Materi 4

Keamanan Sistem Informasi

3 SKS | Semester 8 | S1 Sistem Informasi | UNIKOM | 2015
Nizar Rabbi Radliya | nizar.radliya@yahoo.com

Nama Mahasiswa	
NIM	
Kelas	

Kompetensi Dasar

Memahami manajemen resiko sistem informasi.

Pokok Bahasan

Manajemen Resiko Sistem Informasi
1. Definisi resiko
2. Manajemen resiko
3. Resiko pada sistem informasi
4. Manajemen resiko sistem informasi
5. PMBOK

I. Definisi Resiko

Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko.

Akan tetapi resiko yang ditetapkan pada saat sebelum melakukan kegiatan tidak selalu muncul dan terkadang ada resiko baru diluar resiko yang telah ditetapkan. Maka dari itu resiko juga berkaiatan dengan ketidak pastian. Kesimpulannya, ada resiko yang sudah diketahui diawal dan ada resiko yang belum diketahui diawal tapi muncul pada saat kegiatan sudah berjalan.

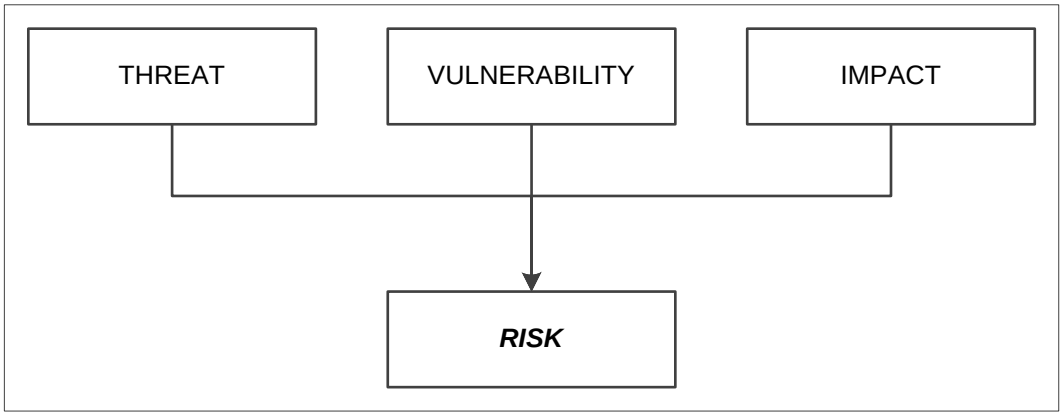
II. Manajemen Resiko

Manajemen resiko merupakan sekumpulan proses dalam mengelolah resiko yang timbul dalam sebuah kegiatan atau proyek. Adapun bentuk pengelolaan terhadap resiko adalah dengan cara mengidentifikasi atau menganalisa resiko yang akan timbul; lalu mengurangi, mencegah atau bisa dikatakan sebagai proses mengupayakan berbagai tindakan preventif untuk meminimalisasi dampak negatif dari resiko yang ada; serta yang terakhir adalah melakukan evaluasi terhadap resiko yang muncul dan penanggulangan terhadap resiko tersebut.

Pengertian diatas telah menyatakan bahwa manajemen resiko bukanlah sebuah produk, melainkan sekumpulan proses yang harus dilakukan mengikuti siklus proyek yang dijalankan guna menanggulangi resiko-resiko yang timbul. Oleh karena itu kita tidak dapat memandang bahwa manajemen resiko merupakan produk yang siap digunakan dan mengabaikan proses-proses dalam manajemen resiko pada saat proyek berlangsung dan sebelum-sesudah pelaksanaan proyek tersebut.

III. Resiko Pada Sistem Informasi

Risk (resiko) merupakan kombinasi dari komponen kejadian yang menyangkut ancaman (*threat*), kelemahan (*vulnerability*), dan dampak (*impact*). Kelemahan sistem sebagai penunjang bisnis perusahaan yang dapat dimanfaatkan oleh pihak lain untuk menguasai sistem dapat dimengerti sebagai *vulnerability*. Sedangkan *impact* merupakan penilaian atas pengaruh ancaman yang dilakukan terhadap aset maupun tujuan dari organisasi, dengan memanfaatkan kelemahan sistem.



Gambar 1. Kombinasi Komponen Berkaitan Dengan Resiko

Berikut jenis *impact* yang menyangkut organisasi yang patut untuk dicermati pada saat menganalisis resiko:

1. Kerugian atas *revenue*
2. Kerugian atas modal organisasi
3. Kerugian mengenai reputasi di pasar
4. Menghilangnya kesempatan bisnis (*business opportunity*)
5. Kerugian di pasar modal
6. Kehilangan kepercayaan pelanggan, karyawan dan pemegang saham
7. Melanggar regulasi dan syarat-syarat hukum/legal
8. Tercemarnya nama baik organisasi.

Terdapat sumber lain yang menyatakan bahwa ada tiga komponen yang memberikan kontribusi kepada *Risk*, yaitu *Asset*, *Vulnerabilities*, dan *Threats*. Beberapa hal yang dapat berkontribusi memberikan resiko dari ketiga komponen tersebut dapat dilihat pada tabel 1 di bawah ini.

Tabel 1. Kontribusi Terdap resiko dari Komponen *Asset*, *Vulnerabilities*, dan *Threats*

Komponen	Contoh Resiko
Asset	hardware software dokumentasi data komunikasi linkungan manusia
Vulnerabilities	pemakai (*users*) teroris kecelakaan (*accidents*) *crackers* penjahat kriminal nasib (*acts of God*) intel luar negeri (*foreign intelligence*)
Threats	*software bugs* *hardware bugs* radiasi (dari layar, transmisi) *tapping*, *crosstalk* *unauthorized users* cetakan, hardcopy atau print out keteledoran (*oversight*) *cracker* via telepon storage media

Untuk menanggulangi resiko (*Risk*) tersebut dilakukan apa yang disebut "*countermeasures*" yang dapat berupa:

1. Usaha untuk mengurangi *Threat*
2. Usaha untuk mengurangi *Vulnerability*
3. Usaha untuk mengurangi *Impact*
4. Mendeteksi kejadian yang tidak bersahabat (*Hostile Event*)
5. Kembali (*Recover*) dari kejadian

Beberapa contoh resiko dalam proyek IT berdasarkan tipe ketidakpastian resiko:

1. Known

Contoh: Mengenai kebutuhan data dan informasi dari pihak yang mengadakan proyek IT (yang akan menggunakan hasil dari proyek tersebut) kadangkala lambat dan

susah diperoleh. Hal ini sudah terbiasa dan merupakan resiko yang dapat diketahui sebelum proyek berlangsung. Maka dari itu pada tahap kontrak pelaksanaan proyek sebagai pihak pelaksana proyek IT harus memberikan pemahaman bahwa guna kelancaran proyek, pihak penyedia data dan informasi harus selalu tanggap pada setiap kebutuhan yang diminta.

2. Known-Unknown

Contoh: Hasil dari proyek IT yang dilaksanakan khususnya proyek yang menghasilkan perangkat lunak terkadang terdapat permasalahan dari segi antarmuka dari sistem yang telah dibangun. Antarmuka sistem biasanya tidak sesuai dengan harapan atau keinginan user. Hal ini merupakan resiko yang dapat diketahui dan tidak diketahui, karena terkadang antarmuka yang telah kita rancang sesuaikan dengan permintaan user hasilnya tidak sesuai dengan kenyataan keinginan user tersebut.

3. Unknown

Contoh: Resiko yang tidak dapat diketahui adalah kesalahan pada tahapan implementasi pemorgraman dalam proyek IT pembangunan perangkat lunak. Bentuk kesalahan yang tidak diketahui tersebut adalah kesalahan dari komponen pemrograman yang telah dibangun oleh pihar programmer.

IV. Manajemen Resiko Sistem Informasi

Manajemen resiko sistem informasi merupakan cikal bakal pembuatan kebijakan keamanan sistem informasi pada setiap organisasi. Sebelum membuat kebijakan keamanan sistem informasi, sangat penting untuk memahami dan mengidentifikasi sumber daya yang dimiliki oleh organisasi sehingga dapat membedakan sumber daya mana yang harus dilindungi dan menetapkan skala prioritas pada setiap sumber daya tersebut. Hal ini sangat penting karena berkaitan dengan biaya.

Manajemen resiko sistem informasi melibatkan penentuang:

1. Apa yang harus diproteksi dan dikontrol oleh organisasi.
2. Apa yang dibutuhkan untuk memproteksinya.
3. Bagaimana cara memproteksi dan mengontrolnya.
4. Menentukan skala prioritas.

Tujuan utama pada saat kegiatan manajeman resiko sistem informasi adalah mengidentifikasikan proteksi dan kontrol terhadap informasi. Dimana nantinya tujuan utama dari proteksi terhadap informasi adalah menciptakan lingkungan yang aman dan terjamin bagi manajemen untuk melakukan tugasnya.

Manajemen resiko proyek juga dapat mengubah resiko menjadi kesempatan yang menguntungkan. Hal tersebut dapat terjadi apabila kita memiliki langkah yang strategis dalam menanggulangi resiko yang muncul pada saat pelaksanaan proyek. Untuk dapat memudahkan pemahaman dari tujuan tersebut kita lihat dari contoh resiko yang muncul pada proyek IT. Misalkan kita dalam pelaksanaan proyek IT terkendala dengan pengadaan server yang terlalu rumit dan memerlukan biaya yang sangat tinggi. Resiko tersebut diketahui setelah proyek berlangsung, sedangkan teknologi dan biaya yang tersedia tidak memungkinkan untuk menanggulangi resiko tersebut. Dalam artian kita akan mengalami kerugian dari segi keuangan apabila kita membangun server tersebut.

Sebetulnya ada cara penanggulangan resiko tersebut. Kita dapat mengubah resiko yang menjadi ancaman tersebut menjadi sebuah kesempatan yang menguntungkan. Penanggulangannya yaitu dengan cara kita tidak perlu membangun server tersebut melainkan menyewa server yang disediakan oleh konsultan IT. Dengan hal tersebut kita dapat menghemat biaya yang tersedia. Untuk biaya penyewaannya kita dapat alokasikan sebagai biaya pemeliharaan dan hasilnya kita sebagai pihak pelaksana proyek akan lebih diuntungkan.

V. PMBOK

PMBOK (*A Guide to the Project Management Body of Knowledge*) adalah suatu buku yang memuat himpunan istilah dan pedoman untuk manajemen proyek. PMBOK diterbitkan oleh *Project Management Institute* (PMI). Edisi pertamanya diterbitkan pada tahun 1996 dan edisi keempatnya pada 31 Desember 2008. PMBOK ini lah yang merupakan metodologi/konsep dasar yang harus dipahami dan diperhatikan oleh seorang *Project Manager* ataupun praktisi dalam proyek managemen. Pedoman PMBOK membagi proyek menjadi 42 proses yang dikelompokkan ke dalam 5 kelompok proses dan 9 area pengetahuan.

Kelompok proses (*process group*) dalam PMBOK adalah sebagai berikut.

1. Inisiasi
2. Perencanaan
3. Pelaksanaan
4. Pemantauan dan pengendalian
5. Penutupan

Area pengetahuan (*knowledge area*) dalam PMBOK adalah sebagai berikut.

1. Integrasi

2. Lingkup
3. Waktu
4. Biaya
5. Kualitas
6. SDM
7. Komunikasi
8. Risiko
9. Pengadaan

Kesembilan area tersebut terbagi atas 2 fungsi, yaitu Fungsi Utama (*Core Function*) dan Fungsi Pendukung (*Facilitating Function*).

Fungsi Utama terdiri dari:

1. Majemen Ruang Lingkup (*Scope Management*)
2. Manajemen Waktu (*Time Management*)
3. Manajemen Biaya (*Cost Management*)
4. Manajemen Kualitas (*Quality Management*)

Fungsi pendukung terdiri dari:

1. Manajemen SDM (*HR Mangement*)
2. Manajemen Komunikasi (*Communication Management*)
3. Manajemen Resiko (*Risk Management*)
4. Manajement Pengadaan Proyek (*Procurement Management*)

Area yang terakhir adalah Manajemen Integrasi proyek (*Project Integration Management*), yang berfungsi mengkolaborasikan antar Fungsi Utama dan Fungsi Pendukung di tambah dengan *Tools* dan Teknik- teknik untuk mencapai kesuksesan sebuah proyek.

VI. Daftar Pustaka

[1] IBISA. 2011. Keamanan Sistem Informasi. Yogyakarta: Andi.
[2] Isa, I. 2012. Evaluasi Pengontrolan Sistem Informasi. Yogyakarta: Graha Ilmu.
[3] Laudon, K.C. & Laudon, J.P. 2005. Sistem Informasi Manajemen: Mengelola Perusahaan Digital, Edisi 8. Yogyakarta: Andi.
[4] Sarno, R. & Iffano, I. 2010. Sistem Manajemen Keamanan Informasi (Berbasis ISO 27001). Surabaya: ITS Press.

VII. Materi Berikutnya

Pokok Bahasan	*Logical Security*
Sub Pokok Bahasan	1. Tujuan *logical security*

	2. Aplikasi *logical security* 3. Tanggung jawab pemberian kontrol 4. Evaluasi pengontrolan