PENGUKURAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI DENGAN METODE OCTTAVE-S

Henny Hendarti; Maryani

School of Information System, BINUS University
Jln. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
henny@binus.edu; yanie@binus.edu

ABSTRACT

The purpose of this paper is to measure risks to identify company's assets and analyze risks, and to do strategic planning of security protection and minimize risk. Research used case study by reading materials dealing with the OCTAVE-S method. Observation was done directly to the relating parties through an interview, as well as using a questionnaire based on the OCTAVE-S method. The result obtained from this research is risk management of information technology in order to minimize the risks. Based on the findings obtained, it is expected company can identify potential risks and mitigate them efficiently and effectively.

Keywords: *OCTAVE-S method, risks, information technology*

ABSTRAK

Tujuan dari penelitian ini adalah melakukan pengukuran risiko untuk mengindetifikasi aset perusahaan dan menganalisis risiko-risiko, dan merencanakan strategi perlindungan keamanan, serta meminimalkan risiko. Metodologi yang digunakan adalah studi kasus berdasarkan literatur yang berhubungan dengan metode OCTAVE-S. Observasi dilakukan dengan pengamatan secara langsung ke perusahaan, wawancara dengan pihak yang berkaitan, serta mengunakan kuesioner berdasarkan metode OCTAVE-S. Hasil yang dicapai dari penelitian ini yaitu pengelolaan risiko teknologi informasi pada perusahaan agar dapat meminimalkan risiko. Dengan temuan yang diperoleh, maka diharapkan perusahaan dapat mengindentifikasi risiko yang mungkin terjadi dan menanggulanginya secara efisien dan efektif.

Kata kunci: *metode OCTAVE-S, risiko, teknologi informasi*

PENDAHULUAN

Teknologi informasi pada perusahaan, selain memberikan keuntungan, juga membawa risiko yang beragam. Timbulnya kesalahan tanpa disengaja--seperti kehilangan data akibat *server* yang terserang virus dan kesalahan yang terjadi karena faktor kesengajaan atau kecurangan adalah beberapa contoh risiko yang mungkin terjadi. Risiko-risiko yang timbul tersebut akan menimbulkan dampak kerugian bagi perusahaan baik secara finansial maupun nonfinansial (Gondodiyoto, 2007).

Suatu pengukuran terhadap risiko yang ada diperlukan dalam penerapan teknologi informasi. Pengukuran risiko TI berguna untuk mengetahui profil risiko TI; melakukan analisis terhadap risiko; dan juga melakukan respons terhadap risiko, sehingga tidak terjadi dampak-dampak yang mungkin muncul dari risiko tersebut (Jordan & Silcock, 2005). Penerapan teknologi informasi didukung dengan sistem pengamanan yang kuat, prosedur yang baik, otorisasi yang baik, dan pemeliharaan berkala terhadap sumber daya komputer. Dukungan tersebut dapat menjamin keamanan aset perusahaan, pemeliharaan integritas data, dan penggunaan sumber daya yang tepat.

Berdasarkan latar belakang, penelitian bertujuan untuk mengetahui risiko-risiko dari penerapan teknologi informasi, mengidentifikasikan nilai dari risiko yang ditemukan pada perusahaan, mengidentifikasikan praktik keamanan yang cocok untuk penanggulangan risiko dan meminimalkan risiko, serta memaksimalkan kinerja dari Teknologi Informasi pada perusahaan. Penelitian ini diharapkan dapat meminimalkan risiko terjadinya ancaman yang datang dari dalam maupun dari luar perusahaan. Selain itu, penelitian ini diharapkan dapat memberikan rekomendasi alternatif terhadap kelemahan atau risiko teknologi informasi perusahaan yang ditemukan dari hasil analisis.

Penelitian dilakukan dengan studi kasus berdasarkan metode OCTAVE-S. Observasi dilakukan dengan pengamatan secara langsung pada objek, wawancara kepada pihak yang berkaitan serta mengunakan kuesioner berdasarkan metode OCTAVE-S (Alberts, et al., 2005). Hasil yang dicapai dari penelitian ini yaitu dapat mengelola risiko teknologi informasi pada perusahaan agar dapat meminimalkan risiko tersebut. Dengan temuan yang diperoleh, maka penelitian ini diharapkan dapat mengindentifikasi risiko yang mungkin terjadi dan menanggulanginya secara efisien dan efektif.

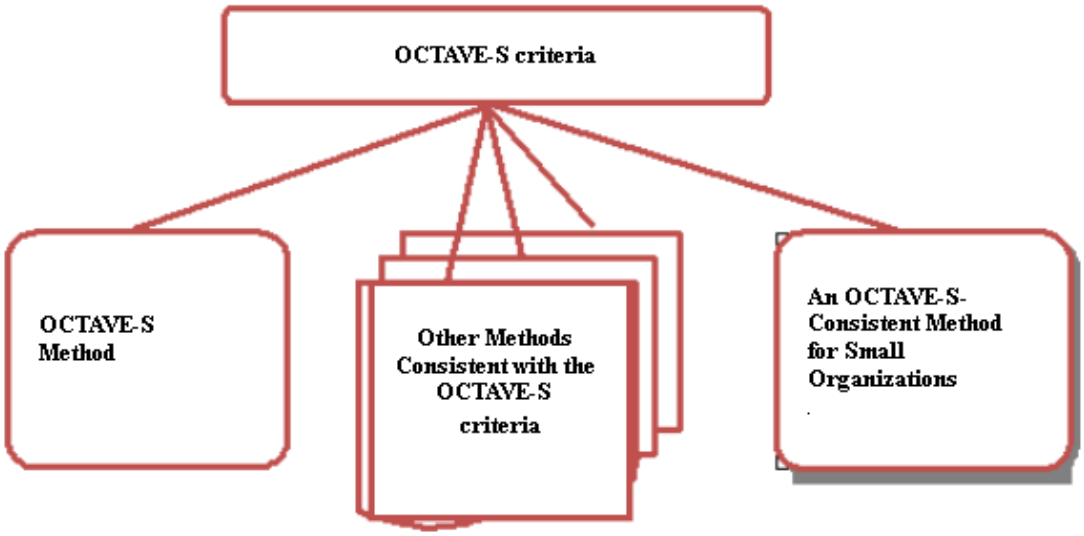
METODE

Penelitian ini merupakan penelitian kualitatif dengan menggunakan pendekatan studi kasus. Teknik pengumpulan data yang digunakan adalah studi pustaka dan penelitian lapangan. Studi pustaka dilakukan dengan mengumpulkan data dari berbagai sumber baik artikel jurnal maupun buku tentang TI, risiko TI, manajemen TI, dan manajemen risiko TI. Materi yang diutamakan adalah sumber yang memuat metode OCTAVE-S sebagai dasar materi pengukuran risiko TI di perusahaan.

Penelitian lapangan dilakukan dengan meninjau langsung yang berlokasi di Wisma Intra Asia lt. 3, Jl. Prof. Dr. Soepomo SH. No. 58, Jakarta 12870, dengan tujuan untuk memperoleh data yang dibutuhkan dalam penelitian. Pada penelitian lapangan dilakukan wawancara, observasi, dan pengisian kuesioner. Wawancara secara langsung dilakukan kepada pihak yang berkepentingan dalam perusahaan, sehingga didapatkan data yang berkualitas. Wawancara dilakukan kepada manajer dan staf komputer di perusahaan. Observasi dan peninjauan secara langsung terhadap objek yang akan diteliti berkaitan dengan kondisi TI yang dipakai perusahaan. Observasi mencakup *hardware*, *software*, *jaringan,* dan *aplikasi* yang diterapkan dalam perusahaan. Kuesioner secara acak dibagikan kepada beberapa responden mengenai sistem pada perusahaan. Data yang sudah terkumpul akan digunakan dalam melakukan pengukuran risiko perusahaan.

Dari berbagai macam teknik yang ada untuk mengukur risiko TI, penelitian ini menggunakan OCTAVE-S sebagai teknik analisis. Teknik ini merupakan variasi dari pendekatan OCTAVE yang dikembangkan untuk mengukur risiko TI bagi organisasi yang beranggotakan 20 sampai 80 orang dan diharapkan juga mempunyai 3 sampai 5 orang yang memahami tentang keamanan. Dengan demikian, pertama, penelitian dilakukan pada operasional bisnis yang berhubungan dengan TI perusahaan; kedua, pengukuran risiko teknologi informasi pada perusahaan menggunakan pendekatan OCTAVE-S.

Kriteria OCTAVE-S (Gambar 1) memerlukan evaluasi yang harus dilakukan oleh sebuah tim (interdisipliner) yang terdiri dari personel teknologi informasi dan bisnis organisasi.

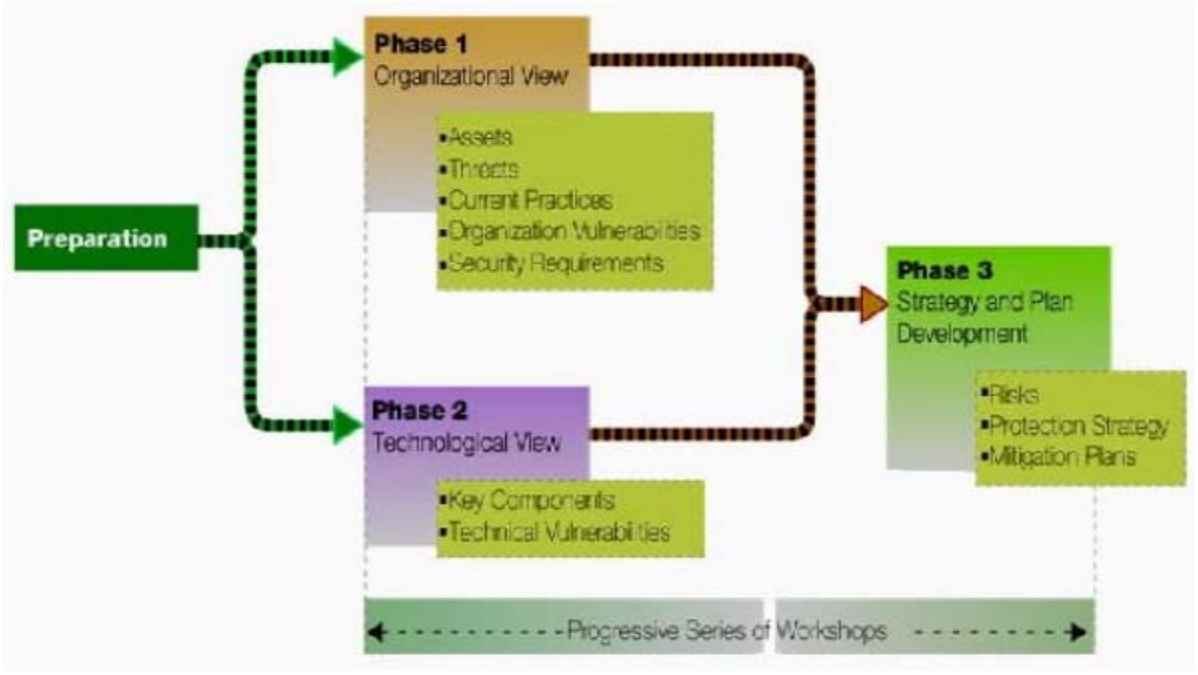


Gambar 1 Octave's Criteria

Anggota tim bekerja sama untuk membuat keputusan berdasarkan risiko terhadap aset informasi kritis organisasi. Pada akhirnya, kriteria OCTAVE-S memerlukan katalog informasi untuk mengukur praktik organisasi, menganalisis ancaman, dan membangun strategi proteksi. Katalog ini meliputi: catalog of practices—sebuah koleksi strategi dan praktek keamanan informasi, generic threat profile—sebuah koleksi sumber ancaman utama, dan catalog of vulnerabilities—sebuah koleksi dari vulnerability berdasarkan platform dan aplikasi.

HASIL DAN PEMBAHASAN

Risiko adalah suatu variasi dari hasil-hasil yang dapat terjadi selama periode tertentu (Jordan & Silcock, 2005). Lebih lanjut, manajemen risiko adalah identifikasi dari ancaman dan implementasi dari pengukuran yang ditujukan pada mengurangi kejadian ancaman tersebut dan menimalkan setiap kerusakan (Jordan & Silcock, 2005). Menurut Alberts, et al., 2005) terdapat 3 fase di dalam metode OCTAVE-S. Fase 1 adalah membangun aset berdasarkan profil ancaman; fase 2 adalah mengidentifikasi tingkat kerentanan infrastruktur; dan fase 3 adalah mengembangkan rencana dan strategi keamanan (Gambar 2).



Gambar 2 Proses Metode OCTAVE'S

Pada Fase 1, membangun aset berdasarkan profil ancaman, terdapat 2 proses, yaitu: proses mengidentifikasi informasi perusahaan dan proses menciptakan profil ancaman. Dalam proses pertama terdapat 3 aktivitas. Aktivitas pertama menetapkan kriteria pengaruh evaluasi. Pada aktivitas ini terdapat sebuah aturan yang sudah ditetapkan sebagai acuan kriteria dan apa saja yang akan dievaluasi. Selama proses bisnis ini berjalan, tingkat kepuasan *customer* sangat diperhatikan. Aktivitas kedua mengidentifikasi aset organisasi perusahaan. Aset perusahaan dibagi menjadi 2 bentuk: aset *tangible* dan aset *intangible.* Sedangkan aktivitas ketiga mengevaluasi pelatihan keamanan organisasi dan perusahaan, yaitu dalam menjalankan pelatihan keamanan seluruh manajemen beserta para karyawan diberikan pelatihan khusus. Pelatihan tersebut biasanya diadakan 2 kali dalam setahun.

Kemudian pada proses kedua terdapat 3 aktivitas. Aktivitas pertama memilih aset yang berharga, pada perusahaan yang berhubungan dengan informasi baik berupa data, *hardware*, *software*, jaringan, maupun *user* sangat diperhatikan untuk menjaga kemanan dan kerahasiaanya. Aktivitas kedua adalah mengidentifikasi syarat-syarat keamanan untuk aset berhaga**.** Identifikasi syarat-syarat pengamanan untuk aset berharga adalah dengan cara memberikan pengamanan terhadap aset-aset yang berada pada perusahaan sesuai dengan kebutuhan dari aset-aset tersebut. Aktivitas ketiga mengidentifikasi ancaman-ancaman untuk aset berhaga. Saat ini, ancaman-ancaman yang terdapat pada perusahaan adalah terjadinya bencana dan juga ancaman yang berupa komputer terkena virus, adanya sabotase data, adanya *hacker* yang merusak sistem.

Pada Fase 2, mengidentifikasi tingkat kerentanan infrastruktur, terdapat 1 proses yaitu melakukan penghitungan aset kritis yang berhubungan dengan aset perusahaan**.** Aktivitas pertama memeriksa jalur akses yaitu memastikan setiap akses karyawannya sesuai dengan wewenang dan tanggung jawabnya. Sistem sangat berhubungan erat dengan aset berharga di perusahaan. Aktivitas kedua menganalisis teknologi yang berkaitan dengan proses. Dalam menganalisis aktivitas ini, penelitian membandingkan informasi dari komponen kelas yang diidentifikasi sebelum aktivitas berlangsung. Informasi ini termasuk aset-aset berharga, bagian dari staf yang bertangung jawab untuk memelihara dan mengamankan aset.

Pada Fase 3, mengembangkan rencana dan strategi keamanan, terdapat 2 proses, yaitu membangun kemungkinan kriteria evaluasi dan mengidentifikasi dan menganalisis risiko-risiko. Dalam proses pertama terdapat 3 aktivitas. Aktivitas pertama, mengevaluasi dampak-dampak dari ancaman. Pengaruh-pengaruh yang terjadi dari ancaman yang dapat menimbulkan kerugian material maupun non-material yaitu berupa sabotase sistem oleh pihak-pihak yang tidak berwenang. Oleh sebab itu, harus dapat meminimalkan risiko-risiko yang terjadi. Aktivitas kedua membangun kemungkinan kriteria evaluasi yang **b**erkaitan erat dengan kejadian yang akan terjadi. Nilai kemungkinan ancaman diukur berdasarkan ukuran kualitatif (*high, medium, low*). Aktivitas ketiga mengevaluasi kemungkinan-kemungkinan ancaman berdasarkan frekuensi yang telah ditetapkan. Kriteria ini berdasarkan waktu harian, mingguan, bulanan, atau tahunan. Dari situ dapat ditemukan risiko yang dapat mengancam serta rekomendasi untuk meminimalkan risiko yang ada.

Dalam proses kedua terdapat 5 aktivitas. Aktivitas pertama menjelaskan arus strategi perlindungan melakukan pemasangan *firewall* terhadap seluruh komputer di setiap jaringan untuk memberikan perlindungan terhadap pihak-pihak yang tidak berwenang. Aktivitas kedua memilih pendekatan-pendekatan peringatan dengan mengadakan pelatihan keamanan pada setiap karyawannya agar ketika terjadi risiko karyawan tersebut dapat meminimalkan risiko tersebut. Aktivitas ketiga mengembangkan risiko rencana-rencana peringatan/mitigasi. Rencana-rencana pengurangan risiko dilakukan dengan cara pelatihan dan kesadaran keamanan, peraturan kebijakan dan kemanan, otentifikasi dan otorisasi. Aktivitas keempat mengidentifikasi perubahan-perubahan untuk strategi perlindungan. Identifikasi perubahan-perubahan untuk strategi perlindungan dilakukan untuk menentukan apakah rencana mitigasi memengaruhi strategi perlindungan sehingga dapat menjalankan perubahan strategi perlindungan yang diharapkan. Aktivitas kelima mengidentifikasi langkah-langkah selanjutnya. Pada tahap ini hasil-hasil evaluasi yang ditemukan apakah dapat diimplementasikan dan meningkatkan keamanan dalam melakukan dan mengembangkan strategi perlindungan dan rencana-rencana peringatan atau mitigasi. (Bojanc & Jerman-Blazik, 2008)

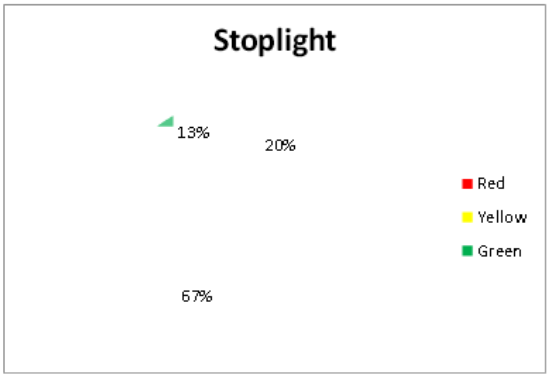
Persiapan dan Perencanaan Manajemen Risiko Teknologi Informasi

Dengan terus berkembangnya teknologi zaman sekarang ini, peranan sistem informasi terhadap perkembangan dunia usaha makin penting. Sistem informasi sebagai media untuk memenuhi kebutuhan akan informasi terutama dalam hal mengolah data menjadi informasi yang akurat guna mendukung pelaksanaan kegiatan perusahaan. Pengendalian terhadap manajemen risiko teknologi informasi sangat penting di dalam perusahaan. Dengan mengelola risiko teknologi informasi dapat ditemukan risiko-risiko serta diminimalkan. Hasil dari temuan risiko dapat dijadikan rekomendasi untuk perbaikan bagi perusahaan dalam menjalankan kegiatan di masa mendatang.

Pada bagian ini dijelaskan mengenai pengelolaan risiko teknologi informasi pada perusahaan. Pengumpulan temuan risiko diperoleh dari hasil kuesioner dengan menggunakan metode OCTAVE-S , wawancara, serta melakukan pengamatan secara langsung.

Analisis OCTAVE-S Wisma Intra Asia

Pertama, identifikasi organisasi dilakukan dengan mengidentifikasi sistem yang digunakan untuk mendukung kinerja *e-performance* dan *email server*. Gambar 3 menunjukkan persentase status *stoplight.*



Gambar 3 Grafik Presentase Status Stoplight (Red, Yellow, and Green)

Kedua, membuat profil ancaman dengan mengidentifikasi aset kritis pada Wisma Intra Asia. Pada *e-performance*, akses jaringan *e-performance*, adalah kelalaian pegawai dalam mengentri data, penyalahgunaan hak otorisasi, dan virus dan spyware; pada akses fisik *e-performance* adalah pegawai yang menginput data dari *hardware* yang mengandung virus, pasokan listrik mengalami masalah, penggunaan jaringan LAN tanpa ada otorisasi. Kemudian pada *email server*, yaitu akses jaringan *email server*, adalah pegawai yang menggunakan email untuk di luar pekerjaan, *hacker* yang memiliki akses untuk merusak *email;* pada akses fisik *email server* adalah pegawai yang tidak teliti menggunakan informasi, alamat email yang tidak dikenal mengirimkan spam atau virus.

Ketiga, perhitungan infrastruktur terkait aset kritis dilakukan pada komponen kritis yang berkaitan dengan aset kritis. Aset-aset tersebut adalah *personal computer*, jaringan, dan *database server*.

Tabel 1 Informasi, Sistem, dan Aplikasi

Aplikasi	Informasi	Pelayanan dan Aplikasi	Aset-aset Lain
General Ledger	sistem yang berwujud software yang mendukung dalam pembuatan laporan neraca laba rugi perusahaan.	a) Laporan rugi laba b) Neraca c) Balance Sheet d) Ledger list	3 Unit Komputer
Account Receivable	Sistem yang berwujud software untuk penjualan dan pembayaran.	a) Laporan penjualan b) Outstanding c) Umur Piutang d) Pembayaran	1 Unit Komputer
Inventory	Sistem yang berwujud software untuk mengecek persediaan di dalam perusahaan.	a) Laporan Material b) Stock list c) Stock Hard	1 Unit Komputer
Account Payble	Sistem yang berwujud software untuk segala transaksi pembelian yang ada didalam perusahaan.	a) Laporan Pembelian b) Laporan Pembayaran hutang	1 Unit Komputer
Cass Flow	Sistem yang berwujud Software yang digunakan untuk mengatur arus kas perusahaan	a) Kas Besar b) Kas Kecil	1 Unit Komputer
Payroll	Sistem yang berwujud Software untuk proses penggajian karyawan.	a) Slip Gaji b) Data Gaji c) Data Karyawan	1 Unit Komputer
Program Produksi	Sistem yang berwujud Software yang digunakan untuk menampilkan penerimaan, pemakaian, pakan pada *farm.*	a) Stock Pakan b) Stock Obat	2 Unit Komputer

Keempat, hasil identifikasi dan analisis risiko adalah seperti pada Tabel 2.

Tabel 2 Hasil identifikasi dan Analisis Risiko

		E-Performance	E-Mail Server
Internal	Tidak disengaja	Low --> denda dan keamanan	Medium --> Finansial & Produktivitas
	Sengaja	High --> Finansial & Produktivitas	High --> Finansial & Produktivitas
Eksternal	Tidak disengaja	Medium --> Finansial & Produktivitas	Medium --> Reputasi & Finansial
	Sengaja	High --> Finansial & Produktivitas	Low --> denda dan keamanan

Kelima, strategi perlindungan dan rencana mitigasi dilakukan dengan: dokumentasi resmi kebijakan keamanan, olaborasi dengan pihak luar untuk membatasi hak akses informasi, pelatihan manajemen insiden, dan melakukan evaluasi metode OCTAVE-S 2 tahun sekarang.

SIMPULAN

Setelah melakukan observasi serta menerapkan tahap-tahap manajemen risiko untuk melakukan evaluasi terhadap risiko Teknologi Informasi, diperoleh simpulan sebagai berikut. Pertama, perusahaan memiliki kebijakan untuk keamanan penggunaan teknologi informasi, tetapi kebijakan tersebut belum terdokumentasi secara resmi dan hanya dilakukan pelatihan (training) saja kepada pegawai-pegawai isntansi yang bersangkutan. Kedua, saat ini perusahaan belum menentukan spesifikasi PC yang akan digunakan oleh setiap karyawannya untuk memenuhi kebutuhan karyawan guna meningkatkan kinerja yang baik. Ketiga, manajemen risiko teknologi informasi pada perusahaan sampai pada saat ini belum cukup efekif. Ini dilihat dari aset informasi perusahaan yang masih dapat disabotase oleh pihak yang tidak berwenang. Keempat, dalam hal keamanan informasi, masih memiliki sedikit kekurangan khususnya risiko-risiko yang melalui akses jaringan. Pengamanan perusahaan melalui jaringan masih kurang terorganisasi dengan baik. Kelima, pada akses jaringan dan akses fisik terdapat ancaman-ancaman pada aset kritis (*e-performance* dan *email server*). Ancaman-ancaman tersebut berasal dari pihak internal dan eksternal instansi dengan motif yang sengaja dan tidak sengaja

DAFTAR PUSTAKA

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S Implementation Guide, Version 1.0*. Pittsburgh: Carnegie Mellon Software Engineering Institute.

Bojanc, R. & Jerman–Blazic, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413–422.

Gondodiyoto, S. (2007). *Audit Sistem Informasi + Pendekatan COBIT*. Edisi Revisi. Jakarta: Mitra Wacana Media.

Jordan, E. & Silcock, L. (2005). *Beating IT Risks*. England: John Wiley and Sons.

Liu, S., Kuhn, R., & Rossman, H. (2009). Understanding insecure IT: Practical risk assessment. *IT Professional*, *11*(3), 57–59.

OCTAVE-S Implementation Guide. (2005). *Volume 10: Example Scenario.* Version 1.0.