PENGELOLAAN RISIKO ASET TEKNOLOGI INFORMASI PADA PERUSAHAAN PROPERTI PT XYZ, TANGERANG BERDASARKAN KERANGKA KERJA COBIT 4.1

Trivina Ayu Megawati[1)], Hanim Maria Astuti[2)] Anisah Herdiyanti[3)]
[1]Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember
Jalan Arief Rahman Hakim, Surabaya, 60111
Telp: (031) 5935214
E-mail : vinaa.santoso@gmail.com[1)]

Abstrak

PT XYZ adalah perusahaan properti terbesar di Indonesia yang mengedepankan penggunaan TI. Sebagian besar proses operasional bisnis perusahaan telah didukung oleh aset teknologi informasi agar lebih efektif dan efisien. Maka, untuk menjamin stabilitas proses bisnis, perusahaan harus memperhatikan dan melindungi aset teknologi informasi tersebut dari ancaman risiko yang dapat menggangu fungsionalitas aset TI. Pada kondisi saat ini, diketahui bahwa perusahaan belum memiliki pengelolaan risiko yang berfokus pada aset TI dan perencanaan pencegahan yang baik terhadap dampak risiko pada aset TI. Padahal, hal tersebut penting bagi perusahaan agar sistem informasi dan teknologinya memiliki konsep high availability. Tujuan peneltian ini adalah menghasilkan dokumen pengelolaan risiko berdasarkan kerangka kerja COBIT 4.1, di mana pada tahapan penilaian risiko menggunakan metode kuantitatif FMEA.

Kata kunci: *Risiko TI, Aset TI, Cobit 4.1, FMEA, Penilaian Risiko, Pengelolaan Risiko*

Abstract

XYZ is the largest property company in Indonesia, which emphasizes the use of IT. Most of the company's business operations have been supported by information technology assets in order to improve business performance. Thus, to ensure the stability of their business process, companies must pay attention to information technology assets and protect them from the threat of risk that may interfere with the functionality of IT assets. Currently, there is no risk management focusing on the management of IT assets and planning a good prevention against the risk of impact on the IT assets. In fact, preparation and prevention planning is essential for companies in order to have high availability of IT system. The purpose of this research is to develop an IT Risk Management based on COBIT 4.1 with FMEA assessment methods, and create controls to control IT risks.

Keywords: *IT Risk, IT Assetm Cobit 4.1, FMEA, Risk Assessment, Risk Management*

1. PENDAHULUAN

PT XYZ merupakan perusahaan yang bergerak di bidang jasa properti terbesar di Indonesia. PT XYZ telah menerapkan teknologi informasi untuk mendukung aktivitas operasional bisnis agar lebih efektif dan efisien. Manfaat yang maksimal dari penerapan teknologi informasi akan dapat diperoleh dengan memiliki tata kelola teknologi informasi yang baik. Salah satu fokus area dari tata kelola teknologi informasi tersebut adalah pengelolaan risiko teknologi informasi [1]. Perusahaan menyadari manfaat dari pengelolaan risiko apabila dilakukan, salah satunya adalah untuk menjamin keamanan informasi perusahaan dan meminimalkan kerugian, sehingga perusahaan memiliki atensi yang tinggi untuk menjaga kemanan aset tenknologi informasi agar tidak hilang, tidak rusak dan terkelola dengan baik, mengingat, perkembangan teknologi informasi tidak terlepas dari kemungkinan risiko yang disebabkan oleh beberapa faktor. Menurut UU no 24 tahun 2007 faktor tersebut terdiri dari faktor alam, faktor non-alam, faktor ulah manusia, dan faktor teknologi. Atensi perusahaan akan diwujudkan dengan membuat pengelolaan risiko.

Namun, kondisi saat ini, perusahaan belum menerapakan pengelolaan risiko teknologi informasi sepenuhnya sehingga perusahaan membutuhkan adanya pedoman pengelolaan risiko yang komprehensif. Maka, melalui penelitian ini, pengelolaan risiko teknologi informasi tersebut akan dilakukan dengan batasan ruang lingkup mulai dari proses identifikasi risiko, penilaian risiko sampai dengan penentuan aksi mitigasi risiko yang mengacu pada aktivitas pengelolaan di dalam kerangka kerja COBIT 4.1 domain *Plan and Organize* yaitu *Assess and Manage Risk*. Proses identifikasi risiko yang akan dilakukan berbasis pada aset teknologi informasi yang telah disusun

sesuai dengan standar ISO 27001. Sedangkan, untuk proses penilaian risiko akan digunakan metode kuantitatif FMEA (*Failure Modes and Effects Analysis*) yang mempertimbangkan probabilitas, akibat, dan keterkaitan dengan kontrol risiko yang ada agar lebih obyektif serta akurat dalam menentukan level risiko. Dengan demikian, penentuan level risiko tersebut akan mempermudah perusahaan dalam mendefinisikan aksi-aksi penangan risiko dengan tepat.

2. PUSTAKA

Berikut ini adalah tinjauan pustaka yang berkaitan dengan topik penelitian yaitu tinjuan risiko dan tinjauan aset teknologi informasi yang digunakan untuk mendukung metode penelitian.

2.1 Pengertian Risiko Teknologi Informasi

Menurut ISO/IEC Guide 73 dalam buku *a Risk Management Standard* [2], risiko adalah perpaduan antara probabilitas atau kemungkinan dari suatu kejadian yang tidak pasti dengan konsekuensinya, di mana konsekuensi tersebut dapat bernilai positif maupun negatif. Dari pendapat mengenai risiko tersebut, maka dapat disimpulkan bahwa risiko adalah bagian dari ketidakpastian suatu kejadian yang dapat memberikan dampak, baik negatif maupun positif dan akan berpengaruh terhadap kemampuan organisasi dalam mencapai tujuan organisasi.

Sedangkan untuk risiko teknologi informasi, merupakan bagian dari risiko operasional karena sifatnya yang terkait dengan penggunaan aset teknologi informasi untuk mendukung operasional proses bisnis di dalam perusahaan [2]. Risiko teknologi informasi antara lain mencakup risiko yang berasal dari internal seperti kegagalan sistem, kegagalan jaringan (network), kerusakan hardware, kerusakan software, kehilangan data, virus, dan risiko lainnya yang berasal dari eksternal seperti bencana alam [3].

2.2 Pengertian Pengelolaan Risiko Teknologi Informasi

Menurut COBIT 4.1 [1], pengelolaan risiko teknologi informasi merupakan bagian dari pengelolaan risiko perusahaan yang mengelola risiko dalam penggunaan teknologi informasi. Upaya yang dilakukan dalam mengelolanya adalah mencakup strategi pencegahan risiko, penanganan risiko, pengalihan risiko dan upaya lainnya untuk menjamin ketercapaian tujuan penggunaan aset teknologi informasi dalam mendukung bisnis. Beberapa manfaat yang diberikan dari pengelolaan risiko teknologi informasi adalah dapat mengidentifikasi kejadian yang berpotensial mengancam aset teknologi informasi dan menyebabkan terganggunya proses bisnis operasional untuk kemudian dapat merencanakan respon apa saja yang harus dilakukan sehingga menjamin proses bisnis operasional tetap berjalan dengan optimal dan meminimalkan kerugian.

2.3 Tahapan Pengelolaan Risiko Teknologi Informasi Berdasarkan COBIT

Pengelolaan risiko pada kerangka kerja COBIT 4.1 [1] yaitu pada domain *Plan and Organize* 9 dengan proses ***Assess and Manage IT Risk*** yang terdiri dari tahapan:

- **PO9.1** ***IT Establishment of Risk Context*****:** menentukan konteks ruang lingkup risiko.
- **PO9.2** ***Event Identification*****:** mengidentifikasi risiko yang relevan dengan kondisi PT XYZ.
- **PO9.3** ***Risk Assessment*****:** menilai risiko yang teridentifikasi dengan metode kuantitatif FMEA.
- **PO9.4** ***Risk Response*****:** merencanakan respon terhadap semua risiko yang teridentifikasi seperti aksi pencegahan risiko, aksi pengalihan risiko, aksi penanganan risiko, dan aksi penerimaan risiko [4].
- **PO9.5** ***Monitoring and Communication of a Risk Action Plan*****:** mendistribusikan hasil perencanaan respon risiko kepada seluruh pemangku kepentingan yang bertanggung jawab.

2.4 Metode FMEA (Failure Mode and Effect Analysis)

FMEA adalah metode yang akan digunakan untuk menilai dan menganalisis risiko secara kuantitatif. FMEA secara sistematis membantu untuk mengidentifikasi dan menilai pemicu (*modes*), probabilitas kejadian, serta dampak (*effects*) dari kegagalan dalam suatu sistem. Hasil analisis dan penilaian tersebut akan membentuk peringkat dari setiap kegagalan sesuai dengan ketiga nilai tersebut. Secara keseluruhan prosesnya, metode FMEA terdiri dari langkah-langkah berikut ini [5]:

Langkah 1: Mengidentifikasi potensial pemicu kegagalan teknologi informasi.
Langkah 2: Menentukan tingkat nilai keparahan (*severity number*) sesuai dengan rentang skala.
Langkah 3: Menentukan tingkat nilai probabilitas (*ocurrance number*) sesuai dengan rentang skala.
Langkah 4: Menentukan tingkat nilai kontrol risiko (*detection number*) sesuai dengan rentang skala.

Tabel 33. Skala Nilai FMEA

Level	Severity	Occurrance	Detection
1	***Catastrophic***	***Very High***	***Absolute Uncertainty***

	Sumber daya tidak tersedia/ kegagalan tidak diketahui	Setiap hari	Kontrol tidak dapat mencegah kegagalan
2	***Extremely High*** Sumber daya tidak tersedia/ kegagalan diketahui namun tidak dapat dikontrol	***Very High*** Setiap 3-4 hari	***Very Remote*** Sangat kecil kemungkinan kontrol dapat mencegah kegagalan
3	***Very High*** Sumber saya tidak tersedia/ kegagalan diketahui dan dapat dikontrol	***High*** Setiap minggu	***Remote*** Kecil kemungkinan kontrol dapat mencegah kegagalan
4	***High*** Sumber daya tersedia/ efek yang besar terhadap kebijakan	***High*** Setiap bulan	***Very Low*** Kemampuan kontrol dalam mencegah kegagalan adalah sangat rendah
5	***Moderate*** Sumber daya tersedia/ efek yang besar terhadap proses	***Moderately High*** Setiap tiga bulan	***Low*** Kemampuan kontrol dalam mencegah kegagalan adalah rendah
6	***Low*** Sumber daya tersedia/ efek yang besar terhadap prosedur	***Moderate*** Setiap enam bulan	***Moderate*** Kemampuan kontrol dalam mencegah kegagalan adalah cukup
7	***Very Low*** Sumber daya tersedia/ efek yang kecil terhadap kebijakan	***Moderately Low*** Setiap tahun	***Moderately High*** Kemampuan kontrol dalam mencegah kegagalan adalah cukup tinggi
8	***Minor*** Sumber daya tersedia/ efek yang kecil terhadap proses	***Low*** Setiap 1-3 tahun	***High*** Kemampuan kontrol dalam mencegah kegagalan adalah tinggi
9	***Very Minor*** Sumber daya tersedia/ efek yang kecil terhadap prosedur	***Very Low*** Setiap 3-5 tahun	***Very High*** Kemampuan kontrol dalam mencegah kegagalan adalah sangat tinggi
10	***None*** Tidak ada efek	***Remote*** Lebih dari lima tahun	***Almost Certain*** Kontrol pasti dapat dan berhasil mencegah kegagalan

Langkah 5: Menentukan nilai RPN (*Risk Priority Number*)
RPN merupakan nilai batasan yang menunjukkan risiko-risiko dengan nilai tertinggi. Nilai RPN diperoleh dengan mengalikan nilai tingkat keparahan efek (*severity*), nilai tingkat probabilitas (*occurrence*), dan nilai tingkat deteksi kontrol risiko (*detection*). Menurut ISO 27001 [6], maka nilai RPN dapat diperoleh dengan rumus:

$$RPN = S \times O \times D$$

Dimana,
S = *Severity Number* (Angka Tingkat Keparahan)
O = *Occurrence Number* (Angka Tingkat Probabilitas Kejadian)
D = *Detection Number* (Angka Tingkat Deteksi Kontrol Risiko)

Langkah 6: Menentukan Level Risiko
Dari hasil RPN yang diperoleh, selanjutnya akan dilakukan penentuan level risiko, apakah risiko termasuk ke dalam golongan risiko dengan level tinggi, sedang atau rendah. Penentuan level risiko didasarkan pada standar skala FMEA berikut ini:

Tabel 34. Skala Nilai RPN FMEA

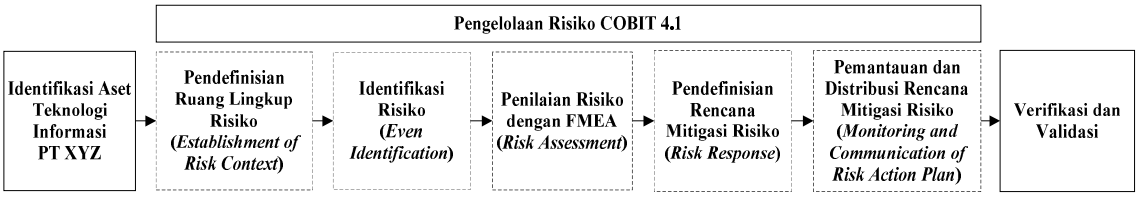
Skala Nilai RPN	Level Risiko
> 200	Very High
< 200	High
< 120	Medium
< 80	Low
< 20	Very Low

2.5 Aset Teknologi Informasi

Menurut penelitian sistem informasi yang dilakukan oleh Jeanne Ross, Cynthia Mathis, dan Dale Goodhue ditemukan bahwa ada tiga jenis aset TI yang terpenting. Penemuan tersebut dinamakan dengan istilah *"The Three IT Assets",* yang mana ketiga aset tersebut adalah Sumber Daya Manusia, Teknologi, dan Relasi [7]. Pada penelitian ini akan berfokus kepada aset Sumber Daya Manusia dan aset teknologi. Aset Sumber Daya Manusia yang dimaksudkan adalah divisi TI, sedangkan aset teknologi adalah seluruh infrastruktur teknologi informasi, yaitu hardware, software, dan database yang tersimpan serta tersistem secara terpusat di pusat data perusahaan. Keseluruhan aset di atas telah disusun berdasarkan standar ISO 27001 pada domain pengelolaan aset atau *Asset Management* yang terdiri dari proses *responsibility of assets* dan *information classification* [8].

3. METODOLOGI

Berikut ini merupakan gambar metodologi penelitian yang dilakukan mulai dari identifikasi aset teknologi informasi sampai dengan pengelolaan risiko teknologi informasi.



Gambar 20. Metodologi Penelitian

4. PEMBAHASAN DAN HASIL

Sesuai dengan metodologi penelitian yang ditentukan, maka pada bagian ini akan dijelaskan mengenai pembahasan dan hasil dari setiap tahapan pada metodologi tersebut.

4.1 Identifikasi Aset Teknologi Informasi

Penelitian ini difokuskan pada aset SDM yaitu divisi TI dan aset teknologi di pusat data perusahaan. Identifikasi aset TI dilakukan dengan mengacu pada domain *Asset Management* ISO 27001 yang terdiri dari proses *responsibility of assets* dan *information classification*. Dari hasil identifikasi aset berdasarkan proses *responsibility of assets*, maka diperoleh hasil jumlah aset SDM adalah enam orang yang memiliki peran penting (*key staff*), jumlah aset hardware sebanyak 49 server, jumlah aset software sebanyak 22 aplikasi, dan jumlah aset database sebanyak 30 database. Sedangkan, hasil identifikasi berdasarkan proses *information classification* menunjukkan bahwa hampir semua aset informasi yang dimiliki oleh perusahaan tergolong sangat penting (*confidential*).

4.2 Pendefinisian Ruang Lingkup Risiko

Ruang lingkup pengelolaan risiko adalah pengelolaan risiko aset teknologi informasi yang telah diidentifikasi pada poin sebelumnya, baik risiko yang berasal dari internal maupun dari eksternal.

4.3 Identifikasi Risiko

Di bawah ini merupakan daftar potensial risiko berbasis jenis aset teknologi informasi:

Tabel 35. Daftar Hasil Identifikasi Risiko

	Faktor	ID	Potensial Risiko	Jenis Aset TI
Risiko Eksternal	**Bencana Alam**	**R-01**	Gempa bumi	SDM dan Teknologi
		R-02	Banjir	Teknologi
	Gangguan Fasilitas Umum	**R-03**	Kebakaran	SDM dan Teknologi
		R-04	*Power Failure*	Teknologi
	Sosial	**R-05**	Terorisme (*bombing*)	SDM dan Teknologi
		R-06	Kerusuhan *(riots)*	SDM
	Kerjasama	**R-07**	Pelanggaran SLA Layanan TI (ketersediaan layanan TI dan keberlanjutan layanan TI)	Teknologi
Risiko Internal	**Operasional**	**R-08**	Kegagalan hardware	Hardware
		R-09	Kegagalan software	Software
		R-10	Kegagalan sistem jaringan	Software
		R-11	Modifikasi dan pencurian database dari user internal	Database
		R-12	*Cybercrime (hacker attacks)*	Database
		R-13	*Backup data failure*	Database
		R-14	Kesalahan dalam memperkerjakan staff *(wrongful hiring)*	Teknologi
		R-15	*Human atau technician error*	SDM dan Database
		R-16	Pelanggaran terhadap peraturan atau regulasi yang berlaku	SDM dan Teknologi

Terdapat 16 risiko yang berpotensi mengancam aset TI dan relevan dengan kondisi PT XYZ saat ini.

4.4 Penilaian Risiko dengan Metode Kuantitatif FMEA

Dalam tahapan ini, 16 risiko yang telah diidentifikasi sebelumnya telah dijabarkan lagi menurut penyebab dan akibat yang ditimbulkan, sehingga 16 risiko tersebut menjadi 36 risiko. Berikut ini adalah penilaian risiko dengan menggunakan metode FMEA:

[O]: Occureness Number **[D]**: Detection Number **[S]** : Severity Number **[L]**: Level

Tabel 36. Hasil Penilaian Risiko

Type of Assets	Potential Causes	Event Risk	O	Potential Effects	Business Consequences	S	Detection Control	D	RPN	L
Teknologi (database)	• Tidak ada pengaturan untuk manajemen hak akses user atau *user privilege* • Tidak ada klasifikasi database	Pencurian database	5	• Manipulasi data • Kebocoran informasi atau data penting • *Data loss* • *Data corruption*	• Mempengaruhi reputasi atau nama baik dari perusahaan • Terganggunya proses bisnis	7	• Kebijakan untuk tidak menyebar luaskan akun ke pihak luar • Menerapkan verifikasi akun sebelum terkoneksi ke internet	5	175	**High**
Teknologi (software)	Virus, mallware, bug	Kegagalan Software	3	Kerusakan aset teknologi (software), kehilangan data, database *corrupt*	Proses bisnis mengalami gangguan dan sebagian bisnis mengalami penundaan sampai aset teknologi (software) pulih	6	Install dan update virus secara berkala, menerapkan scanning virus, dan memonitor antivirus	3	54	**Low**

Hasil penilaian risiko dengan metode kuantitatif FMEA ditunjukkan pada tabel di bawah ini.

Tabel 5. Pelevelan Risiko berdasarkan Penilaian Risiko

Risiko Rendah	Risiko Sedang	Risiko Tinggi
▪ Network failure ▪ Cybercrime ▪ Backup data failure ▪ Kesalahan dalam memperkerjakan staff ▪ Human/ technician error ▪ Pelanggaran terhadap peraturan atau regulasi ▪ Hardware failure ▪ Software failure ▪ Memory full	▪ Kebakaran ▪ Power Failure ▪ Banjir ▪ Gempa Bumi ▪ Terorisme (*bombing*) ▪ Kerusuhan (riots)	▪ Kebakaran ▪ Pelanggaran SLA ▪ Pencurian database ▪ Power failure

Risiko di atas dikategorikan ke dalam kategori risiko level rendah, sedang, dan tinggi. Tidak menutup kemungkinan jika satu risiko dapat tergolong ke dalam dua level sekaligus, karena level risiko juga mempertimbangkan aspek penyebab risiko dan dampak dari risiko tersebut.

4.5 Pendefinisian Rencana Aksi Respon Risiko

Berikut ini adalah perencanaan aksi-aksi untuk merespon risiko dilihat dari faktor penyebab risiko yang terdiri dari respon pencegahan (*avoid*), pengalihan (*transfer*), pengelolaan (*mitigate*), dan penerimaan (*accept*).
Keterangan: **[AC]:** Accept, **[AV]:** Avoid, **[M]:** Mitigate, **[T]:** Transfer

Tabel 6. Hasil Perencanaan Aksi Respon Risiko

Level	P	Potential Causes	Event Risk	Potential Effects	Response				Action
					AC	AV	M	T	
High	2	• Tidak ada pengaturan untuk manajemen hak akses user atau *user privilege* • Tidak ada klasifikasi database • Pelanggaran terhadap hak akses user	Pencurian database dari user internal	• Manipulasi data • Kebocoran informasi atau data penting • *Data loss* • *Data corruption*		V	V		**Avoid** • Mengklasifikasikan database • Melakukan manajemen hak akses user • Memberikan kontrol akses berupa username dan password untuk verifikasi sebelum akses database • Mengganti password secara periodik **Mitigate**

Level	P	Potential Causes	Event Risk	Potential Effects	Response				Action
					AC	AV	M	T	
									• Restore dan repair database
Low	4	Virus, mallware, bug	*Software failure*	Kerusakan aset teknologi (software), kehilangan data, database corrupt		V	V		**Avoid** • Install dan update melakukan antivirus secara periodik • Melakukan backup data sesuai SOP **Mitigate** • Melakukan scanning virus secara periodik

4.6 Pemantauan dan Pendefinisian Distribusi Rencana Mitigasi Risiko

Hasil penilaian risiko dan mitigasi risiko akan didistribusikan kepada pihak yang memiliki kewenangan untuk menjalankan dan memantau pengelolaan risiko yaitu: manajemen eksekutif, kepala divisi TI, dan *core infrastructure* (network, server, database) PT XYZ.

5. VERIFIKASI DAN VALIDASI

Verifikasi dilakukan dengan memetakan tahapan-tahapan yang dilakukan dalam penelitian lalu memeriksa apakah tahapan tersebut telah sesuai dengan setiap poin tahapan pada standar kerangka kerja COBIT 4.1. Hasil dari verifikasi adalah semua tahapan pada kerangka kerja COBIT 4.1 telah dilakukan dalam penelitian ini. Sedangkan, untuk validasi dilakukan dengan pendekatan *acceptance testing* untuk mengetahui apakah hasil dari penelitian telah memenuhi kebutuhan user. Validasi dilakukan dengan cara kuesioner dan korespondensi melalui email kepada *key user*, yaitu head of IT dan *core server and business productivity* yang memiliki kewenangan/ kepentingan. Hasil dari validasi adalah berupa *feedback* dari user berupa persetujuan, perbaikan, dan hasil kuesioner tentang ketepatan, kelengkapan, dan kejelasan konten dokumen.

6. SIMPULAN DAN SARAN

6.1 Simpulan

Hasil penilaian risiko menunjukkan 7 risiko tergolong ke dalam level risiko tinggi yang disebabkan oleh faktor gangguan fasilitas umum dan operasional, yaitu risiko kebakaran, pencurian data, pelanggaran kontrak SLA, dan *power failure.* Masing-masing risiko yang telah diidentifikasi dan dinilai memiliki aksi respon yang berbeda-beda dan apabila dilakukan dapat meminimalkan dampak risiko. Kelebihan dari paper penelitian ini adalah menggunakan standar kerangka kerja COBIT 4.1 untuk seluruh tahapan penilaian dan analisi risiko, serta menggunakan metode kuantitatif FMEA untuk penilaian risiko sehingga lebih akurat. Sedangkan, untuk kelemahan dari paper ini adalah tidak menjelaskan kondisi kekinian penerapan pengelolaan risiko teknologi informasi yang ada di perusahaan secara spesifik.

6.2 Saran

Saran untuk penelitian selanjutnya dengan topik atau ruang lingkup yang sama adalah sebagai berikut:

1. Menambahkan risiko baru yang mengancam aset TI dan relevan dengan kondisi PT XYZ di masa mendatang, seperti jenis *cybercrime* yang semakin berkembang, kelemahan dari metode backup yang saat ini digunakan, dan risiko baru lainnya.
2. Memperluas ruang lingkup penelitian hingga menghasilkan tata kelola untuk mengontrol setiap risiko, seperti tata kelola untuk menghindari risiko kebakaran pada ruang pusat data.

7. DAFTAR RUJUKAN

[1] IT Governance Institue, COBIT 4.1, United State, 2007
[2] IRM, "A Risk Management Standard," United Kingdom, 2002.
[3] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems", National Institute of Standards and Technology, Gaithersburg, 2002.
[4] Enterprise Risk Management, "A Four Step Risk Approach to Strategy Execution", Raleign, 2011
[5] Steven C. Leggett, Problem Solving Using Failure Mode Effects and Analysis, 2001.
[6] ISO 27001, "An Illustration of The Application of Failure Modes and Effects Analysis (FMEA) Techniques to The Analysis of Information Security Risks," United States, 2008.
[7] J. W. Ross, "The Three IT Assets," 1992.
[8] ISO/IEC, "IT-Security Techniques-ISMS-Requirements 1st Edition," London, 2005.