Al-Buhuts e-Journal
On Line ISSN : 2442-823X
Print ISSN : 1907-0977
Volume 17 Nomor 2, Desember 2021

Konsep Pengendalian Intern Untuk Keamanan Sistem Informasi

Sayuthi
Doctoral Student of Accountancy Department at Padjajaran University, Bandung, and Lecturer at Universitas Syiah Kuala
sayuthisiem@gmail.com
sayuthi_siem@unsyiah.ac.id

Abstract: The purpose of this article is to determine the concepts of good control to be applied in a corporate organizational environment. Based on several concepts offered, the control based on Sarbanes-Oxley and Internal Control (COSO Framwork) is still highly recommended by experts. This is because the control concept of this model has adopted all existing aspects of protection, both physical and non-physical. However, security protection for information systems should ideally be focused on access control and IT control. There are three groups of individuals who differ in their normal ability to access hardware, namely; 1) Personal computer systems, which often pose a potential bottleneck because they often have special access to important data and programs. 2) Users, they have narrower access, but they still have the opportunity to commit embezzlement. 3) The intruders, they do not have access at all, but they are often people who have the ability to interfere with company information systems. As for controlling passive threat, it is highly recommended to use back up data, either full back up or incremental back up. And one of the back up systems can use cloud systems /cloud computing.

Keywords: access control, IT control, personal computers, users, intruders

A. PENDAHULUAN

Era globalisasi mengakibatkan perubahan yang begitu cepat dalam bidang teknologi dan informasi. Pemrosesan data dari sistem manual telah berubah menjadi sistem berbasis komputer (*computerise).* Begitu juga dalam hal akses dari suatu tempat ke tempat lain, semua sudah berubah secara komputer dan internet (*internet of thing = IoT*). Teknologi informasi saat ini jauh lebih cepat dan flexibel, serta menyediakan informasi yang begitu banyak.

Namun demikian kecanggihan teknologi informasi yang terus berkembang ternyata memiliki dampak lain yang menjurus ke arah negatif. Dengan keterbukaan akses yang begitu luas dan tanpa batas, terkadang hal-hal privasi suatu individu maupun kelompok menjadi terusik dimana terdapat hal-hal yang tidak semestinya terekspose ke pihak luar dan merugikan pihak lain. Oleh sebab itu pengguna maupun penyedia informasi harus memikirkan bagaimana

mengamankan informasi yang dihasilkan dan juga yang akan diterima. Keterbukaan ini pada akhirmya mengakibatkan para penyedia informasi harus memikirkan bagaimana mengamankan informasi yang ada dan juga informasi yang dihasilkan tersebut. Pengamanan sistem informasi ini pun akhirnya juga harus mengimplementasikan teknologi. Namun demikian hal ini tidaklah menjamin bahwa informasi yang dihasilkan tersebut sudah bebas dari orang-orang yang tidak bertanggung jawab. Seorang *hacker* maupun *cracker* selalu tertantang untuk membobol suatu situs yang menyediakan rahasia-rahasia besar yang menimbulkan kecemasan bagi sebagian pihak. Apa yang terjadi dalam kasus *wikileaks dan sony picture* belakangan ini adalah salah satu contoh nyata.

Pengamanan sistem informasi adalah hal yang mutlak diperlukan dan harus terus dievaluasi keefektifannya. Hall (2011) menyebutkan, berdasarkan Forester Researh, perusahaan dapat menghabiskan banyak sekali anggara keamanan dalam tiga erea utama; *enkripsi data otentikasi digital, dan firewall*. Pengorbanan yang dilakukan perusahaan bertujuan untuk bagaimana sistem informasi yang ada di perusahaan tetap aman dan terpercaya, sehingga tidak menimbulkan masalah-masalah dikemudian yang menyebabkan perusahaan dituntut oleh para pelanggan atau pihak tertentu.

Hall (2011)memberikan suatu ilustrasi yang menyangkut dengan otentikasi digital, contoh, bagaimana pemasok mengetahui dengan pasti bahwa sebuah pesanan pembelian (pesan) untuk 1.000 unit produk yang dikirim oleh seorang pelanggan tidak dicegar oleh *hecker* selama masa transmisi, dan diubah hingga dibaca menjadi 100.000 unit. Jika kejadian tersebut tidak terdeteksi maka pemasok akan menanggung biaya tenaga kerja, bahan baku produksi, dan distribusi atas pesanan tersebut. Akhirnya akan timbul tuntutan hokum di antara kedua pihak yang sama sama tidak bersalah.

Begitu juga dengan kekhawatiran lain yang mungkin terjadi akibat pembobolan sistem, seperti banyak terjadi pada lembaga perbankan. Kita juga tidak sanggup membayangkan dengan era teknologi dan informasi sekarang ini, penipuan dengan teknologi banyak terjadi.

Kita tidak sanggup membayangkan kerugian yang dialami oleh sebuah organisasi yang mempunyai sistem informasi manajemennya sangat tidak aman bila dibobol oleh orang-orang yang tidak bertanggung jawab. Tidak hanya kerugian di bidang materiil tapi kerugian non materil sangat besar akan ditanggung. Oleh sebab itu penulisan artikel ini dipandang sangat perlu untuk dilakukan mengingat keamanan sistem informasi di perusahaan perlu mendapatkan perhatian yang serius dari pihak manajemen puncak.

B. LANDASAN TEORI

Keamanan Sistem Informasi

Menurut Hall (2011), *Computer security is an attempt to avoid such undesirable events as a loss of confidentiality or data integrity. Security systems attempt to prevent fraud and other misuse of computer systems; they act to protect and further the legitimate interests of the system's constituencies*. (Keamanan komputer adalah upaya untuk menghindari kejadian yang tidak diinginkan seperti hilangnya kerahasiaan atau integritas data. Sistem keamanan berusaha untuk mencegah penipuan dan penyalahgunaan sistem komputer lainnya).

Hal senada dikemukan oleh Bodnar (2000), menyebutkan "Sistem keamanan komputer merupakan subsistem organisasi yang mengendalikan risiko-risiko khusus yang berkaitan dengan sistem informasi berdasar komputer. Sistem keamanan komputer memiliki elemen-elemen dasar sistem informasi, seperti perangkat keras, basis data, prosedur, dan laporan. Komputer merupakan sebuah contoh dari bahagian perangkat keras. Sistem keamanan komputer tidak hanya meliputi keamanan fisik tetapi juga menyangkut dengan keamanan non fisik."

Raggad (2010: 11) mengatakan keamanan sistem informasi harus dipahami dalam hal keamanan semua komponennya: keamanan brainware, keamanan kegiatannya, keamanan data, keamanan teknologi, dan keamanan jaringan. Selanjutnya Bagranoff, Simkin & Norman. (2010:380) mengatakan sebuah sistem keamanan terpadu, didukung oleh kebijakan keamanan yang komprehensif, dapat secara signifikan mengurangi risiko serangan karena meningkatkan biaya dan sumber daya yang dibutuhkan oleh penyusup.

Berdasarkan beberapa pengertian di atas maka disimpulkan bahwa sistem keamanan informasi (computer) adalah upaya untuk menghindari kejadian yang tidak diinginkan atau risiko-risiko khusus yang berkaitan dengan sistem informasi dan komponen-komponennya, seperti kehilangan data, kerahasiaan data atau integritas data.

Sistem Keamanan Komputer dalam Organisasi

Keamanan adalah parameter yang paling penting dan tidak dapat dihindari dalam sistem komputer di dunia saat ini (Chauhan, 2014: 509). Dengan peningkatan ketergantungan pada sistem online hari ini, ada peningkatan permintaan dari sistem keamanan. Teori keamanan sistem informasi dari Dhillon (1997), Todorov (2007), Raggad (2011), Kim & solomon (2012),

menyatakan bahwa keamanan sistem informasi merupakan kumpulan kegiatan yang melindungi sistem informasi dan data yang tersimpan di dalamnya, untuk melindungi aset dari ancaman. Efek dari pelanggaran keamanan bisa luas dan dapat menyebabkan hilangnya informasi, korupsi informasi, kesalahan informasi, pelanggaran privasi, *denial-of-service*, dan sebagainya (Chauhan, 2014: 510).

Stair dan Reynolds (2010) mengatakan bahwa, *to protect against threats to your privacy and data, you can install security and control measures* (untuk melindungi privasi dan data Anda dari ancaman, Anda dapat menginstal langkah-langkah keamanan dan control). Misalnya, banyak produk perangkat lunak yang dapat mendeteksi dan menghapus virus dan spam dari sistem komputer. Barclays, sebuah bank internasional, menggunakan perangkat otorisasi identitas genggam untuk mencegah penipuan bank. Perangkat baru ini akan membantu menghilangkan masalah nomor identifikasi dan kata sandi yang dicuri.

Dampak dari semua kejadian tersebut menyebabkan informasi dihasilkan menjadi tidak berkualitas. Bodnar (2000) menyebutkan, jika sistem kemanan komputer ingin efektif, maka harus dikendalikan oleh *Chief Security Officer* (CSO). Orang ini harus bertanggungjawab langsung kepada Dewan Komisaris untuk menjaga keutuhan independensinya. Tugas utama CSO adalah menyajikan laporan kepada Dewan Komisaris. Dengan demikian sebuah pusat penyediaan informasi harus mempunyai struktur organisasi, dan orang yang bertanggung jawab terhadap masalah keamanan informasi ini adalah CSO.

Tabel 1
Siklus Hidup dan Laporan CSO Kepada Dewan Komisaris

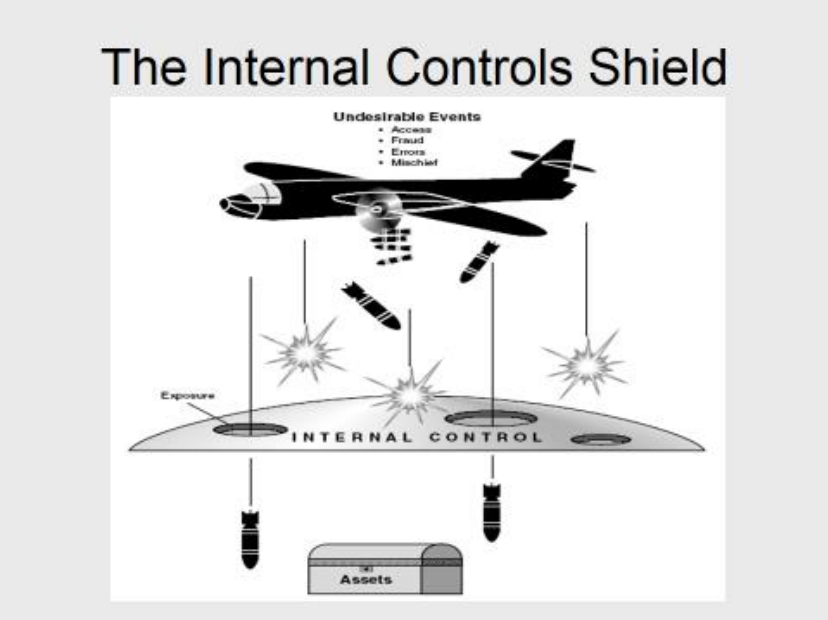
Tahap Siklus-Hidup	*Laporan kepada Dewan Komisaris*
Analisis Sistem	Ikhtisar seluruh kemungkinan kerugian yang relevan.
Perancangan Sistem	Rencana rinci untuk pengendalian dan pengorganisasian kerugian-kerugian, termasuk anggaran sistem keamanan kompute yang lengkap.
Implementasi Sistem Operasi Sistem, Evaluasi dan Pengendalian	Kekhususan-kekhususan pada kinerja sistem keamanan komputer, termasuk pengelompokkan kerugian-kerugian dan pelanggaran keamanan, analisis ketaatan, dan biaya operasi sistem keamanan.

Laporan kepada komisaris ini harus dibuat oleh CSO secara rutin, 3 atau 6 bulan sekali. Sehingga perkembangan pusat penyediaan data informasi dan komunikasi serta sistem keamanannya bisa terus dipantau oleh komisaris.

Konsep Pengendalian Internal

Hall (2011) menyatakan, *the internal control system comprises policies, practices, and procedures employed by the organization to achieve four broad objectives:*

1) *To safeguard assets of the firm.*
2) *To ensure the accuracy and reliability of accounting records and information.*
3) *To promote efficiency in the firm's operations.*
4) *To measure compliance with management's prescribed policies and procedures.*



Sumber: Hall (2011)

Dari gambar di atas dapat dijelaskan bagaimana lapisan pengendalian dapat ditembus karena adanya exposure-exposure yang diakibatkan oleh kelemahan pengendalian.

Menurut Loudon and Loudon (2014) *Sarbanes-Oxley is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in financial statements.* Karena sistem informasi digunakan untuk menghasilkan, menyimpan, dan mengangkut data tersebut, undang-undang mengharuskan perusahaan untuk mempertimbangkan keamanan sistem informasi dan kontrol lain yang diperlukan untuk memastikan integritas, kerahasiaan, dan keakuratan data mereka.

Hal senada dikemukan oleh Hall (2011) mengatakan, "prosedur manual memfasilitasi pemahaman aktivitas pengendalian internal, termasuk pemisahan fungsi, pengawasan, verifikasi independen, jejak audit, dan kontrol akses. Karena sifat manusia merupakan inti dari banyak masalah pengendalian internal, kita tidak boleh mengabaikan pentingnya aspek sistem informasi ini."

Untuk mencapai tujuan-tujuan tersebut ada beberapa konsep pengendalian internal yang diusulkan (Hall, 2011), yaitu:

1) *The Preventive–Detective–Corrective Internal Control Model*
2) *Sarbanes-Oxley and Internal Control*
3) *Control Activities*
4) *IT Contrrol*
5) *Physical Control*

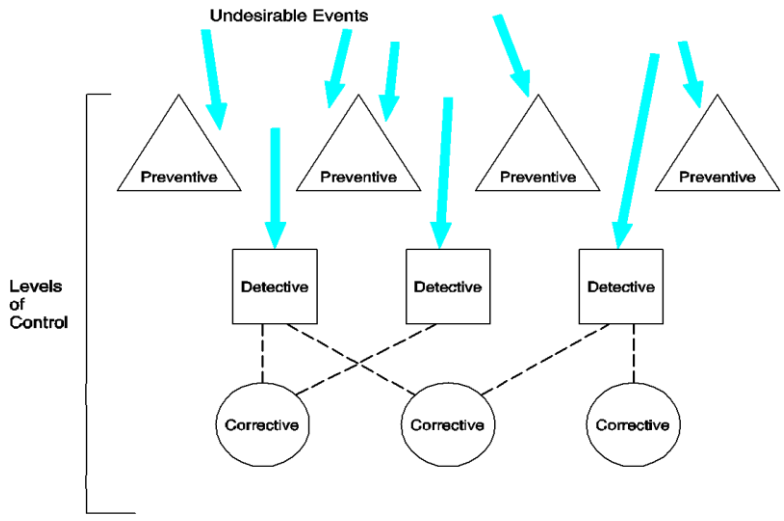
The Preventive–Detective–Corrective Internal Control Model

Preventive control merupakan pengendalian yang dilakukan sebelum sebuah peristiwa penyelewengan/fraud terjadi. Dengan demikian tindakan preventif ini akan meminimalkan biaya, karena tidak ada risiko apapun yang dialami oleh perusahaan.

Detective control merupakan pengendalian yang dilakukan ketika peristiwa penggelapan/penyelewengan sudah terdeteksi sehingga perusahaan perlu melakukan pembaharuan terhadap system informasi atau mengganti atau memberi sanksi pejabat atau oknum karyawan yang terlibat dalam peristiwa penggelapan tersebut.

Detective control merupakan pengendalian yang dilakukan ketika peristiwa penggelapan/penyelewengan sudah terjadi dan orang/karyawan/pejabat yang melakukan tersebut bisa saja sudah mengundurkan diri. Dengan kata lain, perusahaan sudah mengalami risiko akibat ulah pejabat/oknum karyawan tersebut. Penyelewengan ini terjadi bisa saja diakibatkan oleh kelalaian pengendalian di tahap pengendalian preventif dan pengendalian detektif.

Perbedaan ketiga pengendalian tersebut sebagaimana tampak digambar berikut ini.



Slumber: Hall (2011)

Menurut Romney dan Steinbart (2015), "*Internal control are the process implemented to provide reasonable assurance that the following control objectives are achieved. A process it permeates an organization's operating activities and is an integral part of management activities."*

Pengendalian atas sistem informasi sesungguhnya dengan perangkat keras dan lunak pada sistem computer. *Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do* (Sandhu S.Ravi and Samarati, 1994). Jadi kontrol akses dapat membatasi apa yang dapat dilakukan pengguna secara langsung, serta program apa yang dijalankan atas nama pengguna yang diizinkan untuk dilakukan. Dengan cara ini kontrol akses berusaha untuk mencegah aktivitas yang dapat mengakibatkan pelanggaran keamanan sistem informasi. Sedangkan Loudon and Loudon (2014) menyebutkan bahwa, Sarbanes-Oxley pada dasarnya adalah untuk memastikan bahwa pengendalian internal ada untuk mengatur pembuatan dan dokumentasi informasi dalam laporan keuangan. Karena sistem informasi digunakan untuk menghasilkan, menyimpan, dan mengangkut data tersebut, undang-undang mengharuskan perusahaan untuk mempertimbangkan keamanan sistem informasi dan kontrol lain yang diperlukan untuk memastikan integritas, kerahasiaan, dan keakuratan data mereka. Setiap aplikasi sistem yang menangani data pelaporan keuangan penting memerlukan kontrol untuk memastikan data tersebut akurat. Kontrol untuk mengamankan jaringan perusahaan, mencegah akses tidak sah ke sistem dan data, dan memastikan integritas dan ketersediaan data jika terjadi bencana atau gangguan layanan lainnya juga penting

Committee of Sponsoring Organization of The Treadway Commission (COSO) pada tahun 1992 mengeluarkan definisi tentang pengendalian internal. Definisi COSO tentang pengendalian intern sebagai berikut: *Internal control is process, affected by entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*

1. *Effectiveness and efficiency of operations*
2. *Reliability of Financial Reporting*
3. *Compliance with Applicable laws and regulations*

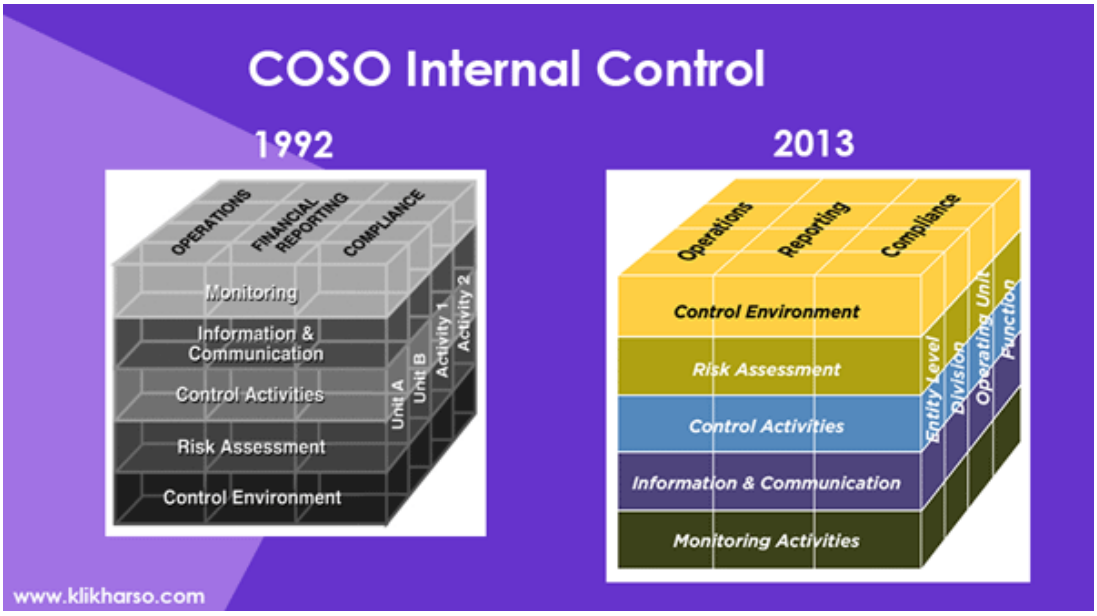
Jadi sistem pengendalian internal menurut COSO merupakan suatu proses yang melibatkan dewan komisaris, manajemen, dan personil lain, yang dirancang untuk memberikan keyakinan memadai tentang pencapaian tiga tujuan berikut ini:

1. Efektivitas dan efisiensi operasi
2. Keandalan pelaporan keuangan
3. Kepatuhan terhadap hukum dan peraturan yang berlaku).

Komponen-komponen pengendalian internal menurut COSO antara lain:

1) *A control environment* (lingkungan pengendalian). Merupakan tanggung jawab manajemen puncak untuk menyatakan dengan jelas nilai-nilai integritas dan kegiatan tidak etis yang tidak dapat ditoleransi.
2) *Risk assessment* (penaksiran risiko). Perusahaan harus mengidentifikasi dan menganalisis faktor-faktor yang menciptakan risiko bisnis dan harus menentukan bagaimana caranya mengelola resiko tersebut.
3) *Control activities* (kegiatan pengendalian). Untuk mengurangi terjadinya kecurangan, manajemen harus merancang kebijakan dan prosedur untuk mengidentifikasi resiko tertentu yang dihadapi perusahaan.
4) *Information and communication* (informasi dan komunikasi). Sistem pengendalian internal harus dikomunikasikan dan diinfokan kepada seluruh karyawan perusahaan dari atas hingga bawah.
5) *Monitoring* (pemantauan). Sistem pengendalian internal harus dipantau secara berkala. Apabila terjadi kekurangan yang signifikan, harus segera dilaporkan kepada manajemen puncak dan ke dewan komisaris.

   Namun pada tahun 2013 dan untuk menindaklanjuti rekomendasi dari komisi treadway, COSO mengembangkan studi mengenai sebuah model untuk mengevaluasi pengendalian internal. Hasil studi tersebut dengan memperkenalkan sebuah "kerangka kerja pengendalian internal" yang akhirnya menjadi sebuah pedoman bagi para eksekutif, dewan direksi, regulator, penyusun standar, organisasi profesi , dan lainnya sebagai kerangka kerja yang komprehensif untuk mengukur efektivitas pengendalian internal mereka. COSO 2013 tidak mengubah lima komponen pengendalian intern yang telah dipakai sejak COSO 1992.



Slumber: McNally (2013)

Gambar; Perbandingan Konsep COSO 1992 dengan 2013

Sehingga COSO kembali merilis definisi dari konsep pengendalian internalnya. Definisi COSO pada tahun 2013 tentang pengendalian intern menjadi: *Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance* (McNally, 2013).

Dari pengertian tersebut dapat dijelaskan bahwa, pengendalian internal adalah sebuah proses, yang dipengaruhi oleh dewan direksi, manajemen dan personil lain, yang dirancang untuk memberikan keyakinan memadai berkenaan dengan pencapaian tujuan terkait operasional, pelaporan dan kepatuhan terhadap aturan. Para praktisi merekomendasi konsep pengendalian model COSO karena konsep model ini sudah mencakup pengendalian dari segi soft (poin no. 1) dan hard (poin no. 2 – 5). Selain itu konsep model COSO juga terintegrasi satu sama lain.

Keseriusan dalam Penggelapan Komputer

Menurut Bodnar (2000), kriminalitas berdasarkan komputer merupakan bagian dari masalah umum kejahatan kerah putih. Masalah kejahatan kerah putih ini sangat serius. Statistik menunjukkan bahwa kerugian-kerugian perusahaan disebabkan oleh adanya pencurian dan penggelapan yang meningkatkan total kerugian karena meningkatnya penyuapan, pencurian, dan pengutilan. Ini sungguh mengejutkan, karena kita jarang membaca kejahatan seperti itu

dikatakan sebagai penggelapan di koran-koran. Ini karena, dalam sebagian besar kasus, penipuan yang berhasil dideteksi tidak pernah diekspose karena masyarakt nantinya bisa menunjukkan kelemahan pengendalian interen dalam organisasi itu sendiri. Para manajer merasa malu jika ada publikasi negatif yang datang dari masyarakat. Keamanan komputer merupakan masalah internasional.

Penipuan manajemen (*management fraud*) adalah tindakan-tindakan penipuan yang dilakukan oleh para manajer untuk mengelabui para investor dan kreditor dengan menggunakan laporan keuangan yang keliru (Bodnar, 2000). Jenis penipuan ini dilakukan oleh orang yang mempunyai tingkatan yang cukup tinggi dalam organisasi untuk mengatur pengendalian akuntansi. Manajemen dapat juga melakukan pengeliruan atau penghilangan lain yang dapat mengelabui karyawan atau investor, tetapi intinya, penipuan manajemen berkaitan dengan manipulasi terhadap laporan keuangan.

Orang-Orang yang Menimbulkan Hambatan pada Sistem Komputer

Serangan atau gangguan yang berhasil terhadap sistem komputer memerlukan adanya akses ke perangkat keras, berkas data sensitif, atau program-program kritis. Menurut Bodnar (2000), terdapat tiga kelompok individu yang berbeda dalam hal kemampuan normalnya untuk berakses dengan perangkat keras. Sistem komputer pribadi seringkali menimbulkan hambatan potensial karena mereka seringkali memiliki akses khusus ke data dan program-program penting. Para pemakai, sebaliknya, memiliki akses yang lebih sempit, tetapi mereka tetap memiliki kesempatan untuk melakukan penggelapan. Para pengganggu tidak memiliki akses sama sekali, tetapi mereka seringkali adalah orang yang memiliki kemampuan untuk mengganggu perusahaan.

Sistem komputer pribadi. Sistem komputer pribadi meliputi karyawan perawatan komputer, para pemogram, para operator, dan karyawan administrasi sistem informasi dan komputer, dan klerk pengendalian data. Masing-masing kelompok akan dibahas berikut ini.

1. Karyawan Sistem Komputer

   Mereka adalah yang menginstalasikan perangkat keras, perangkat lunak, memperbaiki perangkat keras, dan memperbaiki kesalahan kecil pada perangkat lunak.
2. Pemogram

   Pemogram sistem seringkali menuliskan programnya untuk memodifikasi atau memperbaiki sistem operasi.
3. Operator Komputer

Orang-orang yang merencanakan dan memonitor operasi komputer dan jaringan komunikasi tersebut disebut operator komputer dan operator jaringan. Dalam beberapa sistem operator komputer, memonitor operasi melalui sistem *console*, yaitu stasiun kerja atau terminal yang diberikan khusus bagi operator.

4. Karyawan Administratif Sistem Informasi dan Komputer

   Penyelia sistem merupakan orang yang mempunyai posisi dengan kepercayaan besar. Orang-orang ini secara normal memiliki akses ke pengamanan rahasia, berkas, program, dan sebagainya.

5. Klerk Pengendalian Data

   Mereka yang bertanggung jawab atas pemasukan data secara manual maupun terotomatisasi ke sistem komputer disebut klerk pengendalian data.

Pemakai. Para pemakai terdiri dari orang yang beragam dan satu sama lain dapat dibedakan berdasarkan kegiatan fungsionalnya tanpa memandang pengolahan atau komputasi data. Dalam beberapa kasus, para pemakai dapat mengendalikan komputer yang penting seperti mengkredit, tagihan kredit, dan sebagainya.

Pengganggu. Setiap orang yang memiliki peralatan, data atau berkas-berkas komputer tanpa otorisasi yang memadai disebut pengganggu—*intruder*. Pengganggu yang menyerang sistem komputer sekedar untuk kesenangan dan tantangan disebut *hacker*. Jenis dari pengganggu :

1. *Unnoticed Intruders*

   Orang yang berasal dari divisi pemasaran dapat masuk ke pustaka disk atau pita dan mencurinya.

2. *Wire Tappers*

   Sebagian besar informasi yang diproses oleh komputer perusahaan bergerak melalui kabel-kabel. Jalur ini sangat peka terhadap gangguan kabel, yang dapat dilakukan dengan peralatan murah (seperti perekam pita sederhana dan sedikit kabel) yang mampu menjalankan tugas tanpa terlihat seperti potong jalur terhadap kabel.

3. *Piggy-Backers*

   Pihak yang melakukan penetrasi memotong jalur informasi resmi dan menggantinya dengan informasi yang keliru.

4. *Impersonating Intruders*

   Imperating intruders adalah orang yang mendorong orang lain untuk melakukan penggelapan di perusahaan. Salah satu jenis pengganggu menggunakan nomor akun dan

password yang tidak sah untuk mengakses komputer perusahaan. Banyak perusahaan yang sangat lengah terhadap keamanan nomor akun dan password komputer.

5. *Eavesdroppers*

   Setiap informasi yang melalui jaringan komunikasi masyarakat sangat peka terhadap eavesdropping dan piggybaking. Sebagai contoh, dengan hanya memindahkan satu kabel dari alat scan *Tandy* (*Radio Shack)* akan memungkinkan orang untuk memonitor komunikasi telepon selular. Terdapat klub-klub yang memiliki kebiasaan merekam pembicaraan telepon para selebriti dan tokoh masyarakat.

Hambatan Aktif Sistem Komputer

Menurut Bodnar (2000), Terdapat sedikitnya enam metode yang dapat dipakai oleh orang untuk melakukan penggelapan komputer. Metode-metode ini adalah manipulasi masukan, gangguan program, gangguan berkas secara langsung, pencurian data, sabotase, dan penyalahgunaan dan pencurian sumberdaya komputer (Bodnar, 2000).

1. **Manipulasi Masukan**.

   Dalam sebagian besar kasus penggelapan komputer, manipulasi masukan merupakan salah satu metode yag digunakan. Metode ini hanya membutuhkan sedikit kemampuan teknis saja. Orang yang mengganggu masukan komputer bisa saja sama sekali tidak tahu bagaimana komputer beroperasi.

2. **Gangguan Program**.

   Gangguan program barangkali merupakan metode yang paling sedikit digunakan dalam penggelapan komputer. Ini karena untuk melakukannya dibutuhkan kemampuan pemograman yang hanya dipunyai oleh sedikit orang saja.

3. ***Trapdoor***

   Trapdoor adalah bagian program komputer yang memungkinkan seseorang untuk mengakses program dengan melewati pengamanan normal progam tersebut. *Trapdoor* terdapat dalam sistem akuntansi, program-program basis data, sistem operasi, dan sebagainya.

4. **Gangguan Berkas Secara Langsung**.

   Dalam beberapa kasus, ada orang-orang yang melakukan potong jalur terhadap proses normal untuk pemasukan data ke program-program komputer. Jika ini terjadi, maka akibatnya sangat merusak.

5. **Pencurian Data**.

Pencurian terhadap data-data penting merupakan masalah serius dalam bisnis sekarang ini. Dalam banyak industri yang sangat kompetitif, telah terjadi pencurian informasi kuantitatif maupun kualitatif mengenai pesaing.

6. Sabotase.

Sabotase komputer menciptakan bahwa serius terhadap instalasi komputer. Perusakan terhadap komputer atau perangkat lunak dapat mengakibatkan kebangkrutan perusahaan. Karyawan-karyawan yang tidak puas, khususnya yang dipecat, biasanya menjadi sumber sabotase terhadap sistem komputer.

Kadang-kadang program-program komputer digunakan sebagai alat untuk sabotase. Salah satu metode tertua untuk melakukan perbuatan itu adalah dengan *logic bomb.*

a. *Logic bomb,* mencakup kode-kode mati yang ditempatkan dalam program untuk diaktifkan pada saat tertentu.
b. *Trojan horse,* adalah program perusak yang tampak sebagai bagian dari program itu sendiri.
c. Program virus serupa dengan *trojan horse* tetapi dapat menyebar ke program-program lain, dan "menularkan" virus-virus tersebut ke program-program yang dimasukinya.
d. *Worm,* adalah jenis virus yang menyebar dengan sendirinya di jaringan komputer. Karena seluruh komputer dalam jaringan memiliki hubungan satu sama lain, *worm* akan tumbuh terus sesuai banyaknya komputer.

C. METODE PENELITIAN

Jenis penelitian ini merupakan penelitian *literature review*. *Literatur review* adalah sebuah metode yang sistematis, eksplisit dan reprodusibel untuk melakukan identifikasi, evaluasi dan sintesis terhadap karya-karya hasil penelitian dan hasil pemikiran yang sudah dihasilkan oleh para peneliti dan praktisi. Literatur review bertujuan untuk membuat analisis dan sintesis terhadap pengetahuan yang sudah ada terkait topik yang akan diteliti untuk menemukan ruang kosong bagi penelitian yang akan dilakukan. Tujuan yang lebih rinci dijelaskan oleh Okoli & Schabram (2010) yaitu; 1) menyediakan latar/basis teori untuk penelitian yang akan dilakukan, 2) mempelajari kedalaman atau keluasan penelitian yang sudah ada terkait topik yang akan diteliti, dan 3) menjawab pertanyaan-pertanyaan praktis dengan pemahaman terhadap apa yang sudah dihasilkan oleh penelitian terdahulu.

Desain penelitian ini adalah Literature Review atau tinjauan pustaka. Penelitian kepustakaan atau kajian literatur (literature review, literature research) merupakan penelitian yang mengkaji atau meninjau secara kritis pengetahuan, gagasan, atau temuan yang terdapat di dalam tubuh literatur berorientasi akademik (academic-oriented literature), serta merumuskan kontribusi teoritis dan metodologisnya untuk topik tertentu, Cooper (2010).

Literature review dalam penelitian ini dilakukan dengan mengumpulkan konsep-konsep/teori-teori dan penelitian-penelitian yang berhubungan dengan sistem pengendalian intern/*internal control* untuk keamanan sistem informasi (*information systems security)*. Dari hasil pengamatan yang dilakukan baik yang berhubungan dengan konsep/teori-teori dan hasil penelitian sebelumnya maka kemudian dilakukan sintesis dan selanjutnya diambil kesimpulan.

D. PEMBAHASAN

Pengendalian atas Hambatan-Hambatan Aktif

Cara utama mencegah penggelapan dan sabotase adalah dengan menerapkan jenjang memadai pada pengendalian akses Bodnar (2000). Jika seluruh pengendalian umum dan pemrosesan data telah ditempatkan dan dapat berjalan, pertimbangan utama yang kemudian harus ada adalah pembatasan akses tidak terotorisasi ke data dan peralatan sensitif.

Filosofi dasar pendekatan penjenjangan atas pengendalian akses mencakup penerapan penjenjanagn ganda yang memisahkan si pelaku dari target potensialnya. Tiga jenjang yang harus ada adalah : pengandalain akses-fisik, pengandalain akses-sistem, dan pengendalain akses-berkas.

1) **Pengendalian akses-fisik**

   Tujuan pengandalian akses fisik adalah untuk memisahkan secara fisik, individu-individu yang tidak memiliki otorisasi dari sumberdaya komputer yang ada. Pemisahan fisik ini harus diterapkan pada perangkat keras, area masukan-data, area keluaran-data, library data, dan kabel-kabel komunikasi.

2) **Pengendalian akses-sistem**

   Pengandalian akses sistem adalah pengandalian ayng dirancang berbentuk perangkat lunak unuk mencegah pemanfaatan system oleh orang yang tidak berhak. Karena itu, tujuan pengandalian akses-sistem adalah memberi identitas pemakai seperti kode akun, password, dan peralatan perangkat keras.

   Setiap pemakai dapat diberikan nomor identifikasi-pemakai dan password pada sembilan tingkatan; yaitu pada tingkat stasiun kerja atau computer pribadi, pada jaringan,

pada computer induk (*host computer*), pada file server, pada katalog file, pada program, pada berkas data atau basis data, pada catatan dan pada field data, setiap tingkatan ini menyediakan proteksi, yang memisahkan pengganggu dari data penting. Pada tingkatan puncak, tingkatan stasiun kerja, pemakai harus memasukkan informasi identifikasi yang tepat sebelum membuat akses ke jaringan komunikasi. Kemudian, setelah mengakses jaringan, pemakai harus memasukkan tambahan informasi identifikasi sebelum dapat mengakses computer induk (*host computer*) atau server file.

Seluruh masukan ke berkas master dan basis data yang penting harus secara otomatis memuat identifikasi pemakai dan waktu pelaksanaan masukan transaksi. Ini memungkinkan dilakukannya audit terhadap seluruh transaksi.

Password harus dikendalikan secara cermat dengan sistem manajemen *password*.sistem harus memuat *password* bagi para pemakai dan harus dibuat ulang secara periodic. Prosedur paling aman adalah tidak membiarkan para pemakai mengubah sendiri password mereka. Password ideal harus mencakup huruf-huruf besar dan kecil, simbol-simbol khusus, dan angka-angka. Jenjang lain yang dapat digunakan adalah pemanfaatan sistem sinyal-kontrak-sinyal.

Perangkat keras dapat juga dikombinasikan dengan perangkat lunak yang digunakan oleh orang tertentu untuk mendapatkan akses ke beberapa bagian dari sistem. Peringatan lainnya adalah dengan membuat peralatan komunikasi otentik sesuai dengan kebutuhan akses.

Peralatan lain untuk memanfaatkan perangkat keras dan lunak untuk membatasi akses adalah modem panggil-ulang – *call-back modem*. Cara terakhir untuk membatasi akses tidak sah adalah menyembunyikan seluruh data yang dikirim melalui saluran komunikasi.

3) **Pengendalian Akses Berkas**.

Jenjang akhir pengendalian akses diterapkan ditingkat berkas. Pengendalian akses-berkas mencegah akses tidak sah ke berkas data dan program.

Pengendalian akses-berkas paling mendasar adalah penetapan pedoman dan prosedur otorisasi untuk mangakses dan mengubah data. Pembatasan-pembatasan khusus harus ditempatkan di bagian pemograman karena para pemogram inilah yang tahu bagaimana mengubah program. Seharusnyalah tidak ada akses yang diijinkan ke berkas-berkas tanpa adanya otorisasi tertulis.para pemogram harus membuat seluruh pengubahan yang

diotorisasi dalam bentuk rangkapan program asli, jadi bukan pada program asli itu sendiri, dan rangkapan tersebut harus diperiksa sebelum diubah ke program aslinya.

Seluruh program penting harus disimpan dalam berkas terkunci. Artinya, program dapat dijalankan, tetapi tidak dapat dilihat atau diubah. Hanya departemen keaman yang boleh tahu kode (*password*) untuk membuka kunci berkas. Adalah mungkin untuk menginstalkan program persinggahan untuk memeriksa tanda-tanda virus atau gangguan terhadap berkas. Beberapa program ini memiliki nama yang bunyinya mirip jargon dalam dunia kedokteran : Flu-Shot+ (konsep dan Perancangan Perangkat Lunak) dan Macce Vaccine (Perangkat Lunak Paul Mace).

Romney and Steinbart (2006) menyebutkan bahwa, *Sys Trust* menggunakan empat prinsip berikut ini untuk menetapkan apakah suatu sistem andal atau tidak:

1) Ketersediaan (*availability*). Sistem tersebut tersedia untuk dioperasikan dan digunakan dengan mencantumkannya pada pernyataan atau perjanjian tingkat pelayanan.
2) Keamanan *(security).* Sistem dilindungi dari akses fisik maupun logis yang tidak memiliki otorisasi. Hal ini akan membantu mencegah (a) penggunaan yang tidak sesuai, pemutarbalikan, penghancuran atau pengungkapan informasi dan software, serta (b) pencurian sumber daya sistem.
3) Dapat dipelihara *(maintainability)*. Sistem dapat diubah apabila diperlukan tanpa mempengaruhi ketersediaan, keamanan, dan integritas sistem.
4) Integritas *(integrity)*. Pemrosesan sistem bersifat lengkap, akurat, tepat waktu, dan diotorisasi. Sebuah sistem dikatakan memiliki integritas apabila dapat melaksanakan fungsi yang diperuntukkan basi sistem tersebut secara keseluruhan dan bebas dari manipulasi sistem, baik yang tidak diotorisasi maupun yang tidak disengaja.

Berdasarkan pendapat tersebut di atas maka disimpulkan, bagaimana sebuah system tersebut bisa dikatakan handal atau tidak, yaitu bisa dilihat dari segi ketersediaan data/informasi (*availability*) yang dihasilkan, keamanan data dan informasinya *(security)*, integritas *(integrity)*, akurat (*reliability)*, dan terpelihara *(maintainability)*.

- **Pengendalian atas Hambatan-hambatan Pasif**

Hambatan-hambatan pasif meiputi masalah-masalah seperti gangguan pada tenaga dan perangkat keras. Pengendalian-pengendalain pada hambatan-hambatan semacam itu dapat bersifat preventif maupun korektif (Bodnar, 2000).

7. Sistem toleransi-kesalahan.

Sebagian besar metode berkaitan dengan kerusakan komponen dalam hal pemonitorann dan pencadangan. Jika salah satu bagian system gagal, bagian cadangan akan segera mengambil alih, dan sistem akan melanjutkan operasi dengan sedikit atau tanpa interupsi. Sistem semacam itu disebut sistem toleransi-kesalahan.

Jaringan dapat membuat toleransi kesalahan dengan membuat jalur komunikasi duplikat dan prosesor-prosesor komunikasi. Terdapat dua pendekatan utama dalam pemrosesan CPU cadangan. sistem dengan *concensus-based protocols* memuat nomor tak teratur ; jika satu *prosesor* tidak cocok dengan yang lainnya, maka akan diabaikan. Sistem lain menggunakan *watchdog processor* yang akan mengambil alih pemrosesan apabila terjadi sesuatu dengan prosesor pertama.

Toleransi kesalahan dalam hal kegagalan sumber tenaga dilakukan dengan membuat pasokan *uninterruptable power supply* (UPS). Tolleransi yang diterapkan di tingkat transaksi mencakup *rollback processing* dan *basis data shadowing.* Dengan *rollback processing*, transaksi-transaksi tidak akan dituliskan ke dalam disk sebelum benar-benar lengkap. Jika sumber tenaga hilang atau kesalahan lainnya muncul selama transaksi dituliskan, maka pada kesempatan pertama program basis data akan secara otomatis memutar balik ke posisi awal. Basis *data shadowing* mirip dengan *disk shadowing*, kecuali pada dibuatnya duplikat seluruh transaksi, dan kemungkinan dikirim melalui komunikasi ke lokasi yang tepat.

8. Koreksi kesalahan

Berkas pendukung. Beberapa studi menunjukkan bahwa lebih dari 50% pemilik computer pribadi tidak memuat berkas pendukung secara memadai. Oleh karena itu, system perlu membuat pendukung secara sentralisasi. System semacam biasa digunakan untuk mendukung disk yang penting.

Terdapat tiga macam pendukung *: full backups, incremental backups, dan differential backups* . *Full backup* akan mendukung seluruh berkas yang terdapat pada disk tertentu. *Incremental backup* mendukung seluruh berkas yang archieve bitnya diubah menjadi 1. Setiap archieve bit pada berkas kemudian akan diubah lagi menjadi 0 selama proses pendukungan. Oleh karena itu, *incremental backup*, hanya membuat berkas pendukung yang telah dimodifikasi dari *full backup* atau *incremental backup* sebelumnya. Terakhir, *differential backup* sama dengan incremental backup, hanya saja archieve bit tidak diubah menjadi 0 selama proses pendukungan.

E. KESIMPULAN

Berdasarkan beberapa konsep/teori-teori yang ditawarkan tentang pengendalian system informasi maka konsep pengendalian berdasarkan Sarbanes-Oxley and Internal Control (COSO Framwork) masih sangat disarankan oleh para ahli. Hal ini disebabkan karena konsep pengendalian model ini sudah mengadopsi segala aspek perlindungan yang ada, baik phisik maupun non phisik. Namun demikian perlindungan keamanan untuk sistem informasi idealnya harus difokuskan pada pengendalian akses dan pengendalian IT.

Hal ini disebabkan karena ada tiga kelompok individu yang berbeda dalam hal kemampuan normalnya untuk berakses dengan perangkat keras, yaitu; 1) Sistem komputer pribadi, yang seringkali menimbulkan hambatan potensial karena mereka seringkali memiliki akses khusus ke data dan program-program penting. 2) Para pemakai, mereka memiliki akses yang lebih sempit, tetapi mereka tetap memiliki kesempatan untuk melakukan penggelapan. 3) Para pengganggu, mereka memang tidak memiliki akses sama sekali, tetapi mereka seringkali adalah orang yang memiliki kemampuan untuk mengganggu sistem informasi perusahaan. Sedangkan untuk pengendalian atas hambatan pasif maka sangat dianjurkan organisasi untuk melakukan back up data, baik menggunakan *full back up* atau *incremental back up*. Dan salah satu sistem back up sekarang bisa menggunakan *cloud systems /cloud computing.*

DAFTAR PUSTAKA

Bagranoff, Nancy A., Simkin, Mark G. & Norman, Carolyn Strand. (2010). Core Concepts Of Accounting Information Systems Eleventh Edition: Wiley.John Wiley Sons.INC

Bodnar H. George and William S. Hopwood (2000). "Sistem Informasi Akuntansi". Edisi Terjemahan. Buku Satu. Penerbit Salemba Empat, Pearson Education Asia Pte. Ltd. Prentice-Hall. Inc.

Dhillon, Gurpreet. (1997). Managing Information System Security: Macmillan Education UK

Hall A. James (2011), "*Accounting Information Systems*" 7th Edition, Cengage Learning Asia Pte. Ltd. Singapore.

Ibrahim Ibrahim, A. (2010), "Sistem Pemesanan Tiket Pesawat Berbasis Web", *Jurnal Sistem Informasi*, Fasilkom Unsri, Vol. 3.

Loudon, Kenneth C and Jane P Loudon (2014), Management Information Systems Managing the Digital Firm. 13th Edition. Global Edition. Pearson. New York.

Kim, David & Solomon, Michael G. (2012). Fundamentals of information system security: Jones and Bartlett learning book and product are available through most bookstrores and online book sellers.

Raggad. (2010). Information Security Management Concepts and Practice: 1st CRC Press, Inc. Boca Raton, FL, USA.

Romney, Marshall & Steinbart, Paul. 2006. Accounting Information Systems, Tenth Edition. Upper Saddle River, New Jersey, 07458 : Pearson Education, Inc

Sandhu S. Ravi and Pierangela Samarati (1994) Access Control: Princples and Practice lEEE Communication\ Magazine

Stair M. Ralph and George W. Reynolds (2010) Principles of Information Systems A Managerial Approach. Ninth Edition. Course Technology, Cengage Learning. USA

Todorov, Dobromir. (2007). Mechanics of User Identification and Authentication Fundamentals of Identity Management: Auerbach Publications Taylor & Francis Group Boca Raton New York

Okoli, C. and Schabram, K., 2011. A Guide to Conducting Literature Review of Information System Research, Communications of the Association for Information System, 37 (43), 879-910.

Cooper R. Donald , 2010. Metode Penelitian Bisnis. Jakarta . Penerbit: Salemba Empat