pISSN: 2086-3489
Explore IT - Volume 7, Nomor 1, Juni 2015 eISSN: 2549-354X

PENGUKURAN DAN EVALUASI KEAMANAN SIAKAD UNIVERSITAS YUDHARTA MENGGUNAKAN INDEKS KAMI

Muhammad Imron Rosadi[1], Lukman Hakim[2]
[1,2)]Fakultas Teknik, Program Studi Teknik Informatika, Universitas Yudharta Pasuruan
Email: Imron_uyp@yahoo.com[1], lukman@yudharta.ac.id[2]

ABSTRAK

Di Kabupaten pasuruan mempunyai beberapa perguruan tinggi salah satunya yaitu UYP. Di Universitas ini terdapat Badan Administrasi Akademik dan Kemahasiswaan (BAAK) yang bertugas untuk memberikan layanan dan administrasi kepada Mahasiswa dan Dosen.

Untuk memenuhi tugas tersebut maka bekerja sama dengan Pusat Pelayanan Informasi dan Komunikasi (PPIK) untuk Mengembangkan Teknologi Informasi Sistem Informasi Akademik. Perlu dilakukan evaluasi untuk mengukur kesiapan kematangan keamanan informasi berdasarkan Indeks KAMI. Indeks KAMI dibuat oleh MENKOMINFO dan banyak dipakai untuk mengukur kematangan keamanan informasi berdasarkan standart ISO/IEC 27001:2009. Pada evaluasi indeks KAMI ada tahap awal yang digunakan yaitu melakukan penilaian tingkat ketergantungan TIK pada instansi.

Penilaian indeks KAMI yang dilakukan di UYP digunakan untuk menilai tingkat kematangan keamanan informasi. Di penelitian ini didapatkan tingkat kematangan keamanan teknologi berada di level I sampai dengan II, total skor untuk peran TIK adalah 28 (Tinggi), dan hasil pengukuran Indeks KAMI mencapai 200, ini memiliki arti bahwa tingkat kematangan TIK tidak layak. Oleh karena itu hasil dari penelitian ini sebaiknya digunakan untuk bahan evaluasi dan perbaikan keamanan informasi di UYP.

Kata Kunci : KAMI, UYP, ISO/IEC 27001:2009.

1. Pendahuluan

Universitas Yudharta Pasuruan (UYP) merupakan lembaga pendidikan yang bernaung di bawah Kementerian Pendidikan dan Kebudayaan, dan Kementerian Agama berdasarkan SK Mendiknas melalui DIKTI dengan nomor surat : 146/D/O/2002 pada Tanggal 02 Agustus 2002.

Dalam rangka menjalankan roda organisasi, UYP mempunyai BAAK yang bertugas untuk memberikan layanan teknis dan administrasi, dalam prosesnya membutuhkan sistem informasi akademik secara online/jaringan internet. Untuk memenuhi tugas tersebut BAAK bekerja sama dengan PPIK (Pusat Informasi dan Komunikasi) untuk Mengembangkan Teknologi Informasi SIAKAD[1].

Di era milenia ini Teknologi Informasi menjadi faktor paling penting untuk mencapai tujuan suatu organisasi. Teknologi informasi diaplikasikan dalam suatu organisasi/institusi akan mempengaruhi seberapa jauh organisasi/institusi tersebut telah mencapai visi dan misi ataupun tujuan strategisnya. Oleh karena itu UYP menggunakan SIAKAD untuk pengolah data akademik mahasiswa, data dosen dan pegawai serta keuangan.

SIAKAD hanya dapat diakses melalui online yang menggunakan akses internet oleh aktor yaitu pegawai, mahasiswa, dan dosen[2].

DEPKOMINFO mengeluarkan Kajian Kemanan Teknologi dan Sistem Informasi menggunakan Indeks KAMI sesuai dengan standar ISO 27001:2009, Indeks KAMI menerapkan mekanisme pengukuran keamanan informasi suatu organasisasi yang meliputi peran, resiko keamanan, tatakelola, kerangka kerja, dan teknologi.

Pengukuran tingkat keamanan informasi menggunakan indeks KAMI diperlukan untuk mengetahui secara menyeluruh tentang hal yang telah dilakukan oleh PT (Perguruan Tinggi) dalam melakukan tindakan pengamanan informasi [3].

Ada beberapa penelitian yang menggunakan indeks KAMI untuk mengevaluasi kemananan system informasi. Riawan Arbi Kusuma (2014), Audit Keamanan system informasi pada system informasi Akademik UIN Sunan Kali Jaga. Irawan Afrianto, dkk (2015) menggunakan indeks kami untuk pengukuran dan evaluasi keamanan pada Perguruan Tinggi X. Tri Yani Akhirina (2016) Evaluasi Keamanan TIK UYP. Dari beberapa penelitian diatas penulis mencoba menerapkan untuk menggunakan indeks KAMI untuk mengukur dan mengevaluasi SIAKAD UYP.

Untuk menjaga data dan informasi perguruan tinggi dengan baik terhadap ancaman dari berbagai lubang keamanan. Diharapkan hasil dari pengukuran dan evaluasi menggunakan indeks KAMI dapat digunakan UYP sebagai media evaluasi dan perbaikan dalam hal keamanan sitem informasi dan jaringan.

Dari hasil penelitian ini akan diberikan suatu saran perbaikan pada bagian-bagian yang masih kurang, sehingga diharapkan terjadi peningkatan dalam hal kamanan informasi tercapai.

2. Kajian Pustaka

2.1. Pengertian Informasi

Informasi merupakan data yang dikelola menjadi lebih berarti dan berguna dan untuk khalayak umum.

Perubahan yang sering terjadi dari suatu nilai terhadap kejadian nyata yang disebut dengan transaksi sesuai dengan kondisi. Misalnya data Aktifitas Kuliah mahasiswa merupakan data yang berhubungan dengan mahasiswa meliputi KRS, KHS dan keuangan.[4]

2.2. Keamanan Informasi

Keamanan Informasi merupakan perlindungan informasi dari berbagai macam ancaman dari beberapa serangan seperti hacker dan virus agar menjamin kelanjutan usaha/bisnis, mengurangi resiko bisnis dan meningkatkan return of investment serta peluang bisnis (Simanungkalit, 2009 p.6).

Keamanan informasi meliputi perlindungan tiga aspek dari informasi, yaitu Integritas (Integrity), Kerahasiaan (Confidentiality), dan Ketersediaan (Availability) atau CIA Triad[5]. Keamanan Informasi juga bertujuan untuk memberikan perlindungan terhadap komputer dan non peralatan komputer seperti pengutip, faksimile, dan semua media, seperti dokumen kertas serta data, informasi, dan fasilitas dari orang yang tidak bertanggung jawab [6].

2.3. Indeks KAMI (Keamanan Informasi)

Secara umum Indeks KAMI ini digunakan untuk mendapatkan informasi kematangan keamanan informasi program kerja di lingkungan suatu organisasi/institusi.

Evaluasi indeks KAMI ini dilakukan oleh pejabat/staff yang bertanggung jawab dan berwenang untuk mengelola keamanan informasi di lingkungan organisasi/instansi/institusinya [7].

Hal-hal yang dievaluasi menggunakan Indeks KAMI antara lain : Peran TIK di dalam organisasi/Instansi, Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi serta Keamanan dalam informasi. Metode kuisioner/form pengukuran digunakan Indeks KAMI yang mencangkup beberapa pertanyaan pada bagian masing-masing untuk mendapatkan informasi mengenai tingkat keamanan TIK pada organisasi/instansi yang terkait.

Bagian awal dari indeks KAMI dimulai dengan mengukur peran TIK di organisasi/institusi sebelum mengukur kesiapan keamanan infomasi di lingkungan organisasi/instansi yang dimulai dari Tata kelola hingga Teknologi. Setelah dilakukan kuisioner peran TIK dilanjutkan pada bagian kesiapan keamanan informasi berdasarkan standar ISO/IEC 27001:2009.

Dalam pengelompokan ini responden diminta untuk memberikan suatu tanggapan mulai dari area yang berkaitan terhadap bentuk kerangka kerja dasar keamanan TIK (pertanyaan diberi label “1”), efektifitas dan konsistensi penerapan keamanan TIK (label “2”), kekemampuan untuk sering meningkatkan kinerja keamanan TIK(label “3”). Untuk Peran TIK di organisasi/instansi memiliki penilaian yang berbeda dari beberapa bagian lainnya dikarenakan Peranan TIK di organisasi/instansi ini diharapkan mendapatkan nilai dari ketergantungan organisasi/instansi itu sendiri terhadap perananan TIK. Skor penilaian untuk Peran TIK di instansi adalah sebagai berikut :

	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. Pemetaan Skor

Akan tetapi untuk bagian-bagian lainnya seperti Tata kelola keamanan informasi, Pengelolaan resiko keamanan informasi, Kerangka kerja keamanan informasi, Pengelolaan aset informasi, serta Teknologi dan keamanan informasi, memiliki penilain yang berbeda dari tiap pertanyaan yang diajukannya.

Jika sudah mendapatkan hasil dari penilaian atas penerapan dari tiap-tiap bagian yang ada, maka pimpinan instansi dalam penerapan keamanan informasi dapat melihat kebutuhan pembenahan yang diperlukan serta korelasi antara berbagai area. Adapun dalam suatu instansi/organisasi hubungan antara tingkat kepentingan TIK terdefinisikan melalui tabel berikut:

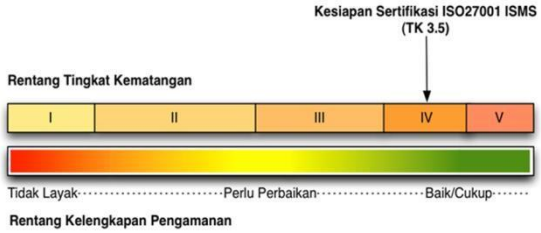
Peran TIK			
Rendah		**Indeks (Skor Akhir)**	**Status Kesiapan**
0	12	0	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	588	Baik/Cukup
Sedang		**Skor Akhir**	**Status Kesiapan**
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi		**Skor Akhir**	**Status Kesiapan**
25	36	0	272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

kerja COBIT atau CMMI. Adapun tingkat kematangan tersebut didefinisikan sebagai berikut:

- Tingkat I - KondisiAwal
- Tingkat II - Penerapan Kerangka Kerja Dasar
- Tingkat III - TerdefiisidanKonsisten
- Tingkat IV - TerkeloladanTerukur
- Tingkat V - Optimal



Gambar 3. Tingkat Kematangan pada Indeks KAMI

Untuk membantu memberikan penjelasan yang lebih mendetail, diantara tingkatan tersebut ditambah tingkatan lagi, antara - I+, II+, III+, dan IV+, sehingga terdiri dari 9 tingkat kematangan. Sebagai awal, responden akan diberikan kategori kematangan Tingkat I. Sebagai padanan terhadap standar ISO/IEC 2700:2009, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifiasi adalah Tingkat III+[7].

Tahapan terakhir dari proses pengerjaan penelitian ini adalah berisi hasil evaluasi dan rekomendasi perbaikan untuk keamanan informasi pada UYP. Pada tahapan ini semua hasil yang telah didapatkan dari tahapan-tahapan sebelumnya didokumentasikan dari tahap awal proses hingga tahap akhir.

3. Metode Penelitian

Metode penelitian yang digunakan penelitian ini bersifat deskriptif kualitatif dimana hasil penelitian dituangkan dalam bentuk deskripsi. Selain itu penelitian ini juga bersifat ekspolatif, sehingga dimana data diperoleh dengan menggali informasi mendalam mengenai kematangan keamanan SIAKAD UYP.

Tahapan-tahapan yang dilakukan dalam menentukan keamanan TIK UYP sebagai berikut:

a) Penelitian Pendahuluan : pada tahapan ini, peneliti melakukan studi awal dengan melihat langsung kondisi yang ada di UYP dalam penerapan tata kelola keamanan TIK.
b) Pengumpulan Data: pada tahapan ini, pengumpulan data didapatkan dari hasil wawancara langsung kepada satu orang responden yaitu Manager IT yang berwenang dalam pengelolaan keamanan teknologi informasi. Wawancara tersebut berdasarkan kuisioner tertutup indeks KAMI dengan skala linkert. Dimana hasil jawaban disesuaikan dengan kondisi dilapangan dengan pilihan jawaban diantaranya tidak dilakukan, dalam perencanaan, diterapkan sebagian/dalam penerapan, ataupun diterapkan secara keseluruhan.
c) Pengolahan data, dimana data tentang Teknologi Informasi yang telah didapatkan dari kuisioner berdasarkan indeks KAMI diolah menggunakan software indeks KAMI untuk melihat tingkat kematangan keamanan teknologi informasi sesuai standarisasi ISO 27001:2009.
d) Analisa dan Kesimpulan: tahapan ini adalah menganalisis hasil dari tahapan sebelumnya sampai dengan diperolehnya kesimpulan apa saja yang sudah diterapkan dan apa saja yang perlu diperbaiki dalam tata kelola kaamanan teknologi informasi pada UYP dimasa yang akan dating.

4. Hasil dan Pembahasan

4.1 Proses Pengukuran dan Evaluasi

Pada tahap ini yang dilakukan adalah dengan survei langsung ke lapangan, untuk melihat kondisi awal di UYP. Data yang diambil adalah untuk mengetahui profil perusahaan, visi dan misi, struktur organisasi, tugas dan wewenang departemen IT, aset-aset yang dikelola oleh bidang IT dan proses bisnis bidang IT. Data awal ini digunakan sebagai langkah awal dalam menentukan tujuan penelitian.

Pengumpulan data yang dilakukan dalam mengevaluasi tingkat kematangan keamanan teknologi informasi adalah dengan wawancara serta penelusuran langsung dengan dokumen-dokumen terkait dalam proses manajemen keamanan TIK UYP. Wawancara dilakukan kepada Kepala PPIK dan admin bidang IT, selaku pihak yang memiliki kewenangan dalam pengembangan aplikasi, sistem informasi dan menentukan suatu kebijakan dalam bidang IT pada UYP.

Selain itu juga memiliki tanggung jawab dalam memonitoring dan mengevaluasi keamanan teknologi informasi di lingkungan UYP Adapun kegiatan wawancara ini dengan menjelaskan pandunan penggunaan indek KAMI dan melakukan penelusuran dokumen-dokumen terkait dengan materi wawancara, selain itu juga dilakukan pengamatan secara langsung untuk menentukan pengukuran berdasarkan indeks kami.

4.2. Analisis dan Evaluasi indeks KAMI

Langkah awal digunakan untuk menjawab dari pertanyaan terkait kesiapan pengamanan informasi untuk mendefinisikan Peran TIK di Instansi responden yang bersangkutan. Tujuan dari proses pada tahap pertama ini adalah untuk mengelompokkan instansi ke “ukuran” tertentu: Rendah, Sedang, Tinggi dan Kritis - Tabel 1.

Setelah itu dilakukan pengukuran terhadap kesiapan keamanan TIK mulai dari tata kelola TIK - Tabel 2., pengelolaan pada resiko keamanan TIK - Tabel 3., pengukuran terhadap kerangka kerja keamanan TIK - Tabel 4., pengukuran terhadap pengelolan aset TIK - Tabel 5., serta pengukuran keamanan TIK - Tabel.6.

Tabel 1. Data Pengukuran Tingkat dan Peran 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; Rendah; Sedang; Tinggi; Kritis				
Jumlah Pertanyaan				12
Jawaban Bagian I				
Minim	Rendah	Sedang	Tinggi	Kritis
1		5	6	
Skor Peran dan Tingkat Kepentingan TIK di Instansi				**28**

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	2	4	6
Dalam penerapan atau diterapkan sebagian	6	2	
Diterapkan secara menyeluruh			
Total Nilai Evaluasi Tata Kelola Keamanan Informasi			**30**

Tabel 3. Data pengukuran Pengolaan Risiko 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	7	4	2
Dalam penerapan atau diterapkan sebagian	2		
Diterapkan secara menyeluruh			
Total Nilai Evaluasi Pengolaan Risiko Keamanan Informasi			**19**

Tabel 4. Data pengukuran Kerangka Kerja Pengolaan 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		7	8	6
Dalam penerapan atau diterapkan sebagian		4		1
Diterapkan secara menyeluruh				
Total Nilai Evaluasi Kerangka Kerja				**31**

Tabel 5. Data pengukuran Pengolaan 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		16	9	4
Dalam penerapan atau diterapkan sebagian		4		
Diterapkan secara menyeluruh		1		
Total Nilai Evaluasi Pengolaan Aset				**45**

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 IV			
Status Pengamanan	Kategori Kontrol		
	1	2	3
Tidak dilakukan			
Dalam perencanaan	3	1	
Dalam penerapan atau diterapkan sebagian	6	7	1
Diterapkan secara menyeluruh	4	2	
Total Nilai Evaluasi Teknologi dan Keamanan			**75**

Tabel 7. Hasil Pengukuran Tingkat/Peran Ketergantungan TIK

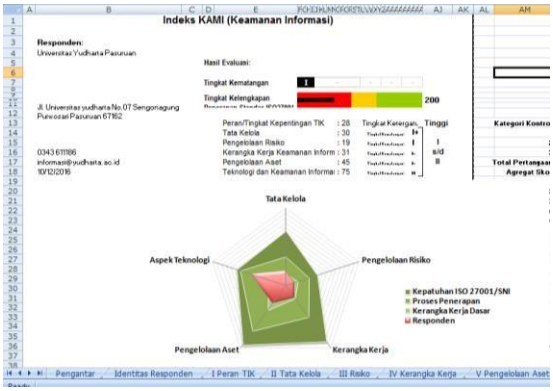
Tk Ketergatungan TIK	**Rendah**	**Tinggi**	**Klasifikasi**
28	0	12	Rendah
Tinggi	13	24	Sedang
	25	36	Tinggi
	37	48	Kritis

Tabel 8. Hasil Pengukuran Bagian-Bagian Keamanan Informasi

Indeks KAMI	**Skor**	**Tingkat kematangan**
Tata Kelola	20	I+
Pengelolaan Risiko	30	I
Kerangka Kerja Keamanan Informasi	19	I+
Pengelolaan Aset	31	I+
Teknologi dan Keamanan Informasi	45	II
Total skor	**200**	**I s/d II**

Tabel 9. Kesimpulan Indeks KAMI

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 4. Tingkat kematangan indeks KAMI

Dari hasil pengukuran yang telah dilakukan terhadap peran TIK di UYP menggunakan Indeks KAMI dengan tingkat kematangan masing-masing bagian keamanan informasi yang terdapat di UYP.

Untuk bagian I pada tabel 7. Yaitu peran dan Kepentingan TIK di UYP menunjukkan bahwa TIK memegang peran penting. Hal ini bias dilihat pada perhitungan Indeks KAMI dengan skor 28. Yang berarti peran TIK tinggi. Sementara untuk Bagian II , III, IV dan V dan VI digunakan untuk mengukur keamanan informasi di UYP.

Hasil pengukuran dapat dilihat pada Gambar 4. Menunjukkan hasil pengukuran Bagian II,III,IV dan V menunjukkan bahwa tingkat kematangan keamanan informasi di UYP berada pada Level I dan I+ yaitu **Kondisi Awal**, sementara untuk bagian VI, tingkat kematangan keamanan informasi di UYP berada pada level II yaitu masih berupa **Penerapan Kerangka Kerja Dasar**.

Sehingga hasil akhir dari pengukuran keamanan informasi menggunakan indeks KAMI untuk UYP mendapatkan kesimpulan bahwa kemanan informasi yang terdapat pada UYP **tidak layak**, seperti pada Tabel 9.

5. Kesimpulan

1. Dengan menggunakan indeks KAMI, tingkat kematangan keamanan TIK pada

UYP yang mencakup enam aspek mulai dari peran TIK, tata kelola, pengelolaan resiko, kerangka kerja, pengelolaan aset serta TIK dapat terukur.

2. Hasil evaluasi tingkat kematangan keamanan TIK pada UYP berada di level I sampai dengan II, dimana tingkat kematangannya dinyatakan dalam kondisi awal sampai dengan penerapan kerangka kerja dasar, hal ini masih dibawah standar ISO 27001:2009 dimana minimal kesiapan dan tingkat kematangannya berada di lavel III.
3. Peran TIK terhadap UYP masuk kedalam katagori tinggi, dan hasil skor evaluasi ke lima bagian mendapat skor 200, Berdasarkan indeks skor kematangan berada pada range 0 -272 yang berarti **tidak layak**.
4. Hasil dari evaluasi di UYP terhadap TIK masih ditahap penerapan sebagian dan dalam perencanaan akan tetapi masih dalam perencanaan.

6. Daftar Pustaka

[1] Team. Buku Akademik UYP. Yudharta Press.

[2] Alexander Setiawan. (2008). Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework *Seminar Nasional Aplikasi Teknologi Informasi 2008 (SNATI 2008) ISSN: 1907-5022Yogyakarta, 21 Juni 2008*

[3] Tri Yani A, dkk. (2016). Evaluasi keamanan TIK UYP menggunakan indeks Keamanan informasi (KAMI). TEKNOSI, Vol. 02, No. 02, Agustus 2016. Hal 54

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

[5] Adi Supriyatna. (2014). Analisis Tingkat Keamanan Sistem Informasi Akademik dengan Mengkombinasikan Standar BS-7799 dengan SSE-CMM. *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2014. No 182*

[6] Simarmata, Janner. (2006). *Pengamanan Sistem Komputer*. Yogyakarta: ANDI.

[7] Tim Direktorat Keamanan Informasi. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi. KOMINFO