Volume 3 Nomor 1 Januari 2018

INFORMASI INTERAKTIF

JURNAL INFORMATIKA DAN TEKNOLOGI INFORMASI

PROGRAM STUDI TEKNIK INFORMATIKA – FAKULTAS TEKNIK -UNIVERSITAS JANABADRA

INFORMASI INTERAKTIF	Vol. 3	No. 1	Hal. 1 - 76	Yogyakarta Januari 2018	ISSN 2527-5240

INFORMASI INTERAKTIF

ISSN 2527-5240

DEWAN EDITORIAL

JURNAL INFORMASI INTERAKTIF merupakan media komunikasi hasil penelitian, studi kasus, dan ulasan ilmiah bagi ilmuwan dan praktisi dibidang Teknik Iinformatika. Diterbitkan oleh Program Studi Teknik Informatika Fakultas Teknik Universitas Janabadra di Yogyakarta, tiga kali setahun pada bulan Januari, Mei dan September.

INFORMASI INTERAKTIF

ISSN 2527-5240

DAFTAR ISI

halaman

ISSN 2527-5240

PENGANTAR REDAKSI

Puji syukur kami panjatkan kehadirat Allah Tuhan Yang Maha Kuasa atas terbitnya JURNAL INFORMASI INTERAKTIF Volume 3, Nomor 1, Edisi Januari 2018. Perlu kami sampaikan, bahwa terhitung mulai tahun 2018, Jurnal Informasi Interaktif kami terbitkan 3 (tiga) kali dalam setahun yaitu bulan Januari, Mei dan September. Pada edisi kali ini menampilkan sembilan artikel di bidang Teknik Informatika.

Harapan kami semoga naskah yang tersaji dalam JURNAL INFORMASI INTERAKTIF edisi Januari tahun 2018 dapat menambah pengetahuan dan wawasan di bidangnya masing-masing dan bagi penulis, jurnal ini diharapkan menjadi salah satu wadah untuk berbagi hasil-hasil penelitian yang telah dilakukan kepada seluruh akademisi maupun masyarakat pada umumnya.

Redaksi

INDEKS PENILAIAN KEAMANAN INFORMASI UNTUK MENGUKUR KEMATANGAN MANAJEMAN KEAMANAN LAYANAN TI (Studi Kasus :BPMP Kabupaten Gresik)

Rahmat Hidayat [1], Mohammad Suyanto[2], Andi Sunyoto[3]

[1, 2 ,3]Magister Teknik Informatika Universitas AMIKOM Yogyakarta
Jl Ring road Utara, Condongcatur, Sleman, Yogyakarta 55283 Telp: (0274) 884201-207

Email : [1]ykoya77@gmail.com, [2]yanto@amikom.ac.id, [3]andi@amikom.ac.id

ABSTRACT

This study contains the results of measurement of the maturity of Information Security Management System (ISMS) in the Gresik District The result of measurement of the completeness and maturity of the ISMS in BPMP Gresik Regency is still relatively low, that is at the level of I to II which means the maturity level is stated in the initial condition up to the implementation of the basic framework, it is still under standard ISO 27001: 2009. And for the evaluation of the level of completeness of the implementation of the five areas with the achievement score of 207, then according to the Indeks KAMI mean readiness status is considered "Not Eligible". The causes of the low maturity level of the ISMS include low levels of awareness from the leadership and related employees of the ISMS, lack of documentation of activities and also for the development of applications and infrastructure that are reactive.Researchers suggest of things need to increase awareness to leaders and employees regarding the importance of the ISMS, and to develop ICT Blueprint that enables BPMP application development and infrastructure to be conducted in a planned and comprehensive manner. And improve SOP in BPMP environment to support business process shift from paper-based to technology-based administration as well as to cultivate the documentation of data and information in BPMP Gresik District.

Keywords: *ISMS, BPMP Gresik District, index KAMI, ISO2700:2009*

1. PENDAHULUAN

BPMP kabupaten Gresik kini telah menggunakan sistem elektronik untuk melayanai masyarakat, maka menurut peraturan menteri komunikasi dan informatika republik Indonesia tentang pedoman teknis audit manajemen keamanan elektronik pada penyelenggra pelayanan publik Pasal 2 ayat (1) menetapkan "setiap penyelenggara sistem elektronik untuk pelayanan publik harus menyeleggarakan sistem elektronik secara aman", di tambah lagi dengan pasal 2 ayat (2) "untuk menjamin keamanan sistem elektronik untuk pelayanan publik sebagaimana dimaksud pada ayat (1) wajib dilakukan audit atas manajemen keamanan sistem elektronik". karena data yang di olah begitu penting dan merupakan aset utama bagi instansi tersebut maka harus menjamin terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi. karena berhadapan dengan beberapa potensi ancaman berupa "disengaja" (misalnya, seorang perusak/cracker individu atau organisasi kriminal) atau "kebetulan" (misalnya, kemungkinan rusak komputer, atau kemungkinan bencana alam seperti gempa bumi, kebakaran dan lain-lain).

Sebelum standardisasi keamanan informasi diterapkan, perlu dilakukan evaluasi sistem keamanan informasi di BPMP kabupaten Gresik untuk mendapatkan gambaran kondisi kesiapan dan kematangan manajemen keamanan informasi tersebut. Berdasarkan hal tersebut penelitian ini akan mengukur tingkat kematangan manajemen keamanan informasi pada BPMP kabupaten Gresik mengunakan model yang di siapkan oleh Kominfo RI tahun 2008, sebagai alat bantu untuk mengukur tingkat kematangan dan kelengkapan keamanan informasi yang disebut dengan indeks KAMI. Indeks KAMI dibuat dengan acuan ISO 27001:2009 yang berisi tentang keamanan informasi.ISO 27001 adalah suatu bentuk kerangka keja standar internasional yang berisi tentang standar-standar dalam area keamanan informasi, lingkup penggunaan teknologi dan pengelolaan aset yang membantu organisasi memastikan bahwa keamanan informasi sudah efektif [1]. Hal ini

termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas atas informasi yang dimilikinya.

Pengukuran keamanan informasi di Instansi BPMP kabupaten Gresik bertujuan untuk mengetahui tingkat kematangan menejemen keamanan layanan TI melalui pengukuran tingkat kematangan*(maturity level)* keamanan informasi berdasarkan indeks KAMI, sehingga dapat digunakan sebagai rekomendasi dan bahan acuan pihak manajemen pengelola TIK dalam pengambilan keputusan untuk peningkatan keamanan sistem informasi [2]. Pelaksanaan pengukuran ini juga dalam rangka penerapan Standar ISO 27001/(SNI 27001:2009), dan juga mengetahui atau mengukur peran dan tingkat Kepentingan TIK dalam Instansi, Bagaimana Tata Kelola Keamanan Informasi di dalam Instansi, Bagaimana mengelola Resiko Keamanan Informasi, bagaimana Kerangka Kerja Pengelolaan Keamanan Informasi, Bagaimana Pengelolaan Aset Informasinya, serta Bagaimana keefektifan Teknologi dan Keamanan Informasi di dalam Instansi.

Penelitian Information Security Readiness of Government Institution in Indonesia [3]. Pada penelitian tersebut memperoleh gambaran status keamanan informasi di Indonesia, sektor pemerintah khususnya, dari tahun 2011 sampai tahun 2013 dan hasil penelitian tersebut menunjukkan bahwa di instansi pemerintah 3% yang mendekati untuk memenuhi standar sementara, dan yang lain masih membutuhkan banyak perbaikan. Berdasarkan hasil yang di temukan bahwa sebagian besar organisasi berfokus pada teknologi, tetapi mengabaikan manajemen risiko dan manajemen keamanan layanan TI, Karena tata kelola organisasi yang baik telah menjadi kebutuhan untuk mereformasi institusi pemerintah. Salah satu upaya yang dilakukan adalah pembangunan pemerintah elektronik adalah untuk meningkatkan kualitas pelayanan publik. Dengan demikian, sumber informasi yang diperlukan untuk memastikan bahwa sumber daya ini dilindungi dengan baik dalam rangka memenuhi aspek keamanan informasi untuk memberikan informasi berkualitas tinggi. Tetapi pada kenyataannya, ada banyak kasus menunjukkan bahwa sumber daya pemerintah diserang dan tidak aman.

Untuk menangani masalah ini, Menkominfo memperkenalkan Indeks KAMI sebagai alat untuk menilai tingkat kematangan institusi untuk memenuhi informasi nasional standar manajemen keamanan. Dan dibutuhkan upaya-upaya besar untuk memperbaiki keamanan informasi di lembaga pemerintahan untuk menerapkan kontrol dasar risiko dan juga dari strategi keamanan informasi.

Penelitian Analysis of Information Security through Asset Management in Academic Institutes of Pakistan [5]. Penelitian menjabarkan kebutuhan untuk standar praktik keamanan terbaik,dan untuk menyediakan tingkat keamanan yang mengacu ISO 27001, dimana salah satu standar yang tepat seperti tujuan dasar adalah untuk memberikan persyaratan atau mendirikan, melaksanakan, menjaga dan terus meningkatkan suatu Sistem Manajemen Keamanan Informasi (SMKI). ISO 27001 memberikan pedoman lengkap untuk organisasi tentang manajemen asset dan juga menjamin manajemen resiko yang sudah di prediksi sebelumnya.

Karena aset yang paling penting dari suatu organisasi adalah informasi yang terdapat pada setiap jenis komponen yaitu elektronik atau dalam bentuk perangkat keras.Aset yang berbeda *seperti backup drive*, *file office* dalam bentuk baik lunak atau keras, perangkat dll jaringan memiliki sejumlah informasi besar yang perlu dilindungi dari akses yang tidak sah. Manajemen aset adalah proses mempertahankan, meningkatkan dan operasi aset. Karena aset memiliki arti besar dan pengaruh besar pada mereka, untuk mencapai tujuan organisasi yang telah ditetapkan. Dan tujuan utama dari keamanan informasi adalah untuk terus menjaga proses informasi yang berkaitan organisasi,

Untuk mencapai tujuan yang di harapkan lembaga akademik harus berstandar ISO 27001 yang bersertifikat. ISO 27001 adalah standar keamanan memberikan kebijakan, prosedur dan pedoman mengenai semua aspek keamanan informasi yaitu keamanan fisik, keamanan jaringan dll, Survei dapat dilakukan di lembaga akademis Pakistan untuk memeriksa tingkat keamanan sesuai dengan aspek-aspek tersebut. Sehingga satu bisa mendapatkan gambaran yang jelas tentang apa yang dilakukan (bagaimana hal itu dilakukan) dan apa yang harus dilakukan.

1.1 Indeks KAMI

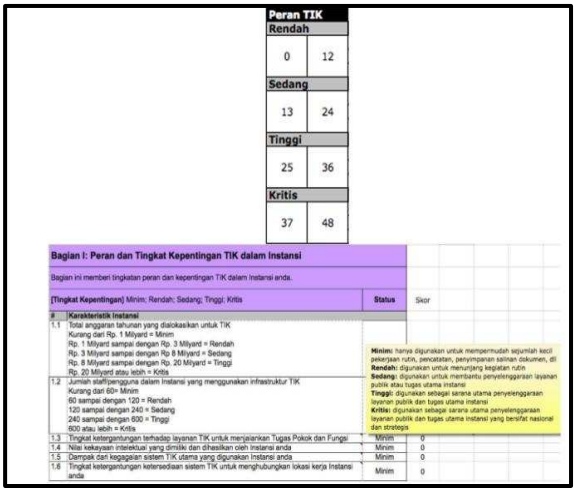
Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di Instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi [4]. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2009. Pengukuran dalam Indeks KAMI dapat dilakukan dengan alur proses berikut :

a. Mendifinisikan Ruang Lingkup
b. Menetapkan Peran atau Tingkat Kepentingan TIK di Instansi
c. Menilai Kelengkapan Pengamanan 5 Area
d. Mengkaji Hasil Indeks KAMI disertai dengan menetapkan langkah-langkah perbaikan.

1.2 Penggunaan *Indeks KAMI*

Sebelum proses penilaian dilakukan secara kuantitatif, proses klasifikasi dilakukan terlebih dahulu terhadap peran TIK dalam instansi atau cakupan evaluasinya. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik kepentingan TIK yang sama. Dapat dilihat pada gambar 1. Memberikan ilustrasi tampilan evaluasi peran TIK berikutpilihannya[Minim (0); Rendah (1); Sedang (2); Tinggi (3); Kritis (4)] dan tabel pemetaan hasil penjumlahan menjadi 4 (empat) klasifikasi (Rendah; Sedang; Tinggi; Kritis).

Data yang digunakan dalam evaluasi ini nantinya akan memberi snapshot indeks kesiapan (kelayakan) dan kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding menyusun langkah-langkah perbaikan dan penetapan prioritasnya.



Gambar 1. Ilustrasi Tampilan Evaluasi

Penggunaan dan publikasi hasil evaluasi indeks KAMI merupakan bentuk tanggung jawab dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi. Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan atau kematangan kepada pihak yang terkait (*stakeholders*). Untuk peran TIK di instansi memiliki penilaian yang berbeda dari beberapa bagian lainnya dikarenakan Peranan TIK di instansi ini diharapkan untuk mendapatkan nilai dari ketergantungan instansi itu sendiri akan perananan teknologi dan sistem informasinya. Skor penilaian untuk peran TIK di instansi dapat dilihat pada tabel 1.

Tabel 1. Skor Penilaian TIK di Instansi

Skor Peran TIK	
Minim	0
Rendah	1
Sedang	2
Tinggi	3
Sangat Tingg / kritis	4

Akan tetapi untuk 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. Seluruh pertanyaan yang ada dalam setiap area dikelompokkan menjadi 3 *(tiga)* kategori pengamanan, sesuai dengan tahapan dalam penerapan standar ISO/IEC 27001. Pertanyaan yang terkait dengan kerangka kerja dasar keamanan informasi masuk dalam kategori "1", untuk efektivitas dan konsistensi penerapannya didefinisikan sebagai kategori "2", dan hal-hal yang merujuk pada kemampuan untuk selalu meningkatkan kinerja keamanan informasi adalah kategori "3".

Responden kemudian diminta untuk menjawab setiap pertanyaan dengan pilihan Status Penerapan:

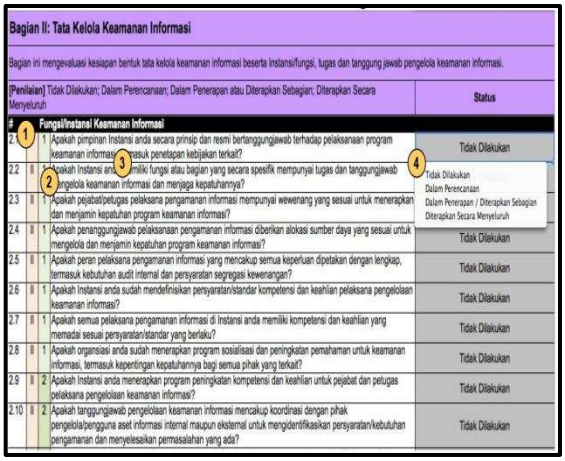
a. Tidak Dilakukan
b. Dalam Perencanaan
c. Dalam Penerapan atau Diterapkan Sebagian
d. Diterapkan Secara Menyeluruh.

Setiap jawaban akan diberikan skor yang nilainya disesuaikan dengan tahapan penerapan (kategori) bentuk pengamanan. Untuk tahapan awal nilainya akan lebih rendah dibandingkan tahapan berikutnya. Demikian halnya untuk status penerapannya, penerapan yang sudah berjalan secara menyeluruh memberikan nilai yang lebih tinggi dibandingkan bentuk penerapan lainnya.Tabel pemetaan skor dapat dilihat pada Tabel 2. Tabel ini merangkum seluruh jumlah jawaban penilaian mandiri dan membentuk matriks antara status pengamanan dan kategori.

Tabel 2. Skor Tahap Pengamanan

Status Pengamanan	Tingkat Kematangan		
	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

Nilai untuk kategori pengamanan yang tahapannya lebih awal, lebih rendah dibandingkan dengan nilai untuk tahapan selanjutnya. Hal ini sesuai dengan tingkat kompleksitas yang terlibat dalam proses penerapannya. Catatan: untuk keseluruhan area pengamanan, pengisian pertanyaan dengan kategori "3" hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan kategori "1" dan "2" sudah di isi dengan status minimal "Diterapkan Sebagian". Dapat di lihat pada gambar 2 berikut.



Gambar 2. Ilustrasi kesiapan dan kematangan keamanan informasi

Keterangan Ilustrasi:

1. Kolom yang menunjukkan kategori kematangan terkait pertanyaan yang dibahas
2. Kolom yang menunjukkan kategori tahap penerapan
3. Daftar pertanyaan
4. Pilihan jawaban

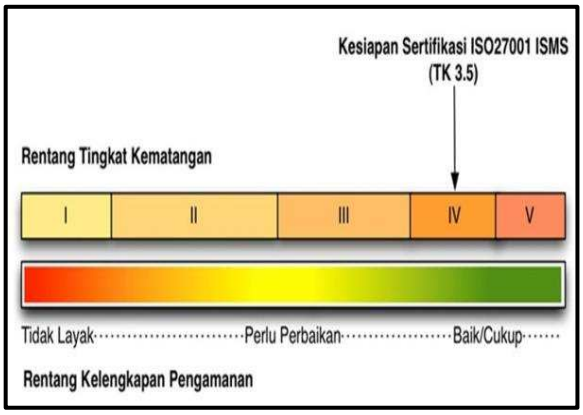
Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan kondisi penerapan keamanan informasi SESUNGGUHNYA. Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan azas keterbukaan dan kejujuran. Jika sudah mendapatkan hasil dari penilaian atas penerapan dari tiap-tiap bagian yang ada, maka pimpinan instansi dapat melihat kebutuhan pembenahan yang diperlukan dan korelasi antara berbagai area penerapan keamanan informasi. Adapun korelasi antara peran atau tingkat kepentingan TIK dalam instansi didefinisikan melalui tabel 3 berikut.

Tabel 3. Matriks peran TIK dan status kesiapan

Peran TIK				
Rendah		Indeks (SkorAkhir)		Status Kesiapan
0	12	0	124	TidakLayak
		125	272	PerluPerbaikan
		273	588	Baik/Cukup
Sedang		SkorAkhir		Status Kesiapan
13	24	0	174	TidakLayak
		175	312	PerluPerbaikan
		313	588	Baik/Cukup
Tinggi		SkorAkhir		Status Kesiapan
25	36	0	272	TidakLayak
		273	392	PerluPerbaikan
		393	588	Baik/Cukup
Kritis		SkorAkhir		Status Kesiapan
37	48	0	333	TidakLayak
		334	453	PerluPerbaikan
		454	588	Baik/Cukup

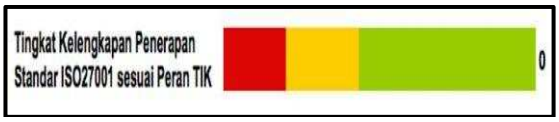
Pengelompokan kedua dilakukan berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan di institusi seperti pada gambar 3. Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefiisikan sebagai berikut:

a. Tingkat I – KondisiAwal
b. Tingkat II PenerapanKerangkaKerjaDasar
c. Tingkat III – TerdefiisidanKonsisten
d. Tingkat IV – TerkeloladanTerukur
e. Tingkat V – Optimal



Gambar 3. Tingkat kematanagn Dalam Indeks KAMI

Status Kesiapan atau Kelengkapan dapat ditampilkan dengan instrumen Bar Chart atau diagram batang seperti terlihat pada gambar 4.



Gambar 4. Bar Chart Tingkat Kelengkapan Penerapan Standar ISO27001

Pencapaian yang masih ada di area berwarna merah masih dalam status kesiapan "Tidak Layak", kemudian pencapaian di area warna kuning masih "Memerlukan Perbaikan", sedangkan pencapaian warna hijau menunjukkan bahwa status kesiapan sudah "Baik/Cukup".

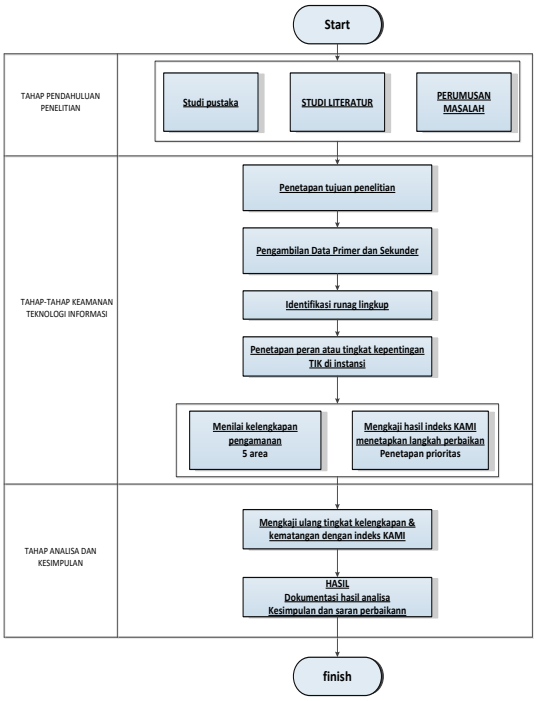
2. METODE PENELITIAN

Metodologi penelitian merupakan suatu metode yang digunakan untuk menentukan langkah-langkah yang harus dilakukan dalam sebuah penelitian. Metode penelitian yang digunakan adalah metode deskriptif dengan pendekatan penelitian kualitatif dan kuantitatif.

a. Perumusan masalah: mengumpulkan permasalahan yang ditemukan dan disatukan dalam suatu *research question*. Selanjutnya *research question* ini digunakan sebagai pedoman, penentu arah atau fokus dari penelitian.
b. Studi literarur: Melakukan review, pembandingan dan melihat literarur yang terkait dengan penelitian.
c. Pengumpulan data: Pada tahapan ini dilakukan pengumpulan data secara kualitatif dengan melakukan wawancara, observasi dan kuisioner.
d. Mendefinisikan ruang lingkup variabel evaluasi
e. Analisa data dan Pembuatan indeks penilaian merujuk pada penggunaan Indeks KAMI.
f. Melakukan verifikasipada tingkat kematanagan pada sistem manajemen keamanan informasi pada BPMP Kabupaten Gresik
g. Kesimpulan dan saran: penarikan kesimpulan berdasarkan hasil penelitian.

2.1. Alur Penelitian

Agar penelitian ini berjalan dengan sistematis dan terstruktur maka peneliti harus membuat alur penelitian seperti yang tercantum pada gambar 5.di bawah ini :



Gambar 5. Alur Penelitian

3. HASIL DAN PEMBAHASAN

Langkah pertama penggunaan indeks KAMI adalah dengan menjawab pertanyaan terkait kesiapan pengamanan informasi, dalam hal ini responden di minta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis.

Setelah itu dilakukan menjawab pertanyaan atau kuisioner terkait pengukuran kesiapan keamanan informasi mulai dari tata kelola informasi, hasilnya pada tabel 6, pengelolaan resiko keamanan informasi pada Tabel 7, pengukuran kerangka kerja keamanan informasi pada tabel 8, pengukuran pengelolan aset informasi pada tabel 9 , dan pengukuran teknologi dan keamanan informasi pada tabel 10. Dari semua pertanyaan yang terbagi menjadi lima bagian tersebut akan mendapatkan hasil berupa skor dari masing-masing area atau bagian yang di evaluasi .

Tabel 5. Pengukuran tingkat kepentingan TIK

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
Total Pertanyaan			12 butir
Hasil Jawaban Responden			
Tingkat Kepentingan	Hasil	Skor	Total
Minim	2	0	0
Rendah	2	1	2
Sedang	1	2	2
Tinggi	5	3	15
Kritis	2	4	8
Total Skor Peran dan Tingkat Kepentingan TIK di BPMP Kabupaten Gresik.			27

Tabel 6. 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.							
Jumlah Pertanyaan	TP 1		TP 2		TP 3		Total
	8		6		6		20 butir
Hasil Jawaban Responden Bagian II							
Status Pengamanan	Tingkat kematangan						
	TP 1	SKOR TP 1	TP 2	SKOR TP2	TK 3	SKOR TP 3	TOTAL
Tidak dilakukan	0	0	0	0	0	0	0
Dalam perencanaan	2	1	0	2	1	3	5
Dalam penerapan atau diterapkan sebagian	2	2	0	4	0	6	4
Diterapkan secara	4	3	5	6	0	9	42
Total Nilai Evaluasi Tata Kelola Keamanan Informasi							51

Tabel 7. Hasil pengukuran Pengelolaan risiko keamanan informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi							
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.							
Jumlah Pertanyaan	TP 1		TP 2		TP 3		Total
	9		4		2		15 butir
Hasil Jawaban Responden Bagian III							
Status Pengamanan	Tingkat Kematangan						
	TP 1	SKOR TP 1	TP 2	SKOR TK2	TK 3	SKOR TK	TOTAL
Tidak dilakukan	7	0	3	1	0	0	0
Dalam perencanaan	0	1	0	2	0	3	0
Dalam penerapan atau diterapkan sebagian	1	2	0	4	0	6	2
Diterapkan secara menyeluruh	1	3	1	6	1	9	9
Total Nilai Evaluasi Pengelolan Resiko Keamanan Informasi							11

Tabel 8. Hasil pengukuran kerangka kerja pengelolaan keamanan informasi

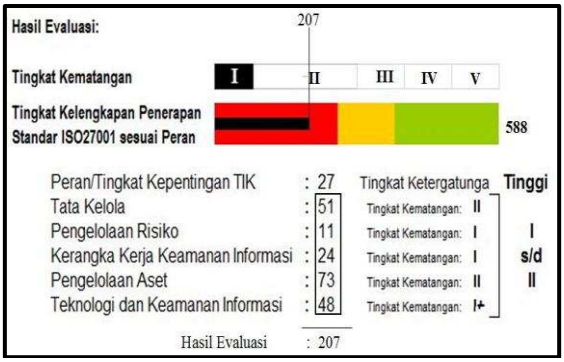
Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi							
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.							
Jumlah Pertanyaan	TP 1		TP 2		TP 3		Total
	11		8		7		26 Butir
Hasil Jawaban Responden Bagian IV							
Status Pengamanan	Tingkat Kematangan						
	TP 1	SKOR TP 1	TP 2	SKOR TP 2	TP 3	SKOR TP 3	TOTAL
Tidak dilakukan	2	0	4	1	4	0	0
Dalam perencanaan	5	1	3	2	0	3	11
Dalam penerapan atau diterapkan sebagian	3	2	1	4	2	6	10
Diterapkan secara menyeluruh	1	3	0	6	1	9	3
Total Nilai Evaluasi kerangka kerja pengelolaan keamanan informasi							24

Tabel 9. Hasil pengukuran pengelolaan aset informasi

Bagian V: Pengelolaan Aset Informasi							
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.							
Jumlah Pertany aan	TK 1		TK 2		TK 3		Total
	21		9		4		34 Butir
Hasil Jawaban Responden Bagian IV							
Status Pengamanan	Tingkat Kematangan						
	TP 1	SKOR TP 1	TP 2	SKOR TP 2	TP 3	SKOR TP 3	TOTAL
Tidak dilakukan	4	0	0	0	0	0	0
Dalam perencanaan	4	1	5	2	3	3	14
Dalam penerapan atau diterapkan sebagian	2	2	1	4	0	6	8
Diterapkan secara menyeluruh	11	3	3	6	1	9	51
Total Nilai Evaluasi Pengelolan Aset Informasi							73

Tabel 10. Hasil pengukuran teknologi keamanan informasi

Bagian VI: TeknologidanKeamananInformasi							
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.							
Jumlah Pertany aan	TP 1		TP 2		TP 3		Total
	13		10		1		24 Butir
Hasil Jawaban Responden Bagian IV							
Status Pengamanan	Tingkat Kematangan						
	TP 1	SKOR TP 1	TP 2	SKOR TP 2	TK 3	SKOR TP 3	TOTAL
Tidak dilakukan	2	0	2	0	0	0	0
Dalam perencanaan	4	1	2	2	0	3	8
Dalam penerapan atau diterapkan sebagian	5	2	6	4	1	6	34
Diterapkan secara menyeluruh	2	3	0	6	0	9	6
Total Nilai Evaluasi Teknologi dan Keamanan Informasi							48



Gambar 6. Hasil evaluasi

Berdasarkan hasil perhitungan total skor kesiapan keamanan informasi dari tiap-tiap bagian pada BPMP Kabupaten Gresik pada gambar 6 tingkat kematangan berada level Is/d II, Pada bagian II: yaitu Tata Kelola Keamanan informasi pada lavel II yang berarti pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif . Sedangkan pada bagian III: Pengelolaan Resiko Keamanan Informasi berada di lavel I yang berarti masih kondisi awal atau mulai adanya pemahaman mengenai perlunya SMKI. Pada bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi berada pada lavel I yaitu berati kondisi awal atau mulai adanya pemahaman mengenai perlunya SMKI. Sedangkan pada bagian V : Pengelolan Aset Informasi, BPMP Kabupaten Gresik berada di Lavel II yaitu penerapan kerangka kerja dasar. Dan bagian VI: Teknologi dan Keamanan Informasi berada di lavel I+ yang berarti dalam penerapan kerangka kerja dasar menuju terdefinisi dan konsisten.

Tabel 11. Kesiapan SMKI BPMP Kabupaten Gresik

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

4. KESIMPULAN

4.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa :

1. Tingkat kelengkapan dan kematangan SMKI pada BPMP Kabupaten Gresik Dengan menggunakan model indeks KAMI masih berada pada level *I s/d II*, dengan nilai skor peran tingkat kepentingan terhadap TIK sebesar 27 atau tingkat ketergantungan terhadap TIK tergolong Tinggi.
2. Nilai hasil evaluasi tingkat kesiapan penerapan dari kelima area medapat skor 207, Maka dalam matriks peran TIK dan Status kesiapan berada pada kondisi "Tidak Layak" karena semakin tinggi ketergantungan terhadap TIK atau semakin penting peran TIK maka harus semakin banyak bentuk pengamanan yang di perlukan dan harus di terapkan sampai tahap tertinggi.

4.2 Saran

Untuk mendapatkan SMKI yang standard ISO27001:2009/SNI maka yang harus di lakukan terkait penerapan SMKI pada BPMP Kabupaten Gresik , Peneliti menyarankan sejumlah hal sebagai berikut:

1. Melaksanakan sejumlah program peningkatan *awareness* pimpinan dan pejabat tentang arti penting SMKI, baik dari sisi aturan maupun penerapannya, seperti program sosialisasi, internalisasi, workshop, seminar dan pelatihan terkait keamanan informasi dengan melibatkan pihak yang pimpinan instansi dan pihak yang terlibat dengan harapan bahwa pengembangan SMKI dapat menjadi bagian dari Rencana Strategis BPMP Kabupaten Gresik.
2. Melakukan evaluasi secara berkala terhadap kerangka kerja keamanan informasi sehingga bisa melihat adanya perubahan kondisi keamanan informasi yang sedang diterapkan.

DAFTAR PUSTAKA

[1] Badan Sertifikasi Nasional. (2009) Standar Nasional Indonesia (SNI)–ISO/IEC 27001:2009), Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan informasi – Persyaratan. Jakarta.

[2] Direktorat Keamanan Informasi, Kementerian Komunikasi dan Informatika. (2011) Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Jakarta.

[3] Kautsarina. *et al.* (2014) *Information Security Readiness of Government Institution in Indonesia*, 978-1-4799-3580-2/14/$31.00©2014 IEEE.

[4] Marco. R. (2016) Indeks Penilaian Tingkat Kematangan (*Maturity*) It Governance pada Manajemen Keamanan Layanan Teknologi Informasi, Jurnal DASI vol. 17 no. 2. Pp 76-82, ISSN: 1411-3201.

[5] Nadia. M. (2015) *Analysis of Information Security through Asset Management in Academic Institutes of Pakistan*, 10.1109/ICICT.2015.7469581 IEEE.