AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO 27002 (Studi Kasus: PT. Aneka Jaya Baut Sejahtera)

[1)]Marliana Halim [2)]Haryanto Tanuwijaya [3)]Ignatius Adrian Mastan

S1 / Jurusan Sistem Informasi, Sekolah Tinggi Manajemen Komputer & Teknik Komputer Surabaya
email: 1)smile05_lia@yahoo.com 2)haryanto@stikom.edu 3)Ignatius@stikom.edu

Abstract: *PT.AJBS is a company that works in providing items/machinery for industrial purposes. PT.AJBS has many product lines Therefore, implementing a new and capable information system is a must. The new system need to have modules such as invetory, transaction, customer & supplier data and accounting journal. These modules need to be integratedto the new system, called Integrated Trading System. In addition, information security management is important because company's information is an important asset for the company. PT.AJBS need to audit their current information security system to find out the level of security PT.AJBS has. ISO 27002 is the standard that PT.AJBS has to be met when auditing. ISO 27002 standard is chosen because of its flexibility. It can be tailored according to the company's needs, company's visions, company's security system requirement, business processes, human resource needa and the structure of the organization, as well as information security system management. The result of maturity level 2.49 is produced from the implementation of information security system audit. The result is categorized to level 2, which is repeatable. This research also produces reccomendations for PT.AJBS such as better information system processes and improvement in level of information security*

Keywords: *audit, information security, ISO 27002*

Perseroan Terbatas Aneka Jaya Baut Sejahtera (PT. AJBS) adalah sebuah perusahaan di bidang pengadaan perlengkapan dan peralatan pendukung industri. PT. AJBS memiliki jenis dan jumlah produk yang besar, hal ini yang mengharuskan PT. AJBS untuk menerapkan teknologi informasi yang memadai. Pengelolaan inventori, transaksi, data pelanggan, dan data supplier, serta keseluruhan pelaporan dan analisa keuangan ditangani dalam sistem operasional yang terintegrasi yang bernama *Integrated Trading System* (ITS). Pengelolaan keamanan informasi sangat penting, karena seluruh informasi perusahaan merupakan aset berharga bagi perusahaan.

Manajemen PT. AJBS saat ini belum mengetahui sampai di mana tingkat keamanan sistem informasi yang dimilikinya. Rahardjo (2005: 1) menyatakan bahwa masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Pentingnya nilai sebuah informasi menyebabkan informasi seringkali ingin diakses oleh orang-orang tertentu secara ilegal. Hal ini dapat menimbulkan kerugian bagi perusahaan misalnya kerugian apabila sistem informasi tidak bekerja selama kurun waktu tertentu, kerugian apabila ada kesalahan data atau informasi dan kehilangan data.

Sementara itu, selama penerapan aplikasi ITS ini telah terjadi beberapa kendala antara lain ditemukannya beberapa kasus penyalahgunaan *password* yang dapat

mengancam kerahasiaan perusahaan. Selain itu dikhawatirkan dapat berdampak pada terjadinya penyalahgunaan informasi yang merugikan PT. AJBS dalam persaingan dengan para kompetitor. Kendala lain yang ditemukan adalah kurangnya pemeliharaan terhadap fasilitas pemrosesan informasi yang dapat menyebabkan sistem menjadi sering *hang*, jaringan *down*, hingga terbakarnya *harddisk* yang menyebabkan hilangnya data perusahaan. Di samping itu, PT. AJBS juga belum memiliki aturan dan prosedur terhadap ancaman virus. Ancaman virus itu dapat menimbulkan gangguan kinerja sistem informasi bahkan dapat mengacau keberlangsungan operasional PT. AJBS.

Selama ini PT. AJBS belum pernah melakukan analisa penyebab terjadinya permasalahan tersebut dan PT. AJBS tidak mengetahui sampai di mana tingkat keamanan sistem informasi yang milikinya. Oleh karena itu PT. AJBS membutuhkan evaluasi keamanan sistem informasi untuk menjaga keamanan sistem informasi yang dimilikinya. Evaluasi keamanan sistem informasi dapat dilakukan dengan audit keamanan sistem informasi (Asmuni dan Firdaus, 2005: 23). Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*Availability*) dari Informasi (ISO/IEC 27002, 2005: 1).

Agar audit keamanan sistem informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukan audit tersebut (Tanuwijaya dan Sarno, 2010: 80). Menurut Sarno dan Iffano (2009: 59) tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh perusahaan untuk melaksanakan audit keamanan sistem informasi. Audit pada PT. AJBS menggunakan standar ISO 27002. Standar ISO 27002 dipilih dengan pertimbangan bahwa standar ini sangat fleksibel dikembangkan tergantung pada kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai dan ukuran struktur organisasi. Selain itu, pertimbangan lainnya adalah ISO 27002 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara internasional yang disebut *Information Security Management Sistem* (ISMS) *certification* (Sarno dan Iffano, 2009: 59-60).

Dengan adanya audit keamanan sistem informasi pada PT. AJBS ini diharapkan dapat mengukur tingkat keamanan teknologi yang dimiliki PT. AJBS. Audit ini juga menghasilkan rekomendasi untuk meningkatkan keamanan informasi pada perusahaan, serta menjadi acuan untuk memperoleh ISMS *certification* dengan standar ISO 27002,

sehingga menambah nilai tambah akan kepercayaan pelanggan terhadap PT. AJBS.

LANDASAN TEORI

Sistem Informasi

Sistem informasi adalah kombinasi dari teknologi informasi dan aktivitas, yang menggunakan teknologi untuk mendukung kinerja, manajemen dan pembuatan keputusan (Beynon, 2004).

Audit

Audit didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokementasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (ISACA, 2006).

Audit Sistem Informasi

Weber (Weber, 1999) mendefinisikan Audit Sistem Informasi sebagai proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif.

Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi resiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (ISO/IEC 27001, 2005).

ISO 27002

ISO 27002: 2005 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan di dalam ISO/IEC 27001. Sarno dan Iffano (2009: 187) mengatakan kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol keamanan (*security control clauses*), 39 objektif kontrol

(*control objectives*) dan 133 kontrol keamanan/ kontrol (*controls*)

Cobit 4.1

COBIT dikembangkan oleh *IT Governance Institute* (ITGI), yang merupakan bagian dari *Information System Audit and* Kontrol *Association* (ISACA).

Pemetaan ISO 27002 dengan COBIT 4.1

Metode ISO 27002 digunakan untuk mengidentifikasi tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu pada kerangka kerja COBIT atau CCMI (*Capability Marturity Model For Integration*). Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di PT. AJBS.

Maturity Level

ISO 17799 memberikan kontrol keamanan tetapi tidak bagaimana kontrol itu dikembangkan atau diatur. Ini disebabkan ISO bukan standar teknis juga bukan untuk teknologi tertentu. Oleh karena itu tidak ada mekanisme penilaian atau metode evaluasi (Gunawan dan Suhono, 2006: 135), sehingga pengidentifikasian *maturity level* mengacu pada kerangka kerja COBIT atau CCMI (*Capability Marturity Model For Integration*). Model yang digunakan untuk mengendalikan proses teknologi informasi yang terdiri dari pengembangan suatu metode penilaian sehingga suatu organisasi dapat mengukur dirinya sendiri dari non-eksisten ke tingkat optimal (*value* 0 sampai dengan *value* 5).

METODOLOGI PENELITIAN

Langkah-langkah pelaksanaan audit keamanan sistem informasi mencangkup:

1. Perencanaan dan persiapan audit sistem informasi.
2. Pelaksanaan audit sistem informasi.
3. Pelaporan audit sistem informasi.

IMPLEMENTASI DAN HASIL

Penentuan Ruang Lingkup Audit Keamanan Sistem Informasi

Penentuan ruang lingkup audit keamanan sistem informasi dilakukan dengan cara menentukan objektif kontrol yang akan digunakan. Perusahaan perlu melakukan pemilihan terhadap kontrol-kontrol yang ada dengan memperhatikan kebutuhan organisasinya, bagaimana cara penerapan dan penetapan resiko jika kontrol tersebut tidak dipenuhi. Kontrol didesain untuk

memberikan kepastian bahwa tindakan manajerial yang dilakukan dapat memberikan kepastian bahwa tujuan bisnis akan dicapai dan kejadian yang tidak diinginkan akan dapat dicegah, dideteksi, dan diperbaiki (Sarno, 2009). Tabel 1 merupakan pemetaan dari pedoman yang digunakan terhadap klausul-klausul ISO 27002.

Tabel 1 Pemetaan Klausul ISO 27002

Klausul	Deskripsi
8	Keamanan SDM
9	Keamanan Fisik dan Lingkungan
10	Manajemen Komunikasi dan Operasi
11	Kontrol Akses
13	Manajemen Kejadian Keamanan Informasi
14	Manajemen Kelangsungan Bisnis

Pelaksanaan Audit Kepatutan dan Penentuan Maturity Level

Pelaksanaan audit kepatutan menghasilkan dokumen wawancara, bukti-bukti audit, temuan audit dan nilai tingkat kematangan tiap kontrol keamanan. Dokumen wawancara diperoleh saat prosedur pembuatan pertanyaan dari pernyataan yang sebelumnya dibuat. Bukti-bukti dan temuan audit diperoleh saat dilakukan wawancara kepada perusahaan. Setelah didapatkan bukti-bukti dan temuan audit tersebut kemudian dievaluasi dan dianalisa lalu menentukan nilai tingkat kemampuan tiap-tiap kontrol keamanan.

Contoh kerangka kerja perhitungan nilai *maturity level* dapat dilihat pada Tabel 2, untuk contoh hasil perhitungan tingkat kemampuan dapat dilihat pada Tabel 3 dan contoh representasi hasilnya ke dalam digram radar dapat dilihat pada Gambar 1.

Tabel 2 Contoh Kerangka Kerja Perhitungan *Maturity Level*

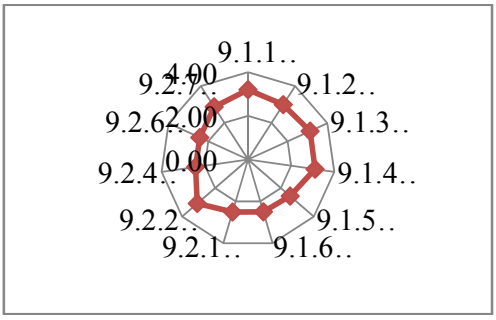
Nama Proses	Mengelola Lingkungan Fisik		
Nomor Proses	**DS12**	**Level Kedewasaan**	**0**
No	**Pernyataan**		**Bobot**
1	Terdapat kebutuhan untuk perlindungan fasilitas sumber daya komputer		1.00
2	Terdapat kebutuhan untuk perlindungan fasilitas sumber daya komputer		1.00
		Total Bobot	**2.00**

	Apakah sepakat?			
Tidak Sama Sekali	Sedikit	Dalam tingkatan tertentu	Seluruhnya	NILAI
0.00	0.33	0.66	1.00	
			√	1.00
			√	1.00
Tingkat Kepatutan		**1.00**	Total Nilai	2.00

Tabel 3 Contoh Hasil *Maturity Level* Klausul 9 Keamanan Fisik dan Lingkungan

Objektif Kontrol	Kontrol Kemananan	Cobit IT Processes	*Maturity* COBIT 4.1	*Maturity* ISO 27002	Rata-Rata Objektif Kontrol
9.1	9.1.1 Pembatas Keamanan Fisik	DS12	3.20	3.20	

Wilayah Aman	9.1.2 Kontrol Masuk Fisik	DS12	2.99	2.99	
	9.1.3 Keamanan Kantor, Ruang, dan Fasilitasnya	DS12	3.13	3.13	
	9.1.4 Perlindungan Terhadap Ancaman Dari Luar dan Sekitar	DS12	3.11	3.11	
Objektif Kontrol	Kontrol Kemananan	Cobit IT Processes	*Maturity* COBIT 4.1	*Maturity* ISO 27002	Rata-Rata Objektif Kontrol
9.1 Wilayah Aman (Lanjutan)	9.1.5 Bekerja di Wilayah Aman	PO4	2.89	2.56	2.95
		PO6	2.54		
		AI3	1.65		
		DS12	3.17		
	9.1.6 Akses Publik, Tempat Pengiriman, dan Penurunan Barang	DS5	1.90	2.50	
		DS12	3.10		
9.2 Keamanan Peralatan	9.2.1 Letak Peralatan dan Pengamanannya	DS5	1.90	2.51	2.66
		DS12	3.11		
	9.2.2 Utilitas Pendukung	DS12	3.08	3.08	
	9.2.4 Pemeliharaan Peralatan	AI3	1.65	2.43	
		DS12	3.08		
		DS13	2.56		
	9.2.6 Keamanan untuk Pembuangan atau Pemanfaatan Kembali Peralatan	DS11	2.43	2.43	
	9.2.7 Hak Pemanfaatan	PO6	2.54	2.87	
		DS12	3.20		
***Maturity Level* Klausul 9**					**2.81**



Gambar 1 Contoh Representasi Nilai *Maturity Level* Klausul 9 Keamanan Fisik dan Lingkungan

Penentuan dan Penyusunan Hasil Audit Sistem Informasi

Hasil audit keamanan sistem informasi berupa temuan dan rekomendasi untuk perusahaan. Temuan dan rekomendasi tersebut berasal dari hasil wawancara yang dilakukan, yang sebelumnya dievaluasi dan dianalisa. Laporan hasil audit yang berupa temuan-temuan dan rekomendasi tersebut digunakan sebagai saran untuk perbaikan kontrol keamanan.

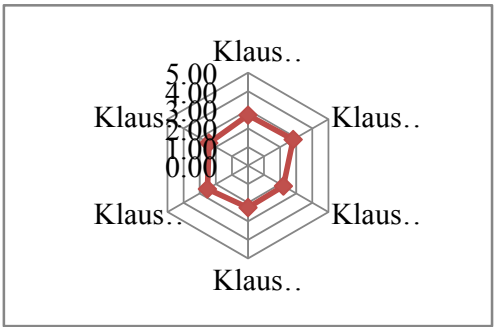
Setelah seluruh perhitungan selesai didapatkan nilai *maturity level* dari rata-rata keseluruhan nilai klasul yang dapat dilihat pada Tabel 4.

Tabel 4 Hasil *Maturity Level* Seluruh Klausul yang Digunakan

Klausul	Deskripsi	*Maturity Level*
8	Keamanan SDM	2.72
9	Keamanan Fisik dan Lingkungan	2.81
10	Manajemen Komunikasi dan	2.20

	Operasi	
11	Kontrol Akses	2.26
13	Manajemen Kejadian Keamanan Informasi	2.52
14	Manajemen Kelangsungan Bisnis	2.43
Nilai *Maturity Level*		**2.49**

Didapat representasi hasil *maturity level* seluruh klausul pada Gambar 2 dan terlihat bahwa Manajemen Aset dan Kejadian Keamanan Informasi memiliki nilai yang belum baik, sehingga harus dimanajemen ulang pada prosedur untuk mengelola kontrol keamanannya.



Gambar 2 Representasi Hasil *Maturity Level* Seluruh Klausul

Penyusunan Temuan

Setelah dilakukan analisa dan evaluasi dari audit keamanan sistem informasi pada PT. AJBS didapatkan beberapa kondisi yang sesuai dengan kontrol keamananan pada ISO 27002 yang telah ditetapkan. Beberapa kondisi tersebut yaitu:

1. Terdapat aturan mengenai tanggung jawab keamanan informasi pada kontrak kerja pegawai.
2. Terdapat perimeter keamanan untuk melindungi ruang yang berisikan fasilitas pemrosesan informasi.
3. Terdapat penetapan persyaratan bisnis untuk kontrol akses.
4. Terdapat tanggung jawab manajemen pada pengelolaan kejadian keamanan informasi.

Sedangkan kondisi yang masih perlu perbaikan yaitu:

1. Perjanjian kerahasiaan belum dijabarkan secara detail dan spesifik.
2. Belum ada pelatihan-pelatihan terkait keamanan informasi, misalnya kriteria *password* yang baik, pelatihan tentang antisipasi serangan virus, dan lain-lain.
3. Belum dilakukan pengkajian ulang dan pembaharuan hak akses secara berkala. Pembaharuan hak akses tidak diwajibkan secara berkala.
4. Banyak prosedur operasi yang belum terdokumentasi, yaitu prosedur pemulihan, program *start-up, close-down*, *back-up*, sistem *restart*, penjadwalan pemeliharaan, instruksi penanganan kesalahan atau kondisi istimewa lain, pembatasan penggunaan fasilitas sistem, dll.

Penyusunan Rekomendasi

Berdasarkan dari temuan yang didapat dari audit keamanan sistem informasi maka

disusun rekomendasi guna perbaikan untuk kondisi-kondisi pada perusahaan yang belum sesuai dengan prosedur. Beberapa rekomendasi tersebut yaitu:

1. Menjabarkan perjanjian kerahasiaan secara detail dan spesifik termasuk menjaga kerahasiaan *password.*
2. Membuat modul-modul pelatihan dan mengadakan pelatihan pada karyawan mengenai keamanan informasi.
3. Melakukan pengkajian ulang tentang hak akses masing-masing dan pembaharuan hak akses apabila terjadi pemindahan bagian maupun kenaikan jabatan sesuai dengan hak akses masing-masing.

Kesimpulan

Berdasarkan hasil audit keamanan sistem informasi, maka didapat kesimpulan:

1. Penyalahgunaan *password* disebabkan karena peraturan perusahaan yang kurang tegas dan kurang spesififk untuk kerahasiaan *password*, belum adanya perjanjian atau pernyataan tertulis yang ditandatangani untuk benar-benar menjaga kerahasiaan *password* masing-masing, kurangnya kesadaran serta pengetahuan karyawan terhadap pentingnya merahasiakan *password*.
2. Terdapat kebijakan dan prosedur yang belum terdokumentasi, bahkan ada beberapa tindakan dalam perusahaan yang dilakukan berdasarkan spontanitas dan tanpa ada aturan baku yang bersifat formal.
3. Nilai *maturity level* yang dihasilkan oleh PT. Aneka Jaya Baut Sejahtera yaitu 2.49 yang termasuk pada kategori level 2 yaitu *repeatable*. Hal tersebut menandakan bahwa proses keamanan sistem informasi pada PT. Aneka Jaya Baut Sejahtera telah dilakukan secara rutin, namun belum berdasarkan aturan dan panduan formal.

Saran

Beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut yaitu:

1. Audit keamanan sistem informasi ini masih belum menggunakan keseluruhan klausul dan kontrol keamanan yang ada pada ISO 27002. Diharapkan dapat dilakukan audit keamanan sistem informasi kembali dengan menggunakan keseluruhan klausul dan kontrol keamanan ISO 27002 setelah pihak

perusahaan melakukan perbaikan keamanan sistem informasinya.

2. Berdasarkan hasil audit keamanan sistem informasi telah dilakukan, didapatkan pernyataan bahwa pihak perusahaan belum pernah diaudit dengan standar-standar lain. Untuk itu dapat dilakukan audit sistem informasi menggunakan standar lain selain ISO.

Daftar Pustaka

Beynon, D.P. 2004. *E-Business*. Basingstoke: Palgrave.

Gunawan, H dan Suhono, R D. 2006. *Studi ISO 17799:2005 Dan Systems Security Engineering Capability Maturity Model (SSE-CMM) Untuk Keamanan Aplikasi Web.* Bandung: Institut Teknologi Bandung.

Information Technology Governance Institute. 2007. *COBIT 4.10: Control Objective, Management Guidelines, Maturity Models*. United States of America: IT Governance Institute.

ISACA. 2006. *CISA Review Manual*.

ISO/IEC. 2005. *Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005*. Switzerland.

ISO/IEC.2005.*Information Technology-Security Techniques-Information Security Management System ISO/IEC 27001: 2005*. Switzerland.

Rahardjo, Budi. 2005. *Keamanan Sistem Informasi Berbasis Internet*. Bandung: PT. Insan Indonesia.

Sarno, Riyanarto. 2009. Audit Sistem & Teknologi Informasi. Surabaya: ITS Press.

Sarno, R. dan Iffano, I. 2009. Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.

Tanuwijaya, H. dan Sarno, R. 2010. *Comparation of CobiT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulations and Information Technology Goals*, International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010.

Weber, Ron. 2000. *Information System Control and Audit.* New Jersey: Prentice Hall, Inc.