Jurnal Penelitian Ilmu Komputer, System Embedded & Logic
p-ISSN: 2303-3304, e-ISSN: 2620-3553
6 (1): 95 - 104 (Maret 2018)

Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001

Mardi Yudhi Putra[1,*], Djajasukma Tjahjadi [2]

[1] Manajemen Informatika; STMIK Bina Insani; Jl.Siliwangi No.6 Rawa Panjang Bekasi-Bekasi Timur 17114 Indonesia, Telp. (021)824 36 886 / (021)824 36 996. Fax. (021)824 009 24; e-mail: mardi@binainsani.ac.id

[2] Sistem Informasi; STMIK LIKMI; Jl. Ir. H.Djuanda No.96, Lebakgede, Coblong, Kota Bandung, Jawa Barat 40132; e-mail: djaja@likmi.ac.id

* Korespondensi: e-mail: mardi@binainsani.ac.id

Diterima: 16 Februari 2018; Review: 2 Maret 2018; Disetujui: 16 Maret 2018

Abstract

Efforts to improve information security are so important to an organization that not only in planning but up to the stage of information security. In reality, there is a lack of awareness of the organization of its importance that it causes the occurrence of security issues such as spam so that it affects the business process of the organization. This study examines the evaluation of the completeness (readiness and maturity) of the Information Security Management System (SMKI) at the Private Higher Education Institution of Bina Insani as measured using the Information Security Index (KAMI). Evaluation carried out refers to the ISO / IEC 27001 information security standard regarding information security requirements. Population and sample of this research consist of 4 working unit that is BAAK, BKEU, PMB and BSIJ & UPT so total amount 20. Sampling technique used is non probability sampling that is saturated sampling. The evaluation results of both the preparedness and maturity of the ISMS are at a very low level with the dependence on the role of information and communication technology at the organization at a moderate level. The level of completeness is at a low level with a score of 167 out of a total of 588 and the level of maturity is at level II. Meanwhile, to obtain ISO / IEC 27001: 2009 certification minimum level of information security is at level III. To achieve the level of maturity of Higher Education Bina Insani need to make improvements gradually starting from kesadaraan importance of information security, such as knowledge sharing and information security related training.

Keywords*: Keywords - Information Security, Index KAMI, ISO 27001*

Abstrak

Upaya meningkatkan keamanan informasi sangat penting pada sebuah organisasi, tidak hanya dalam perencanaan akan tetapi sampai dengan tahap penerapan keamanan informasi. Pada kenyataannya ditemukan kurangnya kesadaran dari organisasi akan pentingnya hal tersebut sehingga menyebabkan terjadinya masalah keamanan informasi sehingga berdampak pada proses bisnis organisasi. Penelitian ini membahas tentang evaluasi kelengkapan (kesiapan dan kematangan) Sistem Manajemen Keamanan Informasi (SMKI) yang ada pada Lembaga Pendidikan Swasta Perguruan Tinggi Bina Insani yang dievaluasi menggunakan Indeks Keamanan Informasi (KAMI). Evaluasi yang dilakukan mengacu pada standar keamanan informasi ISO/IEC 27001 mengenai persyaratan keamanan informasi. Populasi dan sampel penelitian ini terdiri dari 4 unit kerja yakni BAAK, BKEU, PMB dan BSIJ & UPT sehingga jumlah secara keseluruhan 20. Teknik sampling yang digunakan adalah non probability sampling yakni sampling jenuh. Hasil evaluasi baik kesiapan dan kematangan SMKI berada pada tingkat yang

sangat rendah dengan ketergantungan peran teknologi informasi dan komunikasi pada organisasi pada tingkat sedang. Untuk tingkat kelengkapan berada pada tingkat yang rendah dengan skor 167 dari total 588 dan tingkat kematangan berada pada tingkat II. Sementara untuk mendapatkan sertifikasi ISO/IEC 27001:2009 minimal level keamanan informasi adalah berada pada tingkat III. Untuk mencapai tingkat kematangan tersebut Perguruan Tinggi Bina Insani perlu melakukan perbaikan secara bertahap mulai dari kesadaraan pentingnya kemanan informasi, seperti sharing knowledge dan pelatihan terkait keamanan informasi.

Kata kunci: Keamanan Informasi, Indeks KAMI, ISO 27001

1. Pendahuluan

Perkembangan teknologi membuat hampir semua orang dimudahkan dalam hal mengakses informasi. Kemudahan dalam memperoleh informasi tidak menutup kemungkinan adanya ancaman baik secara fisik maupun non fisik sehingga pada akhirnya menimbulkan ancaman. Laporan aduan kasus keamanan juga ikut meningkat seiring meningkatnya pengguna internet, berdasarkan sumber dari ID-SIRTII masalah ancaman yang sering diadukan adalah *malware, spam*, pemalsuan situ web, HaKi dan insiden jaringan.

Disisi lain, pada lingkungan Perguruan Tinggi Bina Insani terkait meningkatnya data pengguna internet, aduan ancaman yang sering terjadi adalah spam. Maka keamanan informasi perlu diperhatikan karena penggunaan teknologi informasi dilakukan dalam mendukung proses bisnis khususnya dalam penggunaan aplikasi email sebagai sarana dalam pertukaran data dan informasi, penggunaan jaringan internet serta layanan Sistem Informasi Akademik. Jika keamanan informasi di lingkungan akademik kurang diperhatikan, ancaman yang akan meningkat selain beberapa ancaman yang telah disebutkan adalah spam, *malware* dan insiden jaringan, sehingga dapat menggangu proses bisnis Perguruan Tinggi tersebut.

Perguruan Tinggi Bina Insani merupakan sebuah lembaga pendidikan swasta, yang memiliki tiga Institusi yakni Akademi Akuntansi, Akademi Sekretaris dan Manajemen, dan Sekolah Tinggi Manajemen Ilmu Komputer. Selain itu memiliki sarana dan prasarana seperti sistem informasi akademik yang digunakan untuk kepentingan layanan akademik. Berdasarkan observasi ditemukan belum pernah melakukan evaluasi terhadap Sistem Manajemen Keamanan Informasi dan adanya rencana untuk meningkatkan sistem keamanan informasi sesuai dengan Standar Nasional Indonesia serta analisis keamanan informasi pada instansi tersebut.

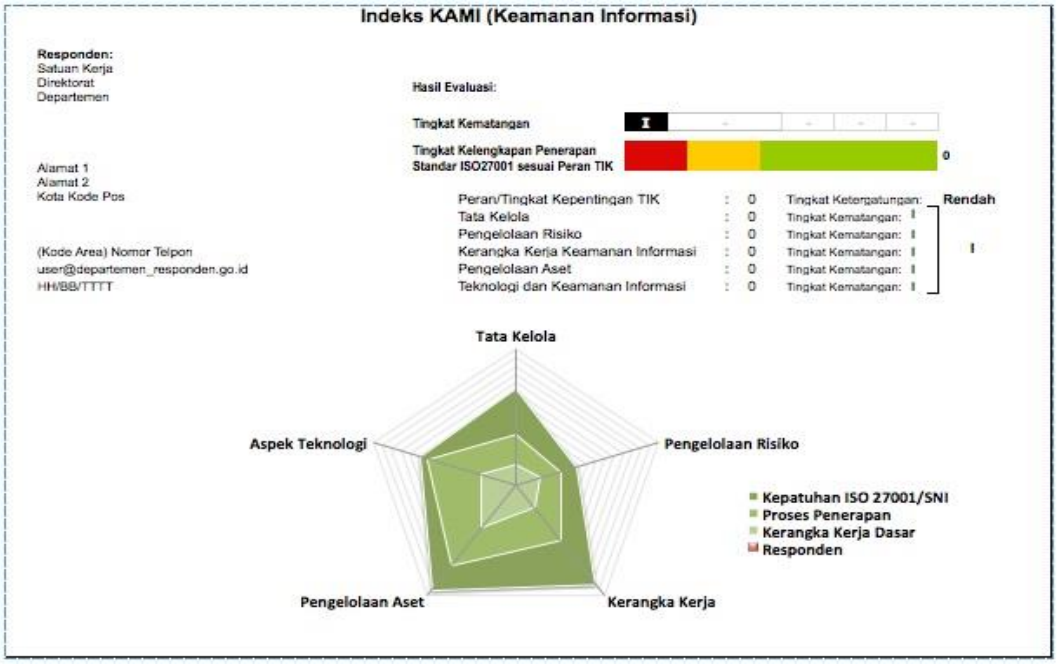
Oleh karena itu dalam pengelolaan keamanan informasi Perguruan Tinggi Bina Insani, penting untuk menganalisis tingkat kesiapan atau kematangan keamanan informasi. Analisis yang dilakukan pada tingkat kelengkapan dan tingkat kematangan keamanan informasi menggunakan indeks Keamanan Informasi (KAMI) yang terdiri dari tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi.

2. Metode Penelitian

Indeks Keamanan Informasi (Indeks KAMI) merupakan alat untuk mengukur dan menganalisis tingkat kelengkapan (kesiapan dan kematangan) pengamanan informasi. Proses evaluasi dilakukan melalui sejumlah pertanyaan di masing-masing area,yakni 1) Peran TIK di dalam Instansi, 2) Tata Kelola Keamanan Informasi, 3) Pengelolaan Risiko Keamanan Informasi, 4) Kerangka Kerja Keamanan Informasi, 5) Pengelolaan Aset Informasi, dan 6) Teknologi dan Keamanan Informasi

Proses penilaian enam area pada Indeks KAMI tersebut dilakukan melalui 2 metode, yakni 1) Tingkat kesiapan penerapan pengamanan, metode ini akan mengevaluasi sejauh mana instansi responden sudah menerapkan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2005. 2) Tingkat kematangan proses pengelolaaan pengamanan informasi, merupakan perluasan dari evaluasi kelengkapan dan digunakan untuk mengidentifikasi tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT (*Control Objective for Information and related Technology*) atau CMMI (*Capability Maturity Model for Integration*).

Hasil akhir penggunaan Indeks KAMI adalah sebuah tampilan *dasboard* yang berguna untuk mengetahui tingkat kesiapan (kelengkapan dan kematangan) keamanan informasi pada SMKI.

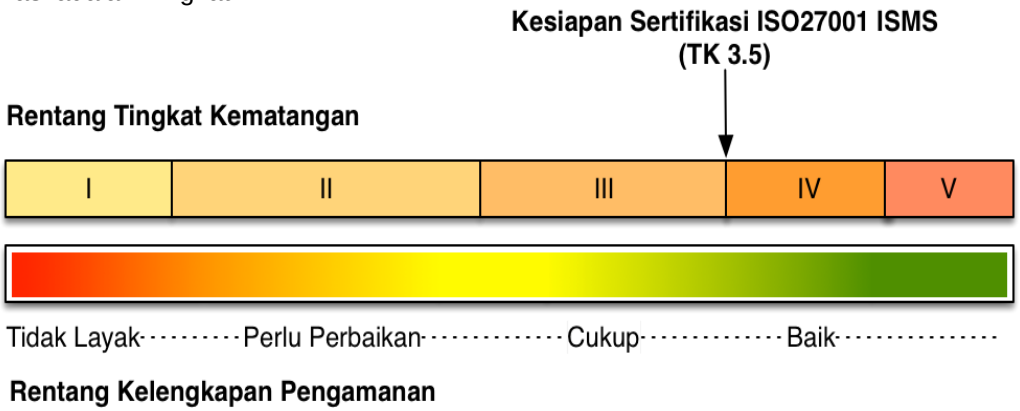


Sumber: Kominfo (2012)

Gambar 1. *Dasboard* Indeks KAMI

Dalam mengidentifikasi tingkat kematangan pada Indeks KAMI, tingkat kematangan dibagi menjadi beberapa tingkatan, yakni 1) Tingkat I - Kondisi Awal, 2) Tingkat II - Penerapan Kerangka Kerja Dasar, 3) Tingkat III - Terdefinisi dan Konsisten, 4) Tingkat IV - Terkelola dan Terukur, 5) Tingkat V – Optimal.

Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi pada instansi. Untuk membantu memberikan uraian yang lebih detil, tingkatan ini ditambah dengan tingkatan antara - I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan Tingkat I. Sebagai padanan terhadap standar ISO/IEC 27000:2005, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.



Sumber: Kominfo (2012)

Gambar 2. Tingkat Kematangan dan Kelengkapan

Kuesioner yang digunakan terkait penelitian merujuk pada Indeks Kami versi.2.3 tahun 2012, yang dibagi menjadi dua, yakni:

a. Peran TIK dalam Instansi

Bagian ini merupakan bagian I pada kuesioner yang diminta untuk memberitingkatan peran dan kepentingan TIK dalam sebuah unit-unit kerja yang ada pada Perguruan Tinggi Bina Insani. Tujuan dari peran TIK adalah untuk mengelompokkan pada tingkatan mana peran TIK pada unit kerja. Tingkat kepentingan yang dimaksud adalah Minim, Rendah, Sedang, Tinggi dan Kritis. Pertama, Minim: jika pengunaan TIK hanya digunakan sebagai penunjang pekerjaan rutin. Untuk skornya minim = 0. Kedua, Rendah: Jika penggunaan TIK digunakan untuk menunjang sejumlah kegiatan tugas pokok. Namun belum pada tingkat signifikan. Untuk skornya sendiri adalah rendah = 1. Ketiga, Sedang: jika penggunaan TIK digunakan untuk membantu proses kerja yang berjalan atau tugas utama instansi, namun hanya digunakan secara internal dan terbatas. Untuk skornya sedang= 2. Keempat, Tinggi: jika peran TIK digunakan sebagai sarana utama pada proses kerja dan tidak dapat dipisahkan, seperti adanya akses ke fungsi administrasi sistem atau basis data dibatasi untuk yang mempunyai otorisasi. Untuk skornya tinggi = 3. Kelima, Kritis: jika peran TIK digunakan sebagai sarana utama dalam menyelesaikan tugas utama instansi yang bersifat nasional dan strategis. Untuk skornya adalah kritis = 4.

Peran TIK yang dievaluasi menggunakan 12 pertanyaan yang tertuang pada kuesioner. Kemudian skor yang dihasilkan dari 12 pertanyaan kuesioner tersebut, ditunjukkan pada Tabel 1.

Tabel 1. Pemetaan Tingkatan Peran TIK

Peran TIK Rendah		**Skor Akhir**		**Status Kesiapan**
0	12	0	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	588	Baik /Cukup
Sedang		**Skor Akhir**		**Status Kesiapan**
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik /Cukup
Tinggi		**Skor Akhir**		**Status Kesiapan**
25	36	0	272	Tidak Layak
		273	392	Perlu Perbaikan
		393	588	Baik /Cukup
Kritis		**Skor Akhir**		**Status Kesiapan**
37	48	0	333	Tidak Layak
		334	453	Perlu Perbaikan
		454	588	Baik /Cukup

Sumber: Kominfo (2012)

b. Area Pengamanan Informasi

Bagian ini merupakan yang memuat bagian II sampai dengan VI yang ada pada kuesioner Indeks KAMI dengan sejumlah pertanyaan terkait keamanan informasi. Terbagi kedalam lima bagian yaitu Bagian II Tata Kelola Keamanan Informasi, untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi dan tanggung jawab pengelola keamanan informasi. Bagian III Pengelolaan Resiko Keamanan Informasi, bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Bagian IV Kerangka Kerja Pengelolaan Keamanan Informasi, bagian ini mengevaluasi kelengkapan dan kesiapan kebijakan & prosedur pengelolaan keamanan informasi dan strategi penerapannya. Bagian V Pengelolaan Aset Informasi, bagian ini mengevaluasi kelengkapan pengamanan aset informasi. Bagian VI Teknologi dan Keamanan Informasi, bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Untuk penilaian sejumlah pertanyaan yang diisi oleh responden di mulai dari bagian I s/d VI pada Indeks KAMI, didefinisikan sebagai berikut a)Tidak Dilakukan, b) Dalam Perencanaan, c) Dalam Penerapan atau Diterapkan Sebagian, d)Diterapkan Secara

Menyeluruh. Jawaban yang telah berikan oleh responden selanjutnya diberikan skor yang nilainya disesuaikan dengan kategori pengamanan. Dalam memberi tanggapan pada area pengamanan mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamaan informasi (pertanyaan diberi label "1"), efektifitas dan konsistensi penerapannya (diberi label "2") dan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (diberi dengan label "3"). Untuk kesiapan minimum yang dipersyaratkan oleh standar ISO/IEC 27001:2005 terdapat pada label "3". Berikut ditunjukkan pada Tabel 2. adalah matriks hubungan antara status penerapan, kategori pengamanan dan skoring.

Tabel 1. Matrik status penerapan dan kategori pengamanan

STATUS PENERAPAN	KATEGORI PENGAMANAN		
	1	**2**	**3**
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan sebagian	2	4	6
Diterapkan secara menyeluruh	3	6	9

Sumber: Kominfo (2012)

3. Hasil dan Pembahasan

3.1 Pembahasan hasil pengolahan data

a. Peran TIK pada Instansi

Hasil dari pengisian kuesioner pada peran dan kepentingan TIK, maka diambil rata-rata dari responden 1 sampai dengan responden 20 yang menjawab pertanyaan pada bagian I Peran TIK dan didapatkan skor sebesar 20. Skor maksimal untuk bagian I Peran TIK sesuai ketentuan pada Indeks KAMI sebesar 48. Skor 20 tersebut diperoleh dari hasil penjumlahan skor pada tiap pertanyaan yang ada pada bagian I Peran TIK. Jika menjawab [minim] diberi skor 0, [Rendah] diberi skor 1, [Sedang] diberi skor 2, [Tinggi] diberi skor 3 dan [kritis] diberi skor 4.

Untuk rincian dari tiap-tiap skor dan jawaban yang di beri respon berikut disajikan pada Tabel 3.

Tabel 3. Peran dan kepentingan TIK

Bagian I : Peran dan Tingkat Kepentingan TIK				
Deskripsi	Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi			
Jawaban Tingkat Kepentingan: Minim(0), Rendah(1), Sedang(2), Tinggi(3), Kritis(4)				
Jumlah Pertanyaan : 12				
Hasil Jawaban Responden pada tingkat Kepentingan:				
Minim	Rendah	Sedang	Tinggi	Kritis
3	1	5	3	-
Skor Peran dan Tingkat Kepentingan TIK				**20**

Sumber: Hasil Penelitian (2012)

Berdasarkan hasil rekap peran TIK, sesuai dengan Pemetaan Tingkatan kesiapan indeks KAMI, bahwa peran atau tingkat kepentingan TIK yang ada di Perguruan Tinggi Bina Insani dengan skor 20 berada pada tingkat ketergantungan Sedang.

b. Penilaian Kelengkapan Pengamanan informasi

Untuk penilaian kelengkapan pengamanan informasi perhitungan skor berbeda dengan penilaian pada Peran TIK. Berikut disajikan mulai dari aspek tata kelola sampai dengan aspek teknologi dan keamanan informasi.

1) Bagian Tata Kelola Keamanan Informasi

Pada Tabel 4 dijelaskan tentang tata kelola informasinya.

Tabel 4. Tata Kelola Keamanan Informasi

Bagian II : Tata Kelola Keamanan Informasi			
Deskripsi	Untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi dan tanggung jawab pengelola keamanan informasi.		
Jawaban [Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan : 20			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Kontrol**		
	1	**2**	**3**
Tidak Dilakukan	1		
Dalam Perencanaan	7	2	2
Dalam Penerapan atau Diterapkan Sebagian		4	4
Diterapkan Secara Menyeluruh			
Total NilaiTata Kelola Informasi			**27**

Sumber: Hasil Penelitian (2012)

2) Pengelolaan Resiko Keamanan Informasi

Tabel 5. Pengelolaan Resiko Keamanan Informasi

Bagian III : Pengelolaan Resiko Keamanan Informasi			
Deskripsi	Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.		
Jawaban [Penilaian]: Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan : 15			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Kontrol**		
	1	**2**	**3**
Tidak Dilakukan			
Dalam Perencanaan	5	4	1
Dalam Penerapan atau Diterapkan Sebagian	4		1
Diterapkan Secara Menyeluruh			
Total Nilai **Pengelolaan Resiko**			**21**

Sumber: Hasil Penelitian (2012)

3) Kerangka Kerja Pengelolaan Keamanan Informasi

Tabel 6. Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV : Kerangka Kerja Pengelolaan Keamanan Informasi			
Deskripsi	Kerangka Kerja Pengelolaan Keamanan Informasi Bagian ini mengevaluasi kelengkapan dan kesiapan kebijakan & prosedur pengelolaan keamanan informasi dan strategi penerapannya.		
Jawaban [Penilaian]: Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan :26			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Kontrol**		
	1	**2**	**3**
Tidak Dilakukan	1		
Dalam Perencanaan	7	7	1
Dalam Penerapan atau Diterapkan Sebagian	3	1	6
Diterapkan Secara Menyeluruh			
Total Nilai **Kerangka Kerja**			**31**

Sumber: Hasil Penelitian (2012)

4) Pengelolaan Aset Informasi

Tabel 7. Pengelolaan Aset Informasi

Bagian V : Pengelolaan Aset Informasi			
Deskripsi	Bagian ini mengevaluasi kelengkapan pengamanan aset informasi		
Jawaban [Penilaian]: Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan : 34			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Kontrol**		
	1	**2**	**3**
Tidak Dilakukan	2		
Dalam Perencanaan	24	9	4
Dalam Penerapan atau Diterapkan Sebagian	4		
Diterapkan Secara Menyeluruh	1		
Total Nilai **Pengelolaan Aset Informasi**			**43**

Sumber: Hasil Penelitian (2012)

5) Teknologi dan Keamanan informasi

Tabel 8. Teknologi dan Keamanan Informasi

Bagian VI :Teknologi dan Keamanan Informasi			
Deskripsi	Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.		
Jawaban [Penilaian]: Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan : 24			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Kontrol**		
	1	**2**	**3**
Tidak Dilakukan	3		
Dalam Perencanaan	5	6	
Dalam Penerapan atau Diterapkan Sebagian	5	3	
Diterapkan Secara Menyeluruh		1	1
Total Nilai **Pengelolaan Aset Informasi**			**45**

Sumber: Hasil Penelitian (2012)

Maka secara keseluruhan total skor dapat ditunjukkan pada tabel mengenai tingkat kesiapan penerapan SMKI area pengamanan informasi sesuai standar ISO27001 dengan nilai 167 dari 588 skor maksimal sesuai kentuan Indeks KAMI.

Tabel 9. Hasil pengolahan kategori 1, 2 dan 3

Kategori Pengamanan	**Tata Kelola**	**Pengelolaan Risiko**	**Kerangka Kerja**	**Pengelolaan Aset**	**Aspek Teknologi**	**Total Skor**
1	8	9	11	21	13	186
2	6	4	8	9	10	222
3	6	2	7	4	1	180
Total Pertanyaan	20	15	26	34	24	588
Responden	27	21	31	43	45	**167**

Sumber: Hasil Penelitian (2012)

c. Tingkat Kematangan Pengamanan Informasi

Untuk hasil penilaian pada tingkat kematangan pada masing-masing area pengamanan pada penelitian ini, akan disajikan dalam bentuk tabel rekap skor tingkat kematangan.

Tabel 10. Hasil Pengolahan Skor Tingkat Kematangan

Skor Tingkatan kematangan	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Aspek Teknologi
Skor Tingkat Kematangan II	17	13	14	35	19
Skor Minimum Tingkat Kematangan II	12	13	12	25	17
Skor Maximum Tingkat Kematangan II	28	18	24	62	26
Status	I+	I+	I+	I+	I+
Skor Tingkat Kematangan III	10	4	17	8	26
Validitas Tingkat Kematangan III	No	No	No	No	No
Skor Minimum Tingkat Kematangan III	8	4	38	33	36
Skor Pencapaian Tingkat Kematangan III	14	8	53	44	56
Status	No	No	No	No	No
Skor Tingkat Kematangan IV	0	4	0	-	0
Validitas Tingkat Kematangan IV	No	No	No	-	No
Skor Minimum Tingkat Kematangan IV	24	8	15	-	6
Skor Pencapaian Tingkat Kematangan IV	54	12	27	-	9
Status	No	No	No	-	No

Sumber: Hasil Penelitian (2012)

Tabel 11. Hasil pengolahan status tingkat kematangan

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Aspek Teknologi
Tingkat II					
Status	I+	I+	I+	I+	I+
Tingkat III					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Tingkat IV					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Tingkat V					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Status Akhir	**I+**	**I+**	**I+**	**I+**	**I+**

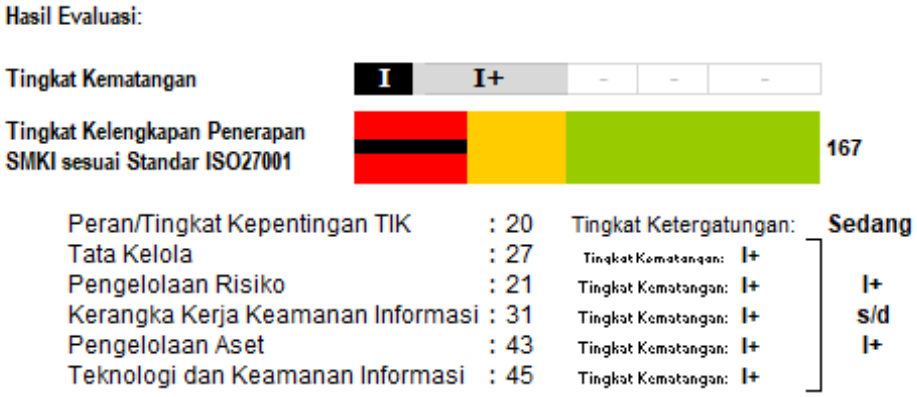
Sumber: Hasil Penelitian (2012)

3.2 Hasil Evaluasi

Pada bagian ini menggambarkan hasil evaluasi atas pembahasan pada bagian sebelumnya dengan data-data yang sudah diolah dan akan disajikan kedalam2 bentuk *BarChart* dan *Diagram Radar*, disajikan sebagai berikut:

a. Tingkat Kelengkapan dan Kematangan penerapan SMKI

Berdasarkan hasil evaluasi pengolahan data penelitian pada Indeks KAMI, tingkat kelengkapan penerapan SMKI ditunjukkan pada gambar 3.

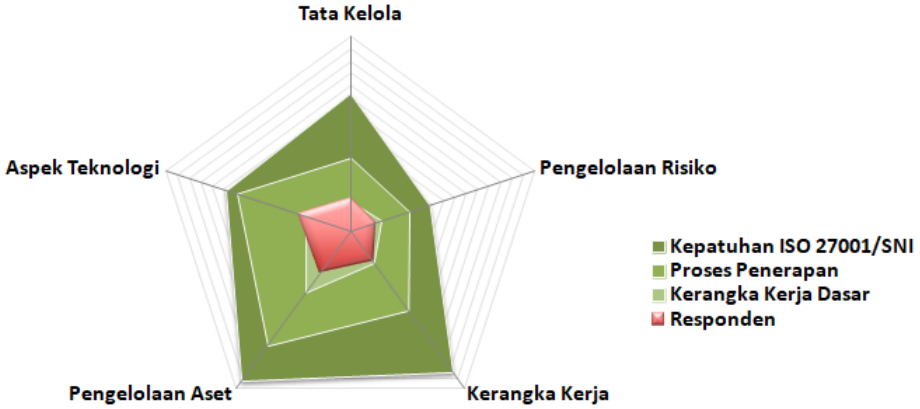


Sumber: Hasil Penelitian (2012)

Gambar 3 . Tingkat kelengkapan dan Kematangan SMKI

Berdasarkan hasil tingkat kelengkapan dan kematangan dapat dinyatakan bahwa peran atau Tingkat Kepentingan TIK di Perguruan Tinggi Bina Insani ditunjukkan pada tingkat ketergantungan Sedang dengan Skor 20. Tingkat kelengkapan penerapan SMKI berada pada area “Merah” skor 174 dan area “Kuning” skor 312. Sedangkan total skor secara keseluruhan atas tingkat kelengkapan penerapan adalah 167, berdasarkan acuan yang telah dipaparkan pada bab landasan teori bagian tabel 2.2 bahwa “Tidak Layak”.

b. Diagram Radar



Sumber: Hasil Penelitian (2012)

Gambar 4 . Diagram Radar

Berdasarkan diagram radar mengenai tingkat kelengkapan SMKI yang mencakup 5 area keamanan informasi, bahwa Diagram yang menunjukkan warna merah adalah gambaran kondisi SMKI Perguruan Tinggi Bina Insani berdasarkan hasil dari pengisian kuesioner oleh responden. Perguruan Tinggi Bina Insani telah memiliki Aspek Teknologi dan Pengelolaan Aset yang jauh lebih baik dibandingkan dengan area keamanan informasi lainnya. Sedangkan Area Pengelolaan Resiko, Perguruan Tinggi Bina Insani memiliki kondisi yang lebih rendah atau kurang baik dari area keamanan informasi lainnya, tetapi sudah memenuhi bagaimana pengelolaan resiko secara mendasar.

4. Kesimpulan

Berdasarkan hasil penelitian pada Perguruan Tinggi Bina Insani khususnya pada 4 unit kerja yang dilakukan menggunakan Indeks KAMI, maka didapat Penerapan SMKI pada

Perguruan Tinggi Bina Insani menggunakan Indeks KAMI yang mencakup Peran TIK, Tata Kelola, Pengelolaan Resiko, Kerangka Kerja, aset informasi dan teknologi keamanan informasi masih rendah dan belum *valid* yang artinya kesiapan penerapan keamanan informasi dibawah batas minimum yang dipersyaratkan oleh standar ISO/IEC 27001. Tingkat kelengkapan dan kematangan masih sangat rendah. Hasil yang diperoleh pada Perguruan Tinggi Bina Insani untuk kelengkapan dengan skor 167 dari 588 artinya tidak layak, sedangkan untuk tingkat kematangan berada pada level I+ hampir memenuhi syarat tingkat kematangan "II", akan tetapi untuk mendapatkan sertifikasi ISO/IEC 27001:2009 level keamanan informasi adalah minimal III. Beberapa hal penyebab rendahnya tingkat kelengkapan dan kematangan adalah kurangnya kesadaran tentang pentingnya Sistem Manajemen Keamanan Informasi. Ini terbukti pada saat observasi dilapangan bahwa masih belum tersedianya kebijakan/aturan, baik yang bersifat umummaupun teknis, yang mendukung penerapan SMKI di setiap area pengamanan, mulai dari bagian II Tata Kelola Keamanan Informasi hingga bagian VI Teknologi dan Keamanan Informasi. Dalam mendukung proses bisnis Perguruan Tinggi Bina Insani saat ditemukan dilapangan beberapa pekerjaan masih berbasis paper-based, sehingga pendokumentasikan data dan informasi sulit untuk diterapkan secara optimal dan menyeluruh. Pengembangan aplikasi dalam menunjang proses bisnis dan infrastruktur pendukungnya masih belum dilakukan pada perencanaan jangka menengah/panjang, sehingga mengakibatkan IT belum menjadi salah satu fasilitas pendukung dalam pelaksanaan tugas-tugas di lingkungan Perguruan Tinggi Bina Insani.

Daftar Pustaka

Afrianto I. 2015. Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI – SNI ISO/IEC 27001:2009 Pada Perguruan Tinggi X. Vol 6 (1).

Direktorat Keamanan Informasi. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik. Jakarta: Kementrian Komunikasi dan Informatika.

Georg D. 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security. Vol 4: 92-100.

Roodhin F. 2013. Penggunaan Indeks Keamanan Informasi Pada PT. PLN Distribusi Jatim. Vol.1(1). Surabaya: Institut Teknologi Sepuluh Nopember.

Umar H. 1998. Metode Penelitian untuk Skripsi dan Tesis Bisnis. Jakarta: Raja Grafindo Persada.

Indrajit RE. 2014. Konsep dan Strategi Keamanan Informasi di Dunia Cyber. 1st ed. Yogyakarta: Graha Ilmu.

Kadir A. 2014. Pengenalan Sistem Informasi edisi Revisi. Yogyakarta: Andi Offset.

Kominfo. 2012. Indeks KAMI (Keamanan Informasi) versi 2.3. Jakarta.

KristantoA. 2003. Komputer dan Teknologi Informasi. Yogyakarta: Graha Ilmu.

Lastyono P. 2014. Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI). Vol.3 (2). Surabaya: Institut Teknologi Sepuluh Nopember.

Mustaqim S. 2014. Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi pada Kantor Wilayah DITJEN Perbendaharaan Negara Jawa Timur. Seminar Nasional Sistem Informasi Indonesia, 22 September 2014.

Soenardi I, Ichsan M. 2013. Analisis Kematangan Sistem Manajemen Keamanan Informasi Badan Pendidikan dan Pelatihan Keuangan diukur menggunakan Indeks Keamanan Informasi. Jakarta: Kementerian Keuangan RI.

Sugiyono, 2011. Metode Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif, dan R&D). Alfabeta: Bandung.

Wardani DR., Pujiono RA. 2015. Evaluasi Keamanan Informasi Pada Pti Pdam TirtaMoedal Kota Semarang Berdasarkan IndeksKeamanan Informasi Sni Iso/Iec 27001:2009. Techno.COM, Vol. 14, No. 3, Agustus 2015: 165-172.

Sujarweni W. 2010. SPSS Untuk Penelitian. Pustaka Baru Press: Yogyakarta.

Zakiyudin A. 2012. Sistem Informasi Manajemen. Jakarta: Mitra Wacana Media.