi
e. Aspek privasi
f. Kesalahan pengopersian computer
g. Evolusi teknologi

Contoh kasus IT Audit di Perusahaan

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.***

Audit TI atau yang pernah disebut sebagai *audit electronic data processing*, *computer information system*, dan IS, pada awalnya merupakan pelebaran dari *audit konvensional*. Dulu, kebutuhan atas fungsi audit TI hanya berasal dari beberapa departemen.

Kemudian auditor sadar bahwa komputer telah mempengaruhi kinerja mereka terkait fungsi utama. Perusahaan dan manajemen pemrosesan informasi pun sadar bahwa komputer adalah jalan keluar terkait permasalahan sumber daya untuk semakin bersaing dalam lingkungan bisnis bahkan antar departemen. Oleh karenanya, muncullah urgensi untuk melakukan kontrol dan audit atas proses yang berjalan. Saat itulah para profesional menyadari tentang kebutuhan audit TI. Audit TI menjadi bagian integral dalam fungsi audit umum, sebab hal itu akan menentukan kualitas dari informasi yang diproses oleh sistem komputer.

Pada mulanya, auditor dengan kemampuan audit TI dilihat sekadar sebagai staf sumber daya teknologi biasa, bahkan sering dilihat hanya sebagai asisten teknikal. Padahal dewasa ini, audit IT

merupakan pekerjaan yang tindakan, tujuan, serta kualitasnya telah diatur dalam standar global; ada aturan etiknya; dan tuntutan profesional. Tentu saja hal ini memerlukan pengetahuan khusus dan kemampuan praktis, yang sebelumnya juga didahului oleh persiapan secara intensif.

Dari penjelasan singkat ini, nampak jelas bahwa masih akan ada banyak tantangan ke depan teruntuk audit TI. ***Setiap pihak harus bisa bekerja sama untuk mampu mendesain, mengimplementasikan, serta mencapai tujuan-tujuan dasar yang sudah umum dipahami.***

https://blog.gamatechno.com/mengenal-pentingnya-audit-teknologi-informasi/

TUGAS IT AUDIT

Nama : Muhammad Devian saputra

NIM :182420126

MTI 20A

SOAL

1. sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.
2. jelaskan dengan adanya contoh kasus yang terkait
3. jangan lupa tambahkan referensi

JAWAB

1. Beberapa jenis resiko sehingga perlu adanya IT atau IS Audit :

   Ancaman TI kondisi perangkat TI, program-program jahat, kegagalan perangkat lunak, virus, spam, phishing dan ancaman terbesar adalah kesalah manusia dalam pengelolaan system TI, pegelolaan data .

   Ancaman TI yang mengarah pada tindakan pelanggaran hukum, misalnya serangan hacker, penipuan menggunakan system TI, pencurian kata kunci (password), serangan pada data, dan lain-lain

   Ancaman TI yang timbul akibat kejadian diluar normal, misalnya terjadinya bencana, baik bencana alam maupun bencana yang dibuat misalnya tindakan teroris.

2. Contoh kasus

   - Hilangnya data akibat ulah pihak yang tidak berwenang mengakses dan mengotak atik data yang ada. Hilangnya hak akses user terhadap suatu sistem , Server down akibat terlalu banyak menerima perintah/permintaan yang mengakibatkan permintaan yang asli tidak terlayani. Pencurian data yang sifatnya penting dari suatu sistem dan diperjual-belikan ke pihak asing sehingga bisa berpotensi merugikan pemilik data.

- Kerusakan software,hardware dan pembatalan eksekusi dan pengolahan data tanpa sepengetahuan pihak yang berwenang(users).

- Berubahnya data yang tersimpan sehingga mengacaukan kerja sistem yang semula berjalan normal. Atau berubahnya password dan username sehingga users yang berhak mengakses sistem tidak dapat mengakses sistem lagi.

- Matinya semua perangkat yang membutuhkan listrik . Ancaman hilangnya daya merupakan ancaman yang berdampak mematikan seluruh perangkat yang hidup menggunakan listrik. Apabila semua mati,maka users tidak dapat melakukan apa-apa karena sistem mati dan server mati .

- ***FRAUD*** (kecurangan) adalah tindakan ilegal yang dilakukan satu orang atau sekelompok orang secara sengaja atau terencana yang menyebabkan orang atau kelompok mendapat keuntungan, dan merugikan orang atau kelompok lain.
  Contoh ***FRAUDulent financial reporting*** (kecurangan laporan keuangan) adalah salah saji atau pengabaian jumlah dan pengungkapan yang disengaja dengan maksud menipu para pemakai laporan.
  Dalam suatu IT service sebuah aplikasi harus diuji apakah aplikasi tersebut dapat bebas dari Fraud

- Risiko keamanan komputer (computer security risk) adalah setiap peristiwa atau tindakan yang dapat mengakibatkan hilang atau rusaknya piranti keras, piranti lunak, data ataupun informasi. Beberapa penyusup tidak melakukan perusakan, mereka hanya mengakses data, informasi, atau program-program pada komputer. Beberapa penyusup lain menunjukkan beberapa bukti keberadaan mereka dengan meninggalkan pesan atau seenaknya mengubah atau merusak data.
  Setiap tindakan ilegal yang melibatkan komputer dalam kegiatannya secara umum dikenal dengan istilah computer crime. Istilah cybercrime mengacu pada tindakan ilegal berbasis online atau internet.
- Virus. Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia. Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

- Denial of Service (DoS) dan Distributed DoS (DDos) attack. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian,penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet.

3. Referensi :

- *Penulis: Andrianto Moeljono, MM, CLA ISO 9001, CLA ISO 27001, selaku Director and Senior Consultant Proxsis IT Sumber foto: a2z-support.com*

- https://theyouthfulideas.blogspot.com/2012/09/tugas-3-manajemen-resiko-it.html
- https://www.researchgate.net/publication/311972151_Framework_Audit_IT
- https://resources.infosecinstitute.com/itac-planning/
- https://makalahblogandress.blogspot.com/2016/07/resiko-keamanan-komputer.html
- https://techno-inmyworld.blogspot.com/2014/12/apa-itu-vulnerability-kelemahan-risk.html

Nama : Putri Armilia Prayesy

Nim : 182420125

Mata Kuliah : IT Audit

MTI 20A

sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit. jelaskan dengan adanya contoh kasus yang terkait jangan lupa tambahkan referensi

Jawab :

Jenis Resiko yang menjadi faktor utama perlunya IT Audit

1. Resiko Inheren (Inheren Risk)

merupakan 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. Dengan mengasumsikan tiadanya pengendalian intern, maka risiko inheren ini dapat dinyatakan sebagai kerentanan laporan keuangan terhadap timbulnya salah saji yang material. Jika auditor, dengan mengabaikan pengendalian intern, menyimpulkan bahwa terdapat suatu kecenderungan yang tinggi atas keberadaan sejumlah salah saji, maka auditor akan menyimpulkan bahwa tingkat risiko inherennya tinggi. pengendalian intern diabaikan dalam menetapkan dalam menetapkan nilai risiko inheren karena pengendalian intern ini dipertimbangkan secara terpisah dalam model risiko audit sebagai risiko pengendalian. Penilaian ini cenderung didasarkan atas sejumlah diskusi yang telah dilakukan dengan pihak manajemen, pemahaman yang dimiliki akan perusahaan, serta hasil-hasil yang diperoleh dari tahun-tahun sebelumnya.

Contoh :

jika risiko inheren atas keusangan persediaan sangat tinggi, maka sangatlah masuk akal bila kantor akuntan publik memilih staf yang berpengalaman untuk melakukan sejumlah tes yang lebih mendalam atas keusangan persediaan ini dan melakukan review yang lebih cermat atas hasil-hasil yang diperoleh dari audit ini.

2. Resiko Pengendalian (Control Risk)

merupakan ukuran yang digunakan oleh auditor untuk menilai adanya kemungkina bahwa terdapat sejumlah salah saji material yang melebihi nilai salah saji yang masi dapat ditoleransi atas segmen tertentu akan tidak terhadang atau tidak terdeteksi oleh pengendalian intern yang dimiliki klien. Resiko pengendalian ini memperhatikan 2 hal berikut:

penilaian tentang apakah pengendalian intern yang dimiliki klien efektif untuk mencegah atau mendeteksi terjadinya salah saji.

kehendak auditor membuat penilaian tersebut senantiasa berada di bawah nilai maksimum (100 persen) sebagai bagian dari rencana audit yang dibuatnya.

Model resiko audit menunjukan hubungan yang erat antara resiko inheren dan resiko pengendalian.

Sama dengan yang terjadi pada resiko inheren, hubungan antara resiko pengendalian dan resiko deteksi terencana adalah saling berlawanan, sementara hubungan antara resiko pengendalian dan bukti substantif merupakan hubungan yang searah.

Contoh :

jika auditor menyimpulkan bahwa pengendalian intern bersifat efektif, maka nilai resiko deteksi terencana dapat meningkat sehingga jumlah bukti audit yang direncanakan akan dikumpulkan akan turun. Auditor dapat meningkatkan resiko deteksi terencana pada saat pengendalian intern bersifat efektif karena pengendalian intern yang efektif akan mengurangi kemungkinan hadirnya salah saji dalam laporan keuangan.

Sebelum auditor dapat menetapkan nilai resiko pengendalian kurang dari 100 persen, auditor harus memahami pengendalian intern yang ada, dan berdasarkan pemahaman itu, auditor melakukan evaluasi tentang bagaimana seharusnya fungsi pengendalian intern tersebut, serta melakukan uji atas efektifitas pengendalian intern tersebut. Hal pertama dari semua ini adalah keharusan untuk memahami semua jenis audit. Dua hal terakhir adalah langkah-langkah penilaian resiko pengendalian yang diperlukan jika auditor memilih untuk memberikan nilai atas resiko pengendalian supaya berada di bawah nilai maksimum

3. Risiko Deteksi Terencana (Planned Detection Risk)

merupakan ukuran risiko bahwa bukti audit atas segmen tertentu akan gagal mendeteksi keberadaan salah saji yang melebihi suatu nilai salah saji yang masih dapat ditoleransi, andaikan salah saji semacam itu ada. Terdapat dua poin utama tentang risiko deteksi terencana ini yaitu sebagai berikut :

Risiko ini tergantung pada ketiga faktor lainnya yang terdapat dalam model. Risiko deteksi terencana hanya akan berubah jika auditor melakukan perubahan pada salah satu dari ketiga faktor lainnya tersebut.

Risiko ini menentukan nilai substantif yang direncanakan oleh auditor untuk dikumpulkan, yang merupakan kebalikan dari ukuran risiko deteksi terencana itu sendiri.

Jika nilai risiko deteksi terencana berkurang, maka auditor harus mengumpulkan lebih banyak bukti audit untuk mencapai nilai risiko deteksi yang berkurang ini.

4. Resiko Audit yang dapat Diterima (Acceptable Audit Risk)

Adalah ukuran ketersediaan auditor untuk menerima bahwa laporan keuangan mengandung salah saji material tanpa pengecualian telah diberikan. Resiko ini telah ditetapkan secara subjektif bahwa auditor bersedia menerima laporan keuangan tidak disajikan wajar setelah audit selesai dan pendapat wajar tanpa pengecualian telah diberikan.

- http://damasburnaman21.blogspot.co.id/2017/11/resiko-yang-mengakibatkan-prosedur.html
- http://darmansyah.weblog.esaunggul.ac.id/2014/06/02/tugas-edp-audit/

Nama : **Putri Eleina Nurrahma**
Nim : **182420138**
Kelas : **MTI. 20A**
DosenPengasuh : **Dr Widya Cholil , S.Kom., M.I.T.**
Mata Kuliah : **IT Audit**

Soal

Sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.
Jelaskan dengan adanya contoh kasus yang terkait
Jangan lupa tambahkan referensi

Jawaban

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.

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.

Referensi

Juliandarini. Handayaningsih, Sri. Audit Sistem Informasi pada Digilib Universitas XYZ Menggunakan Kerangka Kerja COBIT 4.0. Jurnal Sarjana Teknik Informatika. Volume 1 Nomor 1, Juni 2013. Pp. 276-286. e-ISSN: 2338-5197

Romney, Marshall B., Steinbart, Paul John. (2004). Accounting Information Systems. 9th edition.

Weber, Ron. (1999). Information Systems Control and Audit. Prentice-Hall, Inc., New Jersey.

Nama : Rahmad Kartolo
NIM : 182420119
Kelas : MTI Reguler B
Mata Kuliah : IT Audit

Question:
sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.
jelaskan dengan adanya contoh kasus yang terkait

jangan lupa tambahkan referensi !

Answer:

Example:
Dengan ketergantungan kita terhadap Sistem Informasi Akuntansi berbasis komputer maka ada beberapa alasan untuk manajemen memerlukan sebuah Audit Sistem Informasi, yaitu antara lain adalah

1. **Kerugian akibat kehilangan data.**

   Data yang diolah menjadi sebuah informasi, merupakan aset penting dalam organisasi bisnis saat ini. Banyak aktivitas operasi mengandalkan beberapa informasi yang penting. Informasi sebuah organisasi bisnis akan menjadi sebuah potret atau gambaran dari kondisi organisasi tersebut di masa lalu, kini dan masa mendatang. Jika informasi ini hilang akan berakibat cukup fatal bagi organisasi dalam menjalankan aktivitasnya.

   Sebagai contoh adalah jika data nasabah sebuah bank hilang akibat rusak, maka informasi yang terkait akan hilang, misalkan siapa saja nasabah yang mempunyai tagihan pembayaran kredit yang telah jatuh tempo. Atau juga misalkan kapan bank harus mempersiapkan pembayaran simpanan deposito nasabah yang akan jatuh tempo beserta jumlahnya.

   Sehingga organisasi bisnis seperti bank akan benar-benar memperhatikan bagaimana menjaga keamanan datanya. Kehilangan data juga dapat terjadi karena tiadanya pengendalian yang memadai, seperti tidak adanya prosedur back-up file. Kehilangan data dapat disebabkan karena gangguan sistem operasi pemrosesan data, sabotase, atau gangguan karena alam seperti gempa bumi, kebakaran atau banjir

2. **Kerugian akibat kesalahan pemrosesan komputer**.

   Pemrosesan komputer menjadi pusat perhatian utama dalam sebuah sistem informasi berbasis komputer. Banyak organisasi telah menggunakan komputer sebagai sarana untuk meningkatkan kualitas pekerjaan mereka. Mulai dari pekerjaan yang

sederhana, seperti perhitungan bunga berbunga sampai penggunaan komputer sebagai bantuan dalam navigasi pesawat terbang atau peluru kendali. Dan banyak pula di antara organisasi tersebut sudah saling terhubung dan terintegrasi. Akan sangat mengkhawatirkan bila terjadi kesalahan dalam pemrosesan di dalam komputer. Kerugian mulai dari tidak dipercayainya perhitungan matematis sampai kepada ketergantungan kehidupan manusia.

3**. Pengambilan keputusan yang salah akibat informasi yang salah.**

Kualitas sebuah keputusan sangat tergantung kepada kualitas informasi yang disajikan untuk pengambilan keputusan tersebut. Tingkat akurasi dan pentingnya sebuah data atau informasi tergantung kepada jenis keputusan yang akan diambil. Jika top manajer akan mengambil keputusan yang bersifat strategik, mungkin akan dapat ditoleransi berkaitan dengan sifat keputusan yang berjangka panjang. Tetapi kadangkala informasi yang menyesatkan akan berdampak kepada pengambilan keputusan yang menyesatkan pula.

4. Kerugian karena penyalahgunaan komputer (Computer Abused)

Tema utama yang mendorong perkembangan dalam audit sistem informasi dalam sebuah organisasi bisnis adalah karena sering terjadinya kejahatan penyalahgunaan komputer. Beberapa jenis tindak kejahatan dan penyalah-gunaan komputer antara lain adalah virus, hacking, akses langsung yang tak legal (misalnya masuk ke ruang komputer tanpa ijin atau menggunakan sebuah terminal komputer dan dapat berakibat kerusakan fisik atau mengambil data atau program komputer tanpa ijin) dan atau penyalahgunaan akses untuk kepentingan pribadi (seseorang yang mempunyai kewenangan menggunakan komputer tetapi untuk tujuan-tujuan yang tidak semestinya)

- Hacking - seseorang yang dengan tanpa ijin mengakses sistem komputer sehingga dapat melihat, memodifikasi, atau menghapus program komputer atau data atau mengacaukan sistem.

- Virus – virus adalah sebuah program komputer yang menempelkan diri dan menjalankan sendiri sebuah program komputer atau sistem komputer di sebuah disket, data atau program yang bertujuan mengganggu atau merusak jalannya sebuah program atau data komputer yang ada di dalamnya. Virus dirancang dengan dua tujuan, yaitu pertama mereplikasi dirinya sendiri secara aktif dan kedua mengganggu atau merusak sistem operasi, program atau data.

Dampak dari kejahatan dan penyalahgunaan komputer tersebut antara lain:

- Hardware, software, data, fasilitas, dokumentasi dan pendukung lainnya rusak atau hilang dicuri atau dimodifikasi dan disalahgunakan.
- Kerahasiaan data atau informasi penting dari orang atau organisasi rusak atau hilang dicuri atau dimodifikasi.
- Aktivitas operasional rutin akan terganggu.
- Kejahatan dan penyalahgunaan komputer dari waktu ke waktu semakin meningkat, dan hampir 80% pelaku kejahatan komputer adalah 'orang dalam'.

5. Nilai hardware, software dan personil sistem informasi

Dalam sebuah sistem informasi, hardware, software, data dan personil adalah merupakan sumberdaya organisasi. Beberapa organisasi bisnis mengeluarkan dana yang cukup besar untuk investasi dalam penyusunan sebuah sistem informasi, termasuk dalam pengembangan sumberdaya manusianya. Sehingga diperlukan sebuah pengendalian untuk menjaga investasi di bidang ini.

6. Pemeliharaan kerahasiaan informasi

Informasi di dalam sebuah organisasi bisnis sangat beragam, mulai data karyawan, pelanggan, transaksi dan lainya adalah amat riskan bila tidak dijaga dengan benar. Seseorang dapat saja memanfaatkan informasi untuk disalahgunakan. Sebagai contoh bila data pelanggan yang rahasia, dapat digunakan oleh pesaing untuk memperoleh manfaat dalam persaingan.

Referensi : http://silfisulfiyah.blogspot.com/2010/11/mengapa-perlu-audit-sistem-informasi.html

Nama : Reynaldi

Nim : 182420111

Matkul : IT Audit

SOAL

Sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit. Jelaskan dengan adanya contoh kasus yang terkait, sertakan pula refrensinya

JAWAB

1. Berikut adalah beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit :
   - Resiko dalam keamanan Sistem maupun Data
   - Resiko dalam Keaslian Data
   - Resiko dalam konsumi sumber daya dalam organisasi

   Contoh kasus:

   Contoh kasus Risiko dalam keamanan Sistem informasi adalah kasus pada Anti-Virus Kspersky Lab yang berawal pada 13 Juli 2017 saat peerintah Amerika Serikat melarang badan-badan federalnya membeli perangkat lunak dari perusahaan Rusia Kaspersky Lab di tengah kekhawatiran mengenai hubungan perusahaan terseut dengan badan inteijen di Moskow.

   Pada 13 September 2017 departemen keamangan dalam negeri Amerika Serikat (DHS) memerintahkan departemen dan agensi federal untuk mengahpus produk produk Kaspersky Lab dari sistem informasi mereka.

   Departemen tersebut risau dengan hubungan antara beberapa pejabat Kaspersky dan intelijen Rusia dan serta badan pemerintah lainnya, dan berdasarkan undang-undangn Rusia hal itu memungkinkan badan intelijen Rusia untuk meminta atau memaska bantuan dari Kaspersky dan mencegat komunikasi yang melintas jaringan Rusia.

Tidak lama dari itu, pada 6 Oktober 2017, tersiar laporan bahwa para peretas Rusia memanfaatkan Anti-Virus milik Kaspersky Labs untuk mencuri materi rahasia badan keamanan Nasiona AS dari salah satu komputer kontraktor NSA.

Kaspersky bantah dipakai untuk retas komputer intel AS. Perusahaan teknologi itu juga mengklain bahwa sebagai perusahaan swasta mereka tidak memiliki hubungan apapun denguan oemerintah manapun, termasuk Rusia, meskipun mereka bermarkas di ibu kota Rusia, Moscow.

Pada 23 Oktober 2017 kaspersky berupaya kembalikan kepercayaan setelah tuduhan spionase kremlin dengan meluncurkan "inisiatif transparansi global" yang mengizinkan pihak ketiga menganalisis perangkat lunak Anti-Virusnya.

Sebagai bagian dari inisiatif ini, perusahaan bermaksud untuk menyediakan kode sumber perangkat lunaknya – termasuk pembaruan perangkat lunak dan pembaruan peraturan deteksi ancaman – untuk tinjauan dan penilaian independen.

Tidak tinggal diam, pada 20 Desember 2017, Kaspersky Lab dilaporkan mengajukan bandi kepada pengadilan federal (Federal Court) terhadap keputusan departemen keamanan dalam negeri Amerikas Serikat menganai binding Operational Directive 17-01 yang melarang penggunaan priduk perusahaan di lembaga federal.

Kaspersky Lab merasa tindakan DHS tersebut telah menyebabkan kerusakan yang tidak semestinya terhadap reputasi perusahaan di industri keamanan IT dan penjualan di AS.

Dengan mengajukan banding ini. Kaspersky Lab berharap untuk mendapatkan hak untuk melakukan proses penyiapan (Due Process) berdasarkan konstitusi Amerika Serikat dan undang-undang federal dan memperbaiki kerugian yang ditimbulkan terhadap operasi komersial perusahaan, karyawan yang berbasis AS, dan mitra bisnisnya yang berbasis di Amerika Serikat.

Kasus serangan siber terheboh 2017, https://www.antaranews.com/berita/674301/kasus-serangan-siber-terheboh-2017 (diakses 30 Desember 2017)

Nama : Rio Permata
NIM : 182420108
Kelas : MTI Reguler B
Mata Kuliah : IT Audit

FAKTOR UTAMA DIPERLUKAN ADANYA IT AUDIT

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.

Referensi :

1. https://sis.binus.ac.id/2015/06/24/pentingnya-audit-sistem-informasi-bagi-organisasi/
2. Juliandarini. Handayaningsih, Sri. Audit Sistem Informasi pada Digilib Universitas XYZ Menggunakan Kerangka Kerja COBIT 4.0. Jurnal Sarjana Teknik Informatika. Volume 1 Nomor 1, Juni 2013. Pp. 276-286. e-ISSN: 2338-5197
3. Romney, Marshall B., Steinbart, Paul John. (2004). Accounting Information Systems. 9th edition.
4. Weber, Ron. (1999). Information Systems Control and Audit. Prentice-Hall, Inc., New Jersey.

Nama : Yudistira Sira Permana
NIM : 182420104
MK : IT Audit

JENIS – JENIS RESIKO IT / IS AUDIT

1. **Risiko Bisnis (*Business Risk*)**

   Risiko bisnis adalah risiko yang dapat disebabkan oleh faktor-faktor intern maupun ekstern yang berakibat kemungkinan tidak tercapainya tujuan organisasi (*business goal objectives*).

   Contoh : dalam melakukan pengadaan sebuah barang IT biasanya pihak internal sering melakukan Kerjasama dengan pihak external dengan mengiming-imingi bisnis dibalik sebuah transaksi. Resikonya apabila melakukan pencarian suatu barang dengan memilih barang yang lebih murah dengan tidak mengetahui suatu manfaat dari apa yang akan di beli, maka akibatnya barang yang akan di beli bisa sia-sia. Lebih baik membeli yang mahal tetapi barang tersebut sangat berguna.

2. **Risiko Bawaan (*Inherent Risk*)**

   Risiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan jika tidak ada pengendalian internal.

   Contoh : Tahapan dalam membangun system itu seharusnya melalui tahapan Analis, UI/UX, Programmer, dan tester. Tetapi kesalahan dalam melewati tahapan ini tering dilakukan misalkan tanpa melakukan Analis dan UI/UX, user langsung membangun sebuah system langsung berkomunikasi dengan Programmer.

3. **Risiko Pengendalian (*Control Risk*)**

   Dalam suatu organisasi yang baik seharusnya sudah ada *risk assessment*, dan dirancang pengendalian internal secara optimal terhadap setiap potensi risiko. Risiko pengendalian ialah masih adanya risiko meskipun sudah ada pengendalian.

   Contoh : dari system keamanan software pada dasarnya setiap perusahaan sudah mempersiapkan pengendalian dari segi Keamanan System, tetapi tetap saja keamanan belum bisa di pastikan aman, karena setiap software pasti ada titik lemahnya.

4. **Risiko Deteksi (*Detection Risk*)**

   Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya *error* yang cukup matrealitas atau adanya kemungkinan *fraud*.

   Contoh : di dalam tugas seorang tester program terdapat beberapa cara untuk memasikan kualitas suatu program, baik dari sedi automation test, loading test, dan penetration test. Dengan demikian pihak audit dapat mendeteksi kualitas suatu program tersebut dengan dokumentasi yang telah di sediakan oleh tester.

5. **Risiko Audit (*Audit Risk*)**

   Risiko audit sebenarnya adalah kombinasi dari *inherent risk*, *control risk*, dan *detection risk*. Risiko audit adalah risiko bahwa pemeriksaan auditor ternyata belum dapat mencerminkan keadaan yang sesungguhnya.

   Contoh : penilaian yang diberikan audit pada keamanan sebuah system itu sangat tinggi, tetapi keamanan dari system tersebut belum bisa dipastikan karena sebuah system pasti masih terdapat celah-celah yang dapat di tembus.

Referensi :

https://www.academia.edu/35574253/05-Resiko_Audit_SI.ppt?auto=download

Nama : **Adiktia, S. kom**
Kelas : MTI20A
NIM : 182420101
Mata Kuliah : IT AUDIT

RESIKO DALAM PENERAPAN SISTEM INFORMASI DI PERUSAHAAN

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan. Di lain pihak, seiring makin meluasnya implementasi sistem informasi maka kesadaran akan perlunya dilakukan review atas pengembangan suatu sistem informasi semakin meningkat. Kesadaran ini muncul karena munculnya berbagai kasus yang terkait dengan gagalnya sistem informasi, sehingga memberikan akibat yang sangat mempengaruhi kinerja organisasi.

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya “scope creep” (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian

prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contohnya :

Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (*IT Governance*) (Herawan, 2012).

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (*Information System and Control Association*) dan ITGI (*IT Governance Institute*) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.(Wibowo, 2008).

DAFTAR PUSTAKA

Fanani, M. F. (2012, September 24). *Implementasi COBIT Di PT PERTAMINA*. Retrieved November 27, 2012, from http://www.slideshare.net: http://www.slideshare.net/fananifaiz/cobit-pertamina#btnNext

Herawan, R. (2012, April 4). *Implementasi COBIT pada PT Transindo*. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/

Meidyanto, Riky (2009, Juni 19). *Audit Sistem Informasi dengan Menggunakan COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 27, 2012, from http://krikkrikx.blog.binusian.org: http://www.krikkrikx.blog.binusian.org/files/2009/06/untuk-blog221.doc

Susanto, Erdi (2012, November). *Kerangka Kerja COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 28, 2012, from http://erdi-susanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobit-control-objectives.html

Wibowo, M. P. (2008, Agustus 9). *Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective For Information And Related Technology): Studi Kasus Di Perpustakaan Universitas Indonesia*. Retrieved November 27, 2012, from http://sangprabu.multiply.com: http://sangprabu.multiply.com/journal/item/27

Wikipedia. *COBIT*. Retrieved November 27, 2012, from http://www.wikipedia.org: http://en.wikipedia.org/wiki/COBIT

TUGAS IT AUDIT

AGUS SUMITRO / 182420126

MTI 20A

SOAL

1. sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.
2. jelaskan dengan adanya contoh kasus yang terkait
3. jangan lupa tambahkan referensi

JAWAB

1. Beberapa jenis resiko sehingga perlu adanya IT atau IS Audit :

   Ancaman TI kondisi perangkat TI, program-program jahat, kegagalan perangkat lunak, virus, spam, phishing dan ancaman terbesar adalah kesalah manusia dalam pengelolaan system TI, pegelolaan data .

   Ancaman TI yang mengarah pada tindakan pelanggaran hukum, misalnya serangan hacker, penipuan menggunakan system TI, pencurian kata kunci (password), serangan pada data, dan lain-lain

   Ancaman TI yang timbul akibat kejadian diluar normal, misalnya terjadinya bencana, baik bencana alam maupun bencana yang dibuat misalnya tindakan teroris.

2. Contoh kasus

   - Hilangnya data akibat ulah pihak yang tidak berwenang mengakses dan mengotak atik data yang ada. Hilangnya hak akses user terhadap suatu sistem , Server down akibat terlalu banyak menerima perintah/permintaan yang mengakibatkan permintaan yang asli tidak terlayani. Pencurian data yang sifatnya penting dari suatu sistem dan diperjual-belikan ke pihak asing sehingga bisa berpotensi merugikan pemilik data.

- Kerusakan software,hardware dan pembatalan eksekusi dan pengolahan data tanpa sepengetahuan pihak yang berwenang(users).

- Berubahnya data yang tersimpan sehingga mengacaukan kerja sistem yang semula berjalan normal. Atau berubahnya password dan username sehingga users yang berhak mengakses sistem tidak dapat mengakses sistem lagi.

- Matinya semua perangkat yang membutuhkan listrik . Ancaman hilangnya daya merupakan ancaman yang berdampak mematikan seluruh perangkat yang hidup menggunakan listrik. Apabila semua mati,maka users tidak dapat melakukan apa-apa karena sistem mati dan server mati .

- ***FRAUD*** (kecurangan) adalah tindakan ilegal yang dilakukan satu orang atau sekelompok orang secara sengaja atau terencana yang menyebabkan orang atau kelompok mendapat keuntungan, dan merugikan orang atau kelompok lain. Contoh ***FRAUDulent financial reporting*** (kecurangan laporan keuangan) adalah salah saji atau pengabaian jumlah dan pengungkapan yang disengaja dengan maksud menipu para pemakai laporan.
  Dalam suatu IT service sebuah aplikasi harus diuji apakah aplikasi tersebut dapat bebas dari Fraud

- Risiko keamanan komputer (computer security risk) adalah setiap peristiwa atau tindakan yang dapat mengakibatkan hilang atau rusaknya piranti keras, piranti lunak, data ataupun informasi. Beberapa penyusup tidak melakukan perusakan, mereka hanya mengakses data, informasi, atau program-program pada komputer. Beberapa penyusup lain menunjukkan beberapa bukti keberadaan mereka dengan meninggalkan pesan atau seenaknya mengubah atau merusak data.
  Setiap tindakan ilegal yang melibatkan komputer dalam kegiatannya secara umum dikenal dengan istilah computer crime. Istilah cybercrime mengacu pada tindakan ilegal berbasis online atau internet.

- Virus. Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia. Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.
- Denial of Service (DoS) dan Distributed DoS (DDos) attack. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian,penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet.

3. Referensi :

- *Penulis: Andrianto Moeljono, MM, CLA ISO 9001, CLA ISO 27001, selaku Director and Senior Consultant Proxsis IT*
  Sumber foto: a2z-support.com

- https://theyouthfulideas.blogspot.com/2012/09/tugas-3-manajemen-resiko-it.html
- https://www.researchgate.net/publication/311972151_Framework_Audit_IT
- https://resources.infosecinstitute.com/itac-planning/
- https://makalahblogandress.blogspot.com/2016/07/resiko-keamanan-komputer.html
- https://techno-inmyworld.blogspot.com/2014/12/apa-itu-vulnerability-kelemahan-risk.html

AGUS WIRANTO

182420102 ➢ MTI2A1 ➢ IT Audit

➢ Beberapa Jenis Resiko Adanya IT atau IS Audit

➢ Risiko Bisnis (*Business Risk*)

Risiko bisnis adalah risiko yang dapat disebabkan oleh faktor-faktor intern maupun ekstern yang berakibat kemungkinan tidak tercapainya tujuan organisasi (*business goal objectives*).

Contoh : dalam melakukan pengadaan sebuah barang IT biasanya pihak internal sering melakukan Kerjasama dengan pihak external dengan mengiming-imingi bisnis dibalik sebuah transaksi. Resikonya apabila melakukan pencarian suatu barang dengan memilih barang yang lebih murah dengan tidak mengetahui suatu manfaat dari apa yang akan di beli, maka akibatnya barang yang akan di beli bisa sia-sia. Lebih baik membeli yang mahal tetapi barang tersebut sangat berguna.

➢ Risiko Bawaan (*Inherent Risk*)

Risiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan jika tidak ada pengendalian internal.

Contoh : Tahapan dalam membangun system itu seharusnya melalui tahapan Analis, UI/UX, Programmer, dan tester. Tetapi kesalahan dalam melewati tahapan ini tering dilakukan misalkan tanpa melakukan Analis dan UI/UX, user langsung membangun sebuah system langsung berkomunikasi dengan Programmer.

➢ Risiko Pengendalian (*Control Risk*)

Dalam suatu organisasi yang baik seharusnya sudah ada *risk assessment*, dan dirancang pengendalian internal secara optimal terhadap setiap potensi risiko. Risiko pengendalian ialah masih adanya risiko meskipun sudah ada pengendalian.

Contoh : dari system keamanan software pada dasarnya setiap perusahaan sudah mempersiapkan pengendalian dari segi Keamanan System, tetapi tetap saja keamanan belum bisa di pastikan aman, karena setiap software pasti ada titik lemahnya.

➢ Risiko Deteksi (*Detection Risk*)

Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya *error* yang cukup matrealitas atau adanya kemungkinan *fraud*.

Contoh : di dalam tugas seorang tester program terdapat beberapa cara untuk memasikan kualitas suatu program, baik dari sedi automation test, loading test, dan penetration test. Dengan demikian pihak audit dapat mendeteksi kualitas suatu program tersebut dengan dokumentasi yang telah di sediakan oleh tester.

➢ Risiko Audit (*Audit Risk*)

Risiko audit sebenarnya adalah kombinasi dari *inherent risk*, *control risk*, dan *detection risk*. Risiko audit adalah risiko bahwa pemeriksaan auditor ternyata belum dapat mencerminkan keadaan yang sesungguhnya.

Contoh : penilaian yang diberikan audit pada keamanan sebuah system itu sangat tinggi, tetapi keamanan dari system tersebut belum bisa dipastikan karena sebuah system pasti masih terdapat celah-celah yang dapat di tembus.

Referensi :

https://www.academia.edu/35574253/05-Resiko_Audit_SI.ppt?auto=download

Nama : Arie Ansyah
NIM : 182420117
Mata Kuliah : IT AUDIT

Identifikasi Resiko

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya "scope creep" (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat

melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contohnya :

Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (IT Governance) (Herawan, 2012).

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (Control Objectives for Information and Related Technology) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (Information System and Control Association) dan ITGI (IT Governance Institute) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.(Wibowo, 2008).

DAFTAR PUSTAKA

Fanani, M. F. (2012, September 24). Implementasi COBIT Di PT PERTAMINA. Retrieved November 27, 2012, from http://www.slideshare.net: http://www.slideshare.net/fananifaiz/cobit-pertamina#btnNext

Herawan, R. (2012, April 4). Implementasi COBIT pada PT Transindo. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/

Meidyanto, Riky (2009, Juni 19). Audit Sistem Informasi dengan Menggunakan COBIT (Control Objectives For Information And Related Technology). Retrieved November 27, 2012, from http://krikkrikx.blog.binusian.org: http://www.krikkrikx.blog.binusian.org/files/2009/06/untuk-blog221.doc

Susanto, Erdi (2012, November). Kerangka Kerja COBIT (Control Objectives For Information And Related Technology). Retrieved November 28, 2012, from http://erdi-susanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobit-control-objectives.html

Wibowo, M. P. (2008, Agustus 9). Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective For Information And Related Technology): Studi Kasus Di Perpustakaan Universitas Indonesia. Retrieved November 27, 2012, from http://sangprabu.multiply.com: http://sangprabu.multiply.com/journal/item/27

Wikipedia. COBIT. Retrieved November 27, 2012, from http://www.wikipedia.org: http://en.wikipedia.org/wiki/COBIT

Nama : Armansyah
Nim : 182420105
Kelas : MTI.20.A

Materialitas dan Resiko Audit

Materialitas menurut Alrins A Arens dkk, adalah sebagai suatu pertimbangan penting dalam menentukan jenis laporan yang tepat untuk diterbitkan dalam situasi tertentu. Sedangkan menurut FASB 2, materialitas didefinisikan sebagai "besarnya penghapusan atau salah saji informasi keuangan yang dengan memperhitungkan situasinya, menyebabkan pertimbangan seseorang yang bijaksana yang mengandalkan informasi tersebut mungkin atau berubah atau terpengaruh oleh penghapusan atau salah saji tersebut.

1. Faktor – Faktor yang Mempengaruhi Pertimbangan
2. Menetapkan Pertimbangan Pendahuluan Materialitas

Pertimbangan pendahuluan tentang materialitas menurut SAS 107 (AU 312) mengharuskan auditor memutuskan jumlah salah saji gabungan dalam laporan keuangan, yang akan mereka anggap material pada awal audit ketika sedang mengembangkan strategi audit secara keseluruhan. Meskipun merupakan pendapat profesional, hal diatas mungkin dapat berubah selama penugasan. Pertimbangan ini harus didokumentasikan.

Pertimbangan tentang materilitas yang direvisi, adalah perubahan pertimbangan pendahuluan tentang materilaitas yang dialakukan auditor selama melaksanakan audit. Auditor melakukan revisi karena adanya perubahan dalam salah satu faktor yang digunakan untuk mempertimbangkan pendahuluan, karena auditor memutuskan bahwa pertimbangan pendahuluan terlalu besar atau terlalu kecil.

Beberapa faktor akan mempengaruhi pertimbangan pendahuluan auditor tentang materialitas untuk seperangkat laporan keuangan tertentu. Faktor – faktor itu antara lain:

- Materialitas adalah konsep yang bersifat relatif ketimbang absolut.

  Salah saji dalam jumlah tertentu mungkin saja material bagi perusahaan kecil, tetapi dapat saja tidak material bagi perusahaan besar.

- Dasar yang diperlukan untuk mengevaluasi materialitas.

  Karena materialitas bersifat relatif, diperlukan dasar untuk menentukan apakah salah saji itu material.

- Faktor – faktor kualitatif.

  Jenis salah saji tertentu mungkin lebih penting bagi para pemakai dibandingkan salah saji lainnya, sekalipun nilai dolarnya sama.

1. Mengalokasikan Pertimbangan Pendahuluan tentang Materialitas ke Segmen – Segmen (Salah Saji yang Dapat Ditolerinsi)

   Alokasi pertimbangan pendahuluan tentang materialitas ke segmen-segmen perlu dilakukan karena auditor mengumpulkan bukti per segmen dan bukan untuk laporan keuangan secara keseluruhan. Jika auditor memiliki pertimbangan, maka akan membantu auditor dalam memutuskan bukti audit yang tepat yang harus dikumpulkan.

   Salah saji yang dapat ditoleransi menurut SAS 107 (AU 312) terjadi ketika auditor mengalokasikan pertimbangan pendahuluan tentang materialitas ke saldo akun, materialitas yang dialokasikan ke saldo akun tertentu.

1. Etimasi Salah Saji dan Perbandingan dengan Pertimbangan Pendahuluan

- Salah saji yang diketahui, adalah salah saji dalam akun yang jumlahnya dapat ditentukan oleh auditor.
- Salah saji yang mungkin, terbagi menjadi dua macam. Pertama adalah salah saji yang berasal dari perbedaan antara pertimbangan manajemen dan auditor tentang estimasi saldo akun. Kedua adalah proyeksi salah saji berdasarkan pengujian auditor atas sampel dari suatu populasi.
- Perhitungan langsung estimasi salah saji, dapat dihitung dengan cara salah saji dalam sampel dibagi dengan total sampel dan dikalikan dengan total populasi yang tercatat.
- Estimasi kesalahan sampling, timbul karena auditor hanya mengambil sampel dari sebagian populasi dan ada resiko bahwa sampel itu tidak secara akurat mewakili populasi.

1. Resiko

   Resiko adalah ketidakpastian dalam melaksanakan fungsi audit. Auditor menangani resiko dalam merencankan pengumpulan bukti audit terutama dengan menerapkan model resiko audit. Model ini bersumber pada SAS 110 (AU 350) tentang sampling audit serta dalam SAS 107 (AU 312) tentang materialitas dan resiko. Model resiko audit membantu auditor memutuskan seberapa banyak dan jenis bukti apa yang harus dikumpulkan dalam setiap siklusnya. Model ini dinyatakan sebagai:

   $$PDR = \frac{AAR}{IR \times CR}$$

   diamana:

   PDR : resiko deteksi yang direncanakan (planned dtetection risk)

   ASR : resiko audit yang dapat diterima (acceptable audit risk)

   IR : resiko inheren (inherent risk)

   CR : resiko pengendalian (control risk)

1. Jenis – Jenis Resiko
2. Resiko deteksi yang direncanakan : adalah resiko bahwa bukti audit untuk suatu segmen akan gagal mendeteksi salah saji yang melebihi salah saji yang ditoleransi.
3. Resiko inheren : mengukur penilaian auditor atas kemungkinan adanya salah saji (kekeliruan atau kecurangan) yang material dalam segmen, sebelum memperhitungkan keefektifan pengendalian internal.
4. Resiko pengendalian : mengukur penilaian auditor mengenai apakah salah saji yang melebihi jumlah yang ditoleransi dalam sutau segmen akan dicegah atau terdeteksi secara tepat waktu oleh pengendalian internal klien.
5. Resiko audit yang diterima : adalah ukuran kesediaan auditor untuk menerima bahwa laporan keuangan mungkin mengandung salah saji yang material setelah audit selesai, dan pendapat wajar tanpa pengecualian telah dikeluarkan.
6. Menilai Resiko Audit yang Dapat Diterima
7. Resiko penugasan : adalah resiko bahwa auditor atau kantor atau kantor akuntan publik akan menderita kerugian setelah audit selesai, walaupun laporan audit sudah benar.
8. Derajat ketergantungan pemakai eksternal pada laporan keuangan, ada beberapa faktor sebagai indikator derajat ketergantungan, antara lain ukuran klien, distribusi kepemilikan, sifat dan jumlah kewajiban.
9. Kemungkinan bahwa klien akan mengalami kesulitan keuangan setelah laporan audit dikeluarkan, jika klien terpaksa mengajukan permohonan kebangkrutan atau menderita kerugian ang besar setelah audit selesai, auditor menghadapi kemungkianan yang lebih besar untuk membela mutu audit ketimbang jika klien tidak mengalami teknanan keuangan.
10. Evaluasi auditor atas integritas manajemen, jika klien memiliki integritas yang meragukan, auditor mungkin akan menilai resiko audit yang dapat diterima yang lebih rendah.
11. Menilai resiko inheren. Auditor harus mempertimbangkan beberapa faktor utama ketika menilai resiko inheren. Resiko inheren terdiri dari:
12. Sifat bisnis klien
13. Hasil audit sebelumnya
14. Penugasan awal versus penugasan berulang
15. Pihak – pihak yang terkait
16. Transaksi nonrutin
17. Pertimbangan yang diperlukan untuk mencatat saldo akun dan transaksi dengan tepat
18. Unsur – unsur populasi.
19. Faktor-faktor yang berkaitan dengan pelaporan keungan yang curang
20. Faktor – faktor yang berkaitan dengan misaproposiasi aktiva

Faktor – faktor yang mempengaruhi resiko:

- Ketergantungan pemakai eksternal
- Kemungkinan kegagalan keuangan
- Integritas manajemen
- Sifat bisnis
- Hasil audit sebelumnya
- Penugasan awal versus penugasan berulang
- Pihak-pihak yang terkait
- Transaksi non rutin
- Pertimbangan yang diperlukan
- Unsur-unsur populasi
- Faktor-faktor yang berkaitan dengan salah saji yang timbul akibat pelaporan keuangan yang curang

- Ketentuan aktiva terhadap misaproporsi
- Evektivitas pengendalian internal
- Rencana pengandalan

1. Evaluasi Hasil

   Setelah auditor merencanakan penugasan dan mengumpulkan bukti audit, hasil-hasilnya dapat juga dinyatakan dalam versi evaluasi model resiko audit. Model resiko audit dalam untuk mengevaluasi hasil-hasil audit dinyatakan dalam SAS 107 sebagai

   AcRC = IR x CR x AcDR

   dimana:

   AcAR (Achived Audit Risk) = resiko audit yang dicapai

   IR (Inheren Risk) = resiko inheren

   CR (Control Risk) = resiko pengendalian

   AcDR (Achived detecion risk) = resiko deteksi yang dicapai

   Rumus tersebut menunjukkan tiga cara untuk mengurangi resiko audit yang dicapai ke tingkat yang dapat diterima:

- Mengurangi resiko inheren. Karena resiko inheren dinilai oleh auditor berdasarkan keadaan klien, penilain dilakukan selama tahap perencanaan dan biasanya tidak diubah kecuali terungkap fakta-fakta baru selama berlangsungnya audit.
- Mengurangi resiko pengendalian. Penilain resiko pengendalian dipengaruhi oleh pengendalian internal klien serta pengujian yang dilakukan auditor terhadap pengendalian tersebut.
- Mengurangi resiko deteksi yang dicapai dengan meningkatkan pengujian audit substantif. Auditor mengurangi resiko deteksi yang dicapai dengan mengumpulkan bukti dengan menggunakan prosedur analitis, pengujian substantif atas transaksi, dan pengujian atas rincian saldo.

Contoh Kasus Audit Sistem Informasi

Caesario Rian Saputra (182420131)

Rumah Sakit Umum Daerah (RSUD) Kota Tasikmalaya termasuk pada klasifikasi Rumah Sakit Umum Kelas B Non Pendidikan. SIMRS pada RSUD Kota Tasikmalaya sudah didukung oleh Teknologi Informasi (TI) berupa infrastruktur (perangkat komputer, server dan jaringan), sistem aplikasi beserta basis data. Sistem aplikasi yang sudah digunakan terbatas pada lingkup sistem untuk pelayanan kesehatan terhadap pasien, terutama sistem administrasi pembayaran. Dari hasil studi pendahuluan ditemukan bahwa sistem aplikasi untuk pelayanan kesehatan terhadap pasien di RSUD Kota Tasikmalaya masih terkendala oleh lambatnya proses Sistem Informasi (SI) yang menyebabkan pasien harus menunggu lama dalam memperoleh layanan. Lamanya proses SI sering menyebabkan pasien harus antri cukup lama dalam memperoleh layanan. Layanan data dari SI juga sering dikeluhkan pasien karena ketidaksesuain dengan tagihan yang dikenakan kepada pasien saat membayar di kasir. Penyebab terjadinya kesalahan dan keterlambatan pemrosesan yang ada pada SI tersebut belum diketahui dengan pasti.

Guna membuat rekomendasi pengembangan SI dibutuhkan pengetahuan mengenai tingkat kematangan SIMRS saat ini di RSUD Kota Tasikmalaya. Berdasarkan latar belakang tersebut maka dapat disimpulkan bahwa RSUD Kota Tasikmalaya dituntut untuk melakukan audit SIMRS, terutama pada lingkup sistem pelayanan kesehatan terhadap pasien. Atas dasar itu, solusi yang ditawarkan adalah audit sistem informasi menggunakan framework COBIT 4.1. Alasan dipilihnya framework COBIT 4.1, karena memberikan gambaran paling detil mengenai strategi dan kontrol dalam pengaturan proses teknologi informasi yang mendukung keselarasan strategi bisnis dan tujuan teknologi informasi.
Bagi auditor, manfaat COBIT 4.1 adalah membantu dalam mengidentifikasi isu-isu kendali TI dalam infrastruktur TI perusahaan. Hal ini juga membantu auditor dalam memverifikasi temuan audit.

Penentuan ruang lingkup audit dilakukan dengan cara mengidentifikasi tujuan strategi RSUD Kota Tasikmalaya melalui implementasi Balanced Scorecard.

Setelah mengetahui tingkat kematangan dari proses TI COBIT 4.1 yang menjadi cakupan audit, selanjutnya dilakukan analisis kondisi yang terjadi dari masing-masing atribut kematangan. Analisis kondisi dilakukan dengan cara wawancara dan observasi langsung, dimana peneliti mengadakan pengamatan langsung ke lapangan untuk memperoleh data atau informasi yang akurat mengenai kondisi SIMRS yang diimplementasikan RSUD Kota Tasikmalaya.

Sebagai tindak lanjut dari pendefinisian usulan rekomendasi perbaikan, perlu dilakukan pedoman pengawasan dalam bentuk indikator pengukuran. Hal ini diperlukan untuk mengetahui sejauh mana proses peningkatan kematangan sudah dilakukan. Adanya penelitian lain mengenai audit SIMRS menggunakan metode Balanced Scorecard(BSC) dengan perspektif lainnya (keuangan, proses bisnis, pembelajaran dan pertumbuhan) sehingga cakupan audit (proses TI terpilih COBIT 4.1) menjadi lebih luas.

KASUS AUDIT
PT GARUDA INDONESIA

Untuk Memenuhi Salah Satu Tugas Mata Kuliah Auditing 1
Dosen : Rianto, SE, MM, M. Ak

Disusun oleh:

Tutut Setyowati NIM 2320160130

FAKULTAS EKONOMI JURUSAN AKUNTANSI
UNIVERSITAS ISLAM AS-SYAFIIYAH

2019

KATA PENGANTAR

Puji Syukur saya ucapkan kepada Allah Yang Maha Esa, karena atas berkat rahmat dan karunia-Nya, makalah ini dapat terselesaikan dengan baik. Yang berjudul ”KASUS AUDIT PT GARUDA INDONESIA”

Makalah ini untuk memenuhi salah satu tugas Pemeriksaan Akuntansi 1 serta saya harapkan makalah ini dapat bermanfaat untuk menambah informasi mengenai dunia auditing atau pemeriksaan akuntansi.

Saya menyadari bahwa dalam penyusunan makalah ini masih jauh dari kesempurnaan, untuk itu saya sangat mengharapkan kritik dan saran yang bersifat membangun guna sempurnanya makalah ini.

Bekasi, 11 Juli 2019

Tutut Setyowati

DAFTAR ISI

BAB I

PENDAHULUAN

1. Latar Belakang

Dalam menyajikan laporan keuangan manajemen berpotensi dipengaruhi kepentingan pribadi, sementara pihak prinsipal yaitu pemilik modal (investor) sebagai pemakai laporan keuangan sangat berkepentingan untuk mendapatkan laporan keuangan yang akurat, dapat dipercaya dan pertanggungjawaban atas dana yang mereka investasikan. Banyaknya pihak yang berkepentingan atas laporan tersebut, maka diperlukan adanya pihak ketiga yaitu akuntan publik. Akuntan publik adalah pihak independen yang dianggap mampu menjembatani benturan antara kepentingan antara pihak prinsipal (investor) dengan pihak agen (manajemen), yaitu sebagai pengelola perusahaan. Dalam hal ini peran akuntan publik adalah memberi opini terhadap kewajaran 2 laporan keuangan yang dibuat manajemen. Dalam melaksanakan tugasnya auditor harus mampu menghasilkan opini audit yang berkualitas yang akan berguna tidak saja bagi dunia bisnis, tetapi juga masyarakat luas (Wibowo dan Hilda, 2009 dalam Wijayani dan Januari, 2011).

Garuda Indonesia sebagai Perusahaan Go Public melaporkan kinerja keuangan tahun buku 2018 kepada Bursa Efek Indonesia. Kinerja keuangan PT Garuda Indonesia (Persero) yang berhasil membukukan laba bersih US$809 ribu pada 2018, berbanding terbalik dari 2017 yang merugi US$216,58 juta. Kinerja ini terbilang cukup mengejutkan lantaran pada kuartal III 2018 perusahaan masih merugi sebesar US$114,08 juta. Sehingga timbulnya polemik antara pihak pihak yang bersangkutan dengan Laporan keuangan Tahunan PT Garuda Indonesia yang akan dibahas pada makalah ini.

2. Rumusan Masalah

1. Bagaimanakah kronologi skandal keuangan PT Garuda Indonesia
2. Apa Pelanggaran yang dilakukan PT Garuda Indonesia
3. Bagaimanakah sanksi yang diberikan kepada PT Garuda Indonesia

3. Dasar Hukum

1. Pasal 69 Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal (UU PM)
2. Peraturan Bapepam dan LK Nomor VIII.G.7 tentang Penyajian dan Pengungkapan Laporan Keuangan Emiten dan Perusahaan Publik
3. Interpretasi Standar Akuntansi Keuangan (ISAK) 8 tentang Penentuan Apakah Suatu Perjanjian Mengandung Sewa
4. Pernyataan Standar Akuntansi Keuangan (PSAK) 30 tentang Sewa

BAB II

PEMBAHASAN

2.1 Kronologi Polemik Laporan Keuangan Garuda Indonesia

- 1 April 2019
  Sebagai perusahaan publik, Garuda Indonesia melaporkan kinerja keuangan tahun buku 2018 kepada Bursa Efek Indonesia.Kinerja keuangan PT Garuda Indonesia (Persero) yang berhasil membukukan laba bersih US$809 ribu pada 2018, berbanding terbalik dari 2017 yang merugi US$216,58 juta. Kinerja ini terbilang cukup mengejutkan lantaran pada kuartal III 2018 perusahaan masih merugi sebesar US$114,08 juta.

- 24 April 2019
  Perseroan mengadakan Rapat Umum Pemegang Saham Tahunan (RUPST) di Jakarta. Salah satu mata agenda rapat adalah menyetujui laporan keuangan tahun buku 2018.

  Dalam rapat itu, dua komisaris Garuda Indonesia, Chairul Tanjung dan Dony Oskaria selaku perwakilan dari PT Trans Airways menyampaikan keberatan mereka melalui surat keberatan dalam RUPST. Chairal sempat meminta agar keberatan itu dibacakan dalam RUPST, tapi atas keputusan pimpinan rapat permintaan itu tak dikabulkan. Hasil rapat pemegang saham pun akhirnya menyetujui laporan keuangan Garuda Indonesia tahun 2018.

  Trans Airways berpendapat angka transaksi dengan Mahata sebesar US$239,94 juta terlalu signifikan, sehingga mempengaruhi neraca keuangan Garuda Indonesia. Jika nominal dari kerja sama tersebut tidak dicantumkan sebagai pendapatan, maka perusahaan sebenarnya masih merugi US$244,96 juta.

  Catatan tersebut membuat beban yang ditanggung Garuda Indonesia menjadi lebih besar untuk membayar Pajak Penghasilan (PPh) dan Pajak Pertambahan Nilai (PPN). Padahal, beban itu seharusnya belum menjadi kewajiban karena pembayaran dari kerja sama dengan Mahata belum masuk ke kantong perusahaan.

- 25 April 2019
  Pasar merespons kisruh laporan keuangan Garuda Indonesia. Sehari usai kabar penolakan laporan keuangan oleh dua komisaris beredar, saham perusahaan dengan kode GIAA itu merosot tajam 4,4 persen pada penutupan perdagangan sesi pertama, Kamis (25/4).
  Bursa Efek Indonesia (BEI) menyatakan akan memanggil manajemen Garuda Indonesia terkait timbulnya perbedaan opini antara pihak komisaris dengan manajemen terhadap laporan keuangan tahun buku 2018.
  Selain manajemen perseroan, otoritas bursa juga akan memanggil kantor akuntan publik (KAP) Tanubrata Sutanto Fahmi Bambang dan Rekan selaku auditor laporan keuangan perusahaan. Pemanggilan itu dijadwalkan pada Selasa (30/4).

- 26 April 2019
  Komisi VI Dewan Perwakilan Rakyat (DPR) menyatakan bakal memanggil

manajemen perseroan. Sebelum memanggil pihak manajemen, DPR akan membahas kasus tersebut dalam rapat internal. Wakil Ketua Komisi VI DPR RI Inas Nasrullah Zubir mengatakan perseturuan antara komisaris Garuda Indonesia dengan manajemen akan dibahas dalam rapat internal usai reses. Dalam rapat itu akan dipastikan terkait pemanggilan sejumlah pihak yang berkaitan dengan pembuatan laporan keuangan maskapai pelat merah tersebut. Jika sesuai jadwal, DPR kembali bekerja pada 6 Mei 2019.

Selain itu pada hari yang sama, beredar surat dari Sekretariat Bersama Serikat Karyawan Garuda Indonesia (Sekarga) perihal rencana aksi mogok karyawan Garuda Indonesia. Aksi ini berkaitan dengan penolakan laporan keuangan tahun 2018 oleh dua komisaris

Dalam surat tersebut disebutkan pernyataan pemegang saham telah merusak kepercayaan publik terhadap harga saham Garuda Indonesia dan pelanggan setia maskapai tersebut.

Namun, Asosiasi Pilot Garuda (APG) dan Sekarang justru membantah akan melakukan aksi mogok kerja. Presiden APG Bintang Hardiono menegaskan karyawan belum mengambil sikap atas perseteruan salah satu pemegang saham dengan manajemen saat ini.

- 30 April 2019
  BEI telah bertemu dengan manajemen Garuda Indonesia dan kantor akuntan publik (KAP) Tanubrata Sutanto Fahmi Bambang dan Rekan selaku auditor laporan keuangan perusahaan. Pertemuan berlangsung pada pukul 08.30-09.30 WIB. Sayangnya, pertemuan dua belah pihak berlangsung tertutup. Otoritas bursa menyatakan akan mengirimkan penjelasan usai pertemuan tersebut. "Bursa meminta semua pihak untuk mengacu pada tanggapan perseroan yang disampaikan melalui IDXnet dan penjelasan dapat dibaca di website bursa," kata Direktur Penilaian Perusahaan BEI I Gede Nyoman Yetna.
  Sementara Menteri Keuangan mengaku telah meminta Sekretaris Jenderal Kementerian Keuangan Hadiyanto untuk mempelajari kisruh terkait laporan keuangan BUMN tersebut.

2.2 Pelanggaran yang dilakukan PT Garuda Indonesia

Otoritas Jasa Keuangan (OJK) telah memutuskan bahwa PT Garuda Indonesia (Persero) Tbk melakukan kesalahan terkait kasus penyajian Laporan Keuangan Tahunan per 31 Desember 2018.Pihak OJK yang diwakili oleh Deputi Komisioner Hubungan Masyarakat dan Manajemen Strategis, Anto Prabowo, mengungkapkan bahwa Garuda Indonesia telah terbukti melanggar

1. Pasal 69 Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal (UU PM)

“(1) Laporan keuangan yang disampaikan kepada Bapepam wajib disusun berdasarkan prinsip akuntansi yang berlaku umum. (2) Tanpa mengurangi

ketentuan sebagaimana dimaksud dalam ayat (1), Bapepam dapat menentukan ketentuan akuntansi di bidang Pasar Modal."

2. Peraturan Bapepam dan LK Nomor VIII.G.7 tentang Penyajian dan Pengungkapan Laporan Keuangan Emiten dan Perusahaan Publik.

3. Interpretasi Standar Akuntansi Keuangan (ISAK) 8 tentang Penentuan Apakah Suatu Perjanjian Mengandung Sewa.

4. Pernyataan Standar Akuntansi Keuangan (PSAK) 30 tentang Sewa.

2.3 Sanksi Untuk PT Garuda Indonesia

Deputi Komisioner Pengawas Pasar Modal II, Fakhri Hilmi, mengatakan setelah berkoordinasi dengan Kementerian Keuangan Republik Indonesia ,Pusat Pembinaan Profesi Keuangan, PT Bursa Efek Indonesia, dan pihak terkait lainnya, OJK memutuskan memberikan sejumlah sanksi.

1. Memberikan Perintah Tertulis kepada PT Garuda Indonesia (Persero) Tbk untuk memperbaiki dan menyajikan kembali LKT PT Garuda Indonesia (Persero) Tbk per 31 Desember 2018 serta melakukan paparan publik (public expose) atas perbaikan dan penyajian kembali LKT per 31 Desember 2018 dimaksud paling lambat 14 hari setelah ditetapkannya surat sanksi, atas pelanggaran Pasal 69 Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal (UU PM) ,Peraturan Bapepam dan LK Nomor VIII.G.7 tentang Penyajian dan Pengungkapan Laporan Keuangan Emiten dan Perusahaan Publik, Interpretasi Standar Akuntansi Keuangan (ISAK) 8 tentang Penentuan Apakah Suatu Perjanjian Mengandung Sewa, dan Pernyataan Standar Akuntansi Keuangan (PSAK) 30 tentang Sewa.

2. Selain itu juga Perintah Tertulis kepada KAP Tanubrata, Sutanto, Fahmi, Bambang & Rekan (Member of BDO International Limited) untuk melakukan perbaikan kebijakan dan prosedur pengendalian mutu atas pelanggaran Peraturan OJK Nomor 13/POJK.03/2017 jo. SPAP Standar Pengendalian Mutu (SPM 1) paling lambat 3 (tiga) bulan setelah ditetapkannya surat perintah dari OJK.

3. Deputi Komisioner Hubungan Masyarakat dan Manajemen Strategis, Anto Prabowo mengatakan, OJK juga mengenakan Sanksi Administratif berupa denda sebesar Rp 100 juta kepada PT Garuda Indonesia (Persero) Tbk atas pelanggaran Peraturan OJK Nomor 29/POJK.04/2016 tentang Laporan Tahunan Emiten atau Perusahaan Publik.

4. Sanksi denda kepada masing-masing anggota Direksi PT Garuda Indonesia (Persero) Tbk sebesar Rp 100 juta atas pelanggaran Peraturan Bapepam Nomor VIII.G.11 tentang Tanggung Jawab Direksi atas Laporan Keuangan.

5. Bursa Efek Indonesia (BEI) resmi menjatuhkan sanksi kepada PT Garuda Indonesia Tbk (GIAA) atas kasus klaim laporan keuangan perseroan yang menuai polemik. Beberapa sanksi yang dijatuhkan antara lain denda senilai Rp 250 juta dan restatement atau perbaikan laporan keuangan perusahaan dengan paling lambat 26 Juli 2019 ini.

2.4 Pembekuan saham

Direktur Penilaian PT Bursa Efek Indonesia (BEI) I Nyoman Gede Yetna menuturkan, manajemen BEI hingga kini belum sampai pada keputusan untuk membekukan (suspensi) saham PT Garuda Indonesia Tbk (GIAA) meski laporan keuangan perusahaan menuai polemik.

"Kami dari Bursa berpendapat belum perlu melakukan suspensi perdagangan saham Perseroan pada saat ini," ujarnya di **Jakarta**, Jumat (28/6).

Nyoman pun melanjutkan, BEI ke depannya akan terus melihat pergerakan saham Garuda Indonesia untuk mempertimbangkan tindakan selanjutnya. "Selanjutnya, Bursa akan senantiasa memantau pergerakan harga saham dan keterbukaan informasi Perseroan serta melakukan tindak lanjut sesuai ketentuan yang berlaku," papar dia. **[azz]**

BAB III

PENUTUP

3.1 KESIMPULAN DAN SARAN

Kinerja keuangan PT Garuda Indonesia (Persero) menuai polemik karena adanya pencatatan transaksi kerja sama penyediaan layanan konektivitas (wifi) dalam penerbangan dengan PT Mahata Aero Teknologi (Mahata) dalam pos pendapatan yang seharusnya masih menjadi piutang.

Dalam kasus ini PT Garuda Indonesia telah melanggar Pasal 69 Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal (UU PM) ,Peraturan Bapepam dan LK Nomor VIII.G.7 tentang Penyajian dan Pengungkapan Laporan Keuangan Emiten dan Perusahaan Publik, Interpretasi Standar Akuntansi Keuangan (ISAK) 8 tentang Penentuan Apakah Suatu Perjanjian Mengandung Sewa, dan Pernyataan Standar Akuntansi Keuangan (PSAK) 30 tentang Sewa. Dan diberi sanksi sesuai dengan UU yang dilanggar.

Seharusnya untuk menghindari kerancuan, GIAA sebagai perusahaan tercatat di pasar modal seharusnya menjelaskan ke publik nature transaksi yang terjadi serta poin poinnya sudah eksis atau belum. Sehingga tidak menimbulkan pertanyaan bagi publik bahwa perusahaan di kuartal III-2018 yang masih merugi tiba-tiba mengantongi laba di tiga bulan terakhir apalagi sudah disahkan dalam RUPS.

DAFTAR PUSTAKA

https://www.merdeka.com/uang/fakta-fakta-kesalahan-laporan-keuangan-garuda-indonesia-hingga-dikenakan-sanksi/

https://www.cnnindonesia.com/ekonomi/20190430174733-92-390927/kronologi-kisruh-laporan-keuangan-garuda-indonesia

https://akuntansibisnis.files.wordpress.com/2012/11/viii-g-7.pdf

Nama : Dhea Noranita Putri
NIM : 182420112 (MTI REG B 2019)
Tugas : IT Audit
Tanggal : 8 April 2020

SOAL :

sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.

jelaskan dengan adanya contoh kasus yang terkait

jangan lupa tambahkan referensi

Jawab :

Audit Sistem Informasi menurut Ron Weber (1999, p.10) adalah proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah menetapkan dan menerapkan sistem pengendalian intern yang memadai. Semua aktiva dilindungi dengan baik atau tidak disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi berbasis komputer.

Jenis resiko yang menjadi faktor utama sehingga perlu adanya IS/IT Audit :

Menurut (Weber, 2006), Faktor-faktor yang mendorong pentingnya kontrol dan audit sistem informasi adalah :

- Mendeteksi agar komputer tidak dikelola secara kurang terarah.
- Mendeteksi resiko kehilangan data.
- Mendeteksi resiko pengambilan keputusan yang salah akibat informasi hasil proses sistem komputerisasi salah/lambat/tidak lengkap.
- Menjaga aset perusahaan karena nilai hardware, software dan personil yang lazimnya tinggi.
- Mendeteksi resiko error komputer.
- Mendeteksi resiko penyalahgunaan komputer (fraud).
- Menjaga kerahasiaan
- Meningkatkan pengendalian evolusi penggunaan computer

Tujuan ada nya IS audit adalah :

- Availability ketersediaan informasi, apakah informasi pada perusahaan dapat menjamin ketersediaan informasi dapat dengan mudah tersedia setiap saat.
- Confidentiality / kerahasiaan informasi, apakah informasi yang dihasilkan oleh sistem informasi perusahaan hanya dapat diakses oleh pihak-pihak yang berhak dan memiliki otorisasi.
- Integrity, apakah informasi yang tersedia akurat, handal, dan tepat waktu.

Audit sistem informasi dapat digolongkan dalam tipe atau jenis-jenis audit sebagai berikut :

1. Audit Laporan Keuangan (Financial Statement Audit) dalah audit yang dilakukan untuk mengetahui tingkat kewajaran laporan keuangan yang disajikan oleh perusahaan (apakah sesuai dengan standar akuntansi keuangan serta tidak menyalahi uji materialitas)
2. Audit Operasional (Operational Audit) adalah audit terhadap aplikasi komputer terbagi menjadi tiga jenis, antara lain: Post implementation Audit(Audit setelah implementasi), Concurrent audit(audit secara bersama), dan Concurrent Audits(audit secara bersama-sama).

Contoh kasus yang akan saya berikan adalah Audit Laporan Keuangan :

Berdasarkan sumber berita dari laman tirto.id tanggal 29 Juni 2019 oleh Hendra Friana dan makalah dari academia.edu yang ditulis oleh Tutut S pada 11 Juli 2019, yang keduanya membahas tentang Kasus Audit PT Garuda Indonesia. Kesalahan Audit PT Garuda Indonesia(Persero) menuai polemik karena adanya pencatatan transaksi kerja sama penyediaan layanan konektivitas (wifi) dalam penerbangan dengan PT Mahata Aero Teknologi (Mahata) sebesar Rp. 2.9 Triliun dalam pos pendapatan yang seharusnya masih menjadi piutang. Berikut kronologi polemik laporan keuangan PT Garuda Indonesia :

Nama : Dhea Noranita Putri
NIM : 182420112 (MTI REG B 2019)

Tugas : IT Audit
Tanggal : 8 April 2020

1. 1 April 2019

   Sebagai perusahaan publik, Garuda Indonesia melaporkan kinerja keuangan tahun buku 2018 kepada Bursa Efek Indonesia.Kinerja keuangan PT Garuda Indonesia(Persero) yang berhasil membukukan laba bersihUS$809 ribu pada 2018,berbanding terbalik dari 2017 yang merugi US$216,58 juta. Kinerja ini terbilangcukup mengejutkan lantaran pada kuartal III 2018 perusahaan masih merugisebesar US$114,08 juta.

2. 24 April 2019

   Perseroan mengadakan Rapat Umum Pemegang Saham Tahunan (RUPST) diJakarta. Salah satu mata agenda rapat adalah menyetujui laporan keuangan tahunbuku 2018.Dalam rapat itu, dua komisaris Garuda Indonesia, Chairul Tanjung dan DonyOskaria selaku perwakilan dari PT Trans Airways menyampaikan keberatan merekamelalui surat keberatan dalam RUPST. Chairal sempat meminta agar keberatan itudibacakan dalam RUPST, tapi atas keputusan pimpinan rapat permintaan itu takdikabulkan. Hasil rapat pemegang saham pun akhirnya menyetujui laporankeuangan Garuda Indonesia tahun 2018.Trans Airways berpendapat angka transaksi dengan Mahata sebesar US$239,94 juta terlalu signifikan, sehingga mempengaruhi neraca keuangan Garuda Indonesia.Jika nominal dari kerja sama tersebut tidak dicantumkan sebagai pendapatan, makaperusahaan sebenarnya masih merugi US$244,96 juta.Catatan tersebut membuat beban yang ditanggung Garuda Indonesia menjadi lebihbesar untuk membayar Pajak Penghasilan (PPh) dan Pajak Pertambahan Nilai(PPN). Padahal, beban itu seharusnya belum menjadi kewajiban karenapembayaran dari kerja sama dengan Mahata belum masuk ke kantong perusahaan.

3. 25 April 2019

   Pasar merespons kisruh laporan keuangan Garuda Indonesia. Sehari usai kabarpenolakan laporan keuangan oleh dua komisaris beredar, saham perusahaandengan kode GIAA itu merosot tajam 4,4 persen pada penutupan perdagangan sesipertama, Kamis (25/4).Bursa Efek Indonesia (BEI) menyatakan akan memanggil manajemen GarudaIndonesia terkait timbulnya perbedaan opini antara pihak komisaris denganmanajemen terhadap laporan keuangan tahun buku 2018.Selain manajemen perseroan, otoritas bursa juga akan memanggil kantor akuntanpublik (KAP) Tanubrata Sutanto Fahmi Bambang dan Rekan selaku auditor laporankeuangan perusahaan. Pemanggilan itu dijadwalkan pada Selasa (30/4).

4. 26 April 2019

   Komisi VI Dewan Perwakilan Rakyat (DPR) menyatakan bakal memanggil manajemen perseroan. Sebelum memanggil pihak manajemen, DPR akanmembahas kasus tersebut dalam rapat internal. Wakil Ketua Komisi VI DPR RIInas Nasrullah Zubir mengatakan perseturuan antara komisaris Garuda Indonesiadengan manajemen akan dibahas dalam rapat internal usai reses. Dalam rapat ituakan dipastikan terkait pemanggilan sejumlah pihak yang berkaitan denganpembuatan laporan keuangan maskapai pelat merah tersebut. Jika sesuai jadwal,DPR kembali bekerja pada 6 Mei 2019.Selain itu pada hari yang sama, beredar surat dari Sekretariat Bersama SerikatKaryawan Garuda Indonesia (Sekarga) perihal rencana aksi mogok karyawanGaruda Indonesia. Aksi ini berkaitan dengan penolakan laporan keuangan tahun2018 oleh dua komisarisDalam surat tersebut disebutkan pernyataan pemegang saham telah merusakkepercayaan publik terhadap harga saham Garuda Indonesia dan pelanggan setiamaskapai tersebut.Namun, Asosiasi Pilot Garuda (APG) dan Sekarang justru membantah akanmelakukan aksi mogok kerja. Presiden APG Bintang Hardiono menegaskankaryawan belum mengambil sikap atas perseteruan salah satu pemegang sahamdengan manajemen saat ini.

5. 30 April 2019

   BEI telah bertemu dengan manajemen Garuda Indonesia dan kantor akuntan publik(KAP) Tanubrata Sutanto Fahmi Bambang dan Rekan selaku auditor laporankeuangan perusahaan. Pertemuan berlangsung pada pukul 08.30-09.30 WIB.Sayangnya, pertemuan dua belah pihak berlangsung tertutup. Otoritas

bursamenyatakan akan mengirimkan penjelasan usai pertemuan tersebut."Bursa meminta semua pihak untuk mengacu pada tanggapan perseroan yangdisampaikan melalui IDXnet dan penjelasan dapat dibaca di website bursa," kataDirektur Penilaian Perusahaan BEI I Gede Nyoman Yetna.Sementara Menteri Keuangan mengaku telah meminta Sekretaris JenderalKementerian Keuangan Hadiyanto untuk mempelajari kisruh terkait laporankeuangan BUMN tersebut.

Sehingga, Otoritas Jasa Keuangan (OJK) telah memutuskan bahwa PT Garuda Indonesia(Persero) Tbk melakukan kesalahan terkait kasus penyajian Laporan KeuanganTahunan per 31 Desember 2018.Pihak OJK yang diwakili oleh Deputi KomisionerHubungan Masyarakat dan Manajemen Strategis, Anto Prabowo, mengungkapkanbahwa Garuda Indonesia telah terbukti melanggar. Bursa Efek Indonesia (BEI) resmi menjatuhkan sanksi kepada PT Garuda Indonesia Tbk (GIAA) atas kasus klaim laporan keuangan perseroan yang menuai polemik. Beberapa sanksi yang dijatuhkan antara lain denda senilaiRp 250 juta dan restatement atau perbaikan laporan keuangan perusahaandengan paling lambat 26 Juli 2019 ini.

REFERENSI :

http://audit-si-untag.blogspot.com/2015/04/audit-sistem-informasi.html

https://accounting.binus.ac.id/2019/06/10/memahami-audit-sistem-informasi/

https://www.mas-software.com/blog/apa-itu-audit-sistem-informasi/

https://tirto.id/kasus-lapkeu-garuda-bukti-kap-taraf-internasional-bisa-kebobolan-edi1

https://www.academia.edu/40194279/MAKALAH_KASUS_AUDIT_PT_GARUDA_INDONESIA_2019

NAMA **: DINI RAHMADIA**

KELAS **: MTI REG B**

NIM **: 182420134**

TUGAS **: IT AUDIT**

SOAL:

Sebutkan beberapa jenis resiko yang menjadi factor utama sehingga perlu adanya IT atau IS Audit . jelaskan dengan adanya contoh kasus yang terkait beserta referensi

JAWAB:

Audit IT merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang telah digunakan dapat melindungi asset milik perusahaan atau organisasi, menjaga integritas data , dan membantu tujuan organisasi secara efektif,

Risiko Audit atau Audit Risk (AR) adalah kemungkinan risiko bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat. Mengingat risiko itu maka, auditor harus melakuka pemeriksaan risiko (risk assessment) sebelum menjalankan proses audit, tepatnya pada fase perencanaan audit (audit planning).

Jenis-Jenis Resiko Audit

1. Resiko inherent (inherent risk)

   adalah risiko yang mungkin timbul akibat karakter bawaan dari suatu transaksi, entah karena kompleksitas transaksi dan klas transaksi, kompleksitas perhitunganaset yg mudah tercuri/digelapkan dan 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. Dengan kata lain, auditor hanya bisa menemukan tetapi tidak bias melakukan apa-apa.

Contoh kasus,

Perusahaan yang memiliki anak/cabang dalam jumlah banyak dan melibatkan banyak mata uang asing, diasumsikan mengandung IR yang tinggi. Sebab model perusahaan seperti ini cenderung menghasilkan laporan keuangan yang kompleks dan besar kemungkinan terjadi banyak kesalahan dalam proses konsolidasi laporan yang disebabkan oleh kompleksitas data transaksi yang terlibat di dalamnya.

2. **Resiko pengendalian (control risk)**

Adalah risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain—thus tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau. Karakter perusahaan ber CR tinggi,

Contoh kasus,

Contoh Pemeriksaan SPI: Yang paling klasik, anda memeriksa faktor "Pemisahan Tugas" pada departemen-departemen yang berpotensi terjadi "Asset Fraud." Dua jenis asset dimana kerap terjadi fraud adalah wilayah "Persediaan" dan "Kas." Katakanlah anda sedang memeriksa Persediaan. Di sini anda memeriksa apakah ada 2 pekerjaan terkait atau lebih dirangkap oleh satu orang petugas?

Misal

Pegawai Purchasing merangkap sebagai petugas yang penerima barang atau pekerjaan gudang persediaan lainnya (ini buruk); atau Pegawai Shipping merangkap sebagai petugas gudang yang mengurus persediaan barang jadi (ini juga buruk). Foreman di bagian produksi (yang biasa request persediaan untuk keperluan produksi) diijinkan bebas keluar-masuk gudang persediaan bahan baku atau bahan penolong (ini buruk). Pegawai admin yang input Receipt of Goods (ROG) memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Payable (Utang) Pegawai admin yang input picking sheet di Shipping memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Receivable (Piutang)

3. **Resiko deteksi (detection risk)**

adalah risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). DR ada dalam kendali auditor. 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

Contoh kasus,

Salah Mengaplikasikan Prosedur Audit – Contoh kesalahan fatal, misalnya: anda menggunakan rasio untuk mengukur tingkat akurasi angka saldo, dan ternyata anda menggunakan rasio yang salah.

Nama : Ekariva Annas Asmara
NIM : 182420133
Kelas : Reguler A

JENIS RESIKO YANG MENJADI FAKTOR UTAMA PERLU ADANYA IT AUDIT

1. Pengertian Audit

Menurut Sanyoto (2007) yang dimaksud audit adalah proses pengumpulan dan penilaian bahan bukti tentang informasi untuk menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan dan dilakukan oleh orang yang kompeten dan independen

2. Pengertian Sistem

Menurut Abdul Kadir (2003), sistem adalah sekumpulan elemen yang saling terkait atau terpadu dimaksudkan untuk mencapai suatu tujuan, sebagai gambaran jika dalam sebuah sistem terdapat elemen yang tidak memberikan manfaat dalam mencapai tujuan yang sama, maka elemen tersebut dapat dipastikan bukanlah bagian dari sistem.

Menurut Jogiyanto (2005), suatu sistem adalah jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran yang tertentu. Menurut Jogiyanto (2005), system adalah kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu.

MenurutSanyoto (2007), system adalah kumpulan elemen-elemen atau sumber daya yang saling berkaitan secara terpad, terintegrasi dalam suatu hubungan hirarkis tertentu, dan bertujuan untuk mencapai tujuan tertentu.

Berdasarkan pendapat ahli diatas, maka sistem adalah kumpulan dari dua elemen atau lebih yang salig berhubungan dan terintegrasi untuk mencapai tujuan tertentu yang sama.

3. Pengertian Informasi

Dalam kehidupan sehari-hari sebuah informasi yang dapat diartikan sebagai data. Data tersebut merupakan nilai, keadaan, dan memiliki sifat berdiri sendri lepas dari konteks apapun. Menurut Jogiyanto (2005), informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya. Menurut Kenneth dan Jane (2007), menyatakan bahwa informasi sendiri berarti data yang telah dibentuk menjadi suatu yang memiliki arti dan berguna bagi manusia.

Menurut Sanyoto (2007), menyatakan bahwa informasi adalah data yang diolah menjadi bentuk yang lebih berguna, lebih bermanfaat dan lebih berarti bagi yang menerimanya. Berdasarkan pendapat ahli di atas, maka informasi adalah data yang sudah diolah dan terorganisir sehingga memiliki guna dan bermanfaat dalam pengauditan.

4. Pengertian Sistem Informasi

Sistem informasi merupakan suatu sistem dengan komponen-komponen yang bekerja untuk mengolah data menjadi sebuah informasi. Menurut Jogiyanto (2005), sistem informasi adalah suatu sistem di dalam organisasi yang mempertemukan kebutuhan pengelolaan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar terntentu dengan laporan-laporan yang diperlukan.

Menurut Kenneth *and* Jane (2007), menyatakan bahwa sistem informasi secara teknis dapat didefinisikan sebagai sekumpulan komponen yang saling berhubungan, mengumpulkan atau mendapatkan memproses, menyimpan, dan mendistribusikan informasi untuk menunjang pengambilan keputusan dan pengawasan dalam proses suatu organisasi.

Menurut Sanyoto (2007), menyatakan bahwa sistem informasi adalah suatu sistem didalam suatu organisasi yang mempertemukan kebutuhan-kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan

strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan.

5. Audit Sistem Informasi

5.1 Pengertian Audit Sistem Informasi

a) Menurut Sanyoto (2007), audit sistem informasi ialah pemeriksaan atau audit yang dilaksanakan dalam rangka IT Governance (sebenarnya merupakan audit operasional secara khusus terhadap pengelolaan sumber daya informasi)".

b) Menurut Ron Weber (2003) "Audit Sistem Informasi merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien"

c) Menurut Sasongko "Audit Sistem Informasi adalah sebuah proses yang sistematis dalam mengumpulkan dan mengevaluasi bukti-bukti untuk menentukan bahwa sebuah sistem informasi berbasis komputer yang digunakan oleh organisasi telah dapat mencapai tujuannya."

d) Menurut sanyoto gondodiyoto " audit sistem informasi adalah suatu pengevaluasian untuk mengetahui bagaimana tingkat keseuaian antara aplikasi sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah suatu sistem informasi telah didesain dan diimplementasikan secara efektif,efisien, dan ekonomis, memiliki mekanisme pengamanan aset yang memadai,serta menjamin integritas data yang memadai.

e) Menurut Gede Karya (2004), Audit sistem informasi didefinisikan sebagai proses pengumpulan dan evaluasi fakta/*evidence* untuk menentukan apakah suatu sistem informasi telah melindungi aset,menjaga integritas data, dan memungkinkan tujuan organisasi tercapai secara efektif dengan menggunakan sumber daya secara efisien.

Berdasarkan beberapa pendapat diatas disimpulkan bahwa Audit Sistem Informasi merupakan suatu proses pengumpulan dan penilaian bukti – bukti untuk menentukan apakah sistem dapat memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien.

5.2 Tujuan Audit Sistem Informasi

Berdasarkan pendapat Sanyoto (2007), tujuan audit sistem informasi dilakukan untuk dapat menilai :

a. Pengamanan *Asset.*

   Dalam model COBIT, tujuan audit tidak dinyatakan eksplisit (tidak tertulis). Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, *file* / data dan fasilitas lain harus dijaga dengan sistem pengendalian *intern* yang baik agar tidak terjadi penyalahgunaan asset perusahaan. Dengan demikian sistem pengamanan asset merupukan suatu hal yang sangat penting yang harus dipenuhi oleh perusahaan

b. Efektifitas Sistem.

   Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dilakukan efektif bila sistem informasi tersebut sudah dirancang dengan benar (*doing the right thing*), telah sesuai dengan kebutuhan user. Informasi yang dibutuhkan oleh para manajer dapat dipenuhi dengan baik.

c. Efisiensi Sistem.

   Efisiensi menjadi sangat penting ketika sumber daya kapasitasnya terbatas. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan user dengan sumber daya informasi yang minimal. Cara kerja sistem benar (*doing thing right*).

Adapun ekonomis mencerminkan kalkukasi untung rugi ekonomi (*coast / benefit*) yang lebih bersifat kuatifikasi nilai *moneter* (uang).Efisien berarti sumber daya minimum untuk mencapai hasil maksimal, sedangkan ekonomis lebih bersifat pertimbangan ekonomi.

d. Ketersediaan (*Avaiability*)

Berhubungan dengan ketersediaan dukungan/ layanan teknologi informasi (TI). TI hendaknya dapat mendukung secara bersambung terhadap proses bisnis kegiatan perusahaan. Makin sering terjadi gangguan (*system down*) maka berarti tingkat ketersediaan sistem rendah.

e. Kerahasiaan (*Confidentiality*)

Fokusnya ialah pada proteksi terhadap informasi dan supaya terlindungi dari akses dari pihak-pihak yang tidak berwenang.

f. Kehandalan (*Realibility*)

Berhubungan dengan kesuaian dan keakuratan bagi manajemen dalam pengelolaan organisasi, pelaporan dan pertanggungjawaban.

g. Menjaga Integritas Data

Integritasdata (*data integrity*) adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut seperti: kelengkapan, kebenaran, dan keakuratan. Jika integritas data tidak terpelihara, maka suatu perusahaan tidak akan lagi memiliki informasi/laporan yang benar, bahkan perusahaan dapat menderita kerugian karena pengawasan tidak tepat atau keputusan-keputusan yang salah. Faktor utama yang membuat data berharga bagi organisasi dan pentingnya untuk menjaga integritas data adalah :

1. Makna penting data/informasi bagi pengambilan keputusan. Peningkatan data sehingga dapat memberikan informasi bagi para pengambil keputusan.
2. Nilai data bagi pesaing, jika data tersebut berguna bagi pesaing maka kehilangan data akan memberikan dampak buruk bagi organisasi tersebut. Pesaing dapat menggunakan data tersebut untuk mengalahkan organisasi sehingga mengakibatkan organisasi menjadi kehilangan pasar (*market*), berkurangnya keuntungan, dan sebagainya.

Apabila audit sistem informasi akan dilaksanakan secara lengkap maka auditor harus berusaha untuk memenuhi setiap tujuan berikut ini :

1. Untuk menemukan bahwa sistem keamanan yang ada berfungsi dengan baik untuk memperoleh peralatan, program, file data dari pemankaian dan perubahan oleh yang tidak berhak.
2. Untuk menemukan bahwa desain dan implementasi program aplikasi sesuai dengan spesifikasi dan otorisasi manajemen.
3. Untuk menemukan bahwa semua modifikasi program aplikasi memiliki otorisasi dan persetujuan level item
4. Untuk menemukan akurasi dan integrasi dari proses transaksi, file, laporan dan *record-record* lainnya.
5. Untuk menentukan sumber data dari program aplikasi yang tidak akurat dan mengidentifikasi serta menyesuaikan dengan kebijakan pengadaan material.
6. Untuk menemukan apakah ada usaha untuk memenuhi syarat akurasi proses data, kelengkapan data, serta tingkat kerahasian file data.

5.3 Prosedur Audit Sistem Informasi

Berdasarkan pendapat Sanyoto (2007), prosedur audit sistem informasi dimaksudkan untuk memberikan informasi kepada manajemen puncak agar manajemen mempunyai *a clear assessment* terhadap sistem informasi yang diimplementasikan pada organisasi tersebut. Didalam prosedur audit sistem informasi terdapat berbagai jenis penugasan audit sistem informasi yang dapat dilaksanakan pada suatu organiasasi, misalnya sebagai berikut :

a. Untuk mengidentifikasi sistem yang ada (*inventory existing systems*), baik yang ada pada tiap divisi/unit/departemen ataupun yang digunakan menyeluruh
b. Untuk dapat lebih memahami seberapa besar sistem informasi mendukung kebutuhan strategis perusahaan, operasi perusahaan, mendukung kegiatan operasional departemen/unit/divisi, kelompok kerja, maupun para petugas dalam melaksanakan kegiatannya.

c. Untuk mengetahui pada bidang atau area mana, fungsi, kegiatan atau *business processes* yang didukung dengan sistem serta teknologi informasi yang ada.
d. Untuk menganalisis tingkat pentingnya data/informasi yang dihasilkan oleh sistem dalam rangka mendukung kebutuhan para pemakainya.
e. Untuk mengetahui keterkaitan antara data, sistem pengolahan dan transfer kebutuhan.
f. Untuk membuat peta (*map*) dari *information flows* yang ada.

Keuntungan utama dari prosedur ini adalah dapat meningkatan kekuatan terhadap pengujian sistem aplikasi secara efektif, dimana kemampuan dari pengujian yang dilakukan dapat diperluas sehingga tingkat kepercayaan terhadap kehandalan dari pengumpulan dan pengevaluasi bukti dapat ditingkatkan. Selain itu dengan memeriksa secara langsung logika pemrosesan dari sistem aplikasi, dapat diperkirakan kemampuan sistem dalam menagani perubahan dan kemungkinan kehilangan yang terjadi pada masa yang akan datang.

6. Jenis Resiko Yang Menjadi Faktor Utama Perlu Adanya IT Audit

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 :

a. 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.

b. **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.

c. **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.

d. **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.

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

e. 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.

7. Studi Kasus

Audit sistem informasi diperlukan oleh perusahaan dalam pencapaian tujuan perusahaan, oleh karena itu perusahaan harus membuat prosedur pengendalian dalam menjaga aset perusahaan dan memeriksa pengendalian tersebut dengan menguji pengendalian. Menguji pengendalian digunakan untuk mengevaluasi apakah telah berjalan sesuai dengan prosedur atau tidak .Dibawah ini merupakan contoh kasus yang terjadi di sebuah perusahaan yang bernama PT Corona.

Perusahaan ini sudah berjalan selama kurang lebih sepuluh tahun yang kegiatannya menjual jus buah yang terdiri dari beberapa buah-buahan. Suatu ketika perusahaan ini mendapatkan masalah yang sangat rumit dan kompleks. Sebelumnya perusahaan ini telah menyediakan pemberdayaan karyawan internal perusahaan, untuk mempelajari cara menggunakan software audit untuk komputer. Karyawan tersebut langsung mencari masalah-masalahnya lalu mengatasi masalah tersebut, membuat prosedur pengendalian dan dibuat pengujian pengendaliannya. Masalah-masalah tersebut diantaranya yaitu akses yang tidak sah pada program komputer,

sehingga website pada perusahaan yang digunakan untuk berhubungan dengan pihak eksternal perusahaan, seperti *customers* dan masyarakat tidak dapat dibuka. Departemen penjualan perusahaan menggunakan program komputer yang baru untuk mencatat transaksi keuangan dengan menggunakan *software* akuntansi keuangan dan mengubahnya untuk cara menghitung komisi penjualan. Ada kesalahan dalam pemodifikasian program ini karena hasil hitungnya lebih kecil dari biasanya. Salah seorang karyawan bagian departemen produksi yang mempunyai wewenang penuh atas pemesanan pembelian pada pemasok dan menerima laporan, melakukan pemesanan palsu untuk kepentingan pribadinya.

Karena banyaknya masalah yang terjadi diperusahaan tentang audit sistem informasi maka perusahaan juga memeriksa pemrosesan komputer perusahaan, apakah prosedur edit pada komputer telah mendeteksi *in put* yang salah atau tidak. Untuk mengatasi berbagai masalah yang ada di perusahaan Corona tersebut perusahaan menugaskan salahsatu karyawan untuk melakukan audit sistem informasi pada komputer. Di bawah ini merupakan cara mengatasi masalah perusahaan,pengendalian masalah dan menguji pengendalian terbut yang dilakukan oleh auditor internal perusahaan Corona :

1. **Pemeriksaan pada Komputer**

   Masalah website yang tidak dapat dibuka karena dirusak oleh cracker. Cracker adalah sebutan untuk orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang di masuki seperti: pencurian data, penghapusan, dan banyak yang lainnya. Cracker mempunyai kemampuan menganalisa kelemahan suatu sistem atau situs. Jika suatu sistem dapat dianalisa kelemahannya maka kerusakan dapat terjadi pada *hardware* atau *file*,selain itu dapat kehilangan *file* data dan sumber daya sistem lainnya.

   Auditor internal perusahaan mengambil keputusan untuk membuat website baru dan kemudian di beritahukan kepada masyarakat melalui media massa. Kemudian tindak lanjutnya yaitu dengan membuat mengaudit keamanan komputer, membuat prosedur pengendalian pada perusahaan dengan menggunakan beberapa pengamanan komputer diantaranya yaitu:

Membuat prosedur *Log-On* pada sistem komputer yang pada saat pemakai memulai proses ,komputer akan menampilkan sebuah kotak dialog yang meminta nomor identitas dan kata sandinya. nomor identitas dan kata sandinya cocok maka proses *log on* berhasil tapi jika tidak cocok maka proses *log on* tidak berhasil. Fungsi prosedur *log-on* ini sebagai pertahanan pertama pada sistem operasi terhadap akses-akses tidak memiliki otoritasasi pada perusahaan. Membuat kartu akses setelah proses *log on*. Kartu akses ini memberikan informasi berupa persetujuan dalam penggunaan komputer selama sesi tersebut. Daftar kontrol Akses ini berisiskan hak-hak istimewa akses untuk semua pemakai sumber daya yang sah. Akses kesumber daya sistem seperti direktori-direktori,*file-file*,program dan *printer*, dikontrol oleh daftar kontrol akses ini.

Menggunakan *Firewall* pada komputer. *Firewall* berfungsi sebagai "penjaga gerbang" sistem yang melindungi intranet perusahaan dan jaringan lain perusahaan dari penerobosan, dengan menyediakan saringan dan poin transfer yang aman untuk akses ke dan dari Internet serta jaringan lainnya. *Firewall* menyaring semua lalu lintas jaringan untuk password yang tepat atau kode keamanan lainnya, dan hanya mengizinkan transmisi sah untuk masuk serta keluar dari jaringan. Software *firewall* juga telah menjadi komponen sistem komputer yang penting untuk para individu yang terhubung dengan Internet melalui DSL atau modem kabel, karena status koneksi mereka yang rentan dan "selalu menyala".

Enkripsi merupakan konversi data menjadi kode rahasia untuk disimpan dalam database dan ditransmisikan melalui jaringan. Pengiriman berupa alogaritma enkripsi yang mengkonversikan pesan orisinal. *Enkripsi* data telah menjadi yang penting untuk melindungi data dan sumber daya jaringan komputer perusahaan terutama di Internet, intranet, dan ekstranet. *Password*, pesan, *file*, dan data lainnya dapat ditransmisikan dalam bentuk acak serta dibentuk kembali oleh sistem komputer untuk para pemakai yang berhak saja. Dua pendekatan umum enkripsi yaitu enkripsi kunci privat dan kunci publik. Enkripsi privat menggunakan sebuah kunci tunggal sedangkan enkripsi publik menggunakan dua kunci yang berbeda. Metode enkripsi yang digunakan oleh

perusahaan ini adalah menggunakan sepasang kunci publik *(public key)* dan kunci pribadi *(private key)* yang berbeda untuk setiap orang. Misalnya email karyawan dapat diacak dan di-enkode-kan dengan menggunakan kunci publik khusus bagi penerima yang dikenal oleh pengirim. Setelah email ditransmisikan, hanya kunci pribadi penerima yang rahasia tersebut dapat membentuk kembali pesan tersebut.

Pengendalian terhadap virus. Virus akan menghancurkan data, salah satunya adalah *Logic bomb* merupakan program komputer untuk diaktifkan pada waktu tertentu. *Logic bomb* merupakan metode tertua yang digunakan untuk tujuan sabotase. Perusahaan tidak mau mengambil resiko seperti apa yang terjadi pada perusahaan di Amerika yang dilakukan oleh Donald Burleson. Perusahaan tidak ingin karyawannya melakukan hal seperti itu, maka perusahaan membuat antivirus.

Kontrol pendukung dalam lingkungan database. Database mempunyai sistem pendukung (backup) sebagai prosedur otomatis yang harus dilakukan sedikitnya satu kali dalam sehari. Salinan pendukung ini kemudian harus disimpan dalam area yang terpisah dan aman. Untuk mencegah kehilangan data maka perusahaan menggunakan *back up.*

Setelah itu perusahaan membuat prosedur audit keamanan komputer dengan:

Kode Keamanan. Sistem *password* bertingkat digunakan untuk manajemen keamanan. Pertama, pemakai akhir *log on* ke sistem komputer dengan memasukkan kode identifikasi khususnya, atau ID pemakai. Pemakai akhir tersebut kemudian diminta untuk memasukkan *password* agar dapat memperoleh akses ke sistem. Password harus sering diubah (pengubahan *password* dilakukan setiap periode tertentu) dan terdiri dari kombinasi aneh antara huruf besar, huruf kecil, dan angka. Kemudian, untuk mengakses sebuah *file*, nama *file* khusus harus dimasukkan. Di dalam beberapa sistem, *password* untuk membaca sistem *file* berbeda dari yang diminta untuk menulis ke sebuah *file*. Fitur ini menambahkan tingkat perlindungan untuk sumber daya data yang disimpan. Akan tetapi, untuk keamanan yang lebih keras, *password* dapat diacak, atau dienkripsi, untuk menghindari pencurian

atau penyalahgunaannya. Selain itu *Smart Card*, yaitu kartu berisi mikrprosesossor yang menghasilkan angka acak untuk ditambahkan ke *password* pemakai akhir, digunakan dalam beberapa sistem terbatas.

Pembuatan Cadangan *File*. *Backup File* (pembuatan cadangan file) yang menduplikasi berbagai *file* data atau program, adalah alat keamanan penting lainnya. *File* juga dapat dilindungi dengan alat *file retention* yang melibatkan penyimpanan berbagai *copy file* dari periode sebelumnya.

Pemonitor Keadaaan. *System Security Monitor* (pemonitor keamanan sistem). Pemonitor keamanan adalah program yang memonitor penggunaan sistem komputer dan jaringan serta melindungi mereka dari penggunaan tidak sah, penipuan, dan kehancuran. Program semacam itu menyediakan alat keamanan yang dibutuhkan untuk memungkinkan hanya para pemakai sah yang dapat mengakses jaringan. Contohnya, kode indetifikasi dan *password* sering kali digunakan untuk tujuan ini. Pemonitor keamanan juga mengendalikan penggunaan *hardware, software,* dan sumber daya data dari sistem komputer.

Keamanan Biometris. *Biometris Security* adalah bidang keamanan komputer yang mengalami pertumbuhan pesat. Ini adalah alat keamanan yang disediakan oleh peralatan komputer, yang mengukur ciri khas fisik yang membedakan setiap undividu. Hal ini meliputi verifikasi suara, sidik jari, geometri tangan, dinamika tanda tangan, analisis penekanan tombol, pemindai retina mata, pengenalan wajah, serta analisis pola genetik. Peralatan pengendalian biometris menggunakan sensor untuk tujuan khusus agar dapat mengukur dan mendigitalkan profil biometris dari sidik jari, suara, atau ciri khas fisik seseorang.

Sistem Toleransi Kegagalan. perusahaan menggunakan sistem komputer *Fault Tolerant* (pentoleransi kegagalan) yang memiliki banyak prosesor, periferal, dan *software* yang memberikan kemampuan *fail-over* untuk mendukung berbagai komponen ketika terjadi kegagalan sistem. Sistem ini

dapat memberikan kemampuan *fail-safe* dengan sistem komputer tetap beroperasi di tingkat yang sama bahkan jika terdapat kegagalan besar pada *hardware* atau *software*. Akan tetapi, banyak sistem komputer pentoleransi kegagalan menawarkan kemampuan *fail-soft* yang memungkinkan sistem komputer terus beroperasi dalam tingkat yang lebih rendah tetapi dapat diterima jika ada kegagalan sistem besar.

Pengembangan Sistem

Auditor internal perusahaan meneliti masalah penggunaan program baru tersebut dan memverifikasi program baru tersebut. diadakan pengujian dengan perbandingan kode sumber. Perbandingan kode sumber merupakan program yang akan melaksanakan suatu perbandingan terperinci mengenai versi program aplikasi yang berjalan dengan sebelumnya. Pemeriksa atau auditor harus menguji secara menyeluruh versi sebelumnya atau mempunyai alsan baik lainnya untuk mendapatkan keyakinan dalam integritasnya. Lalu mengidentifikasi perbedaan-perbedaan diantara dua program.

Dan membuat pengendalian pengembangan sistem pada komputer perusahaan agar kesalahan terebut tidak terulang kembali. Pengendaliannya yaitu dengan cara meminta otorisasi serta persetujuan dari pihak manajemen dan pemakai, dokumentasi yang memadai dan pengujian program. Setelah itu Auditor internal perusahaan menguji pengendalian pengembangan sistem perusahaan dengan Auditor internal perusahaan dan staf-sataf audit internal yang independen lainnya menguji pengendalian sistem dengan basis yang berkala dan *continue.* Aktivitas audit dapat dibangun dalam berbagai titik pemeriksaan dalam pengembangan sistem. Dengan memilki perwakilan audit internal pada tim-tim proyek, setiap departemen perusahaan diperiksa,apakah sesuai dengan kebijakan manajemen atau tidak, secara menyeluruh melalui semua tahap pengendalian pengembangan sistem. Kesalahan-kesalahan yang tidak normal sejak awal dapat diperbaiki. Kemudian memeriksa dokumentasi secara menyeluruh, wawancara dengan pemakai mengenai keterlibatan

karyawan dalam pengembangan serta implementasi sistem, tinjauan atas spesifikasi pengujian,data uji, dan hasil pengujian sistem.

Perubahan Program

Penggunaan program yang baru dan pemodifikasian yang salah, kesalahan tersebut ditindak lanjuti oleh Auditor internal perusahaan mengadakan pengujian dengan perbandingan kode sumber. Perbandingan kode sumber merupakan program yang akan melaksanakan suatu perbandingan terperinci mengenai versi program aplikasi yang berjalan dengan sebelumnya.

Auditor internal perusahaan menguji secara menyeluruh versi sebelumnya atau mempunyai alasan baik lainnya untuk mendapatkan keyakinan dalam integritasnya. Lalu mengidentifikasi perbedaan-perbedaan diantara dua program. lalu Auditor internal perusahaan membuat beberapa prosedur pengendalian, yaitu: dengan mengurutkan berbagai komponen yang akan dimodifikasi,otorisas dan persetujuan pihak manajemen atas modifikasi, persetujuan pemakai atas perubahan program, pengujian keseluruhan atas perubahan program termasuk uji penerimaan pemakai,dokumentasi penerimaan program yang lengkap termasuk perihal persetujuan,perubahan yang diimplementasikan oleh yang pegawai independen serta programmer, dan pengendalian akses logika.

Setelah itu menguji pengendalian perubahan program dengan memverifikasi semua prosedur pengendalian apakah telah sesuai dengan prosedur dan standar. Menguji perubahan yang tidak sah atau salah, gunakan program perbandingan kode sumber,pemrosesan ulang dan simulasi paralel.

Pemrosesan Komputer

Auditor internal perusahaan memeriksa pemrosesan komputer dan menemukan kesalahan pada prosedur edit. Selama pemrosesan berlangsung ternyata prosuder edit gagal untuk mendeteksi input data yang salah, tidak lengkap, dan tidak sah. Oleh karena itu perusahaan mengambil keputusan untuk membuat pengendalian pada pemrosesan komputer, yaitu dengan rutinitas edit data yang salah pada komputer, penggunaan dengan benar label file eksternal dan internal, dokumentasi dan serangkaian buku petunjuk operasional yang mudah dipahami, supervisi atas yang kompeten operasional

komputer, penanganan yang efektif atas input dan output data oleh personil pengendalian data, daftar dan ringkasan perubahan file yang disiapkan untuk tinjauan atas departemen pemakai.

Menggunakan kontrol *run to run* yang dalam penggunaannya dengan angka-angka *batch* yang berfungsi untuk mengawasi *batch* seakan-akan dia bergerak dari satu prosedur yang terprogram (run) ke prosedur program lainnya. Kontrol ini memastikan run memproses *batch* secara benar dan lengkap. Kontrol *run to run* ini digunakan untuk menghitung kembali total kontrol,kode-kode transaskis, dan pemeriksaan urutan.

Menggunakan Kontrol Intervensi Operator untuk memasukan total *control* untuk sebuah batch *record*,menyediakan nilai-nilai parameter untuk operasi logis, dan mengaktifkan sebuah program dari titik yang berbeda ketika memasukkan kembali *record* yang salah yang setengah diproses.

Lalu Auditor internal perusahaan menguji pengendalian tersebut apakah telah sesuai prosedur atau tidak. Uji pengendalian pemrosesan komputer itu dengan: memverifikasi kepatuhan pada prosedur pengendalian pemrosesan dengan cara mengamati operasional komputer dan fungsi pengendalian. Memverifikasi bahwa output sistem aplikasi yang dipilih telah distribusi dengan benar. Merekonsiliasi sampel total *batch* dan menindak lanjuti penyimpangan. Menelusuri pengaturan sampel kesalahan yang ditandai oleh rutinitas edit data untuk memastikan adanya penanganan yang tepat. Memeriksa akurasi dan kelengkapan pengendalian pemrosesan dengan menggunakan data uji. Memverifikasi akurasi transaksi pilihan yang dihasilkan komputer.

Dokumen Sumber

Masalah salah seorang karyawan bagian departemen produksi yang mempunyai wewenang penuh atas pemesanan pembelian pada pemasok dan menerima laporan, melakukan pemesanan palsu untuk kepentingan pribadinya.

Hal ini diketahui oleh Auditor internal perusahaan ketika memeriksa laporan-laporan yang tidak sesuai dengan daftar-daftar laporan. diketahui pemesanan bahan baku dan sebuah faktur pemasok rekaan, dalam menginput suatu data kedalam komputer juga terdapat kesalahan yaitu ketidak akuratan dokumen sumber. Hal ini

terjadi karena kurangnya pengawasan internal perusahaan maka untuk itu perusahaan membuat prosedur pengendalian dengan:

1) Menggunakan dokumen sumber yang sebelumnya telah diberi nomor urut. Dokumen-dokumen sumber harus diberi nomor urut melalui printer dengan nomor urut yang unik untuk setiap dokumen. Nomor dokumen sumber memungkinkan perhitungan secara akurat dan tepat dan sebagai jejak audit.

2) Menggunakan dokumen secara berurutan. Dokumen sumber harus di distribusikan ke pamakai dan digunakan secara berurutan. Hal ini memerlukan pengamanan fisik,ketika dokumen sumber ini tidak digunakan maka disimpan di tempat yang terkunci. Akses ke dokumen sumber ini hanya orang-orang yang mempunyai otoritas saja.

3) Mengaudit dokumen sumber secara berkala. Hilangnya dokumen sumber harus direkonsiliasi nomor-nomor urut dokumen sumber. Secara berkala auditor membandingkan nomor tersebut. Semua dokumen sumber harus dibandingkan dari yang digunakan saat ini,yang tersisa di tempat penyimpanan ataupun dokumen sumber yang salah atau sudah jatuh tempo. Dokumen-dokumen yang tidak dihitung harus dilaporkan ke manajemen.

8. Kesimpulan

Audit Sistem Informasi merupakan suatu proses pengumpulan dan penilaian bukti – bukti untuk menentukan apakah sistem dapat memelihara integritas data, . pengevaluasian pengendalian perusahaan yang dapat mendorong pencapaian tujuan perusahaan atau organisasi secara efektif dan menggunakan sumberdaya secara efisien untuk mencapai tujuan perusahaan atau organisasi

Audit sistem informasi dibutuhkan dalam suatu organisasi/perusahaan untuk mengetahui apakah suatu pengendalian dalam sistem informasi di sebuah organisasi tersebut tujuannya sudah tercapai atau belum. Audit internal dalam melakukan audit sistem informasi diperlukan prosedur pengendalian dan lalu di ujikan, untuk pencapaian tujuan pengendalian tersebut.

REFERENSI

Jurnal Sistem informasi MTI-UI, Volume 4, Nomor 1,ISBN 1412-8896

Jurnal Sistem Informasi, Vol 6, No 1, maret 2011 : 15 – 33

Jurnal Analisis Faktor Yang Mempengaruhi Pelaksanaan Adit Berbasis teknologi Informasi, Michelle Kristian & Elsa Imelda

http://nanienuneno.blogspot.co.id/2010/11/audit-sistem-informasi-berbasis.html

Gunawan (2004). 6 Alasan Mengapa Audit IT diperlukan. Retrieved Mei, 17, 2004. From http://www.ebizzasia.com/0217-2004/focus,0217,03.htm

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.

Nama : Fajar Prayoga
NIM : 182420136
IT Audit

Nama : Fajar Prayoga
Nim : 182420136
Kelas : MTI. 20A
DosenPengasuh : Dr Widya Cholil , S.Kom., M.I.T.
Mata Kuliah : IT Audit

Soal

Sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit.
Jelaskan dengan adanya contoh kasus yang terkait
Jangan lupa tambahkan referensi

Jawaban

***information technology (IT) audit atau information systems (IS) audit*)** adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi 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 teknologi informasi** 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.

A. Salah satu jenis yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit adalah risiko audit dalam penerapan sistem informasi di perusahaan.

RESIKO DALAM PENERAPAN SISTEM INFORMASI DI PERUSAHAAN

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan. Di lain pihak, seiring makin meluasnya implementasi sistem informasi maka kesadaran akan perlunya dilakukan review atas pengembangan suatu sistem informasi semakin meningkat. Kesadaran ini muncul karena munculnya berbagai kasus yang terkait dengan gagalnya sistem informasi, sehingga memberikan akibat yang sangat mempengaruhi kinerja organisasi.

Nama : Fajar Prayoga
NIM : 182420136
IT Audit

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya "scope creep" (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah **CISA® (Certified Information Systems Auditor)** yang dikeluarkan oleh **ISACA (Information Systems Audit and Control Association).** **Audit sistem informasi** dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contohnya :

Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (*IT Governance*) (Herawan, 2012).

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu

diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (*Information System and Control Association*) dan ITGI (*IT Governance Institute*) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.(Wibowo, 2008).

Referensi

Fanani, M. F. (2012, September 24). *Implementasi COBIT Di PT PERTAMINA*. Retrieved November 27, 2012, from http://www.slideshare.net: http://www.slideshare.net/fananifaiz/cobit-pertamina#btnNext

Herawan, R. (2012, April 4). *Implementasi COBIT pada PT Transindo*. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/

Meidyanto, Riky (2009, Juni 19). *Audit Sistem Informasi dengan Menggunakan COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 27, 2012, from http://krikkrikx.blog.binusian.org: http://www.krikkrikx.blog.binusian.org/files/2009/06/untuk-blog221.doc

Susanto, Erdi (2012, November). *Kerangka Kerja COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 28, 2012, from http://erdi-susanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobit-control-objectives.html

Wibowo, M. P. (2008, Agustus 9). *Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective For Information And Related Technology): Studi Kasus Di Perpustakaan Universitas Indonesia*. Retrieved November 27, 2012, from http://sangprabu.multiply.com: http://sangprabu.multiply.com/journal/item/27

Wikipedia. *COBIT*. Retrieved November 27, 2012, from http://www.wikipedia.org: http://en.wikipedia.org/wiki/COBIT

Sumber : https://sis.binus.ac.id/2015/07/01/resiko-dalam-penerapan-sistem-informasi-di-perusahaan/

Nama : Gian Pratama, S.Kom.

NIM : 182420116

Kelas : MTI 20 A

Mata Kuliah : IT Audit

Materi : Identified Resiko

1. Sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit!
2. Jelaskan dengan adanya contoh kasus yang terkait!
3. Jangan lupa tambahkan referensi.

Jawab :

A. Resiko kehilangan data.

Setiap perusahaan & bisnis yang berhubungan secara langsung dengan pemrosesan dengan IT/IS memiliki resiko kehilangan data akibat penyalahgunaan dan ketidakmampuan pengendalian terhadap penggunaan sistem. Kurang tersedianya sumber daya *backup* yang baik, sabotase, *human error*, kerusakan normal file juga menjadi resiko yang harus diatasi dengan diadakannya IT Audit. Dengan demikian, proses audit dapat menganalisa, menemukan dan mencegah kemunculan resiko ataupun dapat meminimalisir resiko ini dikemudian hari.

B. Resiko *decision making* yang tidak sesuai.

Pengambilan keputusan biasanya dilakukan oleh pihak berwenang di suatu perusahaan ataupun bisnis, misalnya jajaran direksi. Sebelum mengambil kebijakan dan keputusan, tentunya direksi akan mempertimbangkan dari sumber data yang dikelola menggunakan IT/IS. Pentingnya akurasi data menjadi hal mutlak, untuk itu diperlukan audit IT yang mampu memvalidasi keabsahan proses aktual di lapangan, data yang di input, data yang diproses dan dihasilkan menjadi sekumpulan *summary* penting bagi yang membutuhkan.

C. Resiko *hardware, software & brainware.*

Selain data, *hardware, software* dan *brainware* menjadi faktor penting dalam suatu organisasi. *Hardware* yang ada hendaknya diasuransikan dan terjaga keamanannya dari kehilangan ataupun pencurian. *Software* menggunakan aplikasi yang memiliki tingkat kemanan tinggi, sehingga data dan informasi yang ada didalamnya tetap aman dari penyalahgunaan. *Brainware* atau sering disebut sebagai operator juga harus terdidik agar handal dalam mengoperasikan IT/IS yang ada. Poin-poin tersebut adalah unit audit yang biasa dilakukan dalam menghadapi resiko jenis ini.

D. Kerahasiaan.

Selanjutnya adalah kerahasiaan, yang menjadi salah satu faktor penting dibutuhkannya IT/IS Audit. Kebocoran data maupun informasi kepada pihak-pihak yang tidak berwenang dapat memunculkan resiko penyalahgunaan data tersebut. Sistem penggajian pada suatu organisasi misalnya, apabila kerahasiaan IS nya sudah dapat dimasuki pihak tidak berwenang, sistem dapat diubahsuaikan dan menjadi kerugian bagi perusahaan tersebut. IT Audit perlu menjamin bahwa IT/IS yang ada dalam sistem penggajian tersebut sudah memenuhi standara kelayakan dan keamanan tingkat tinggi.

Referensi :

https://sis.binus.ac.id/2015/06/24/pentingnya-audit-sistem-informasi-bagi-organisasi/

Hamzah Ramadhan
182420124 – MTI2B1

IT Audit

Information Technology (IT) audit atau information systems (IS) audit) adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi 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 teknologi informasi 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 menurut Ron Webber (Dekan Fakultas Teknologi Informasi, Monash University) dalam bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

- Kerugian akibat kehilangan data.
- Kesalahan dalam pengambilan keputusan.
- Resiko kebocoran data.
- Penyalahgunaan komputer.
- Kerugian akibat kesalahan proses perhitungan.
- Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Mengingat adanya beberapa risiko tersebut di atas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisasi. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan di atas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contoh

JAKARTA – Masyarakat resah melihat kasus pembobolan dana nasabah di bank yang intensitasnya meningkat sejak awal 2011. Kasus-kasus yang terjadi dalam rentang waktu berdekatan ini pun berdampak pada makin kurangnya kepercayaan publik terhadap perbankan.

Dengan begitu, pengamat perbankan Mirza Adityaswara mengatakan, masyarakat akan lebih berhati-hati menggunakan layanan perbankan setelah mencuatnya kasus-kasus yang terjadi. "Masyarakat yang semula kurang awas, akan lebih waspada," katanya, Ahad (2/5).

Mirza berpendapat sistem perbankan yang ada saat ini memang belum sempurna. Ini, jelas dia, bukan hanya terlihat dari sisi pegawai bank, melainkan juga nasabah.

"Jangan tergoda melakukan penyelewengan," katanya.

Tony Prasetyantono, pengamat perbankan, mengatakan berkurangnya kepercayaan publik pasti akan terjadi menyusul berbagai kasus tersebut. Namun, nasabah belum sampai pada satu tindakan menarik uangnya besar-besaran. Karena, jelas Tony, nasabah tidak memiliki pilihan lain yang lebih baik untuk menempatkan uangnya.

Sejauh ini, ujar Tony, bank masih dinilai sebagai tempat terbaik menyimpan aset.

"Apalagi yang bersifat likuid, seperti rekening giro dan tabungan," katanya. "Namun, nasabah akan lebih selektif memilih bank."

Nasabah, lanjut dia, juga akan lebih memantau rekeningnya agar luput dari pembobolan. Tony menilai, kejahatan perbankan yang terjadi belakangan lebih mengarah pada kesalahan kolektif. Penyebabnya, ia menjelaskan, muncul dari sisi perbankan, nasabah, Bank Indonesia, maupun aturan hukumnya.

Tony mencontohkan, bank kerap menyembunyikan penyimpangan karena takut reputasinya rusak, sedangkan nasabah tidak aktif memantau rekening miliknya. Sementara, BI memiliki keterbatasan dalam memantau banyaknya perbankan yang ada di Tanah Air. "Hukuman terhadap pelaku fraud juga kurang maksimal sehingga kurang menimbulkan efek jera," jelasnya.

Saat ini. Direktorat Kriminal Khusus (Ditkrimsus) Polda Metro Jaya sedang menangani sembilan kasus perbankan sejak Januari 2011. Bulan lalu, dana deposito milik PT Elnusa Rp 111 miliar di Bank Mega dicairkan tanpa seizin manajemen perusahaan tersebut dengan pelaku melibatkan orang dalam bank. Sebelumnya, simpanan nasabah prioritas Citibank dibobol oleh karyawan bank asing tersebut yang bernama Inong Malinda alias Malinda Dee

Referensi

- Fanani, M. F. (2012, September 24). *Implementasi COBIT Di PT PERTAMINA*. Retrieved November 27, 2012, from http://www.slideshare.net: http://www.slideshare.net/fananifaiz/cobit-pertamina#btnNext
- Herawan, R. (2012, April 4). *Implementasi COBIT pada PT Transindo*. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/
- Meidyanto, Riky (2009, Juni 19). *Audit Sistem Informasi dengan Menggunakan COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 27, 2012, from http://krikkrikx.blog.binusian.org:

http://www.krikkrikx.blog.binusian.org/files/2009/06/untuk-blog221.doc

- Susanto, Erdi (2012, November). *Kerangka Kerja COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 28, 2012, from http://erdisusanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobitcontrol-objectives.html
- Wibowo, M. P. (2008, Agustus 9). *Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective For Information And Related Technology): Studi Kasus Di Perpustakaan Universitas Indonesia*. Retrieved November 27, 2012, from http://sangprabu.multiply.com: http://sangprabu.multiply.com/journal/item/27
- Wikipedia. *COBIT*. Retrieved November 27, 2012, from http://www.wikipedia.org: http://en.wikipedia.org/wiki/COBIT
- https://dendyoktavianto23.wordpress.com/2017/10/09/studi-kasus-audit-teknologiinformasi/

Nama : **Hari Febriadi**
Nim : **182420127**
Kelas : **MTI. 20A**
DosenPengasuh : **Dr Widya, S.Kom., M.I.T.**
Mata Kuliah : **IT Audit**

Jawaban

Audit teknologi informasi adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi 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 teknologi informasi 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.

Resiko-resiko umum TI

Pengendalian dan audit atas teknologi informasi perlu dilakukan mengingat besarnya risiko yang harus dihadapi oleh organisasi berkaitan dengan penggunaan teknologi informai. Risiko-risiko tersebut antara lain:

1. Kehilangan Data

   Data merupakan aset teknologi informasi yang sangat kritikal bagikelangsungan operasional perusahaan. Dapat dibayangkan apabila sebuah organisasi mengalami data, misalnya data piutang atau data pelanggan. Apa yang akan terjadi?
2. Kesalahan pengambilan keputusan

   Sebuah keputusan pada umumnya diambil berdasarkan data dan informasi yang tersedia. Apa yang akan terjadi apabila data dan informasi yang tersedia tidak akurat, tidak lengkap, tidak tepat waktu, dan tidak relevan.
3. Penyalahgunaan komputer

   Risiko kemungkinan penyalahgunaan teknologi yang dapat mengakibatkan kerugian yang bahkan tidak terbayangkan. Risiko tersebut dapat berupa ancaman fisik seperti penghancuran dan pencurian aset dan non-fisik seperti hacking, virus, penyalahgunaan akses.
4. Nilai investasi

Sebagian besar investasi dalam teknologi informasi memerlukan dana yang tidak sedikit dan cenderung sulit dikendalikan. Di indonesia, belum banyak organisasi yang melakukan analisa cost & benefit sebelum melakukan investasi teknolodi informasi.

5. Aspek privasi

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

6. Kesalahan pengoperasian komputer

   Akibat kesalahan pengoperasian komputer dapat berupa kerugian finansial dari Rp.0 sampai kepada kebangkrutan bahkan kerugian jiwa

7. Evolusi teknologi

   Teknologi informasi, seperti halnya teknologi yang lain mempunyai sifat netral. Sisi baik dan sisi buruk akibat pemanfaatannya tergantung kepada siapa penggunanya dan untuk apa digunakan.

Contoh KASUS AUDIT UMUM PT KAI

Menerapkan proses GCG (Good Corporate Governance) dalam suatu perusahaan Pembedahan kasus-kasus yang telah terjadi di perusahaan atas proses pengawasan yang efektif akan menjadi pembelajaran yang menarik dan kiranya dapat kita hindari apabila kita dihadapkan pada situasi yang sama.

bukan suatu proses yang mudah. Diperlukan konsistensi, komitmen, dan pemahaman yang jelas dari seluruh stakeholders perusahaan mengenai bagaimana seharusnya proses tersebut dijalankan. Namun, dari kasus-kasus yang terjadi di BUMN ataupun Perusahaan Publik dapat ditarik kesimpulan sementara bahwa penerapan proses GCG belum dipahami dan diterapkan sepenuhnya.

Salah satu contohnya adalah kasus audit umum yang dialami oleh PT. Kereta Api Indonesia (PT. KAI). Kasus ini menunjukkan bagaimana proses tata kelola yang dijalankan dalam suatu perusahaan dan bagaimana peran dari tiap-tiap organ pengawas dalam memastikan penyajian laporan keuangan tidak salah saji dan mampu menggambarkan keadaan keuangan perusahaan yang sebenarnya.

Kasus PT. KAI berawal dari perbedaan pandangan antara Manajemen dan Komisaris, khususnya Ketua Komite Audit dimana Komisaris menolak menyetujui dan menandatangani laporan keuangan yang telah diaudit oleh Auditor Eksternal. Komisaris meminta untuk dilakukan audit ulang agar laporan keuangan dapat disajikan secara transparan dan sesuai dengan fakta yang ada. Salah satu faktor yang menyebabkan terjadinya kasus PT. KAI adalah rumitnya laporan keuangan PT. KAI. Perbedaan pandangan antara manajemen dan komisaris tersebut bersumber pada perbedaan mengenai:

1. Masalah piutang PPN.

Piutang PPN per 31 Desember 2005 senilai Rp. 95,2 milyar, menurut Komite Audit harus dicadangkan penghapusannya pada tahun 2005 karena diragukan kolektibilitasnya, tetapi tidak dilakukan oleh manajemen dan tidak dikoreksi oleh auditor.

2. Masalah Beban Ditangguhkan yang berasal dari penurunan nilai persediaan.

Saldo beban yang ditangguhkan per 31 Desember 2005 sebesar Rp. 6 milyar yang merupakan penurunan nilai persediaan tahun 2002 yang belum diamortisasi, menurut Komite Audit harus dibebankan sekaligus pada tahun 2005 sebagai beban usaha.

3. Masalah persediaan dalam perjalanan.
Berkaitan dengan pengalihan persediaan suku cadang Rp. 1,4 milyar yang dialihkan dari satu unit kerja ke unit kerja lainnya di lingkungan PT. KAI yang belum selesai proses akuntansinya per 31 Desember 2005, menurut Komite Audit seharusnya telah menjadi beban tahun 2005.
4. Masalah uang muka gaji.
Biaya dibayar dimuka sebesar Rp. 28 milyar yang merupakan gaji Januari 2006 dan seharusnya dibayar tanggal 1 Januari 2006 tetapi telah dibayar per 31 Desember 2005 diperlakukan sebagai uang muka biaya gaji, yang menurut Komite Audit harus dibebankan pada tahun 2005.
5. Masalah Bantuan Pemerintah Yang Belum Ditentukan Statusnya (BPYDBS) dan Penyertaan Modal Negara (PMN).
BPYDBS sebesar Rp. 674,5 milyar dan PMN sebesar Rp. 70 milyar yang dalam laporan audit digolongkan sebagai pos tersendiri di bawah hutang jangka panjang, menurut Komite Audit harus direklasifikasi menjadi kelompok ekuitas dalam neraca tahun buku 2005.
Beberapa hal yang direfentifikasi turut berperan dalam masalah pada laporan keuangan PT. KAI Indonesia:
1. Auditor internal tidak berperan aktif dalam proses audit, yang berperan hanya auditor Eksternal.
2. Komite audit tidak ikut serta dalam proses penunjukkan auditor sehingga tidak terlibat proses audit.
3. Manajemen (tidak termasuk auditor eksternal) tidak melaporkan kepada komite audit dan komite audit tidak menanyakannya.
4. Adanya ketidakyakinan manajemen akan laporan keuangan yang telah disusun, sehingga ketika komite audit mempertanyakan manajemen merasa tidak yakin.
Terlepas dari pihak mana yang benar, permasalahan ini tentunya didasari oleh tidak berjalannya fungsi check and balances yang merupakan fungsi substantif dalam perusahaan. Yang terpenting adalah mengidentifikasi kelemahan yang ada sehingga dapat dilakukan penyempurnaan untuk menghindari munculnya permasalahan yang sama di masa yang akan datang.
Berikut ini beberapa solusi dan rekomendasi yang disarankan kepada PT KAI untuk memperbaiki kondisi yang telah terjadi:
1. Apabila Dewan Komisaris ini merasa direksi tidak capable (mampu) memimpin perusahaan, Dewan Komisaris dapat mengusulkan kepada pemegang saham untuk mengganti direksi.
2. Diperlukannya kebijaksanaan (wisdom) dari Anggota Dewan Komisaris untuk memilah-milah informasi apa saja yang merupakan private domain.
3. Komunikasi yang intens sangat diperlukan antara Auditor Eksternal dengan Komite Audit.
4. Komite Audit sangat mengandalkan Internal Auditor dalam menjalankan tugasnya untuk mengetahui berbagai hal yang terjadi dalam operasional perusahaan.
5. Komite Audit tidak memberikan second judge atas opini Auditor Eksternal, karena opini sepenuhnya merupakan tanggung jawab Auditor Eksternal.
6. Harus ada upaya untuk membenarkan kesalahan tahun-tahun lalu, karena konsistensi yang salah tidak boleh dipertahankan.
7. Komite Audit tidak berbicara kepada publik karena esensinya Komite Audit adalah organ Dewan Komisaris sehingga pendapat dan masukan Komite Audit harus disampaikan kepada Dewan Komisaris. Apabila Dewan Komisaris tidak setuju dengan Komite Audit, tetapi Komite Audit tetap pada pendiriannya, Komite Audit dapat mencantumkan pendapatnya pada Laporan Komite Audit yang terdapat dalam laporan tahunan perusahaan.
8. Manajemen menyusun laporan keuangan secara tepat waktu, akurat dan full disclosure.
9. Komite Audit dan Dewan Komisaris sebaiknya melakukan inisiatif untuk membangun budaya pengawasan dalam perusahaan melalui proses internalisasi, sehingga pengawasan merupakan bagian tidak terpisahkan dari setiap organ dan individu dalam organisasi.

Referensi

http://garaptugaskampus.blogspot.com/2019/11/contoh-kasus-audit.html
https://itgid.org/it-audit/

Nama : Harli Septia Fani
NIM : 182420122
Kelas : MTI 20A
Mata Kuliah : IT Audit
Dosen : Dr. Widya Cholil, S. Kom., M. IT.

Sebutkan beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit. Jelaskan dengan adanya contoh kasus yang terkait.
Jangan lupa tambahkan referensi

PENTINGNYA IT / IS AUDIT BAGI 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 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.

Referensi :

1. Juliandarini. Handayaningsih, Sri. Audit Sistem Informasi pada Digilib Universitas XYZ Menggunakan Kerangka Kerja COBIT 4.0. Jurnal Sarjana Teknik Informatika. Volume 1 Nomor 1, Juni 2013. Pp. 276-286. e-ISSN: 2338-5197
2. Romney, Marshall B., Steinbart, Paul John. (2004). Accounting Information Systems. 9th edition.
3. Weber, Ron. (1999). Information Systems Control and Audit. Prentice-Hall, Inc., New Jersey.

CONTOH KASUS

1. **Audit Sistem Informasi Manajemen Rumah Sakit (Studi Kasus Pada RSUD Kota Tasikmalaya)**

   Referensi : https://ojs.unikom.ac.id/index.php/jtk3ti/article/download/295/267/
2. **Usulan Model Audit Sistem Informasi (Studi Kasus: Sistem Informasi Perawatan Pesawat Terbang)**

   Referensi : https://www.scribd.com/doc/70797185/Studi-Kasus-Audit-Sistem-Informasi-Perawatan-Pesawat-Terbang-Menggunakan-Cobit
3. **Kasus Audit IT Bank Indonesia**

   Referensi : http://auditit50.blogspot.com/2012/11/studi-kasus.html
4. **Kasus Audit Sistem Informasi Pada PT. ANTAM (PERSERO) TBK Menggunakan Pendekatan CobIT**

Referensi : http://ridzkythepupilzboys.blogspot.com/2017/10/kasus-audit-sistem-informasi-pada-pt.html

5. Studi Kasus PT Setia Jaya Teknologi
   Referensi :
   https://www.researchgate.net/publication/321017187_Audit_Sistem_Informasi_pada_Aplikasi_Accurate_Menggunakan_Model_Cobit_Framework_41_Studi_Kasus_PT_Setia_Jaya_Teknologi/link/5a08317aa6fdcc65eab3d1b7/download

Nama : I Made Harya Wijaya Oka Rafflesia
NIM : 182420129
Matkul : IT Audit

RESIKO DALAM PENERAPAN SISTEM INFORMASI DI PERUSAHAAN

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan. Di lain pihak, seiring makin meluasnya implementasi sistem informasi maka kesadaran akan perlunya dilakukan review atas pengembangan suatu sistem informasi semakin meningkat. Kesadaran ini muncul karena munculnya berbagai kasus yang terkait dengan gagalnya sistem informasi, sehingga memberikan akibat yang sangat mempengaruhi kinerja organisasi.
Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi. Melonjaknya biaya pengembangan sistem informasi karena adanya “scope creep” (atau pengembangan berlebihan) yang tanpa terkendali. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisas Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contohnya :
Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan

dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (IT Governance) (Herawan, 2012).

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (Control Objectives for Information and Related Technology) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (Information System and Control Association) dan ITGI (IT Governance Institute) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.(Wibowo, 2008).

Referensi :

Herawan, R. (2012, April 4). *Implementasi COBIT pada PT Transindo*. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/

Susanto, Erdi (2012, November). *Kerangka Kerja COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 28, 2012, from http://erdi-susanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobit-control-objectives.html

https://sis.binus.ac.id/2015/07/01/resiko-dalam-penerapan-sistem-informasi-di-perusahaan/

Terima Kasih, salam.

JENIS RESIKO YANG MENJADI FAKTOR ADANYA IT AUDIT

IT atau IS Audit adalah Proses pengujian terhadap infrastruktur teknologi informasi, dimana berhubungan dengan masalah audit finansial dan audit internal. IT Audit lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing) Yang artinya adalah audit komputer untuk menentukan apakah aset sistem infromasi perusahaan itu telah bekerja secara :

- Efektif
- Intergratif
- Mencapai target organisasi

Tujuan IT Audit

- Avalability (Ketersediaan Informasi)
- Confidentiality (Kerahasiaan Informasi)
- Integrity (Keakuratan, dan Ketepatan Waktu)

Pada dunia teknologi terutama dibidang teknologi informasi atau sistem jenis – jenis resiko [1] di bagi menjadi 6 (enam bagian)yaitu :

1. Resiko Technologi Risk

- Komponen file tidak lengkap
- Sistem operasi tidak kompatibel, device tidak dikenal
- Perangkat keras tidak mendukung (mis: resolusi monitor, resolusi printer)
- Spesifikasi tidak memenuhi
- Kualitas Network dibawah standar kebutuhan
- Browser, software tidak memenuhi

2. Resiko Orang

- Keluarnya programmer utama
- Skill/kemampuan tidak memenuhi
- Project manager tidak mampu membuat/melakukan koordinasi

- Tim yang terlibat tidak mematuhi job disk
- Tim tidak punya disiplin dan target(hanya berorientasi hasil, proses diabaikan)

3. Resiko Organisasi

- Restruturisasi
- Pembuatan fungsi dan tugas
- Perpindahan penugasan/kebijakan
- Overload/kemampuan organisasi tidak sesuai kapasitasnya

4. Resiko Tools

- hasil pengembangan tidak bisa diintegrasikan
- Tools yang dikehendaki tidak dikuasai pengembang
- Versi pengembangan tidak memenuhi kebutuhan

5. Resiko Requirement

- Adanya pemahaman yang berbeda antar bagian yang terlibat
- Adanya batasan yang melebihi ruang lingkup
- Adanya informasi yang tidak lengkap
- Kurang detailnya proses bisnis
- Ketidak jelasan dari costumer tentang proses bisnisnya

6. Resiko Estimate

- Berkaitan dengan over budget, perlunya menghitung ulang akibat kesalahan estimasi
- Berkaitan denganketepatan waktu, perlunya menskedule ulang jadwal
- Berkaitan dengan Resource

Beberapa jenis resiko yang menjadi faktor utama sehingga perlu adanya IT atau IS Audit[2] :

1. Kerugian kehilangan data

2. Kesalahan pengambil keputusan
3. Resiko kebocoran data
4. Penyalahgunaan komputer
5. Kerugian kesalahan proses perhitungan
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer

Contoh:

- Akses jauh oleh para pemakai yang tidak sah (Remote access by unauthorized users)
- Akses di tempat oleh orang yang tidak sah (On-site access by unauthorized)
- Tentukan menerima Risiko Terukur (Determine Acceptable Risk Levels)
- Nilai Probability Vulnerabilities (Assess the Probability of Vulnerabilities)
- Kesempatan untuk mengakses remote dari para pemakai yang tidak sah sebesar 5 persen (Chance of remote access by unauthorized users is 5 percent)
- Tabel Kejadian yang menggangu pencapainya objek perusahaan [3] :

Objektif	**Kejadian**
Effectiveness and Efficiency	Manajement yang buruk (perencanaan dan kebijakan)
	Sistem (Hardware, software dan teknogi)
	Kemampuan TI dan non-TI
	Manajement proses (desain dan eksekusi)
Confidentiality	Manajeman Keamanan (Kebijakan dan prosedur)
	Kesadaran pengguna
	Hacker dan virus
Integrity and Reliability	Desain sistem (input, proses, output)
	Hacker dan pelanggar akses
	Prosedur pemberian otoritas yang buruk
Availability	Desain system dan jaringan
	Kegagalan hardware
	Virus dan serangan
	Tidak ada BCP, backup dan recovery

Compliance	Tidak sabar atau tidak mengerti terhadap aturan dan regulasi
	Tidak ada monitoring

Referensi :

[1] Sagilaman, “artikel lawas: Pengertian dan jenis resiko dalam proyek sistem informasi,” *artikel lawas*, Sep. 27, 2010. http://segruckchemonk.blogspot.com/2010/09/pengertian-dan-jenis-resiko-dalam.html (accessed Apr. 09, 2020).

[2] “YouTube.” https://www.youtube.com/watch?v=HjeGKRWg03Y&feature=youtu.be (accessed Apr. 09, 2020).

[3] “RISK IT,” *Audit sistem informasi*. http://auditsi-tommyhizkia.weebly.com/risk-it.html (accessed Apr. 09, 2020).

NAMA : Lailatur rahmi

Nim : 182420118

Mata Kuliah : IT Audit

Sebutkan beberapa jenis resiko yang menjadi factor utama sehingga perlu adanya IT atau IS Audit. Jelaskan dengan adanya contoh kasus yang terkait

- Risiko bawaan (Inherent risk) merupakan 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.

  Contoh kasus , Laporan pengadaan peningkatan kouta pemakaian akses internet kepada salah satu cabang perusahaan dikarenakan lambatnya akses internet. Tetapi setelah dikalukan audit ternyata akses internet tidak digunakan untuk urusan pekerjaan oleh pegawai sehingga akses kuota internet menjadi cepat habis.

- Risiko Pengendalian (Control Risk) merupakan ukuran yang digunakan oleh auditor untuk menilai adanya kemungkinan bahwa terdapat sejumlah salah saji material yang melebihi nilai salah saji yang masih dapat ditoleransi atas segmen tertentu akan tidak terhadang atau tidak terdeteksi oleh pengendalian intern yang dimiliki klien

  Contoh kasus dengan adanya kasus penggunaan akses internet pada salah satu cabang perusahaan, makan dilakukan pengandalian dengan cara IT pada kantor tersebut membatasi akses internet pada setiap computer yang digunakan pegawai.
-
- Risiko Deteksi (Detection Risk) merupakan risiko bahwa auditor tidak dapat mendeteksi salah saji yang material dalam suatu perusahaan. Risiko ini merupakan fungsi keefektifan prosedur audit dan aplikasinya oleh auditor.
  Contoh kasus : dalam contoh kasus penggunaan akses internet pada salah satu cabang perusahaan , tetapi tidak dilakukan pengechekan full terhadap semua akes internet pada pegawa perusahaan tersebut.

Alasan perlu adanya IT Audit

- Perlengkapan keamanan melindungi perlengkapan komputer, program, komunikasi, dan data dari akses yang tidak sah, modifikasi, atau penghancuran.
- Pengembangan dan perolehan program dilaksanakan sesuai dengan otorisasi khusus dan umum dari pihak manajemen.
- Modifikasi program dilaksanakan dengan otorisasi dan persetujuan pihak manajemen.
- Pemrosesan transaksi, file, laporan, dan catatan komputer lainnya telah akurat dan lengkap.
- Data sumber yang tidak akurat atau yang tidak memiliki otorisasi yang tepat diidentifikasi dan ditangani sesuai dengan kebijakan manajerial yang telah ditetapkan.
- File data komputer telah akurat, lengkap, dan dijaga kerahasiaannya

Referensi

1. Rianto wahyudi 2017.resiko yang mengakibatkan prosedur prosedur audit yang gagal Di kutio dari https://riantotriwahyudi.wordpress.com/2017/12/04/jelaskan-dan-berikan-contoh-resiko-yang-mengakibatkan-prosedur-prosedur-audit-yang-gagal-resiko-tersebut-adalah-inherent-risk-control-risk-detection-risk-audit-gagal-mendeteksi-kerugian/. (Di akses 8 April 2020).

2. hanggary yudha 2012. Resiko audit. https://hanggaryudha.wordpress.com/2012/11/06/risiko-audit/ (Di akses 8 April 2020)

3. http://maksi.febulm.ac.id/index.php/info-kampus/artikel-paper-jurnal-akuntansi/item/47-audit-sistem-informasi-dan-penggunaannya (Di akses 8 April 2020)

M. ANGGA OKTAHARISETIA

182420123 – MTI2A1 – IT AUDIT

IT AUDIT

Information Technology (IT) audit atau information systems (IS) audit) adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi 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 teknologi informasi 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 menurut Ron Webber (Dekan Fakultas Teknologi Informasi, Monash University) dalam bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

- Kerugian akibat kehilangan data.
- Kesalahan dalam pengambilan keputusan.
- Resiko kebocoran data.
- Penyalahgunaan komputer.
- Kerugian akibat kesalahan proses perhitungan.
- Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and

Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

1. Contoh

JAKARTA – Masyarakat resah melihat kasus pembobolan dana nasabah di bank yang intensitasnya meningkat sejak awal 2011. Kasus-kasus yang terjadi dalam rentang waktu berdekatan ini pun berdampak pada makin kurangnya kepercayaan publik terhadap perbankan.

Dengan begitu, pengamat perbankan Mirza Adityaswara mengatakan, masyarakat akan lebih berhati-hati menggunakan layanan perbankan setelah mencuatnya kasus-kasus yang terjadi. “Masyarakat yang semula kurang awas, akan lebih waspada,” katanya, Ahad (2/5).

Mirza berpendapat sistem perbankan yang ada saat ini memang belum sempurna. Ini, jelas dia, bukan hanya terlihat dari sisi pegawai bank, melainkan juga nasabah. “Jangan tergoda melakukan penyelewengan,” katanya.

Tony Prasetyantono, pengamat perbankan, mengatakan berkurangnya kepercayaan publik pasti akan terjadi menyusul berbagai kasus tersebut. Namun, nasabah belum sampai pada satu tindakan menarik uangnya besar-besaran. Karena, jelas Tony, nasabah tidak memiliki pilihan lain yang lebih baik untuk menempatkan uangnya.

Sejauh ini, ujar Tony, bank masih dinilai sebagai tempat terbaik menyimpan aset. “Apalagi yang bersifat likuid, seperti rekening giro dan tabungan,” katanya. “Namun, nasabah akan lebih se-lektif memilih bank.”

Nasabah, lanjut dia, juga akan lebih memantau rekeningnya agar luput dari pembobolan. Tony menilai, kejahatan perbankan yang terjadi belakangan lebih mengarah pada kesalahan kolektif. Penyebabnya, ia menjelaskan, muncul dari sisi perbankan, nasabah, Bank Indonesia, maupun aturan hukumnya.

Tony mencontohkan, bank kerap menyembunyikan penyimpangan karena takut reputasinya rusak, sedangkan nasabah tidak aktif memantau rekening miliknya. Sementara, BI memiliki keterbatasan dalam memantau banyaknya perbankan yang ada di Tanah Air. “Hukuman terhadap pelaku fra ud juga ku-rang maksimal sehingga kurang menimbulkan efek jera,” jelasnya.

Saat ini. Direktorat Kriminal Khusus (Ditkrimsus) Polda Metro Jaya sedang menangani sembilan kasus perbankan sejak Januari 2011. Bulan lalu, dana deposito milik PT Elnusa Rp 111 miliar di Bank Mega dicairkan tanpa seizin manajemen perusahaan tersebut dengan pelaku melibatkan orang dalam bank. Sebelumnya, simpanan nasabah prioritas Citibank dibobol oleh karyawan bank asing tersebut yang bernama Inong Malinda alias Malinda Dee.

Kepala Bidang Humas Polda Metro Jaya Kombes Baharudin Djafar mengatakan, kasus pembobolan bank tak ha-nya terjadi di bank swasta. Menurutnya, akhir pekan lalu, bank milik negara pun tak luput dari jarahan oknum pegawainya yang nakal. Dari sembilan kasus perbankan itu, polisi berhasil menangkap 30 tersangkanya.

Kasat Fiskal, Moneter, dan Devisa Ditkrimsus Polda Metro Jaya AKBP Arismunandar menambahkan, kasus pembobolan dana perbankan biasanya melibatkan orang dalam bank. Sementara itu, Corporate Secretary BSB, Evi Yulia Kurniawati, mengatakan pihaknya menjalankan tata tertib sesuai standar dan memperketat kontrol internal agar terhindar dari kejahatan perbankan.

2. Referensi

Berikut ini merupakan sumber referensi.

- Fanani, M. F. (2012, September 24). *Implementasi COBIT Di PT PERTAMINA*. Retrieved November 27, 2012, from http://www.slideshare.net: http://www.slideshare.net/fananifaiz/cobit-pertamina#btnNext
- Herawan, R. (2012, April 4). *Implementasi COBIT pada PT Transindo*. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/
- Meidyanto, Riky (2009, Juni 19). *Audit Sistem Informasi dengan Menggunakan COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 27, 2012, from http://krikkrikx.blog.binusian.org: http://www.krikkrikx.blog.binusian.org/files/2009/06/untuk-blog221.doc
- Susanto, Erdi (2012, November). *Kerangka Kerja COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 28, 2012, from http://erdi-susanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobit-control-objectives.html
- Wibowo, M. P. (2008, Agustus 9). *Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective For Information And Related Technology): Studi Kasus Di Perpustakaan Universitas Indonesia*. Retrieved November 27, 2012, from http://sangprabu.multiply.com: http://sangprabu.multiply.com/journal/item/27

- Wikipedia. *COBIT*. Retrieved November 27, 2012, from http://www.wikipedia.org: http://en.wikipedia.org/wiki/COBIT
- https://dendyoktavianto23.wordpress.com/2017/10/09/studi-kasus-audit-teknologi-informasi/

IT AUDIT

Dosen Pengampu : Dr. Widya Cholil , S.Kom., M.I.T.

JENIS RESIKO YANG MENJADI FAKTOR UTAMA SEHINGGA PERLU ADANYA IT AUDIT

Nama : Masroni Dedi Kiswanto

NIM : 182420139

Kelas : MTI Reguler B

PROGRAM PASCASARJANA

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

Tahun 2020

JENIS RESIKO YANG MENJADI FAKTOR UTAMA SEHINGGA PERLU ADANYA IT AUDIT

Teknologi Informasi (TI) di sebuah organisasi berperan mendukung pencapaian tujuan organisasi. Untuk mencapai tujuan tersebut maka perlu dipastikan adanya keselarasan (IT Alignment) antara Arsitektur Teknologi Informasi dengan visi dan misi organisasi tersebut. Proses manajemen strategik teknologi informasi dapat dimanfaatkan untuk memahami berbagai kekuatan kompetitif dan mengembangkan keunggulan kompetitif secara sistematis, konsisten, dan berkesinambungan sejalan dengan kecenderungan pada kompetisi baru berdasarkan perkembangan teknologi dan globalisasi.

IT Strategic/Master Plan merupakan sebuah rencana induk bagi Teknologi Informasi sebuah organisasi yang sangat diperlukan guna menjamin Teknologi Informasi dan implementasinya dapat benar- benar optimal mendukung pencapaian tujuan strategis jangka panjang organisasi tersebut. Salah satu kegiatan yang terdapat pada IT Strategic adalah Audit IT. Dalam melaksanakan audit Teknologi Informasi terdapat berbagai tools yang sudah siap digunakan saat ini. Tools tersebut dikembangkan dan distandarisasikan oleh berbagai badan di dunia. Standard tools tersebut dikembangkan sebagai framework yang disusun berdasarkan best pratices dari hasil riset serta pengalaman bertahun-tahun dalam kegiatan audit Teknologi Informasi . Framework tersebut tentunya mengalami penyempurnaan yang berkelanjutan sebagai upaya menciptakan standar yang semakin baik, efektif dan efisien. standard tools/framework yang banyak digunakan di dunia diantaranya adalah: COBIT® (Control Objectives for Information and related Technology), COSO (Committee of Sponsoring Organisations of the Treadway Commission) Internal Control—Integrated Framework, FIPS PUB 200, PRINCE2, PMBOK, TickIT, CMMI,TOGAF 8.1, IT Baseline Protection Manual. Diantara framework yang banyak digunakan, yang paling popular dan sering ditemukan adalah COBIT.

CONTOH KASUS IT AUDIT PT. BANK SYARIAH MANDIRI CABANG DENPASAR

Setelah dilakukan penelitian audit TI yang dilakukan di PT. Bank Syariah Mandiri cabang Denpasar, ada beberapa kesimpulan yang dapat diambil adalah sebagai berikut : a. Tata kelola TI PT. Bank Syariah Mandiri cabang Denpasar sudah dilakukan walaupun masih belum berjalan secara optimal karena belum mencapai pada tingkat kematangan yang diharapkan yaitu level 3 (Perusahaan telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari). b. Maturity Level yang ada pada setiap proses TI yang terdapat dalam domain Deliver and Support (DS) rata-rata berada pada level 2 (Perusahaan telah memiliki pola yang berulangkali dilakukan dalam melakukan manajemen aktivitas terkait dengan pengelolaan TI, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi

SUMBER :

[1] IT Governence Institute 2007. IT Governence Roundtable: IT Governence Trends

[2] Kim, 1999. A Report of the American collage of cardiology/American Heart Association Task Force on Prectice Guidelines (Commite to update the 1999Guideline for Coronery Artery bypass Graft Surgery)

[3]. Dajtmiko, Bambang. 2007. Audit Sistem Informasi Untuk Menilai Proses Penyampaian dan Dukungan (Delivery and Support) Dalam Pelayanan Informasi Dengan Menggunakan Framework COBIT Studi Kasus : PT. Telekomunikasi Indonesia, Tbk. R&D Center. Program Magister Informatika, Sekolah Tinggi Elektro dan Informatika Institut Teknologi Bandung.
[4]. Riasetiawan, Mardhani. 2007. Pembuatan Pedoman Tata Kelola Teknologi Informasi Menggunakan IT Governance Design Framework Pada UGM. Program Studi Magister Teknologi Informasi, Jurusan Teknik Elekto Yogyakarta.

[5]. Solikin. 2004. Pengelolaan Informasi Sekolah Tinggi Manajemen Informatika dan Komputer "AMIK BANDUNG. Program Magister Sistem Informasi, Departemen Teknik Informatika Institut Teknologi Bandung.

[6]. Sarno, Riyanarto., 2009. Audit Sistem dan Teknologi Informasi. Cetakan pertama. Surabaya: ITS Press.

Nama : Mefta Eko Saputra
Nim. : 182430113
Kelas : MTI 20A
Study : IT Audit

RESIKO YANG TERJADI DI PERUSAAN DALAM PENERAPAN SISTEM INFORMASI

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi key-enabler (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi stakeholders. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan. Di lain pihak, seiring makin meluasnya implementasi sistem informasi maka kesadaran akan perlunya dilakukan review atas pengembangan suatu sistem informasi semakin meningkat. Kesadaran ini muncul karena munculnya berbagai kasus yang terkait dengan gagalnya sistem informasi, sehingga memberikan akibat yang sangat mempengaruhi kinerja organisasi.

Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:

1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.
2. Melonjaknya biaya pengembangan sistem informasi karena adanya “scope creep” (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Mengingat adanya beberapa resiko tersebut diatas yang dapat memberikan dampak terhadap kelangsungan organisasi maka setiap organisasi harus melakukan review dan evaluasi terdapat pengembangan sistem informasi yang dilakukan. Review dan evaluasi ini dilakukan oleh internal organisasi ataupun pihak eksternal organisasi yang berkompeten dan diminta oleh organisai. Kegiatan review dan evaluasi ini biasanya dilakukan oleh Auditor Sistem Informasi. Selain wawasan, pengetahuan dan ketrampilan diatas seorang spesialis audit sistem informasi juga dituntut memenuhi syarat akreditasi pribadi terkait suatu sistem sertifikasi kualitas yang diakui secara internasional. Salah satu sertifikasi profesional sebagai standar pencapaian

prestasi dalam bidang audit, kontrol, dan keamanan sistem informasi yang telah diterima secara internasional adalah CISA® (Certified Information Systems Auditor) yang dikeluarkan oleh ISACA (Information Systems Audit and Control Association). Audit sistem informasi dilakukan untuk menjamin agar sistem informasi dapat melindungi aset milik organisasi dan terutama membantu pencapaian tujuan organisasi secara efektif.

Contohnya :

Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (*IT Governance*) (Herawan, 2012).

Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi. COBIT (*Control Objectives for Information and Related Technology*) adalah standar internasional untuk tata kelola TIyang dikembangkan oleh ISACA (*Information System and Control Association*) dan ITGI (*IT Governance Institute*) yang bisa dijadikan model pengelolaan TI mulai dari tahap perencanaan hingga evaluasi.(Wibowo, 2008).

DAFTAR PUSTAKA

Fanani, M. F. (2012, September 24). *Implementasi COBIT Di PT PERTAMINA*. Retrieved November 27, 2012, from http://www.slideshare.net: http://www.slideshare.net/fananifaiz/cobit-pertamina#btnNext

Herawan, R. (2012, April 4). *Implementasi COBIT pada PT Transindo*. Retrieved 11 27, 2012, from http://dosenindonesia.wordpress.com: http://dosenindonesia.wordpress.com/tag/cobit/

Meidyanto, Riky (2009, Juni 19). *Audit Sistem Informasi dengan Menggunakan COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 27, 2012, from http://krikkrikx.blog.binusian.org: http://www.krikkrikx.blog.binusian.org/files/2009/06/untuk-blog221.doc

Susanto, Erdi (2012, November). *Kerangka Kerja COBIT (Control Objectives For Information And Related Technology)*. Retrieved November 28, 2012, from http://erdi-susanto.blogspot.com: http://erdi-susanto.blogspot.com/2012/11/kerangka-kerja-cobit-control-objectives.html

Wibowo, M. P. (2008, Agustus 9). *Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective For Information And Related Technology): Studi Kasus Di Perpustakaan Universitas Indonesia*. Retrieved November 27, 2012, from http://sangprabu.multiply.com: http://sangprabu.multiply.com/journal/item/27

Wikipedia. *COBIT*. Retrieved November 27, 2012, from http://www.wikipedia.org: http://en.wikipedia.org/wiki/COBIT