ANALISIS TATA KELOLA KEAMANAN SISTEM INFORMASI BERDASARKAN ISO/IEC 27002:2005 (STUDI KASUS : PT. XYZ)

Irlon Dahil
Program Studi Teknik Informatika, FTI, Institut Teknologi Budi Utomo
dahil.irlon@gmail.com

Abstract
Information technology, which has long been considered a driver and supporter of corporate strategy, is now considered an integrated part of business strategy. The existence of IT Governance will align so that IT goals and business goals are aligned. Good IT governance, one of which is emphasizing the need to maintain the integrity of information and protect IT assets that require an information security management process. Information security management includes monitoring security, testing and implementing corrective actions on a regular basis to identify system weaknesses and incidents.
This study provides recommendations for improving PT XYZ's information security. This study uses the ISO 27002:2005 standard to develop recommendations for improving PT XYZ's information security. Data collection techniques used to compile this research are questionnaires, interviews with related personnel at PT XYZ and literature studies. The existing data is then processed to produce information security management recommendations for PT XYZ.
Keywords*: governance, security, information system, ISO 27002:2005*

1. PENDAHULUAN

Tidak dapat dipungkiri bahwa saat ini keberadaan Teknologi Informasi bagi perusahaan di anggap sebagai pendorong dan sebagai bagian terintegrasi dari strategi bisnis. Para pimpinan perusahaan sepakat bahwa keselarasan antara Tujuan binis dan. TI merupakan factor sukses kritis (Critical Success Factor) di perusahaan. Keberadaan Tata Kelola TI membantu pemenuhan factor tersebut dengan secara pemenuhan kebutuhan akan informasi yang dapat di andalkan dan terjamin.

Oleh karena pentinganya keberadaan informasi, maka sebagai pencari dan penemu informasi (information seeker) kita perlu mengetahui bagaimana cara untuk mengamankan informasi yang kita miliki, sehingga tidak sembarang orang dapat mengakses dan menggunakan informas tersebut dengan sembarangan.

PT XYZ adalah sebuah perusahaan Penanaman Modal Asing (PMA) yang bergerak di bidang manufaktur pembuatan ban kendaraan bermotor. PT XYZ menggunakan Teknologi Informasi untuk menunjang kegiatan bisnisnya. Seiring dengan kebutuhan bisnis yang meningkat, maka kebutuhan Teknologi Informasi yang menunjang kegiatan bisnis juga meningkat.

Untuk mengelola Teknologi Informasi maka PT XYZ perlu menerapkan Tata Kelola TI yang baik. Tata kelola TI yang baik salah satunya adalah menekankan perlunya memelihara integritas informasi dan melindungi aset TI yang membutuhkan suatu proses menajemen keamanan. Manajemen keamanan di dalamnya termasuk mengukur tingkat kematangan keamanan, memonitor keamanan, pengujian dan pengimplementasian tindakan perbaikan secara berkala untuk mengidentifikasi adanya kelemahan sistem dan insiden. Manajemen yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis akan adanya kelemahan dan insiden

Untuk memastikan kesesuaian penerapan tata kelola keamanan system informasi di PT XYZ dengan kebutuhan informasi, maka harus dikelola dengan baik sebagai aset berharga dan perlu dilakukan analisis terhadap kebutuhannya, agar mampu memperkecil risiko yang mungkin akan terjadi. Analisa pengukuran tata kelola keamanan sistem informasi akan dapat dilakukan dengan baik apabila ditunjang dengan suatu pengelolaan TI (IT Governance) dari mulai perencanaan sampai implementasinya,

Adapun salah satu standard manajemen keamanan informasi yang dikenal luas secara global yaitu, Standar ISO/IEC 27002 untuk membantu organisasi dalam menganalisa sistem keamanan informasi..

2. METODELOGI PENELITIAN

2.1 Instrumen Penelitian

Instrumen yang digunakan dalam penelitian ini berupa kuesioner yang disusun dan dikelompokan berdasarkan pemberian sejumlah pertanyaan untuk setiap level kematangan pada setiap *control objective* pada domain ISO/IEC 27002 yang terdiri dari 5 level dengan urutan dari lebel 0 sampai dengan level 5. Setiap *control objective ISO/IEC 27002* pada masing-masing level mempuyai beberapa pertanyaan, sehingga setiap *control objective* pada domain ISO/IEC 27002 mempunyai banyak pertanyaan. Jumlah pertanyaan pada setiap *control objective* pada domain ISO/IEC 27002 dapat dilihat pada tabel berikut ini:

Tabel 3. Jumlah Domain dan Kontrol ISO/IEC 27002:2005

NO	Klausul	Proses	JumalhControl
1	5	Security policy	2
2	6	Organisasi Keamanan Informasi	11
3	7	Manajemen Aset	5
4	8	Keamanan Sumber Daya Manusia	9
5	9	Keamanan Fisik dan Lingkungan	13
6	10	Manajemen komunikasi dan operasi	31
7	11	Kontrol Akses	25
8	12	Akusisi Sistem Infromasi, Pembangunan dan Pemeliharaan	16
9	13	Manajemen kejadian keamanan informasi	5
10	14	Manajemen kelangsungan bisnis	5
11	15	Kepatuhan (*Complience*)	10
			132

Berhubung luasnya domain masalah yang terdapat pada standard tersebut dan terbatasnya waktu penelitian yang ada, focus dari penulisan tesis ini lebih dititikberatkan pada domain/klausul 5, 6, 7, 8, 11 dan 13.

Tabel 4. Pemilihan Domain/Klausul yang di Pilih

3. ANALISA DAN PEMBAHASAN

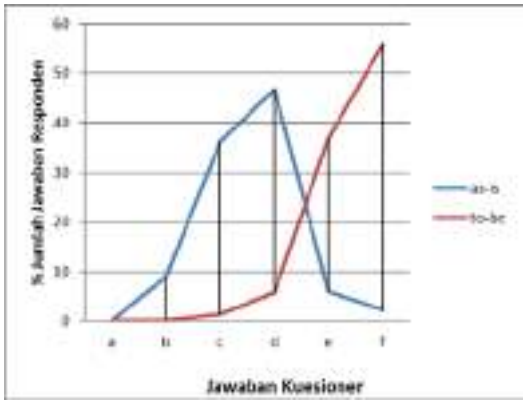
3.1 Hasil Tingkat Kematangan Keamanan Sistem Informasi

Dari Analisis terhadap penilaian tingkat kematangan pada keamanan sistem informasi, kemudian dilakukan rekapitulasi, seperti tampak pada tabel 5 dan dinyatakan dalam bentuk grafik seperti tampak pada gambar 3

Tabel 5 Rekapitulasi Jawaban Responden Pada Kuesioner Maturity Level

NO	DOMAIN		DISTRIBUSI JAWABAN					
			a	b	c	d	e	f
			(%)	(%)	(%)	(%)	(%)	(%)
1	SP	as-is	0.00	0.00	40.00	60.00	0.00	0.00
		to-be	0.00	0.00	6.67	20.00	26.67	46.67
2	OIS	as-is	0.00	0.00	65.45	33.94	0.61	0.00
		to-be	0.00	0.00	0.00	0.00	40.00	60.00
3	AM	as-is	0.00	13.33	52.00	20.00	14.67	0.00
		to-be	0.00	0.00	1.33	13.33	12.00	73.33
4	HRS	as-is	0.00	20.00	13.33	53.33	0.00	13.33
		to-be	0.00	0.00	0.00	0.00	57.78	42.22
5	AC	as-is	0.00	0.00	26.40	66.40	7.20	0.00
		to-be	0.00	0.00	0.00	1.07	39.20	59.73
6	ISIM	as-is	0.00	20.00	20.00	46.67	13.33	0.00
		to-be	0.00	0.00	0.00	0.00	46.67	53.33
as-is			0.00	8.89	36.20	**46.72**	5.97	2.22
to-be			0.00	0.00	1.33	5.73	37.05	**55.88**

SP : Security Policy
OIS : Organization of Informastion Security
AM : Asset management
HRS : Human Resouces Security
AC : Access Control
ISIM : Information Security Incident Management)



Gambar 3 Grafik Distribusi Jawaban Kuesioner Maturity Level

Secara umum, kesimpulan yang dapat diambil dari hasil jawaban responden pada kuesioner adalah:

1) Persentase tertinggi untuk keadaan saat ini (*as-is)* adalah sebanyak 46.72% responden memilih jawaban "d" atas pertanyaan yang berorientasi pada keadaan saat ini (*as-is*), artinya untuk keadaan saat ini (*as-is*) hasil responden terbanyak menunjukan di diposisi level 3.
2) Dan persentase jawaban tertinggi untuk keadaan pada masa depan adalah sebanyak 55.88% responden memilih jawaban "f" untuk pertanyaan yang berorientasi pada masa depan (*to-be*), artinya untuk hasil pertanyaan ke responden terbanyak menunjukan harapan (*to-be*) ke level

Pola kecenderungan tersebut ditunjukan secara jelas pada gambar 4.1, dimana posisi puncak kurva *as-is* lebih dekat pada jawaban "d", dan puncak untuk kurva *to-be* lebih dekat pada jawaban "f"

3.2 PERHITUNGAN TINGKAT KEMATANGAN

Pehitungan tingkat kematangan dilakukan dengan menggunakan acuan nilai model kematangan COBIT. Sehingga untuk tiap pilihan jawaban kuesioner diberikan bobot kedalam nilai kematangan tersebut, bobot untuk setiap jawaban kuesioner dapat dilihat pada tabel 6

Tabel 6 Bobot Jawaban dan Nilai/Tingkat Kematangan Kuesioner Maturity Level

NO	Jawaban	Nilai Kematangan	Tingkat Kematangan
1	a	0	*0 No-existent*
2	b	1	*1 Initial/Ad Hoc*
3	c	2	*2 Respeatable but Intuitive*
4	d	3	*3 Defined Process*
5	e	4	*4 Manage and Measurable*
6	f	5	*5 Optimised*

Dengan mengasumsikan bahwa setiap domain mempunyai bobot yang sama terhadap tingkat kematangan pada Keamanan sistem informasi, maka tingkat kematangan untuk status *as-is* dan *to-be* dapat dilihat pada tabel 7

Tabel 7 Nilai dan Tingkat Kematangan Hasil Kuesioner Maturity Level

NO	DOMAIN	NILAI KEMATANGAN		TINGKAT KEMATANGAN	
		(as-is)	(to-be)	(as-is)	(to-be)
1	SP	3.60	4.73	3	4
2	OIS	2.35	4.60	2	5
3	AM	2.36	4.57	2	5
4	HRS	2.76	4.67	3	4
5	AC	2.81	4.60	3	5
6	ISIM	2.53	4.53	3	5
RATA-RATA		2.56	4.62	3	4

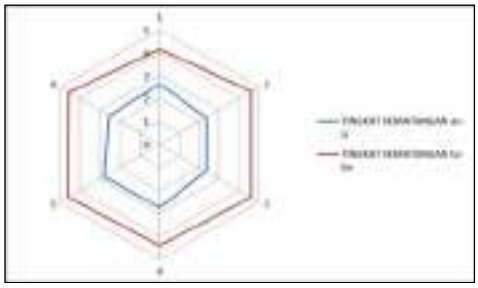
SP : Security Policy

OIS	:	Organization of Informastion Security
AM	:	Asset management
HRS	:	Human Resouces Security
AC	:	Access Control
ISIM	:	Information Security Incident Management)

Dari tabel 7, dapat diperoleh informasi, bahwa

1) Tingkat kematangan saat ini (*as-is*), pada Keamanan sistem informasi secara keseluruhan berada pada tingkat 3 atau Proses terdefinisi (*Define Process*).
2) Tingkat kematangan yang diharapkan (*to-be),* pada Keamanan sistem informasi secara keseluruhan berada pada tingkat 4 atau Terkelola dan Terukur (*Managed dan Measurable*)

Kedua kondisi kematangan tersebut (*as-is* dan *to-be*) jika dibuat representasinya dalam bentuk grafik radar, akan terlihat seperti pada gambar 4



Gambar 4 Grafik Nilai Kematangan Keadaan Saat ini (as-is) dan Keadaan Yang Akan Datang (to-be)

Dari bentuk tabel 7 dan gambar 4, dengan melihat rata-rata nilai kematangan (*as-is*) pada masing-masing domain, dilakukan penyusunan urutan skala perioritas dalam upaya perbaikan dimasa berikutnya. Urutan skala prioritas tersebut dapat dilihat pada tabel 8

Tabel 8 Urutan Skala Prioritas Domain Nilai Kematangan

NO	DOMAIN	NILAI KEMATANGAN		TINGKAT KEMATANGAN	
		as-is	*to-be*	*as-is*	*to-be*
1	OIS	2.35	4.60	2	5
2	AM	2.36	4.57	2	5
3	AC	2.81	4.30	3	5
4	HRS	2.53	4.53	3	5
5	SP	2.60	4.13	3	4
6	ISIM	2.73	4.42	3	4
RATA-RATA		2.56	4.43	3	4

Ket:

SP	:	Security Policy
OIS	:	Organization of Informastion Security
AM	:	Asset management
HRS	:	Human Resouces Security
AC	:	Access Control
ISIM	:	Information Security Incident Management)

3.3 Hasil Kematangan Saat Ini (*as is*)

Dari hasil perolehan pada tabel 4.10, untuk kondisi saat ini (*as-is*), sehubungan dengan tingkat kematangan domain, diperoleh kajian sebagai berikut:

1) Tingkat kematangan domain pada kondisi saat ini (*as-is*), bekisar Antara level 2 dan 3. Domain dengan tingkat kematangan 2 akan menjadi prioritas yang lebih tinggi, dibandingkan domain dengan tingkat kematangan 3. Domain dengan tingkat kematangan 2 yang meliputi domain OIS dan AM dalam penetapan strategi pencapaian *improvemen*t akan mendapatkan kesempatan pertama untuk dilakukan *improvement*. Sedangkan domain lainnya, yaitu AC, ISIM, SP dan HRS akan mendapat kesempatan berikutnya.

2) Kematangan yang relatif tinggi ada pada domain AC, ISIM, SP dan HRS merefleksikan bahwa sudah ada penerapan tujuan dan indikator pengukuran dalam pelaksanaan tugas, adanya kepedulian dari pihak

manajemen walaupun belum dikatakan tinggi, pelatihan keterampilan dan keahlian telah dilakukan secara informal sesuai dengan kebutuhan saat itu, serta telah didefiniskannya peran dalam manajemen keamanan system informasi, walaupun hanya sebatas pada kemampuan pada perorangan karena dianggap telah biasa dan berpengalaman. Namun dalam pelaksanaanya sudah dapatdipertanggungjawabkan, karena telah terdefinisi dalam tugas.

3) Rendahnya tingkat kematangan domain AM secara umum dikarenakan belum adanya pengelolaan aset informasi perusahaan untuk menyusun dan mengklasifikasikan secara jelas yang mana semua aset informasi kritis perusahaan direkam dan didokumentasikan. Semua aset belum dipertanggungjawabkan dan memiliki pemilik. Pemilik harus diidentifikasi untuk seluruh aset dan tanggung jawab untuk pemeliharaan kontrol yang tepat belum diberikan. Pelaksanaan kontrol tertentu dapat didelegasikan oleh pemilik sesuai tapi pemilik belum bertanggung jawab untuk perlindungan yang tepat dari aset..
4) Rendahnya tingkat kematangan domain OIS secara umum di karenakan Kerangka manajemen belum ditetapkan untuk memulai dan mengendalikan pelaksanaan keamanan informasi dalam organisasi. Manajemen belum meninjau pelaksanaan keamanan di seluruh organisasi. Dan juga belum adanya, sumber nasihat spesialis keamanan informasi yang ditetapkan dan tersedia dalam organisasi.

Dari hasil rata-rata kondisi kematangan saat ini *as-is*, yang berada pada level 3, ini dapat di simpulkan bahwa tingkat kematangan AM and OIS masih berada di level 2, sesuai dengan keadaan di lapangan, dimana belum adanya tanggung jawab kepemilikan aset dan pengklasifikasian aset. Pimpinan belum mengetahui akan lemahnya sistem yang ada, dan manajemen belum meninjau pelaksanaan keamanan di seluruh organisasi.

3.4 Hasil Kematangan diharapkan (*to be*)

Hal-hal yang perlu diperhatikan pada kondisi *to b*e, sehubungan dengan tingkat kematangan domain, dapat dikaji sebagai berikut:

1) Tingkat kematangan seluruh domain pada kondisi *to-be* bervariasi, mulai dari level 4 (terkelola dan terukur/*managed* and *measurable*) dan level 5 (*optimis/optimized*). Semua domain akan diarahkan mencapai kepada level yang diharapkan, dengan melakukan perbaikan ataupun peningkatan pada segi keamanan.
2) Domain AM berada di kematangan yang diharapkan ada pada level 5, ini menunjukan keinginan perusahaan untuk penata asset IT perusahaan yang lebih baik dengan mengklasifikasikan asset informasi menurut nilainya, kepetingannya dan tingkat kritikalnya terhadap organisasi. Seluruh asset harus di inventarisasi dan dipelihara, seluruh informasi dan asset yang berhubungan dengan fasilitas pemrosesan informasi harfus ditentukan kepemilikannya dan juga aturan-aturan penggunaannya juga harus jelas.
3) Domain OIS berada di kematangan yang diharapkan ada pada level 5, ini menunjukan keinginan manajemen perusahaan untuk mengelola keamanan informasi di dalam organiasi secara aktif dengan memberi dukungan tentang keamanan dalam organiasi melalui arahan dan komitmen yang jelas serta rasa tanggung jawab terhadap keamanan, sedangkan untuk di luar organisasi manajemen berkeinginan untuk membuat dan memberikan perjanjian

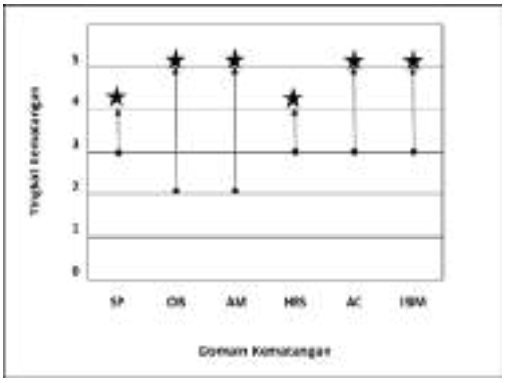
dengan pihak ketiga yang meliputi pengaksesan, pemrosesan, komunikasi dan pengelolaan informasi organisasi atau penambahan produk terhadap fasilitas permrosesan informasi dengan melibatkan seluruh persayaratan keamanan yang dibutuhkan organisasi.

4) Domain ISIM berada di kematangan yang diharapkan ada pada level 5, ini menunjukan keinginan manajemen perusahaan untuk semua karyawan, kontraktor dan pengguna pihak ketiga dari system informasi dan layanan, disyaratkan untuk mencatat dan melaporkan temuan/dugaan apapun dari kelemehan keamanan dalam sistem/layanan. Dan juga manajemen akan membuat prosedur-prosedur untuk memastikan kecepatan dan keefektifan dalam penanganan kejadian keamanan informasi.
5) Untuk *security Policy* (SP), kebijakan keamanan informasi harus di tinjau ulang secara berkala, jika terjadi perubahan harus dipastikan hal tersebut merupakan pengembangan dari kebijakan sebelumnya sehingga menjadi lebih sesuai, mencukupi kebutuhan organisasi dan lebih efektif dalam pelaksanaannya.
6) Domain human resource security (HRS) , manajemen perusahaan berkeinginan membuat aturan-aturan dan tanggung jawab jelas keamanan dari pegawai, kontraktor dan pengguna pihak ketiga, sehingga dapat didefinisikan, didokumentasikan sesuai dengan kebijakan keamanan informasi organisasi.

Dengan melihat hasil tingkat kematangan pada kondisi yang diharapkan (*to-be*), terlihat bahwa harapan yang diinginkan sangatlah tinggi. Hal tersebut merupakan adanya kesadaran responden akan pentingnya tata kelola keamanan sistem informasi. Tentu saja, untuk mencapai tingkat kematangan tersebut harus didukung oleh banyak faktor, mulai dari komitmen pimpinan PT. XYZ di dalam meningkatkan kesadaran dalam hal keamanan sistem informasi

3.5 Representasi Tingkat Kematangan

Untuk mendapatkan gambaran yang lebih jelas terhadap tingkat kematangan pada kondisi saat ini (*as-is*) maupun kondisi yang diharapkan (*to-be*), dan upaya menutupi kesenjangan yang ada, dapat dibuat sebuah diagram seperti terlihat pada gambar 5



Gambar 5. Diagram Rising Star Tingkat Kematangan as-is dan to-be dari Domain Kematangan.

Ket:

SP	:	Security Policy
OIS	:	Organization of Informastion Security
AM	:	Asset management
HRS	:	Human Resouces Security
AC	:	Access Control
ISIM	:	Information Security Incident Management)

Pada gambar 5 proses pencapaian kematangan yang diharapkan ditunjukan dengan pergerakkan bintang dari bawah (*as-is*) ke atas (*to-be*).

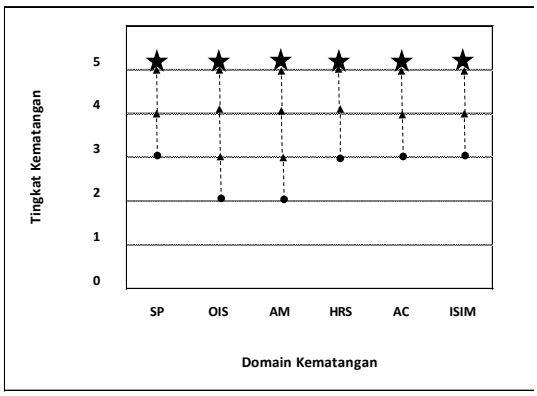
3.6 Penetapan Strategi Pencapaian Kematangan

Agar terjadi keseimbangn dalam pencapaian tingkat kematangan untuk

seluruh atribut, maka penetapan pencapaian kematangan akan diasumsikan mencapai keseragaman pencapaian pada level 5. Penetapan strategi pencapaian kematangan dilakukan dengan skenario, sebagai berikut:

1) Domain OIS dan AM dengan tingkat kematangan lebih rendah pada kondisi saat ini (*as-is*) menjadi prioritas utama untuk dilakukan perbaikan, mencapai tingkat kematangan 3 terlebih dahulu.
2) Pada saat kondisi mencapai keseimbangan pada tingkat 3, maka domain OIS dan AM bersama seluruh domain yang berada pada level 3 secara bersama-sama dilakukan peningkatan pencapaian pada level 4.
3) Setelah domain telah mencapai level 4, maka secara bersama-sama akan dilakukan perbaikan menuju kondisi pada tingkat kematangan *to-be*, yaitu menuju pada tingkat kematangan level 6.

Sekenario diatas, jika di presentasikan dalam bentuk diagram *rising star* dapat dilihat pada gambar 6



Gambar 6 Diagram Rising Star Strategi Pencapaian Tingkat Kematangan

Ket:

SP	:	Security Policy
OIS	:	Organization of Informastion Security
AM	:	Asset management
HRS	:	Human Resouces Security
AC	:	Access Control
ISIM	:	Information Security Incident Management)

4 PENUTUP

4.1 SIMPULAN

Setelah melakukan penelitian, maka dapat disimpulkan hal-hal sebagai berikut:

1) Tingkat kematangan saat ini berada di level 3, yang artinya kontrol keamanan telah didokumentasikan rinci dan dikomunikasikan melalui pelatihan, kesadaran akan keamanan sudah dipertimbangkan oleh pihak manajemen. Prosedur keamanan TI didefinisikan dan diselaraskan dengan kebijakan keamanan TI. Tanggung jawab keamanan TI ditentukan dan dipahami tetapi tidak ada pengukuran kepatuhan. Perusahaan akan meningkatkan tingkat kematangan menjadi level 4 artinya perusahaan akan melakukan pengukuran efektivitas kontrol keamanan, dimana tanggung jawab keamanan TI harus di tentukan secara jelas, dikelola dan diselenggarakan. Analisis risiko dan dampak keamanan secara konsisten dilakukan. Kebijakan dan prosedur keamanan dilengkapi dengan dasar keamanan yang sepsifik.
2) Dari tata kelola keamanan sistem informasi di PT. XYZ berdasarkan Standar ISO/IEC 27002 memiliki kelebihan yaitu merupakan proses keamanan yang menyeluruh dan seimbang antara fisik, keamanan secara teknikal dan prosedur, serta keamanan pribadi
3) Untuk meningkatkan tingkat kematangan pengelolaan keamanan sistem informasi, pada ISO/IEC 27002 menyediakan kerangka tujuan kontrol berdasarkan proses TI sesuai dengan tujuan perusahaan secara detail dan memberikan gambaran yang lebih spesifik tindakan kontrol yang seharusnya dilakukan, pihak yang terkait di dalamnya dan tujuan tindakan tersebut dilakukan.

DAFTAR PUSTAKA

Aries Fajar Kurnia, Perencanaan Kebihkan Keamanan Informasi Berdasarkan Informasi Security Management System (ISMS) ISO/IEC 27001, Universitas Indonesia.

Brown, S., & Vranesic, Z. (2005). *Fundamentals of Digital Logic with VHDL Design* (Vol. II). New York: Mc Graw-Hill.

Hamblen, J. O., Hall, T. S., & Furman, M. D. (2006). *Rapid Prototyping of Digital Sistems Quartus II Edition.* New York: Springer.

Harpananda Eka Sarwadhamana, Pembuatan Tata Kelola Keamanan Informasi Kontrol Suber Daya Manusia Berbasis ISO/IEC 27001:2005Pada Kantor Pelayanan Perbendaharaan Negara SurabayaI, Jurnal Teknik Pomits Vol. I, No. 1, (2012)1-6.

ISACA, The IT Governance Institute, COBIT 4.1 , USA, 2007

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

ISO, *Information Technology – Security Technique – Information Security Management Systems ISO/IEC 27001:2005,* Switzerland, 2005.

IT Governance Institut, 2003, *COBIT 4.1 4.0 Control Objectives, Management Guidelines, Maturity Model*, USA

Muspa, Aziz Maidy, Perancangan Sistem Manajemen Sekuritas Informasi (SMSI) Berdasarkan ISO/IEC 27001, Tesis ITS Library.

Mochammad Anchar, Strategi Keamanan Informasi Perusahaan Media Cetak/Online Menggunakan Tinjauan Informasi Security Management System, Universitas Budi Luhur.

Kurniawan, Y. (2008). *Algoritma Enkripsi Indonesia BC3*. Diakses tanggal 31 Maret 2008, dari http://ysfk2008.wordpress.com/2008/05/09/algoritma-enkripsi-indonesia-bc3/.

Perry, D. L. (2002). *VHDL Programming by Example*. New York, USA: McGraw-Hill Companies.

Robinson, N., (2005). IT Excellence Starts With Governance. *The Journal of Investment Compliance, 6.3,* 45-49.

Riyanarto Sarno dan Irsyat Iffano, *Sistem Manajemen Keamanan Informasi*, ITS Press, Surabaya, 2009

Satoh, A., Morioka, S., Takano, K., & Munetoh, S. (2001, Januari 01). *A Compact Rijndael Hardware Architecture.* Diakses tanggal 10 Maret 2009, dari http://www.springerlink.com/content/5942q6ytbga2kwbt/fulltext.pdf.

Smith, D. J. (1999). *HDL Chip Design.* Madison, USA: Doone Publications.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices* (Fourth Edition ed.). New Jersey: Prentice Hall.

Sutikno, S., & Kurniawan, Y. (2006). *The Cryptanalysis of Block Cipher*.