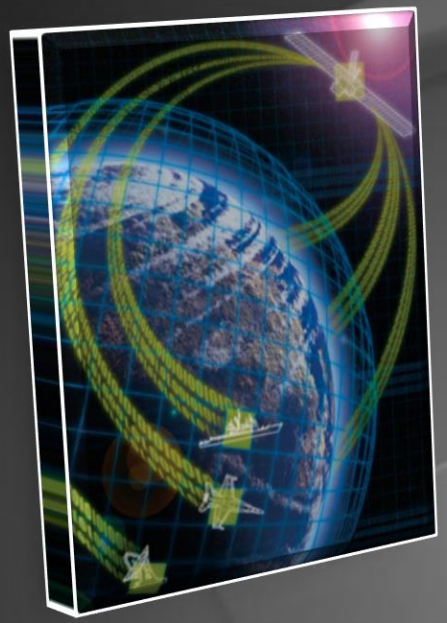
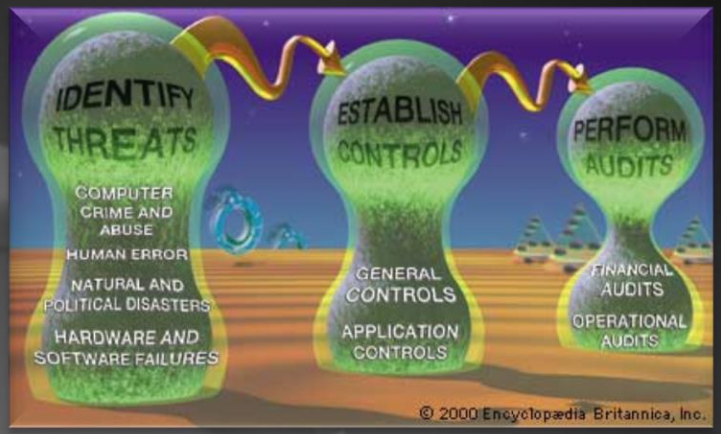
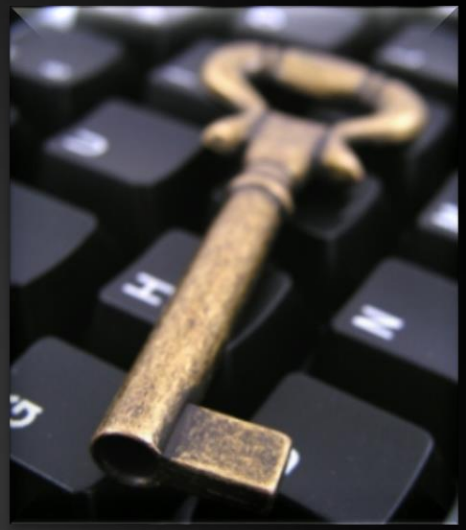
TEKNOLOGI INFORMASI

Keamanan Sistem Informasi







Keamanan Sistem Informasi

Pendahuluan

- Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah “information-based society”.
- Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi).

Pendahuluan

- Survey Information Week (USA), 1271 system or network manager, hanya 22% yang menganggap keamanan sistem informasi sebagai komponen penting.
- Kesadaran akan masalah keamanan masih rendah!

Pendahuluan

- 1988. Keamanan sistem mail *sendmail dieksploitasi oleh Robert* Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai "*denial of service attack*". Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar $100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda $10.000.
- 10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi sebuah airport lokal (Worcester, Mass.) sehingga memutuskan komunikasi di control tower dan menghalau pesawat yang hendak mendarat.

Pendahuluan

Jumlah kejahatan komputer (*computer crime), terutama yang* berhubungan dengan sistem informasi, akan terus meningkat dikarenakan beberapa hal, antara lain:

- Aplikasi bisnis yang menggunakan (berbasis) teknologi informasi dan jaringan komputer semakin meningkat.
- Desentralisasi server sehingga lebih banyak sistem yang harus ditangani dan membutuhkan lebih banyak operator dan administrator yang handal. Padahal mencari operator dan administrator yang handal adalah sangat sulit.

Pendahuluan

- Transisi dari single vendor ke multi-vendor sehingga lebih banyak yang harus dimengerti dan masalah interoperability antar vendor yang lebih sulit ditangani.
- Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya.
- Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat.

Pendahuluan

- Semakin kompleksnya sistem yang digunakan, seperti semakin besarnya program (*source code) yang digunakan sehingga* semakin besar probabilitas terjadinya lubang keamanan.
- Semakin banyak perusahaan yang menghubungkan sistem informasinya dengan jaringan komputer yang global seperti Internet. Potensi sistem informasi yang dapat dijebol menjadi lebih besar.

Pendahuluan

- 1999 Computer Security Institute (CSI) / FBI Computer Crime Survey menunjukkan beberapa statistik yang menarik, seperti misalnya ditunjukkan bahwa “disgruntled worker” merupakan potensi attack / abuse. Http://www.gocsi.com
- Pada tahun 2000 beberapa situs web di Indonesia dijebol. Contoh terakhir: Bank BCA, Bank Lippo, Bank Bali.
- Cracker Indonesia ditangkap di Singapura

Pendahuluan

Mungkinkah Aman?

- Sangat sulit mencapai 100% aman
- Ada timbal balik antara keamanan vs. kenyamanan (security vs convenience)

Pendahuluan

- Definisi computer security:

(Garfinkel & Spafford)

A computer is secure if you can depend on it and its software to behave as you expect

G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating) atau, paling tidak, mendeteksi*

- adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

Pendahuluan

- Jika kita berbicara tentang keamanan sistem informasi, selalu kata kunci yang dirujuk adalah pencegahan dari kemungkinan adanya virus, hacker, cracker dan lain-lain.
- Padahal berbicara masalah keamanan sistem informasi maka kita akan berbicara kepada kemungkinan adanya resiko yang muncul atas sistem tersebut.

Pendahuluan

Sehingga pembicaraan tentang keamanan sistem tersebut maka kita akan berbicara 2 masalah utama yaitu :

1. Threats (Ancaman) atas sistem dan
2. Vulnerability (Kelemahan) atas sistem

Pendahuluan

Masalah tersebut pada gilirannya berdampak kepada 6 hal yang utama dalam sistem informasi yaitu :

- ✓ Efektifitas
- ✓ Efisiensi
- ✓ Kerahaasiaan
- ✓ Integritas
- ✓ Keberadaan (availability)
- ✓ Kepatuhan (compliance)
- ✓ Keandalan (reliability)

Pendahuluan

Adapun kriteria yag perlu di perhatikan dalam masalah keamanan sistem informasi membutuhkan 10 domain keamanan yang perlu di perhatikan yaitu :

1. Akses kontrol sistem yang digunakan
2. Telekomunikasi dan jaringan yang dipakai
3. Manajemen praktis yang di pakai
4. Pengembangan sistem aplikasi yang digunakan
5. Cryptographs yang diterapkan
6. Arsitektur dari sistem informasi yang diterapkan
7. Pengoperasian yang ada
8. Busineess Continuity Plan (BCP) dan Disaster Recovery Plan (DRP)
9. Kebutuhan Hukum, bentuk investigasi dan kode etik yang diterapkan
10. Tata letak fisik dari sistem yang ada

ANCAMAN (Threats)

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman yang mungkin timbul dari kegiatan pengolahan informasi berasal dari 3 hal utama, yaitu :

- Ancaman Alam
- Ancaman Manusia
- Ancaman Lingkungan

ANCAMAN (Threats)

☼*Ancaman Alam*

Yang termasuk dalam kategori ancaman alam terdiri atas :

- Ancaman air, seperti : Banjir, Stunami, Intrusi air laut, kelembaban tinggi, badai, pencairan salju
- Ancaman Tanah, seperti : Longsor, Gempa bumi, gunung meletus
- Ancaman Alam lain, seperti : Kebakaran hutan, Petir, tornado, angin ribut

ANCAMAN (Threats)

☼ *Ancaman Manusia*

Yang dapat dikategorikan sebagai ancaman manusia, diantaranya adalah :

- Malicious code
- Virus, Logic bombs, Trojan horse, Worm, active contents, Countermeasures
- Social engineering
- Hacking, cracking, akses ke sistem oleh orang yang tidak berhak, DDOS, backdoor
- Kriminal
- Pencurian, penipuan, penyuapan, pengkopian tanpa ijin, perusakan
- Teroris
- Peledakan, Surat kaleng, perang informasi, perusakan

ANCAMAN (Threats)

☼ *Ancaman Lingkungan*

Yang dapat dikategorikan sebagai ancaman lingkungan seperti :

- Penurunan tegangan listrik atau kenaikan tegangan listrik secara tiba-tiba dan dalam jangka waktu yang cukup lama
- Polusi
- Efek bahan kimia seperti semprotan obat pembunuh serangga, semprotan anti api, dll
- Kebocoran seperti A/C, atap bocor saat hujan

KELEMAHAN (Vurnerability)

Adalah cacat atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang mencoba menyusup terhadap sistem tersebut.

KELEMAHAN (Vurnerability)

Cacat sistem bisa terjadi pada prosedur, peralatan, maupun perangkat lunak yang dimiliki, contoh yang mungkin terjadi seperti : Seting firewall yang membuka telnet sehingga dapat diakses dari luar, atau Seting VPN yang tidak di ikuti oleh penerapan kerberos atau NAT.

KELEMAHAN (Vurnerability)

Suatu pendekatan keamanan sistem informasi minimal menggunakan 3 pendekatan, yaitu :

1. Pendekatan *preventif* yang bersifat mencegah dari kemungkinan terjadikan ancaman dan kelemahan
2. Pendekatan *detective* yang bersifat mendeteksi dari adanya penyusupan dan proses yang mengubah sistem dari keadaan normal menjadi keadaan abnormal

KELEMAHAN (Vurnerability)

3. Pendekatan *Corrective* yang bersifat mengkoreksi keadaan sistem yang sudah tidak seimbang untuk dikembalikan dalam keadaan normal

PENGENDALIAN KEAMANAN SISTEM INFORMASI

Berkaitan dengan keamanan system informasi, diperlukan tindakan berupa pengendalian terhadap sistem informasi. Kontrol-kontrol untuk pengamanan sistem informasi antara lain:

a) Kontrol Administratif
b) Kontrol Pengembangan dan Pemeliharaan Sistem
c) Kontrol Operasi
d) Proteksi Fisik terhadap Pusat Data

PENGENDALIAN KEAMANAN SISTEM INFORMASI

Kontrol-kontrol untuk pengamanan sistem informasi antara lain (Cont):

e) Kontrol Perangkat Keras
f) Kontrol Akses terhadap Sistem computer
g) Kontrol terhadap Akses Informasi
h) Kontrol terhadap Bencana
i) Kontrol Terhadap Perlidungan Terakhir
j) Kontrol Aplikasi

Kontrol Administratif

Kontrol administratif dimaksudkan untuk menjamin bahwa seluruh kerangka control dilaksanakan sepenuhnya dalam organisasi berdasarkan prosedur-prosedur yang jelas. Kontrol ini mencakup hal-hal berikut:

- Mempublikasikan kebijakan control yang membuat semua pengendalian sistem informasi dapat dilaksanakan dengan jelas dan serius oleh semua pihak dalam organisasi.

Kontrol Administratif

- Prosedur yang bersifat formal dan standar pengoperasian disosialisasikan dan dilaksanakan dengan tegas. Termasuk hal ini adalah proses pengembangan sistem, prosedur untuk *backup*, pemulihan data, dan manajemen pengarsipan data.
- Perekrutan pegawai secara berhati-hati yang diikuti dengan orientasi pembinaan, dan pelatihan yang diperlukan.

Kontrol Administratif

- Supervisi terhadap para pegawai. Termasuk pula cara melakukan control kalau pegawai melakukan penyimpangan terhadap yang diharapkan.
- Pemisahan tugas-tugas dalam pekerjaan dengan tujuan agar tak seorangpun yang dapat menguasai suatu proses yang lengkap. Sebagai contoh, seorang pemrogram harus diusahakan tidak mempunyai akses terhadap data produksi (operasional) agar tidak memberikan kesempatan untuk melakukan kecurangan.

Kontrol Pengembangan dan Pemeliharaan Sistem

Untuk melindungi kontrol ini, peran auditor sistem informasi sangatlah penting. Auditor sistem informasi harus dilibatkan dari masa pengembangan hingga pemeliharaan system, untuk memastikan bahwa system benar-benar terkendali, termasuk dalam hal otorisasi pemakai system. Aplikasi dilengkapi dengan *audit trail* sehingga kronologi transaksi mudah untuk ditelusuri

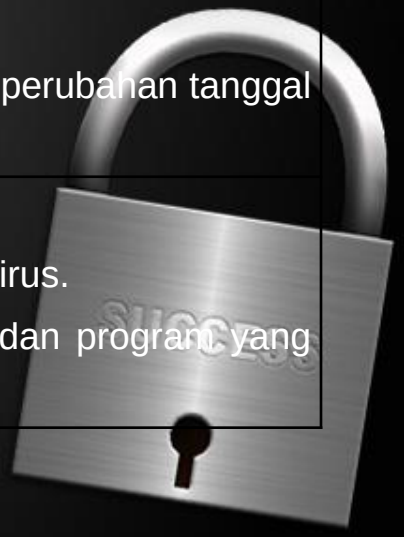
Kontrol Operasi

Kontrol operasi dimaksudkan agar system beroperasi sesuai dengan yang diharapkan. Termasuk dalam kontrol ini:

- Pembatasan akan akses terhadap data
- Kontrol terhadap personel pengoperasi
- Kontrol terhadap peralatan
- Kontrol terhadap penyimpanan arsip
- Pengendalian terhadap virus

  Untuk mengurangi terjangkitnya virus, administrator sistem harus melakukan tiga kontrol berupa preventif, detektif, dan korektif.

Kontrol	Contoh
Preventif	o Menggunakan salinan perangkat lunak atau berkas yang berisi makro yang benar-benar bersih. o Mengindari pemakaian perangkat lunak *freeware* atau *shareware* dari sumber yang belum bisa dipercaya. o Menghindari pengambilan berkas yang mengandung makro dari sembarang tempat. o Memeriksa program baru atau berkas-berkas baru yang mengandung makro dengan program anti virus sebelum dipakai. o Menyadarkan pada setiap pemakai untuk waspada terhadap virus.
Detektif	o Secara rutin menjalankan program antivirus untuk mendeteksi infeksi virus. o Melakukan pembandingan ukuran-ukuran berkas untuk mendeteksi perubahan ukuran pada berkas o Melakukan pembandingan tanggal berkas untuk mendeteksi perubahan tanggal berkas.
Korektif	o Memastikan pem-*backup*-an yang bersih o Memiliki rencana terdokumentasi tentang pemulihan infeksi virus. o Menjalankan program antivirus untuk menghilangkan virus dan program yang tertular.



Proteksi Fisik terhadap Pusat Data

- Untuk menjaga hal-hal yang tidak diinginkan terhadap pusat data.
- Faktor lingkungan yang menyangkut suhu, kebersihan, kelembaban udara, bahaya banjir, dan keamanan fisik ruangan perlu diperhatikan dengan benar.

Kontrol Perangkat Keras

- Untuk mengatisipasi kegagalan sistem komputer, terkadang organisasi menerapkan sistem komputer yang berbasis *fault-tolerant* (toleran terhadap kegagalan).
- Pada sistem ini, jika komponen dalam sistem mengalami kegagalan maka komponen cadangan atau kembarannya segera mengambil alih peran komponen yang rusak

Kontrol Perangkat Keras

Sistem *fault-tolerant* dapat diterapkan pada lima level, yaitu pada

- komunikasi jaringan, toleransi kegagalan terhadap jaringan dilakukan dengan menduplikasi jalur komunikasi dan prosesor komunikasi.
- prosesor, redundasi prosesor dilakukan antaralain dengan teknik *watchdog processor*, yang akan mengambil alih prosesor yang bermasalah.

Kontrol Perangkat Keras

- penyimpan eksternal,terhadap kegagalan pada penyimpan eksternal antara lain dilakukan melalui *disk memoring* atau *disk shadowing*, yang menggunakan teknik dengan menulis seluruh data ke dua *disk* secara pararel. Jika salah satu disk mengalami kegagalan, program aplikasi tetap bisa berjalan dengan menggunakan *disk* yang masih baik.

Kontrol Perangkat Keras

- catu daya, toleransi kegagalan pada catu daya diatasi melalui UPS.
- transaksi, toleransi kegagalan pada level transaksi ditanganimelalui mekanisme basis data yang disebut *rollback*, yang akan mengembalikan ke keadaan semula yaitu keadaan seperti sebelum transaksi dimulai sekiranya di pertengahan pemrosesan transaksi terjadi kegagalan.

Kontrol Akses terhadap Sistem Komputer

- untuk melakukan pembatasan akses terhadap sistem, setiap pemakai sistem diberi otorisasi yang berbeda-beda. Setiap pemakai dilengkapi dengan nama pemakai dan *password*.
- sistem-sistem yang lebih maju mengombinasikan dengan teknologi lain. Misalnya, mesin ATM menggunakan kartu magnetic atau bahkan kartu cerdas sebagai langkah awal untuk mengakses sistem dan kemudian baru diikuti dengan pemasukan PIN (*personal identification number*).

Kontrol Akses terhadap Sistem Komputer

- Teknologi yang lebih canggih menggunakan sifat-sifat biologis manusia yang bersifat unik, seperti sidik jari dan retina mata, sebagai kunci untuk mengakses sistem
- Pada sistem yang terhubung ke Internet, akses Intranet dari pemakai luar (via Internet) dapat dicegar dengan menggunakan *firewall*. *Firewall* dapat berupa program ataupun perangkat keras yang memblokir akses dari luar intranet.

Kontrol terhadap Akses Informasi

- Ada kemungkinan bahwa seseorang yang tak berhak terhadap suatu informasi berhasil membaca informasi tersebut melalui jaringan (dengan menggunakan teknik *sniffer*). Untuk mengantisipasi keadaan seperti ini, alangkah lebih baik sekiranya informasi tersebut dikodekan dalam bentuk yang hanya bisa dibaca oleh yang berhak

Kontrol terhadap Akses Informasi

- Studi tentang cara mengubah suatu informasi ke dalam bentuk yang tak dapat dibaca oleh orang lain dikenal dengan istilah **kriptografi**. Adapun sistemnya disebut **sistem kripto**. Secara lebih khusus, proses untuk mengubah teks asli (*cleartext* atau *plaintext*) menjadi teks yang telah dilacak (*cliphertext*) dinamakan **enskripsi,** sedangkan proses kebalikannya, dari *chiphertext* menjadi *cleratext*, disebut **dekrpisi.**

Kontrol terhadap Akses Informasi

Dua teknik yang popular untuk melakukan enskripsi yaitu DES dan *public-key encryption*

DES merupakan teknik untuk melakukan enskripsi dan deskripsi yang dikembangkan oleh IBM pada tahun 1970-an. Kunci yang digunakan berupa kunci privat yang bentuknya sama. Panjang kunci yang digunakan sebesar 64 bit. Algoritma yang digunakan mengonversi satu blok berukuran 64 bit (8karakter) menjadi blok data berukuran 64 bit.

Kontrol terhadap Akses Informasi

- Sistem DES yang menggunakan kunci privat memiliki kelemahan yang terletak pada keharusan untuk mendistribusikan kunci ini. Pendistribusian inilah yang menjadi titik rawan untuk diketahui oleh pihak penyadap.

Kontrol terhadap Akses Informasi

- Untuk mengatasi kelemahan sistem kripto simetrik, diperkenalkan teknik yang disebut kriptografi kunci publik. Sistem ini merupakan model sistem kripto asimetrik, yang menggunakan kunci enkripsi dan dekripsi yang berbeda. Caranya adalah dengan menggunakan kunci privat dan kunci publik. Sebagai gambaran, bila pengirim S mengirimkan pesan ke penerima R, ia menggunakan kunci publik R dan kemudian R melakukan dekripsi dengan menggunakan kunci privat R.

Kontrol Terhadap Bencana

Zwass (1998) membagi rencana pemulihan terhadap bencana ke dalam 4 komponen:

- Rencana darurat (*emergency plan)* menentukan tidakan-tindakan yang harus dilakukan oleh para pegawai manakala bencana terjadi.
- Rencana cadangan (*backup plan*) menentukan bagaimana pemrosesan informasi akan dilaksanakan selama masa darurat.

Kontrol Terhadap Bencana

- Rencana pemulihan (*recovery plan*) menentukan bagaimana pemrosesan akan dikembalikan ke keadaan seperti aslinya secara lengkap, termasu mencakup tanggung jawab masing-masing personil.
- Rencana pengujian (*test plan*) menentukan bagaimana komponen-komponen dalam rencana pemulihan akan diuji atau disimulasikan

Kontrol Terhadap Perlidungan Terakhir

Kontrol terhadap perlindungan terakhir dapat berupa:

- Rencana pemulihan terhadap bencana.
- Asuransi.

  Asuransi merupakan upaya untuk mengurangi kerugian sekiranya terjadi bencana. Itulah sebabnya, biasanya organisasi mengansurasikan gedung atau asset-aset tertentu dengan tujuan kalau bencana terjadi, klaim asuransi dapat digunakan untuk meringankan beban organisasi

Kontrol Aplikasi

Kontrol aplikasi adalah kontrol yang diwujudkan secara sesifik dalam suatu aplikasi sistem informasi. Wilayah yang dicakup oleh kontrol ini meliputi:

- Kontrol Masukan
- Kontrol Pemrosesan
- Kontrol Keluaran
- Kontrol Basis Data
- Kontrol Telekomunikasi

Kesimpulan

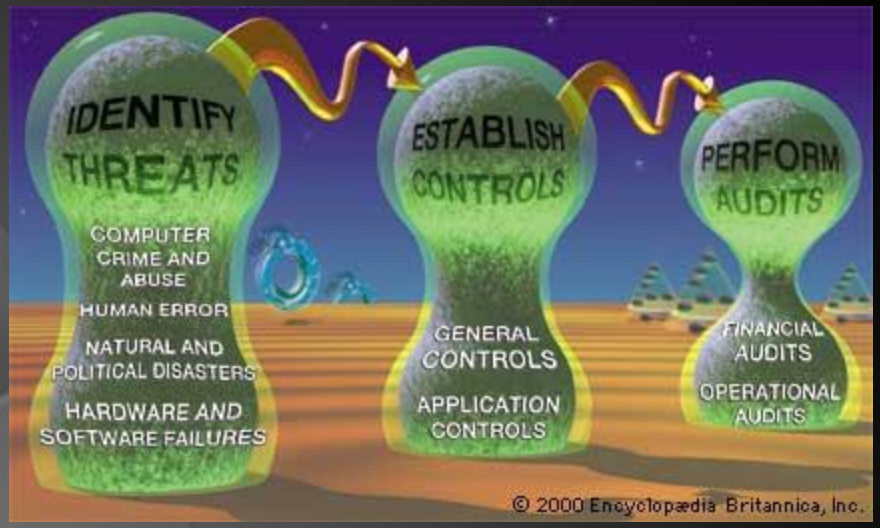
- Keamanan sistem informasi tidak dilihat hanya dari kaca mata timbulnya serangan dari virus, mallware, spy ware dan masalah lain, akan tetapi dilihat dari berbagai segi sesuai dengan domain keamanan sistem itu sendiri.

Daftar Pustaka

- Budi Rahardjo, *Keamanan Sistem Informasi Berbasis Internet*, *ismailzone.com/download/cryptography/Rahard-sec-handbook.pdf* , Juli 2009
- Kentaro, *Keamanan Sistem Informasi Apa dan Bagaimana*, http://www.sisteminformasi.com/2009/04/keamanan-sistem-informasi-apa-dan.html, Juli 2009


PKI
ISAPI
3DES
PKCS#11
SSL


SUCCESS


IDENTIFY THREATS
COMPUTER CRIME AND ABUSE
HUMAN ERROR
NATURAL AND POLITICAL DISASTERS
HARDWARE AND SOFTWARE FAILURES
ESTABLISH CONTROLS
GENERAL CONTROLS
APPLICATION CONTROLS
PERFORM AUDITS
FINANCIAL AUDITS
OPERATIONAL AUDITS
© 2000 Encyclopædia Britannica, Inc.


SUCCESS