PERTEMUAN 8

PENGAMANAN INFORMASI BERBASIS KOMPUTER

A. CAPAIAN PEMBELAJARAN

Di Pertemuan 8, kali inimaterinya mencakup tentang pengamanan informasi berbasis computer, dan anda harus mampu:

1. Menguraikan pengertian, tujuan, dan cakupan pengawasan umum.
2. Menjelaskan secara komprehensif jenis-jenis pengawasan umum yang dapat diterapkan pada perusahaan.
3. Menjelaskan pengertian, tujuan dan cakupan pengawasan aplikasi.
4. Menguraikan cara-cara pengawasan terhadap input.
5. Menguraikan secara komperhensif cara cara pengawasan terhadap proses.
6. Menguraikan cara-cara pengawasan terhadap output

B. URAIAN MATERI

1. Pengertian, tujuan, dan cakupan pengawasan umum

Saat ini, informasi telah menjadi aset penting. Beberapa orang berpikir kita sudah berada dalam "*information-based society*". Bisnis, universitas, instansi pemerintah, dan individu mengandalkan kemampuan untuk mengakses dan menyediakan informasi secara cepat dan efisien.

Berdasarrkan *Survey Information Week* (USA), 1271 *system or network manager* "hanya 22% yang menganggap keamanan sistem informasi sebagai komponen penting". Maka dari itu rendahnya tingkat kesadaran akan masalah keamanan.

April 1617, 2004, Dani (seorang hacker konsultan IT), menyerang sistem pertahanan situs KPU, memperbarui tabel nama-nama partai dan mengacak-acak jumlah suara (dikali 10). Nama-nama peserta pemilu diubah karena menimbulkan kehebohan di negeri ini.Yang jelas Dani diduga melakukan hal itu secara iseng dengan mengganti nama parpol baru.

Tahun 2009, seorang hacker berhasil meretas situs resmi Kabupaten Ngajuk. situs tersebut diretas dengan konten video porno.

Pada tahun 2009, website Kementerian Komunikasi dan Informatika (Depkominfo) yang merupakan salah satu subdomain Kementerian Komunikasi dan Informatika yang beralamat www.ecom.depkominfo.go.id diketahui memiliki web security yang lemah. sistem. Jika Anda memasuki situs, sebuah pesan akan muncul:

"Dengan ini kami beritahukan bahwa *security web* ini masih sangat lemah. Mohon untuk diperiksa kembali." tulis hacker dalam jejak yang ditinggalkannya di situs Depkominfo.

Meningkatnya jumlah kejahatan komputer (*computer crime),*dikarenakan beberapa halterutama yang berhubungan dengan sistem informasi, antara lain:

a. Semakin meningkatnya aplikasi bisnis yang menggunakan (berbasis) teknologi informasi dan jaringan computer.
b. Banyak sistem yang perlu dikelola, dan itu membutuhkan operator dan administrator yang lebih efektif. Memang, sangat rumit untuk menemukan operator dan administrator yang andal.
c. Sulit ditanganinya masalah *interoperability* antar *vendor* dan banyaknya Transisi dari *single vendor* ke *multi vendor* yag harus dimengerti.
d. Banyaknya pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakan, sehingga tingkat kemampuan pemakai di bidang komputer menjadi meningkat.
e. Sulitnya mengejar kemajuan di dunia komputer dan telekomunikasi, yang sangat cepat dilakukan oleh lembaga penegak hukum
f. Sistem yang digunakan semakin kompleks, misalkan "semakin besarnya program (*source code)* yang digunakan sehinggasemakin besar probabilitas terjadinya lubang keamanan".
g. Semakin banyak perusahaan menggunakan sistem informasi mereka, yang terhubung ke jaringan komputer global, seperti Internet. Dengan sistem informasi yang dibobolnya, potensi sistem informasi semakin besar.

Mungkinkah Aman?

- Sangat sulitnya tercapai 100% aman
- Adanya timbal balik antara keamanan vs. kenyamanan (*security vs convenience*).

a. Definisi *Computer Security*

Definisi *Computer Security* menurut Garfinkel & Spafford *"A computer is secure if you can depend on it and its Software to behave as you expect".* Sedangkan menurut G. J. Simons "Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating)* atau, paling tidak, mendeteksiadanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik".

Jika kita memiliki sistem keamanan yang kuat, maka selalu ada pencegahan dari virus, hacker, dan cracker. Ketika berbicara tentang masalah keamanan sistem informasi, risiko keamanan sistem mungkin muncul.

Dua (2) masalah utama keamanan sistem yaitu :

1) Terdapat *Threats* (Ancaman) pada sistem dan
2) *Terdapat Vulnerability* (Kelemahan) pada sistem

Enam(6) hal utama dalam system informasi yang berdampak dari masalah tersebut yaitu

1) Efektifitas
2) Efisiensi
3) Kerahasiaan
4) Integritas
5) Keberadaan (availability)
6) Kepatuhan (compliance)
7) Keandalan (reliability)

Adapun kriteria 10 domain keamanan yang perlu di perhatikan dalam masalah keamanan yaitu :

1) Penggunaan akses kontrol sistem
2) Telekomunikasi dan jaringan yang dipakai
3) Pemakaian manajemen praktis
4) Penggunaan sistem aplikasi yang dikembangkan
5) *Cryptographs* yang diterapkan
6) Penerapan sistem informasi untuk arsitektur
7) Pengoperasian yang ada
8) *Busineess Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP)
9) Penerapan kebutuhan Hukum, bentuk investigasi dan kode etik
10) Tata letak fisik dari sistem yang ada

b. Ancaman (*Threats*)

Ancaman merupakan aksi yang dapat mengganggu keseimbangan sistem informasi di dalam dan di luar sistem. Tiga (3) hal yang utama dari ancaman yang dapat timbul dari pengolahan informasi, yaitu:

1) Ancaman berasal dari Alam
2) Ancaman berasal dari Manusia
3) Ancaman berasal dari Lingkungan

c. Kelemahan (*Vurnerability*)

Kelemahan adalah tidak kuatnya pertahanan pada suatu sistem yang dapat muncul pada saat perancangan, definisi proses, implementasi, atau kelemahan pada sistem kendali yang ada, hal ini menyebabkan pelaku sistem untuk masuk. Cacat sistem dapat terjadi pada prosedur, peralatan atau perangkat lunak yang dimiliki. Yang bisa terjadi adalah: Setting Firewall yang membuka Telnet untuk diakses dari luar, atau Setting VPN yang tidak diikuti oleh aplikasi Kerberos atau NAT.

Tiga (3) pendekatan keamanan sistem informasi, yaitu:

1) Pendekatan preventif berguna untuk mencegah kemungkinan ancaman dan kelemahan yang terjadi
2) Pendekatan investigasi berguna untuk mendeteksi intrusi dan proses yang memodifikasi sistem dari keadaan normal ke keadaan tidak normal

3) Pendekatan korektif berguna untuk kembali normal jika keadaan sistem tidak seimbang ketika dikoreksi.

2. Pengawasan Umum yang dapat diterapkan pada Perusahaan

a. Pengendalian Keamanan Sistem Informasi

Berkaitan dengan keamanan sistem informasi, perlu dilakukan tindakan berupa pengendalian sistem informasi. Kontrol keamanan sistem informasi meliputi:

1) Kontrol administratif
2) Kontrol pengembangan dan pemeliharaan sistem
3) Kontrol operasional
4) Perlindungan fisik pusat data
5) Kontrol perangkat keras
6) akses ke sistem komputer
7) Kontrol akses informasi
8) Pengendalian bencana
9) Pengendalian perlindungan akhir
10) Pengendalian aplikasi

Tabel 8.2 Contoh Pengendalian Keamanan Sistem Informasi

Kontrol	Contoh
Preventif	- Gunakan salinan bersih perangkat lunak atau file yang mengandung makro - Hindari penggunaan Perangkat lunak freeware atau shareware dari sumber yang tidak dapat dipercaya - Hindari mengambil file yang berisi

	makro dari mana saja - Periksa program atau file baru yang berisi makro dengan perangkat lunak antivirus sebelum digunakan - Meningkatkan kewaspadaan terhadap virus untuk pengguna
Detektif	- Menjalankan secara rutin program anti virus untuk mendeteksi infeksi virus - untuk mendeteksi perubahan ukuran pada berkas dapat melakukan perbandingan ukuran-ukuran berkas - Untuk mendeteksi perubahan tanggal file, Anda dapat membandingkan tanggal file
Korektif	- Pastikan cadangan bersih - Memiliki rencana pemulihan virus yang terdokumentasi - Untuk menghapus virus dan program yang terinfeksi dapat menjalankan program antivirus

b. Terdapat 4 Prinsip Keandalan system

1) Availability, saat dibutuhkan sistem tersedia.
2) Keamanan adalah fitur utama dari sistem.
3) Dapat dipertahankan, jika perlu sistem dapat dimodifikasi tanpa mempengaruhi ketersediaan, keamanan, dan integritas sistem.
4) Integritas, pemrosesan sistem yang lengkap, akurat, tepat waktu dan resmi.

c. Cara- cara pengawasan terhadap input

1) Ancaman terhadap SIA

Bencana alam dan politik merupakan salah satu ancaman yang dihadapi oleh perusahaan, seperti:

a) Kebakaran atau panas yang berlebihan

b) Banjir, gempa bumi

c) Badai angin dan perang

2) Ancaman kesalahan perangkat lunak dan malfungsi peralatan , seperti:

a) Kegagalan perangkat keras

b) Kesalahan atau kerusakan perangkat lunak, kegagalan sistem operasi, gangguan listrik dan fluktuasi.

c) Serta kesalahan transmisi data yang tidak terdeteksi

3) Ancaman terhadap perusahaan karena tindakan yang tidak disengaja, seperti:

a) Kecelakaan yang disebabkan oleh kelalaian manusia

b) Kesalahan yang tidak disengaja karena kecerobohan

c) Kehilangan atau kerugian

d) Kesalahan logis

e) Sistem tidak memenuhi kebutuhan perusahaan

4) Ancaman perusahaan dari tindakan jahat, seperti:

a) sabotase

b) Penipuan komputer

c) Penggelapan

3. Pengendalian Internal

a. Definisi dari pengendalian internal

Pengendalian internal adalah strategi bisnis yang digunakan untuk menjaga aset, memberikan informasi yang akurat dan andal, mendorong dan

meningkatkan efisiensi operasi organisasi, dan mendorong kepatuhan terhadap kebijakan yang ditetapkan.

b. Komponen Pengendalian

Menurut COSO ada lima Komponen pengendalian intern yaitu :

1) *Control envirenment* atau lingkungan pengendalian
2) *Control activities* atau kegiatan pengawasan
3) *Risk Assessment* atau pemahaman resiko
4) *Information and communication* atau informasi dan komunikasi
5) *Monitoring* atau pemantauan

Penelitian oleh *Information Systems Audit and Control Foundation*

1) *Information Systems Audit and Control Foundation (ISACF) mengembangkan Control Objectives for Information and related Technology (COBIT)*.
2) COBIT, yang mengkosolidasi standar dari 36 sumber berbeda ke dalam satu kerangka, memberikan dampak yang besar atas profesi sistem informasi.

Berdasarkan 3 poin atau dimensi, kerangka tersebut menangani isu pengendalian yang menguntungkan, yaitu :

1) Tujuan bisnis, Agar tujuan bisnis terpenuhi, kriteria informasi harus sesuai dengan COBIT sebagai persyaratan bisnis atas informasi.
2) Sumber daya IT, Sumber daya IT meliputi: orang, sistem aplikasi, teknologi, fasilitas, dan data.
3) Proses TI, adalah proses yang digunakan untuk mengelola proyek TI. Proses TI dibagi menjadi empat bidang, yaitu: perencanaan dan organisasi, proses akuisisi dan implementasi, pengiriman dan dukungan, dan pemantauan.

c. Lingkungan Pengendalian

Faktor-faktor lingkungan pengendalian terdiri atas:

1) Komitmen atas integritas dan nilai-nilai etika
2) Filosopi hak manajemen dan gaya beroperasi

3) Struktur organisasional

4) Badan audit dewan komisaris

5) Metode untuk memberikan otoritas dan tanggungjawab

6) Kebijakan dan praktik-praktik dalam sumberdaya manusia

7) Pengaruh-pengaruh eksternal

d. Kegiatan dalam Pengendalian

Secara umum kategori prosedur-prosedur pengendalian kegiatan dibagi menjadi lima, antara lain:

1) Otorisasi transaksi dan kegiatan yang memadai

2) Pemisahan tugas

3) Desain dan penggunaan dokumen serta catatan yang memadai

4) Penjagaanasetdancatatanyang memadai

5) Pemeriksaan indepen den atas kinerja.

4. Pengawasan terhadap output (Resiko)

Jenis-jenis ancaman yang dihadapi perusahaan, ialah:

a. Salahnya melakukan hal strategis

b. Operasi melakukan hal yang benar, tetapi dengan cara yang salah, tanpa banyak keberhasilan.

c. Ada kerugian finansial, pemborosan, pencurian, atau kewajiban yang tidak semestinya atas sumber daya keuangan

d. Salahnya menerima informasi atau tidak relevan, tidak andalnya sistem, dan laporan yang tidak benar atau menyesatkan.

a. Informasi dan Komunikasi

Seorang Akuntan harus memahami berikut ini:

1) Bagaimana awalnya transaksi

2) Mesin membaca data dalam bentuk yang dapat diproses

3) Bagaimana mengakses dan memperbaharui file komputer

4) Bagaimana mempersiapkan data yang diproses untuk sebuah informasi

5) Bagaimana melaporkan informasi

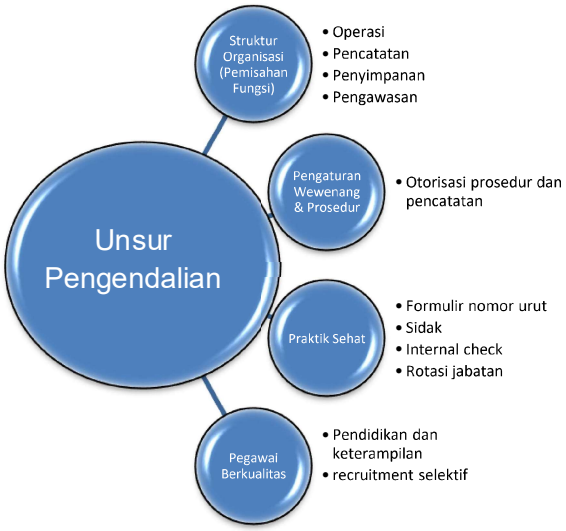
6) Bagaimana berakhirnya transaksi

Metode utama untuk mengawasi kinerja mencakup:

1) Supervisi yang efektif

2) Pelaporanyang bertanggung jawab

3) Audit internal



Gambar 8.1 Struktur dalam Unsur Pengendalian

Kesimpulan :

Pengendalian sistem informasi berbasis computer meliputi pengendalian umum dan pengendalian aplikasi. Kontrol umum adalah kontrol yang diterapkan dalam lingkungan pengolaan data.

Tujuan dari pengendalian global adalah untuk memastikan bahwa kegiatan pengolahan data dilakukan dengan lancar dan sesuai rencana. Ruang lingkup pengendalian umum adalah pembuatan rencana keamanan, Fungsi SIA dipisahkan menjadi empat bagian yang terpisah: kontrol akses fisik, kontrol akses logis, kontrol akses pengarsipan data, dan kontrol transfer data. Standar dokumentasi dan

minimalisasi sistem informasi juga dibahas. Waktu henti, rencana perbaikan kerusakan, perlindungan komputer dan jaringan, dan kontrol internet. Penilaian keamanan tidak hanya tentang terjadinya masalah, tetapi juga pada berbagai aspek pada sistem itu sendiri.

C. LATIHAN SOAL

1. Secara umum apa pengertian pengendalian intern?
2. Sebutkan 3 dari 5 komponen model pengendalian internal COSO! Jelaskan secara singkat 3 komponen yang Anda sebutkan!

D. DAFTAR PUSTAKA

Bodnar., George H. and William S. Hopwood (2005), Sistem Informasi Akuntansi, 9th ed Andi Yogyakarta.

Hall, A James (2004), Accounting Information System, 4th ed., South Western Publising Co.

Krismiaji (2002), Sistem Informasi Akuntansi. Yogyakarta: Unit Penerbit dan Percetakan AMP YKPN.

Marshall., Romney B. dan Steinbart John Paul Steinbart (2005), Accounting Information *System*, 9th ed Salemba Empat Jakarta.