PROTEKSI ASET SISTEM INFORMASI; ANALISIS DAN DESAIN MODEL PROTEKSI TERHADAP ASET SISTEM INFORMASI TERINTEGRASI

Ali Masjono
Jurusan Akuntansi, Politeknik Negeri Jakarta Jln Prof Dr. Ir. Siwabessy, Kampus UI Depok 16424

amasjono@yahoo.com

Abstrak

Kemajuan TIK, Teknologi Informasi dan Komunikasi membawa perubahan yang sangat mendasar kepada cara pengelolaan data menjadi informasi. Dengan menggunanan SIM-Integrasi diharapkan proses pengambilan keputusan bisa lebih akuntable, transparan, reliable, cepat, baik dan tepat. SIM-Integrasi ini ditujukan untuk meningkatkan kinerja manajemen agar dapat bertahan diera kompetisi seperti sekarang ini. SIM-Integrasi didesain agar dapat membantu pihak manajemen untuk melakukan kegiatan sehari hari dalam hal manajemen Sumber daya Manusia, Manajemen Akademik, Manajamen Aset, Manajemen Keuangan, Manajemen, Manajemen bahan habis pakai. Implementasi SIM-Integrasi terfokus kepada bagaimana SIM-Integrasi tersebut dapat berfungsi sesuai dengan kriteria yang telah disepakati. Hasil desain SIM-Integrasi yang sekarang digunakan belum sepenuhnya memberikan tingkat proteksi yang memadai. Karena itu, penelitian ini memberikan solusi terhadap apa yang harus dilakukan oleh pihak manajemen PNJ untuk mengamankan aset sistem informasi yang dikondisikan untuk SIM-Integrasi PNJ. Diperlukan kebijakan dan prosedur yang lebih mendukung implementasi SIM-Integrasi dan pengamamannya. Pengamanan dan pengendalian aset SIM-Integrasi meliputi lima domain yaitu Pengendalian akses logikal. pengendalian dan pengamanan sistem jaringan, pengendalian lingkungan, pengendalian akses pisikal, pengendalian penggunan PC/laptop. Untuk implementasi diperlukan kebijakan umum tentang komitmen penggunaan dan pengamanan SIM-Integrasi, kebijakan dan prosedur tentang Pengamanan aset SIM-Integrasi

SIM Integrasi, domain, akses, securtiy, ekposure

Abstract

Development of Information Communication and Technology has a huge impact on the way of management tranforming data becomes information. Using Integrated Management Information System (I-MIS), the process of decision-making can be easier and the result will be accountable, the process will be tranparence and reliable, fast and accurate. I-MIS uses to increase the management performance and to stay the competitive advanctage era. I-MIS consists of human resource management, asset management, inventory management, academic management, and financial management. The I-MIS has already exist in the Politeknik Negeri Jakarta (PNJ). This research focus on the protection of I-MIS to find out what are the best wasy to protect the I-MIS from internal and externat intruders. Based on CISA Manual, this research was designed. There are five components need to be considered to implement the best way to protect the I-MIS. The five components are Locical access exposure and control/Pengendalian akses logikal, Network Infrastructure security/Pengendalian dan pengamanan sistem jaringan, Environmental exposure and control/Pengendalian lingkungan, Physical access exposures and control/Pengendalian akses pisikal, Personal computer Security/Pengendalian penggunan PC/Lapotop/Notesbook

Key words; MIS Integrated, domain, acses, securtiy, exposure

Pendahuluan

Kemajuan TIK, Teknologi Informasi dan Komunikasi telah membawa perubahan yang sangat mendasar kepada cara pengelolaan data menjadi informasi. Sejalan dengan program I-MHERE, PNJ sedang dalam proses pengembangan SIM-Integrasi, Integrated Managemen Information System. SIM-Integrasi ini ditujukan untuk meningkatkan kinerja manajemen agar dapat bertahan diera kompetisi seperti sekarang ini. SIM-Integrasi didesain agar dapat membantu pihak manajemen PNJ untuk melakukan kegiatan sehari hari dalam hal manajemen Sumber daya Manusia, Manajemen Akademik, Manajamen Aset, Manajemen Keuangan, Manajemen, Manajemen bahan habis pakai.

Implementasi SIM-Integrasi saat ini terfokus kepada bagaimana SIM-Integrasi tersebut dapat berfungsi sesuai dengan kriteria yang telah disepakati. Hasil desain SIM-Integrasi yang sekarang digunakan belum sepenuhnya memberikan tingkat proteksi yang memadai.

Karena itu, penelitian ini akan memberikan solusi terhadap apa yang harus dilakukan oleh pihak manajemen PNJ untuk mengamankan aset sistem informasi yang dikondisikan untuk SIM-Integrasi PNJ.

Kegagalan dalam menangani masalah kemaman sistem inforamasi bisa memakan beban/biaya tinggi. Kehilangan akan menghasilkan kegagalan itu sendiri sedangkan beban terjadi untuk memperbaiki (recover) dari kerusakan yang terjadi. Dan biasanya akan diikuti oeh biaya untuk mengamankan sistem dan mencegah kerusakan/kerugian lebih lanjut. Sistem pengamanan, kebijakan pengamanan dan prosedur yang didesain dengan baik dan benar akan mencegah kerusakan dan penghematan uang.

Permasalahan

Dalam pembuatan desain SIM-Integrasi, desainnya terfokus pada bagaimana data untuk masing msing subsistem disimpan dalam bentuk elektronik atau dengan kata lain fokusnya hanya pada model atau metode penyimpanan data dan cara mengintegrasikan data data tersebut kedalam suatu sistem. Sedangkan masalah bagaimana mengamankan SIM-Integrasi dari *Physical Acces* dan *Logical Access* secara terinci belum dianalisis dan didesain. Penelitian ini akan fokus kepada masalah tersebut yaitu bagaimana memberikan proteksi optimal kepada SIM-Integrasi agar dapat memberikan layanan selama 24 jam sehari.

Tujuan

Penelitian ini bertujuan untuk

- Mendesain Model dari *SIM-Integrasi Security Managemen* yang dapat digunakan dalam SIM-Integrasi PNJ.
- Menentukan *standard policy dan procedure* untuk meyakinkan bahwa SIM-Integrasi PNJ memiliki *standar Security Policy dan procedure* yang memadai.

Dasar Teori

Meningkatnya kemudahan akses ke ranah sistem informasi akan meningkatkan *security exposure* terhadap suatu sistem dan konsekwensinya adalah pemilik sumber informasi harus meningkatkan pengamanan terhadap *exposure* data dan informasi yang disimpan. Hal ini sebagai konsekwensi logis dari kemudahan akses. Semakin mudah akses ke sistem informasi semakin banyak orang yang ingin masuk, sebaliknya semakin sulit akses ke sistem informasi semakin sedikit orang yang ingin masuk. Dilema ini harus diterima oleh pengelolan sistem karena tujuan dari dibuatnya sistem adalah untuk memudahkan pengguna akses ke sistem database, kemudahan berarti harus meningkatkan keamanan dari sistem tersebut.

Akses Pisik dan Akses Logikal

Ancaman terbesar untuk aset sistem informasi tertuju kepada data. Data merupakan aset sistem informasi yang paling penting diantara

aset sistem informasi lainnya.[i](Masjono, 2007). Masuk/akses ke tempat penyimpanan data perlu diproteksi sedemikian rupa agar hanya orang yang diberi otoritas saja yang dapat masuk dan jika bisa masuk/akses, tidak akan memilik hak yang luarbiasa, pasti ada batasannya sehingga untuk melakukan sesuatu tindakan curang terhadap data dipastikan ada orang ke 2 dan atau ke 3 yang akan terlibat didalamnya.

Nilsen (2002) mengatakan bahwa memaintain akses pisik secara baik sama pentingya dengan memaintaian akses logikal, tetapi keduanya sangat saling bergantung. Lebih jauh dikatakan bahwa ada beberapa sumber malapetaka yang dapat timbul karena faktor alam atau faktor manusia dan dapat mengakibatkan kegiatan bisnis suatu organisasi tidak dapat dilanjutkan. Organisasi dapat menganalisis berbagai resiko yang mungkin timbul dan melakukan tindakan yang penting untuk mengamankan aset sistem informasi. Salah satunya adalah program manajemen pengamanan aset sistem informasi didasarkan kepada adanya kebijakan komunikasi yang jelas, praktis dan mudah dipahami.

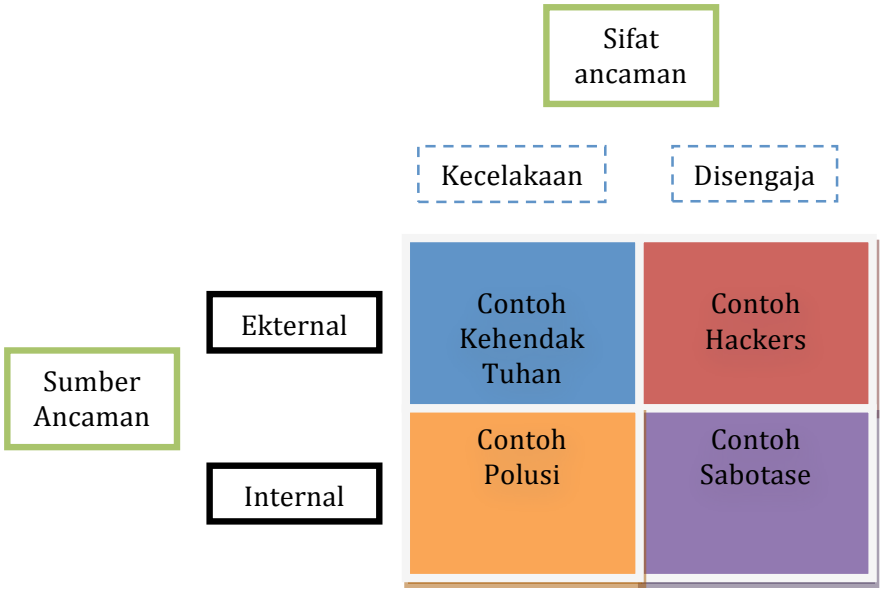
Pengendalian Keamanan

Pengendalian keamanan suatu SIM-Integrasi artinya merencanakan dan mengendalikan bagaimana cara terbaik untuk menghadapi berbagai kemungkinan gangguan keamanan terhadap suatu SIM Pengendalian Keamanan suatu SIM-Integrasi merupakan suatu keharusan bagi pihak manajemen untuk merencanakannya dengan baik. Pengembangan perencanaan keamanan sistem secara menyeluruh sering terabaikan karena umumnya perusahaan lebih terfokus kepada beroperasinya SIM-Inegrasi untuk memperlancar proses bisnis. Ketika suatu kejadian menimpa SIM-Inegrasi dan berakibat fatal, misalnya *Server Down* sehingga tidak dapat melayani aktivitas bisnis, maka setelah kejadian tersebut baru disadari betapa pentingnya merencakan keamanan sistem secara menyeluruh.

Pengendalian keamanan secara komprehensive yang telah dibuat perlu di *update* secara terus menerus karena ada kecenderungan bahwa ancaman terhadap SIM-Inegrasi semakin canggih dan semakin gampang untuk diterobos oleh penyusup (*intruder*). Salah satu hal yang terpenting adalah meng*update* secara terus menerus metode keamanan sistem secara komprehensive.

SIM-Inegrasi menghadapi ancaman dari berbagai sudut, secara umum ancaman tersebut datang dari dua kelompok besar yaitu karena kecelakaan, karena disengaja kedua kelompok ancaman ini bisa datang dari ekternal organisasi maupun internal organisasi. Lihat gambar berikut ini

Gambar 1. Ancam terhadap SIM-Integrasi



Tanggung jawab masalah keamanan SIM-Integrasi terletak pada administrator keamanan sistem informasi. Bagi organisasi yang besar dan mampu bisa mendudukan administrator keamanan ini dalam suatu struktur organisasi resmi sedangkan untuk organisasi kecil bisa mendelegasikan tugas administrator keamanan sistem secara bergilir, misalnya direktur utama atau seorang akuntan atau salah satu wakil direktur. Dalam organisasi yang menengah peran keamanan sistem informasi dapat ditugaskan kepada direktur sistem informasi.

Tugas utama dari adaministrator keamanan sistem informasi adalah menjalankan program keamanan sistem informasi diantarnya adalah secara reguler mereview kembali program keamanan untuk meyakinkan aset sistem informasi terlindungan dari berbagai ancaman secara baik. Dalam program keamanan sistem informasi dapat digunakan dua tipe proteksi yang dapat digunakan untuk menjaga aset sistem informasi. Pertama *proteksi terhadap akses ke sistem informasi secara pisik*. Kedua *proteksi terhadap akses secara logikal terhadap sistem informasi.*

Pengendalian askes secara logikal adalah pengendalian akan kemampuan masuk ke sistem informasi dengan menggunakan fasilitas atau sistem operasi atau infrastuktur telekomunikasi untuk membaca, memodifikasi mengeksekusi file dan menghapus data yang ada di suatu sistem informasi. Sedangkan pengendalian akses pisik adalah membatasi akses secara pisik ke fasilitas sistem informasi.

Faktor kritis untuk sukses mengamankan sistem informasi terletak pada komitmen manajemen akan pentingnya proteksi sistem informasi karena untuk mengimplementasikan manajemen keamanan sistem informasi dengan baik diperlukan kebijakan dan prosedur dan organisasi yang diperlukan pengesahan dari pihak manajemen.

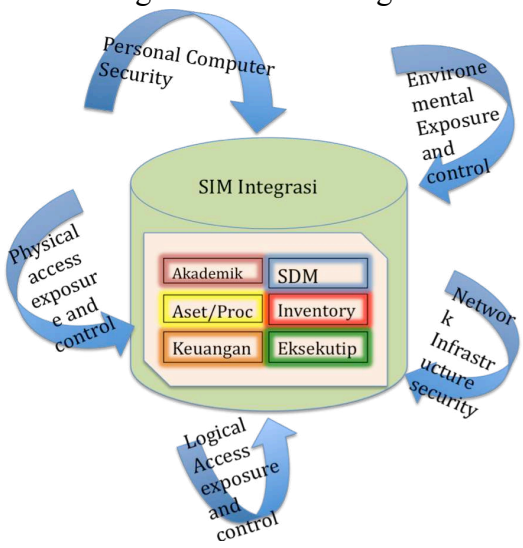
Metode Penelitian

I-MIS yang sedang dibangun akan melibatkan semua unit dan jurusan yang ada di PNJ. PC yang tersebar di masing masing unit dan jurusan tesebut akan di analisis terhadap keberadaan perangkat keras dan perangkat lunak yang saat ini digunakan untuk mengetahui jumlah dan penggunaan PC, kegunaan, pengamanan dan siapa saja yang

berhak menggunakan peralatan tersebut. Disamping itu juga akan dikaji tingkat pengamanan yang ada. Untuk mendapatkan informasi ini akan dilakukan survei dengan menggunakan kuesioner yang mencakup keberadaan PC, sistem jaringan, kegunaan, intensitas penggunaan, metode yang ada untuk mengamankan perangkat keras dan perangkat lunak. Kesesuaian dengan domain pengamanan yang ada pada CISA review Manual merupakan indikator dari keberhasilan survei ini. Hasil dari susrvei ini adalah model, sistem dan prosedur yang harus ada dalam mengimplementasikan I-MIS agar aman dan dapat digunakan tanpa ada gangguan.

Hasil dan pembahasan

Gambar 2: Model Pengendalian dan Pengamanan SIM-Integrasi



Untuk menghadapai berbagai ancaman yang ada pada suatu sistem informasi. Diperlukan berbagai bentuk pengendalian agar ancaman tersebut dapat di minimalkan hingga pada tingkat terendah.

Model yang ada di gambar diatas mencerminkan pengendalian yang harus ada pada suatu sistem informasi manajemen yang terintegrasi. Lima domain pengendalian yang ada pada model tersebut pada tingkat minimal sudah harus diimplementasikan pada masing masing aplikasi yang digunakan.

Kelima domain tersebut adalah

1. *Locical access exposure and control*

Dalam mengimpelementasikan desain dan prosedur untuk proteksi SIM-Integrasi pengendalian logikal merupakan cara atau alat utama untuk memprotek semua sumber daya yang ada pada SIM-Integrasi guna meminimalkan kerugian sampai pada tingkat yang dapat diterima organisasi.

2. *Network Infrastructure security*

Sistem jaringan dan komunikasi (LAN,WAN) termasuk program, file pendukung dan peralatan yang terhubung ke sistem jaringan. Pengendalian terhadap sistem jaringan ini dapat dilakukan melalui *network terminal control* dan menggunakan software khusus untuk pengendalian sistem jaringan dan komunikasi

3. *Environmental exposure and control*

Pengendalian lingkungan umumnya ditujukan kepada pengendalian terhadap gangguan ganguan yang sifatnya dari alam, misalnya ganguan tegangan petir, tegangan dan arus listrik, gempa bumi, letusan gunung api, angin topan, keadaan cuaca yang luar biasa. Situasi ini akan menimbulkan beberapa masalah, salah satunya adalah kehilangan sumber daya (listrik) yang akan berakibat kepada gangguan jasa pelayanan SIM-Integrasi.

4. *Physical access exposures and control*

Pemberian akses pisik ke SIM-Integrasi dapat mengakibatkan kerugian, legal repercussion, kehilangan kredibilitas dan kerugian kompetitive. Kerugian tersebut bisa terjadi karena bencana alam dan karena kelalaian manusia yang berakibat kepada akses secara tidak sah terhadap SIM-Integrasi.

5. *Personal computer Security/Laptop/Notesbook*

Dalam lingkungan sistem komputer yang *mobile*, adalah sangat umum jika data yang sensitip dibawa dalam notesbook dan CD atau Flashdisk dimana di laptop/notesbook tersebut sulit untuk menerapkan pengendalian akses logikal dan pengendalian akses pisikal. Untuk memprotek data sensitip di

laptop/notesbook tersebut mensyaratkan pendekatan pengamanan berlapis pada akses logikal dan akses pisikal.

KEBIJAKAN DAN PROSEDUR

Untuk dapat mengamankan asset SIM-Integrasi diperlukan kebijakan dari pimpinan tertinggi dan prosedur untuk mengimplementasikan kebijakan tersebut. Kebijakan tersebut antara lain:

Kebijakan Pengendalian dan Proteksi Aset SIM-Integrasi.	**Keterangan**
Kebijakan umum tentang komitmen penggunaan dan pengamanan SIM-Integrasi	
• Komitmen tertulis dari pimpinan terhadap penggunaan dan pengamanannya SIM Integrasi dan prosedur penggunaannya.	Pimpinan dan badan normatif tertinggi
Kebijakan tentang Pengamanan SIM-Integrasi	
1. *Locical access exposure and control* Tersedianya • Kebijakan terulis, prosedur dan standard. • Kebijakan tertulis mengenai pengamanan SIM-Integrasi. • Kepedulian dan pelatihan tentang pengamanan Aset SIM-Intergasi. • Kebijakan dan prosedur kepemilikan data • Kebijakan dan prosedur pemilik data • Kebijakan dan prosedur penanggung jawab data • Kebijakan dan prosedur administrator keamanan SIM-Integrasi • Kebijakan dan prosedur pemakai SIM-Integrasi • Dokumentasi otorisasi • Kebijakan dan prosedur penghentian dan rekkretmen pegawai di SIM-Integrasi. • Kebijakan dan proses akses standard	Eksekutip
2. *Network Infrastructure security* Tersedianya • Kebijakan dan prosedur mengenai diagram sistem jaringan. • Kebijakan dan prosedur pengamanan akses remote/jarak jauh. • Kebijakan dan prosedur mengenai infrastruktur sistem jaringan dan SIM – Integrasi • Kebijakan dan prosedur pengembangan dan perubahan • Kebijakan dan prosedur perubahan yang tidak di otorisasi • Kebijakan dan prosedur pengamanan secar logikal.	Eksekutip
3. *Environmental exposure and control* Tersedianya • Detektor anti api dan asap • Pemadam kebakaran dan di inspeksi secara reguler oleh aparat pengamanan kebakaran. • Penggunaan dinding, lantai, dan ruangan komputer anti api. • Pengatur daya dan arus listrik • Adanya *Busines Continuity Plan* • Susunan pengkabelan,	Eksekutip

panel listrik. • UPS/Generator • Sistem evakuasi yang terdokumentasi dan telah di ujicobakan. • Pengotrol ruangan.	
4. *Physical access exposures and control* • Tersedianya alat pengaman akses ke ruangan SIM-Integrasi. Pengamanan akses ke o Lokasi komputer pengendali SIM-Integrasi o Ruangan printer o UPS/Generator o Peralatan komunikasi o Tape Library o Ruangan backup di luar gedung SIM-Integrasi. o Semua pintu masuk o Jendela kaca dan dinding o Dinding yang bisa dirobah posisinya o Ventilasi	Eksekutip
5. Personal computer Security Tersedianya o Serial number dari masing masing lapotop/PC o Penggunaan lock pada masing masing laptop/PC o Backup terhadap data secara reguler o Penggunaan enkripsi pada data sensitip o Password untuk sensitip data dan hanya orang yang diberi otorisasi	Eksekutip
yang bisa membaca data tersebut. o Respon cepat terhadap terjadinya pencurian laptop/notes books.	

Kesimpulan

Lingkungan organisasi telah sangat mendukung penggunaan SIM-Integrasi. Adanya sistem jaringan yang penggunaan belum optimal masih menyimpan potensi besar untuk digunakan sebagai basis SIM-Intergasi.

Pengguna dilevel pimpinan sudah penduli dengan penggunaan sistem jaringan dan komputer namun baru sebatas alat pengolah infomasi. Diperlukan kebijakan dan prosedur yang lebih mendukung implementasi SIM-Integrasi dan pengamamannya.

SIM-Integrasi memerlukan dukungan dari pimpinan dan jajarannya untuk di implementasikan serta diamankan penggunaannya dari berbagai potensi gangguan. Pengamanan dan pengendalian aset SIM-Integrasi meliputi lima domain yaitu

- *Locical access exposure and control/Pengendalian akses logikal*
- *Network Infrastructure security/Pengendalian dan pengamanan sistem jaringan*
- *Environmental exposure and control/Pengendalian lingkungan*
- *Physical access exposures and control/Pengendalian akses pisikal*
- *Personal computer Security/Pengendalian penggunan PC/Lapotop/Notesbook*.

Untuk dapat di implementasikannya SIM-Integrasi dan pengamanannya diperlukan kebijakan dan prosedur

- Kebijakan umum tentang komitmen penggunaan dan pengamanan SIM-Integrasi

- Kebijakan dan prosedur tentang Pengamanan aset SIM-Integrasi

Saran

Untuk mengimplementasikan SIM-INtegrasi diperlukan beberapa pijakan atau komitment dari pimpinan yang diikuti oleh prosedur untuk implementasinya. Dimulai dari kebijakan umum tentang penggunaan SIM-Integrasi hingga proseudur pengamaman SIM-Integrasi yang mengacu kepada lima domain proteksi asset sistem informasi

Daftar Acuan

[1] Masjono, Ali. (2008). "Teknik Audit Berbantuan Komputer". Depok:UP2AI- Politeknik Negeri Jakarta

[2] Nilsen, Odd (2002). "Protection of Infomation Asset" SAN Institute InfoSec Reading Room

[3] ISACA (2007). " Information System Audit and Control"; CISA Review Manual 2007.

[4]Weber, R (1999). "Infomation Systems Control and Audit" New Jersy: Prentice-Hall, Inc.

[5] Gondowiyoto, Sanyoto(2007) "Audit Sistem Informasi+Pendekatan CobIT" Edisi revisi, Jakarta: Mitra Wacana Media.

[6] Hall, James A (2006) "Sistem Informasi Akuntansi" buku 1,2 Jakarta:Salemba Empat.

[7] Hall, James A (2011)"Information Technology Auditing" Internatonal Edition, Third Edition, United States; South-Western Cengage Learning.