ISSN 2085-4579

Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009

Studi Kasus Perguruan Tinggi X

Irawan Afrianto[1], Taryana Suryana[2], Sufa'atin[3]
[1,2,3] Program Studi Teknik Informatika – Fakultas Teknik dan Ilmu Komputer - Unikom
irawan_afrianto@yahoo.com[1], taryanarx@yahoo.com[2], zufa08@yahoo.co.id[3]

Diterima 13 Mei 2015
Disetujui 06 Juni 2015

***Abstract*— Information is a valuable asset for the college. The need for safeguards against information becomes very necessary thing for a college. One standard that can be used to measure the maturity level of information security in an organization is the KAMI index developed by Depkominfo standards refer to ISO standard ISO / IEC 27001: 2009.**

This assessment is used to see how far the maturity level of information security in the college environment, which results can be used as a medium for evaluation in order to improve the information security of the college in the future.

***Index Terms*—Assessment, Information security, KAMI Index, Maturity Level, College X**

I. PENDAHULUAN

Informasi merupakan aset yang sangat berharga bagi perguruan tinggi. Pengelolaan informasi yang baik, akan menjadikan perguruan tinggi memiliki kemampuan manajerial yang baik serta meningkatkan daya saing perguruan tinggi tersebut. Mengingat pentingnya arti informasi tersebut, perguruan tinggi perlu untuk melakukan kegiatan tata kelola keamanan informasi dilingkungannya. Salah satu standar yang dapat digunakan untuk mengukur tingkat kematangan keamanan informasi di suatu organisasi adalah menggunakan Indeks KAMI (Keamanan Informasi) yang dikembangkan oleh Depkominfo yang merujuk pada standar SNI-ISO/IEC 27001: 2009.

Indeks KAMI menerapkan mekanisme pengukuran keamanan informasi suatu organasisasi mulai dari peran, tatakelola, resiko keamanan, kerangka kerja, pengelolaan aset dan teknologi. Pengukuran tingkat keamanan informasi diperlukan guna melihat secara menyeluruh hal-hal yang telah dilakukan oleh perguruan tinggi dalam melakukan tindakan pengamanan informasi dilingkungannya.

Hasil pengukuran ini akan menghasilkan tingkat kematangan keamanan informasi di perguruan tinggi tersebut, yang nantinya akan dievaluasi dan digunakan sebagai referensi guna peningkatan tingkat keamanan informasi perguruan tinggi X (PT.X) dimasa mendatang.

II. TINJAUAN PUSTAKA

A. Pengertian Informasi

Informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya. Sumber dari informasi adalah data. Data merupakan bentuk jamak dari bentuk tunggal data-item. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata. Kejadian (event) adalah sesuatu yang terjadi pada saat tertentu. Kejadian-kejadian nyata yang sering terjadi perubahan dari suatu nilai yang disebut dengan transaksi. Misalnya penjualan adalah transaksi perubahan nilai barang menjadi nilai uang. Kesatuan nyata adalah suatu objek nyata seperti tempat, benda, dan orang yang betul-betul ada dan terjadi.[1]

B. Keamanan Informasi

Keamanan Informasi menggambarkan

usaha untuk melindungi komputer dan non-peralatan komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab Definisi ini meliputi pengutip, fax mesin, dan semua jenis media, termasuk dokumen kertas [2].

Keamanan informasi dimaksudkan untuk mencapai kerahasiaan, ketersediaan, dan integritas di dalam sumber daya informasi perusahaan.

Manajemen keamanan informasi terdiri dari:

1) Perlindungan Sehari-hari disebut Manajemen Keamanan Informasi (*information security management*/ ISM)

2) Persiapan untuk menghadapi operasi setelah bencana disebut Manajemen Kesinambungan Bisnis (*business continuity management* / BCM)

C. Indeks KAMI (Keamanan Informasi)

Indeks KAMI ini secara umum ditujukan untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang ada didalam lingkungan organisasi/institusi. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya [3].

Evaluasi menggunakan Indeks KAMI mencakup hal-hal sebagai berikut :

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

Indeks KAMI menggunakan metode kuisioner / form pengukuran yang terdiri dari beberapa pertanyaan pada masing-masing bagian indeks KAMI untuk mendapatkan gambaran mengenai tingkat kemanan informasi pada institusi. Penggunaan indeks KAMI dimulai dengan mengukur peran TIK di institusi sebelum mengukur kesiapan keamanan infomasi di lingkungan instansi yang dimulai dari Tata kelola hingga Teknologi. Adapun pertanyaan pada bagian kesiapan keamanan informasi dikelompokkan menjadi 2 bagian kepentingan yaitu, Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan **kelengkapan** kontrol yang diminta oleh standar ISO/IEC 27001:2009. Dalam pengelompokan ini responden diminta untuk memberi tanggapan mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (pertanyaan diberi label "1"), efektifitas dan konsistensi penerapannya (label "2"), sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (label "3") seperti terlihat pada Gambar 1. Tingkat terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar ISO/IEC 27001:2009 [4] .

	Kategori Pengamanan		
Status 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

Gambar 1. Ukuran Kerangka Kerja Kemanan Informasi

Adapun korelasi antara peran atau tingkat kepentingan TIK dalam instansi didefinisikan pada Gambar 2.

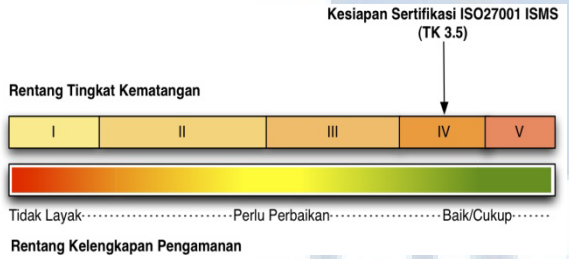
Peran TIK			
Rendah		**Indeks (Skor Akhir)**	**Status Kesiapan**
0	12	0	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	588	Baik/Cukup
Sedang		**Skor Akhir**	**Status Kesiapan**
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi		**Skor Akhir**	**Status Kesiapan**
25	36	0	272	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

Gambar 2. Korelasi Peran TIK pada Indeks KAMI

Pengelompokan kedua dilakukan berdasarkan tingkat **kematangan** penerapan pengamanan dengan kategorisasi yang mengacu kepada

tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan di institusi seperti pada Gambar 3. Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai:

- Tingkat I - Kondisi Awal
- Tingkat II - Penerapan Kerangka Kerja Dasar
- Tingkat III - Terdefinisi dan Konsisten
- Tingkat IV - Terkelola dan Terukur
- Tingkat V – Optimal



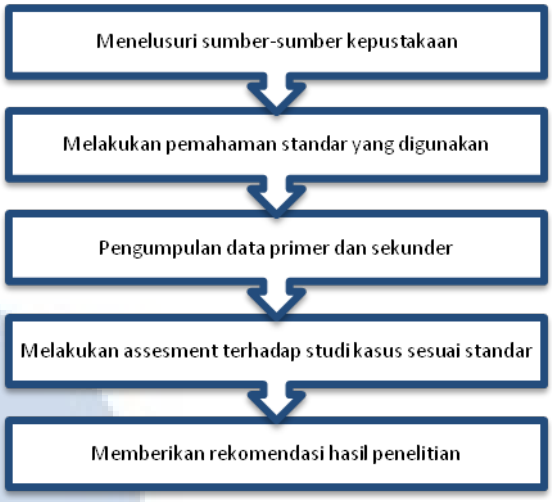
Gambar 3.Tingkat Kematangan pada Indeks KAMI

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 2700:2009, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.[5]

III. TUJUAN DAN METODE PENELITIAN

Tujuan pada penelitian ini adalah melakukan pengukuran dan evaluasi keamanan informasi menggunakan Indeks KAMI pada tata kelola keamanan informasi di PT.X.

Sementara metode penelitiannya dapat dilihat pada Gambar 4.



Gambar 4. Metode Penelitian

IV. HASIL DAN PEMBAHASAN

Pada bagian hasil dan pembahasan akan dijelaskan hal-hal terkait data penelitian, kegiatan assessment keamanan informasi menggunakan Indeks KAMI dan hasil yang diperoleh

A. Mekanisme Pengumpulan Data .

Pengumpulan data untuk melakukan pengukuran Indeks KAMI adalah dengan melakukan wanwacara dan penelusuran dokumen-dokumen yang terkait dengan kegiatan-kegiatan manajemen keamanan informasi di PT.X.

Kegiatan wawancara dilakukan dengan Direktur ICT dan Multimedia PT.X yang memiliki fungsi dan wewenang dalam pengambangan aplikasi dan sistem informasi di PT.X, monitoring dan mengevaluasi kegiatan-kegiatan TIK dilingkungan PT.X.

Adapun kegiatan pengumpulan data dilakukan dengan wawancara, memberikan panduan pengisian Indeks KAMI, serta menelusuri dokumen-dokumen terkait kebijakan TIK, penggunaan dan evaluasi TIK yang terdapat di PT.X baik berupa SK maupun buku-buku

panduan TIK PT.X.

B. Data Pengukuran Indeks KAMI Pada PT.X

Langkah pertama penggunaan indeks KAMI adalah dengan menjawab pertanyaan terkait kesiapan pengamanan informasi, responden diminta untuk mendefinisikan Peran TIK (atau Tingkat Kepentingan TIK) di Instansinya. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis – Tabel 1. Setelah itu dilakukan pengukuran kesiapan keamanan informasi mulai dari tata kelola informasi – Tabel 2., pengelolaan resiko keamanan informasi – Tabel 3., pengukuran kerangka kerja keamanan informasi – Tabel 4., pengukuran pengelolan aset informasi – Tabel 5., dan pengukuran teknologi dan keamanan informasi – Tabel.6.

Tabel 1. Data Pengukuran Peran dan Tingkat Kepentingan TIK dalam Instansi

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi				
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.				
Tingkat Kepentingan] Minim [0]; Rendah[1]; Sedang[2]; Tinggi[3]; Kritis [4]				
Jumlah Pertanyaan				12
Jawaban Bagian I				
Minim	Rendah	Sedang	Tinggi	Kritis
-	4	3	5	-
Skor Peran dan Tingkat Kepentingan TIK di Instansi				**25**

Tabel 2. Data Pengukuran Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi			
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan			20
Jawaban Bagian II			
Status pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan	-	-	-
Dalam Perencanaan	-	1	2
Dalam Penerapan atau Diterapkan Sebagian	6	4	4
Diterapkan Secara Menyeluruh	2	1	-
Total Nilai Evaluasi Tata Kelola			**72**

Tabel 3. Data Pengukuran Pengelolaan Resiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi			
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan			15
Jawaban Bagian III			
Status pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan			
Dalam Perencanaan			
Dalam Penerapan atau Diterapkan Sebagian	7	4	2
Diterapkan Secara Menyeluruh	2		
Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi			**48**

Tabel 4. Data Pengukuran Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan			26
Jawaban Bagian IV			
Status pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan			
Dalam Perencanaan			
Dalam Penerapan atau Diterapkan Sebagian	11	8	7
Diterapkan Secara Menyeluruh			
Total Nilai Evaluasi Kerangka Kerja			**96**

Tabel 5. Data Pengukuran Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi			
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan			34
Jawaban Bagian V			
Status pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan			
Dalam Perencanaan	2	4	1
Dalam Penerapan atau Diterapkan Sebagian	17	4	3
Diterapkan Secara Menyeluruh	2	1	
Total Nilai Evaluasi Pengelolaan Aset			**72**

Tabel 6. Data Pengukuran Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan			24
Jawaban Bagian VI			
Status pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan			
Dalam Perencanaan	1		
Dalam Penerapan atau Diterapkan Sebagian	5	6	1
Diterapkan Secara Menyeluruh	7	4	
Total Nilai Evaluasi Teknologi dan Keamanan Informasi			**86**

C. Hasil Pengukuran Indeks KAMI Pada PT.X

Dari data pengukuran yang telah dilakukan menggunakan indeks KAMI diperoleh hasil yang mencakup peran TIK di PT.X, serta tingkat kematangan masing-masing bagian keamanan informasi yang terdapat di PT.X.

Untuk Bagian I pada Tabel 7., yaitu Peran dan Kepentingan TIK di Instansi menunjukkan bahwa TIK memegang peran yang penting di PT.X, hal ini ditunjukkan oleh perhitungan indek KAMI, untuk bagian I PT.X memiliki Skor 25 yang berarti Peran TIK di PT.X **Tinggi**.

Tabel 7. Hasil Pengukuran Peran/Tingkat Kepentingan TIK

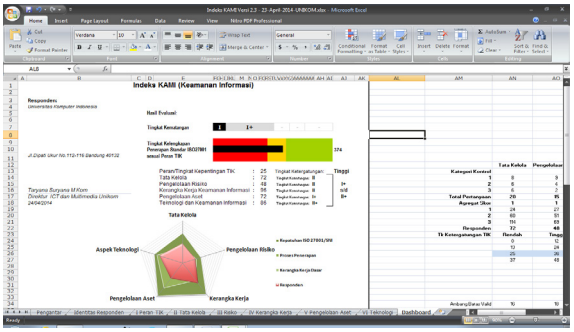
Bagian I **Peran dan Tingkat Kepentingan TIK di Instansi**		**Skor PT.X**
Skor	**Tingkat**	
0 – 12	[Rendah]	25
13 – 24	[Sedang]	**Tinggi**
25 – 36	[Tinggi]	
37 – 48	[Kritis]	

Sementara untuk Bagian II , III, IV dan V dan VI digunakan untuk mengukur tingkat kematangan keamanan informasi di PT.X. Hasil pengukuran dapat dilihat pada Tabel 8.

Tabel 8. Hasil Pengukuran Bagian-bagian Keamanan Informasi PT.X

Indeks KAMI	**Skor PT.X**	**Tingkat kematangan**
Bagian II: Tata Kelola Keamanan Informasi	72	II
Bagian III: Pengelolaan Risiko Keamanan Informasi	48	II
Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi	96	II
Bagian V: Pengelolaan Aset Informasi	72	I+
Bagian VI: Teknologi dan Keamanan Informasi	86	II+
Total Skor (II+III+IV+V+VI)	**374**	**I+ s/d II+**

Gambar 5. Menunjukkan hasil pengukuran Bagian II , III, IV dan VI menunjukkan bawa tingkat kematangan keamanan informasi di PT.X berada pada Level II dan II+ yaitu **Penerapan Kerangka Kerja Dasar,** sementara untuk bagian V, tingkat kematangan keamanan informasi di PT.X masih berupa **Kondisi Awal.**

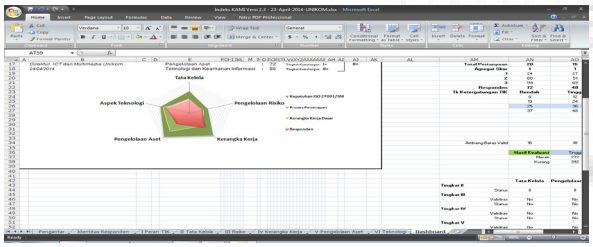


Gambar 5.Tingkat Kematangan Indeks KAMI PT.X

Sehingga hasil akhir dari pengukuran keamanan informasi menggunakan indeks KAMI untuk PT.X mendapatkan kesimpulan bahwa kemanan informasi yang terdapat pada PT.X masih **Perlu Perbaikan**, seperti pada Tabel 9., dan diagram radar pada Gambar 6.

Tabel 9. Kesimpulan Indeks KAMI PT.X

Skor Bagian I			Skor Bagian II+III+IV+V+VI		Kesimpulan
0	12	Rendah	0	124	Tidak Layak
			125	272	Perlu Perbaikan
			273	588	Baik/Cukup
13	24	Sedang	0	174	Tidak Layak
			175	312	Perlu Perbaikan
			313	588	Baik/Cukup
25	36	Tinggi	0	272	Tidak Layak
			273	392	**Perlu Perbaikan**
			393	588	Baik/Cukup
37	48	Kritis	0	333	Tidak Layak
			334	453	Perlu Perbaikan
			454	588	Baik/Cukup



Gambar 6. Diagram Radar Indeks KAMI PT.X

D. Rekomendasi Keamanan Informasi Untuk PT.X

Hasil pengukuran kemananan informasi menggunakan indeks KAMI untuk PT.X menunjukkan tingkat kematangan keamanan informasi I+ s/d II+ . Sementara untuk mendapatkan kesiapan sertifikasi ISO/IEC 27001:2009, tingkat kematangan kemanan informasi minimal berada pada level III (Terdefinisi dan Konsisten). Adapun hal-hal yang dapat direkomendasi untuk meningkatkan tingkat kematangan informasi di PT.X adalah sebagai berikut :

1. Bagian I Peran dan Tingkat kepentingan TIK [Tinggi] : Perlunya perencanaan pada anggaran untuk keamanan informasi, guna meningkatkatkan hal-hal terkait operasional dan monitoring kegiatan keamanan informasi.

2. Bagian II Tata Kelola Keamanan Informasi [II] → [III] : Perlunya perencanaan dan pendokumentasian yang jelas kepada fungsi dan tanggungjawab pengelola kemanan informasi serta tindakan-tindakan pengembangan berkelanjutan terkait tata kelola keamanan informasi.

3. Bagian III Pengelolaan Resiko Keamanan Informasi [II] → [III] : Perlunya pendokumentasiaan rencana-rencana terkait resiko keamanan informasi , kerangka kerja penanganan resiko keamanan informasi yang terdefinisi dan tindakan-tindakan yang berkelenjutan, dalam penanganan hal-hal terkait resiko keamanan informasi.

4. Bagian IV Kerangka Kerja Pengelolaan Keamanan Informasi [II] → [III] : Perlunya pendokumentasian yang jelas (terdefinisi) terhadap kerangka kerja (kebijakan dan prosedur) keamanan informasi serta melakukan uji coba dan monitoring kerangka kerja keamanan informasi secara berkelanjutan .

5. Bagian V Pengelolaan Aset Keamanan Informasi [I+] → [III] : Perlunya perencanaan pengolaan aset keamanan informasi yang lebih terdefinisi dan terkomentasi, prosedur dan kebijakan mengenai operasional aset keamanan dan perlu diperjelas fungsi dan peranannya dari aset keamanan informasi, serta melakukan evaluasi / monitoring berkala mengenai keberadaan dan fungsi aset keamanan informasi tersebut

6. Bagian VI Teknologi dan Keamanan Informasi [II+] → [III] : Perlu adanya

dokumentasi yang jelas (terdefinisi) terkait kelengkapan, evaluasi dan efektifitas penggunaan teknologi, monitoring yang dilakukan secara berkala guna mendapatkan infomasi secara menyeluruh terhadap keamanan informasi di instansi.

V. SIMPULAN

1) Dengan indeks KAMI, dapat diukur tingkat kematangan keamanan informasi di PT.X yang mencakup Peran TIK, Tata kelola, resiko, kerangka kerja, aset dan teknologi keamanan informasi

2) Hasil yang diperoleh adalah bahwa tingkat kematangan keamanan informasi PT.X berada pada level I+ s/d II+, dimana untuk mendapatkan sertifikasi ISO/IEC 27001:2009 level keamanan informasi adalah minimal III.

3) Hasil evaluasi dengan indeks KAMI menunjukkan bahwa sebagian besar kegiatan keamanan informasi di PT.X masih dilakukan sebagian, belum menyeluruh dan berkelanjutan.

UCAPAN TERIMA KASIH

Terima kasih kepada Direktorat CSR Unikom yang telah membiayai penelitian ini sebagai bagian dari Kegiatan Hibah Penelitian Intern Unikom tahun 2013/2014.

DAFTAR PUSTAKA

[1] HM, Jogiyanto. 1989. *Analisis & Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis.* Yogyakarta: Penerbit ANDI.

[2] Simarmata, Janner. 2006. *Pengamanan Sistem Komputer*. Yogyakarta: ANDI.

[3] http://blog.binadarma.ac.id/ilmanzuhriyadi/wp-content/uploads/2012/11/Urgensi-Penerapan-SNI-27001-untuk-Sekuriti-Infrastruktur-TIK-pada-Kemenag-RI-Sumsel.pdf, diakses pada 1 Februari 2014.

[4] http://publikasi.kominfo.go.id/bitstream/handle/54323613/119/Panduan Penerapan Tata Kelola KIPPP.pdf, diakses pada 1 Februari 2014.

[5] http://digilib.its.ac.id/public/ITS-paper-24460-5208100011-Paper.pdf, diakses 21 Februari 2014.