ANALISA RESIKO KEAMANAN INFORMASI SEBAGAI STRATEGI MITIGASI RESIKO PADA TOKO ONLINE "X"

Tony Soebijono[1)]
1) Program Studi/Jurusan Sistem Informasi, STIKOM Surabaya, email: tonys@stikom.edu

Abstract: One important factor for the company is to take into account in any of its operations, so that the risk need to be managed. These activities include process, namely risk analysis and, risk mitigation. Quantitative risk analysis tries to give an objectively monetary value to a component for the assessment of risk and potential losses. In this research, it was done asset grouping related directly to the operations of online store 'X', which resulted in several tables of assets.

The results of the analysis were used as a risk mitigation strategy that can be used to conduct risk reduction recommendations, which is to be divided into four quadrants, so the grouping of threat and vulnerability in performing risk mitigation strategy was focused. After doing calculation using ROI, not all electoral safeguards to address the threat deserves to be implemented.

Keywords: Keywords: Management, Risk, Assessment, Mitigation, Quantitative, ROI.

Peranan teknologi informasi (TI) dalam dunia bisnis mempunyai peranan penting bagi perusahaan serta para manajer bisnisnya. Dalam pengambilan keputusan strategis, TI akan mempengaruhi keberlanjutan operasional, yang akan membawa perubahan pada organisasi tersebut. Setiap perusahaan memiliki cara yang berbeda dalam menghadapi resiko TI. Perbedaan yang pertama, resiko-resiko tersebut tidak secara terbuka dipertimbangkan. Kedua, hanya terdapat sedikit *tools* atau *instruments* untuk menangani resiko yang tampak. Ketiga, terdapat proses-proses dalam perusahaan yang tidak bereaksi terhadap resiko (Ernie Jordan; 2005). Semakin besar ketergantungan perusahaan pada TI, semakin besar pula resiko yang akan dihadapi perusahaan tersebut.

Resiko adalah suatu kesempatan yang berdampak negatif, perusahaan dapat memperkecil resiko dengan melakukan antisipasi berupa kontrol, namun tidak mungkin dapat sepenuhnya menghindari resiko, bahkan dengan struktur pengendalian maksimal sekalipun (Gondodiyoto; 2007). Analisa terhadap resiko pada dasarnya menggunakan pendekatan *risk management*, yang digunakan untuk membantu mengidentifikasikan ancaman dan memilih kriteria ukuran keamanan yang menghasilkan *cost effective* (Hiles; 2002).

Oleh karena itu untuk meningkatkan jaminan tercapainya tujuan, strategi, sasaran dan target organisasi, perlu melakuan identifikasi resiko, melakukan pengukuran resiko serta mengelola resiko.

Toko online "X" adalah toko yang memanfaatkan *online webstore* sebagai media penjualan berbagai produk *shopping goods*, salah satu fitur layanan yang dimiliki adalah dengan memberikan layanan dalam bentuk pembayaran dengan menggunakan kartu kredit selain menggunakan transaksi transfer bank. Hal ini terkait dengan database pelanggan, maka keamanan informasi menjadi prioritas untuk diperhatikan. Tingkat keamanan informasi yang rendah akan mendorong para *hacker* untuk melakukan penyerangan dan penyusupan untuk mendapatkan database pelanggan *(unauthorized access)*. Akan tetapi selain resiko tersebut ada beberapa resiko yang juga mungkin akan terjadi yaitu: *malicious code, internet service down, administration failure, theft of laptop or pc, earthquake or fire, client or server failure, power failure.*

Terkait dengan permasalahan diatas, maka dapat diidentifikasikan permasalahan penelitian yaitu, bagaimana melakukan analisa resiko sebagai strategi mitigasi resiko pada toko online "X" terkait dengan

keamanan informasi. Penelitian ini bertujuan untuk melakukan analisa resiko keamanan informasi serta memperoleh hasil yang berguna untuk pemitigasian resiko. Beberapa perangkat yang dapat dipergunakan untuk menganalisa resiko adalah *Single Lost Expectancy* (SLE), *Annualized Rate of Occurance* (ARO), *Exposure Factor* (EF), *Annual Loss Expectancy* (ALE) dan *Return on Investment* (ROI).

Manajemen resiko merupakan suatu tindakan untuk meminimalisir kemungkinan terjadinya resiko pada aset organisasi. Menghilangkan sama sekali resiko adalah merupakan sesuatu yang tidak mungkin, dari adanya resiko yang mungkin terjadi terdapat beberapa parameter yang menjadi pertimbangan untuk dimanajemen. Diantara parameter tersebut adalah *impact* (akibat) dan probabilitas atas kejadian resiko tersebut. Variabel kunci dan persamaan yang dipergunakan untuk melaksanakan suatu analisis resiko kuantitatif adalah sebagai berikut (Ding; 2003).

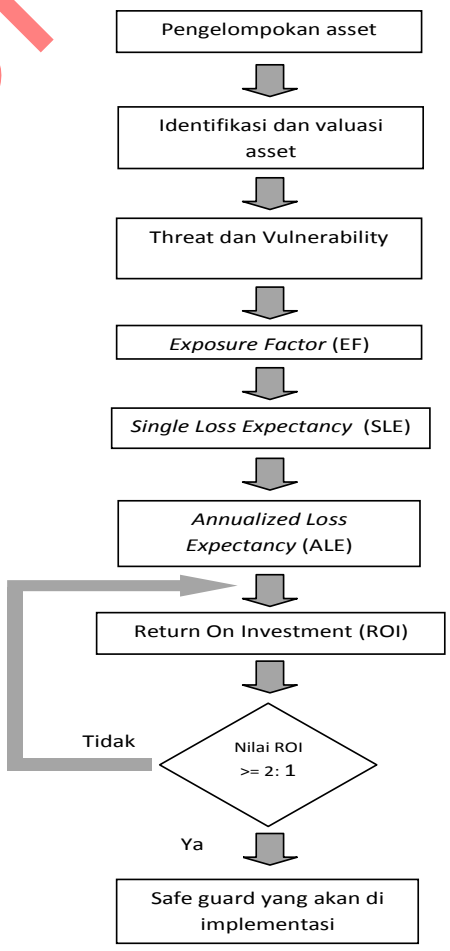
a. *Exposure Factor* (EF) = Persentase suatu asset loss yang disebabkan oleh identifikasi threat yang ranges-nya antara 0% sampai 100%.
b. *Single Loss Expectancy* (SLE) adalah nilai kerugian terhadap asset bila sebuah resiko yang teridentifikasi terjadi.
   SLE = Asset Value x EF,
c. *Annualized Rate of Occurrence* (ARO) adalah perkiraan atau estimasi frekuensi sebuah resiko yang dapat terjadi dalam setahun.
d. *Annualized Loss Expectancy* (ALE) adalah nilai estimasi kerugian pertahun terhadap asset, jika sebuah resiko yang teridentifikasi terjadi.
   ALE=SLE x ARO,
e. *Return On Investment* (ROI) adalah rasio nilai perolehan suatu investasi relatif terhadap sejumlah nilai yang diinvestasikan. Pada analisa resiko keamanan informasi, ROI digunakan untuk mengambil keputusan apakah suatu tindakan penanganan resiko hasil analisa resiko pantas untuk dilaksanakan.
   ROI=(ALE *current* – ALE *projected*) / *Annual Cost Investation.*

ALE *current* adalah estimasi ALE saat sebelum dilakukan tindakan penanggulangan terhadap resiko, sedangkan ALE *projected* adalah estimasi ALE saat setelah dilakukan tindakan penanggulangan terhadap resiko *(safeguard).*

Safeguard digunakan untuk mengidentifikasi mekanisme, service, atau prosedur yang dapat mencegah atau mengurangi terjadinya *threat* yang dapat mengeksploitasi *vulnerability*. Secara fungsional, *safeguard* berhubungan dengan area *confidentiality*, *integrity*, dan *available*.

METODE

Untuk melakukan suatu analisis resiko secara kuantitatif, perlu menentukan hubungan suatu nilai



Gambar 1. Alur Metode Penelitian

dari kerugian-kerugian potensial dengan proses yang tertunda, kerusakan properti, atau data. Kemudian perlu juga dilakukan perkiraan kemungkinan kejadian dari kegagalan resiko, sehingga akhirnya dapat diperhitungkan perkiraan kerugian pertahunnya. Dalam penelitian ini, diterapkan metodologi *risk assessment* yang digambarkan pada Gambar 1.

Analisis karakteristik dari sistem TI, melakukan identifikasi ancaman, melakukan identifikasi kelemahan, penentuan kecenderungan, analisis dampak yang kurang baik dapat dilakukan secara kuantitatif, menentukan tingkatan resiko dan melakukan rekomendasi pengendalian mengurangi resiko.

Setelah melakukan analisa resiko, langkah berikutnya adalah menerapkan metodologi *risk mitigation* yang terdiri dari: prioritas tindakan untuk suatu resiko, rekomendasi pengendalian dalam proses penilaian resiko, analisis dan pemilihan pengendalian *cost-effective*, mengembangkan rencana implementasi untuk *safeguard*, dan pengendalian implementasi yang dipilih.

Pengelompokkan Asset

Di dalam memperkirakan penilaian resiko untuk suatu sistem IT, langkah yang pertama adalah menggambarkan lingkup usahanya *(scope of the effort)*. Pada langkah ini, batasan-batasan dari IT mulai diidentifikasi, bersama dengan sumber daya dan informasi yang menjadi dasar sistemnya. Karakter suatu sistem IT dikenali, untuk menetapkan ruang lingkup usaha penilaian resiko, menggambarkan batasan-batasan otorisasi operasional, dan menyediakan informasi yang penting untuk menjelaskan resiko, konektifitas sistem, dan bagian yang bertanggung jawab atau dukungan sumber daya manusianya.

Dari hasil analisis sistem pada toko online “X” secara umum, didapatkan pengelompokan aset mengenai aset sebagai berikut:

a. *Information Aset*, terdiri dari juklak, juknis, data keuangan perusahaan, data konsumen, dan data personil perusahaan.
b. *Paper Document*, terdiri dari surat izin usaha, kontrak kerja.
c. *Software Aset*, terdiri dari website, database, aplikasi perkantoran, sistem operasi.
d. *Physical Aset*, terdiri dari gedung, PC desktop, notebook dan server.
e. *People*, terdiri dari karyawan toko online “X” dan karyawan *outsourching*,

Identifikasi dan Valuasi Aset

Berdasarkan data-data dari hasil analisis sistem yang sedang terjadi di toko online “X” dan formula perhitungan analisis resiko secara kuantitatif, didapatkan hasil yang sudah bernilai *tangible*.

Tabel 1.Valuasi Aset

No.	Asset	Jumlah	Nilai Satuan	Total
1	PC desktop: Client Dell Vostro 460 MT	4 unit	8.816.000	35.264.000
2	PC Notebook: Client Toshiba Satellit L735	3 unit	6.570.000	19.710.000
3	Server Dell Power Edge T310	1 unit	14.720.000	14.720.000
4	Printer Epson L100	2 unit	1.395.000	2.790.000
5	Switch Allied Telesis AT-G S950	1 unit	2.683.000	2.683.000
6	Operating System	8 paket	1.800.000	14.400.000
7	Aplikasi Toko Online	1 paket	10.000.000	10.000.000
8	Website	1 paket	4.000.000	4.000.000
9	Database Konsumen	1 paket	18.000.000	18.000.000
10	Aplikasi Kantor	1 paket	2.600.000	2.600.000
11	Karyawan Toko Online "X"	8 orang	2.750.000	22.000.000
12	Karyawan Outsourcing	4 orang	1.250.000	5.000.000
13	Data Elektronik	1 unit	15.000.000	15.000.000
14	Gedung dan Sarana	1 unit	750.000.000	750.000.000

Sumber: Inventaris Toko Online "X" Diolah

Threat and Vulnerability pada Toko Online "X"

Vulnerability merupakan kelemahan yang ada pada aset dalam suatu organisasi. *Vulnerability* tidak menyebabkan rusaknya suatu aset, melainkan menciptakan suatu kondisi yang dapat mengakibatkan *threat* terjadi. Hal ini dapat dialkukan dengan mengembangkan daftar rincian *vulnerability* (kekurangan atau kelemahan) yang dapat dieksploitasi atau dimanfaatkan oleh potensi *threat*.

Sumber ancaman tidak akan menghasilkan resiko jika tidak ada *vulnerability* yang digunakan. Tujuan dari langkah ini adalah untuk mengidentifikasi potensi dari sumber ancaman dan melakukan penyusunan suatu daftar yang memaparkan ancaman potensi sumber ancaman sehingga dapat diterapkan pada sistem TI yang dievaluasi. Suatu sumber ancaman digambarkan sebagai suatu keadaan atau peristiwa yang memiliki potensi dapat menyebabkan kerusakan pada suatu sistem TI. Pada umumnya, sumber ancaman berasal dari alam, manusia, atau lingkungan.

Tabel 2. Threat pada Toko Online X

Classifi-cation	Threat	ARO	Source	C	I	A
Deliberate	Unauthorized Access	1	Information Gathering Techniques	x	x	
Deliberate	Malicious Code (Virus, Trojan, etc)	2			x	x
Accidental	Internet Service Down	8		x	x	x
Accidental	Administration Failure	4		x	x	x
Deliberate	Theft of Laptop/PC	0.25		x	x	
Nature	Earthquake/ Fire	0.1				x
Accidental	Client/Server Failure	6			x	x
Accidental	Power Failure	5				x

Exposure rating (EF) yang dimiliki setiap aset nilainya berbeda terhadap suatu *threat*, sehingga terdapat asset yang *invulnerable* terhadap *threat* dan terdapat pula aset yang sangat *vulnerable* terhadap *threat.* Persentase penilaian suatu aset loss yang disebabkan oleh identifikasi threat, pemberian estimasi range-nya diantara 0% sampai 100%.

Tabel 3. Estimasi Nilai EF

Value	Description
0%	Aset tahan terhadap ancaman (threat)
20%	Kerusakan kecil
40%	Tingkat kerusakan menengah, akan terjadi delay dalam pekerjaan
60%	Tingkat kerusakan besar, pekerjaan sudah mengalami delay
80%	Tingkat kerusakan besar, pekerjaan sudah mengalami interupsi
100%	Kerusakan fatal, pekerjaan terhenti dan sistem membutuhkan total replacement

HASIL DAN PEMBAHASAN

Berdasarkan daftar aset hasil identifikasi valuasi aset (Tabel 1), maka dilakukan analisa resiko, dari hasil analisa diharapkan akan didapatkan nilai ROI untuk mengetahui apakah tindakan penanganan resiko memiliki kepantasan untuk dieksekusi. Adapun biaya-biaya *safeguards* yang muncul akan menjadi *Annual Cost Investation*.

a. *Unauthorized Access*, diperkirakan dalam 1 tahun terjadi 1 kali *unauthorized access* pada toko online "X". Kejadian ini akan berdampak pada kerusakan software dan terganggunya layanan. Adapun tindakan penanganan *(safeguards)* untuk mengurangi resiko adalah: pembinaan SDM secara berkala, pembuatan Standard Operational Procedure (SOP) dan Implementasi *Cisco Intrusion Prevention Services*. Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Dari hasil perhitungan diperoleh nilai ROI: (75.245.600 – 19.721.400) / 45.500.000 = 1,22

b. *Malicious Code*, diperkirakan dalam 1 tahun terjadi 2 kali *malicious code* pada toko online "X". Kejadian ini akan berdampak pada kerusakan software dan terganggunya layanan. Adapun tindakan *safeguards* untuk mengurangi

resiko adalah: pembelian anti virus, pembuatan SOP dan pelatihan komputer. Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Karena frekuensi *malicious code* menjadi berkurang menjadi 1 kali dalam satu tahun. Dari hasil peritungan didapatkan nilai ROI: (156.491.200 – 78.245.600) / 26.500.000 = 2,95

c. *Internet Service Down*, diperkirakan dalam 1 tahun terjadi 8 kali ganguan dari *internet down* pada toko online "X". Kejadian ini akan berdampak pada terganggunya layanan dan berdampak pada menurunnya tingkat kepercayaan *customer*. Adapun tindakan *safeguards* untuk mengurangi resiko adalah: mengganti penyedia layanan internet service dan pelatihan komputer. Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Dari hasil perhitungan didapatkan nilai ROI: (354.924.800 – 26.500.000) / 177.462.400 = 6,70.

d. *Administration Failure*, diperkirakan dalam 1 tahun terjadi 6 kali kesalahan administratif yang dilakukan oleh karyawan toko. Kejadian ini akan berdampak pada menurunnya tingkat kepercayaan customer. Adapun tindakan *safeguards* untuk mengurangi resiko adalah: pembinaan SDM secara berkala, pelatihan komputer-administratif dan pembuatan SOP. Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Dari hasil perhitungan didapatkan nilai ROI: (153.600.000 – 38.400.000) / 23.500.000 = 4,90

e. *Theft of laptop or PC*, diperkirakan dalam 2 tahun terjadi 1 kali tindak pencurian pada toko online "X". Kejadian ini akan berdampak pada terhentinya operasional toko. Adapun tindakan *safeguards* untuk mengurangi resiko adalah: pemasangan CCTV, penambahan SATPAM untuk shift malam dan aplikasi asuransi kerugian. Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Dari hasil perhitungan didapatkan nilai ROI: (142.546.500 – 35.636.625) / 40.500.000 = 2,64

f. *Earthquake or Fire*, diperkirakan dalam 10 tahun terjadi 1 kali bencana alam atau kejadian kebakaran. Kejadian ini akan berdampak pada terhentinya operasional toko. Adapun tindakan *safeguards* untuk mengurangi resiko adalah: pembelian alat pemadam dan detektor asap, aplikasi asuransi gedung serta menyewa data center untuk backup data toko. Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Dari hasil perhitungan didapatkan nilai ROI: (91.216.700 – 54.730.020) / 24.000.000 = 1,52

g. *Client or Server failure*, diperkirakan dalam 1 tahun terjadi 4 kali kerusakan / kesalahan penggunaan oleh operator toko. Kejadian ini akan berdampak pada terganggunya operasional toko. Adapun tindakan *safeguards* untuk mengurangi resiko adalah: pelatihan komputer, pembuatan prosedur penggunaan dan pemeliharaan jaringan. Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Dari hasil perhitungan didapatkan nilai ROI: (320.932.000 – 160.466.000) / 26.000.000 = 6,17.

h. *Power Failure*, diperkirakan dalam 1 tahun terjadi 5 kali pemadaman listrik oleh PLN. Kejadian ini akan berdampak pada terganggunya operasional toko. Adapun tindakan *safeguards* untuk mengurangi resiko adalah: pembelian UPS, pembelian genset 10 KVA beserta bahan bakar. Setelah dilakukan tindakan penanganan terhadap resiko, diperkirakan tingkat kerugian menjadi berkurang. Dari hasil perhitungan

didapatkan nilai ROI: (138.251.000 – 0) / 16.000.000 = 8,64

Dari hasil analisa diharapkan akan didapatkan nilai ROI untuk mengetahui apakah tindakan penanganan resiko memiliki kepantasan untuk dieksekusi. ROI adalah rasio nilai perolehan suatu investasi relatif terhadap sejumlah nilai yang diinvestasikan. Pada analisa resiko keamanan informasi, ROI digunakan untuk mengambil keputusan apakah suatu tindakan penanganan resiko hasil analisa pantas untuk dilaksanakan / dieksekusi. Kepantasan tersebut adalah bila ROI memiliki nilai lebih besar dari 2:1 (Palmer; 1989). Berikut adalah rekapitulasi ROI hasil analisa resiko:

Tabel 4. Rekapitulasi Nilai ROI

Rekapitulasi ROI

No.	Threat	ROI	
1	Unauthorize Access	1.22	1 : 1
2	Malicious Code	2.95	3 : 1
3	Internet Service Down	6.70	7 : 1
4	Administration Failure	4.90	5 : 1
5	Theft of Laptop or PC	2.64	3 : 1
6	Earthquake or Fire	1.52	2 : 1
7	Client/Server Failure	6.17	6 : 1
8	Power Failure	8.64	9 : 1

Adapun *threat* yang memiliki nilai ROI lebih besar dari 2:1 adalah: *Malicious code, Internet service down, administration failure, theft of laptop or PC, client/server failure dan power failure.*

Sedangkan *threat unauthorized access* dan *earthquake or fire* kurang pantas untuk diimplementasi atau dilaksanakan karena pemilihan investasi *safeguards* yang terlalu tinggi.

Risk Mitigation

Merupakan suatu metodologi yang digunakan oleh manajemen guna mengurangi resiko dari misi yang dibuat. Berdasarkan pada hasil analisa, maka toko online "X" dapat menerapkan strategi sebagai berikut:

a. Menerima sebagian atau semua potensi resiko dan melanjutkan operasional sistem atau menerapkan pengendalian untuk menurunkan resiko menjadi suatu tingkatan yang bisa diterima (kuadran I).
b. Mengurangi efek negatif dari resiko yaitu mengatur resiko dengan mengembangkan suatu rencana risk mitigation (kuadran II).
c. Menghindari resiko, dengan melakukan penanganan terhadap penyebab resiko dan konsekuensinya (kuadran III).
d. Melakukan transfer resiko kepada pihak lain dengan menggunakan suatu pilihan, untuk mengganti kerugian. Seperti pembelian polis asuransi (kuadran IV).

Berikut merupakan tabulasi dari hasil mitigasi resiko, dengan melakukan pengelompokan berdasarkan empat kuadran tersebut di atas:

Tabel 5. Strategi Mitigasi Resiko

No	Risk		Kuadran	Safeguards
	Threat	Vuherability		
1	Unauthorized Access	Toko online "X" tidak memiliki personil/alat khusus yang menangani masalah teknis hardware/networking	III	Pembinaan SDM secara berkala Pembuatan Standard Opertional Procedure (SOP); Implementasi Cisco Intrusion Prevention Service
2	Malicious Code	Antivirus yang sudah terinstall tidak diupdate untuk versi yang terbaru	II	Pembelian anti virus Pembuatan Standard Operational Procedure (SOP) Pelatihan komputer
3	Internet Service Down	Internet service provide yang selama ini digunakan tidak memberikan performa yang bagus	III	Ganti penyedia layanan internet service Pelatihan komputer

No	Risk		Kuadran	Safeguards
	Threat	Vuherability		
4	Administration failure	Pengembangan wawasan mengenai tatacara transaksi online tidak dilakukan pada semua personil	II	Pembinaan SDM secara berkala Pelatihan komputer - administratif Pembuatan Standard Opertional Procedure (SOP)
5	Theft of laptop or PC	Untuk lokasi umum yang strategis dalam melaksanakan fungsi operasional tidak dilengkapi dengan alat pemantauan	II	Penambahan CCTV pada 4 titik lokasi Penambahan 1 anggota SATPAM untuk shift malam Asuransi kerugian
6	Earthquake or fire	Belum dilakukannya kerjasama dengan pihak asuransi, khususmya terkait dengan asuransi kerugian	IV	Pembelian alat pemadam dan detektor asap Asuransi Gedung; Sewa data center untuk backup data toko
7	Client/server failure	Beberapa barang / hardware tidak sesuai dengan spesifikasi kebutuhan operasional	I	Pelatihan komputer Pembuatan prosedur penggunaan Pemeliharaan jaringan
8	Power failure	UPS sudah terinstall tapi kapasitas tidak mencukupi	I	Pembelian UPS pembelian Genset 10 KVA Bahan bakar

SIMPULAN

Untuk melakukan analisa resiko sebagai strategi mitigasi resiko pada toko online "X" terkait dengan keamanan informasi, maka dilakukan pengelompokkan aset yang terkait secara langsung dengan operasional toko online "X", sehingga menghasilkan tabel aset terkait dengan TI, yang dijadikan acuan untuk melakukan analisa. Adapun data untuk pengelompokkan aset tersebut berasal dari studi lapangan dan dokumentasi peraturan yang dimiliki perusahaan. Kemudian dilakukan analisis resiko secara kuantitatif, dan resiko-resiko akan terjadi pada perusahaan, yaitu: *Unauthorized Access, Malicious Code, Internet Service Down, Administration Failure, Theft of laptop or PC, Earthquake or Fire, Client or Server failure, Power Failure.*

Dari hasil analisa akan didapatkan nilai *Return On Investment* (ROI) untuk mengetahui apakah tindakan penanganan resiko (*safeguard)* memiliki kepantasan untuk diaplikasikan.

Hasil dari analisa digunakan sebagai strategi mitigasi resiko yang dapat dijadikan rekomendasi dalam melakukan pengurangan resiko, dengan dibagi menjadi empat kuadran. Sehingga pengelompokkan *threat* dan *vulnerability* dalam melakukan strategi mitigasi resiko menjadi terarah.

Setelah dilakukan perhitungan dengan ROI, ternyata tidak semua pemilihan *safeguards* untuk menangani *threat* pantas untuk diimplementasikan.

Untuk menangani *unauthorized access threat*, melakukan *safeguard* dengan mengimplementasikan *Intrusion Prevention Service*, kurang pantas untuk diimplementasikan karena nilai investasi yang diperlukan terlalu tinggi.

Untuk menangani *earthquake or fire threat*, melakukan *safeguard* dengan menyewa *data center* untuk keperluan *backup data*, kurang pantas untuk diimplemantasikan karena nilai investasi yang diperlukan terlalu tinggi.

RUJUKAN

Ding Tan, "Quantitative Risk Analysis Step-By-Step", December 2002 SANS Institute 2003

Ernie Jordan and Luke Silcock, "Beating IT Risks", 2005 Published in 2005 by John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester

Gondodiyoto, Sanyoto. 2007. *Audit Sistem Informasi+Pendekatan CobIT Edisi Revisi.* Jakarta: Penerbit Mitra Wacana Media.

G. Stoneburner, A. Goguen and A. Feringa, "Risk Management Guide for Information Technology System", Recommedation of National Institute of Standards and Technology Special Publication 800-30, July, 2002.

Hiles, A., "Enterprise Risk Assessment and Business Impact Analysis", Rothstein Assoc., 2002.

Palmer, I.C.`& G.A. Porter. (1989), Computer Security Risk management., Van Nostrand Reinhold.