ANALISA TINGKAP KESIAPAN PENERAPAN KEAMANAN TEKNOLOGI INFORMASI DALAM PELAKSANAAN *e-GOVERNMENT* BERBASIS INDEKS KEAMANAN INFORMASI (KAMI) STUDI KASUS PEMERINTAH KOTA KEDIRI

I Gede Putu Krisna Juliharta
Program Studi Sistem Informasi
STMIK PRIMAKARA
krisna@primakara.ac.id

ABSTRACT

e-Governement in Indonesia is a must this time. Good E-Governments certainly have the ability to provide good information to the public and fulfill aspects of confidentiality, integrity and availability, Kediri in East Java is one of the government that use e-Government. To measure these three aspects the system must be measured. Indeks KAMI (Keamanan Informasi) is an application that is used as a tool to analyze and evaluate the level of readiness (completeness and maturity) for implementing information security in an organization in accordance with SNI ISO / IEC 27001 criteria. Government of Kediri the score for the electronic system category was 20, for the governance assessment the score was 75, risk management score 18, the information security framework was 58, asset management 74, and the application of security and information technology had a value of 83, and the results measurement says the City Government of Kediri needs to improve the system management.

Keywords**:** *Index,* KAMI *, Security, Information Technology*

ABSTRAK

Penerapan *e-Governement* dalam tata kelola Pemerintahan di Indonesia saat ini merupakan sebuah keharusan. *E-Governement* yang baik tentu memiliki kemampuan untuk memberikan Informasi yang baik kepada masyarakat dan memenuhi aspek kerahasiaan *(confidentiality),* keutuhan *(integrity)* dan ketersediaan *(availability),* Pemerintah Kota (Pemkot) Kediri adalah salah lembaga pemerintah yang menggunakan *e-Government.* Untuk mengukur ketiga aspek tersebut sistem haruslah diukur. Indeks KAMI (Keamanan Informasi) merupakan aplikasi yang digunakan sebagai alat bantu untuk menganalisa dan mengevalusi tingkat kesiapan (kelengkapan dan kematangan) penerapan keamanan informasi di sebuah organisasi sesuai dengan kriteria pada SNI ISO/IEC 27001. Untuk Pemkot Kediri didapatkan skor kategori sistem elektronik (SE) adalah 20, untuk penilaian tata kelola skornya adalah 75, pengelolaan resiko skornya 18, kerangka kerja keamanan informasi nilainya 58, pengelolaan asset 74, dan penerapan teknologi keamanan dan informasi memiliki nilai 83, dan hasil pengukuran menyebutkan Pemkot Kediri perlu meningkatkan system pengelolaan system yang dimiliki.

Kata Kunci : *indeks, KAMI,* keamanan, teknologi informasi.

PENDAHULUAN

Penerapan *e-Governement* dalam tata kelola Pemerintahan di Indonesia saat ini merupakan sebuah keharusan. *e-Governement* yang baik tentu memiliki kemampuan untuk memberikan Informasi yang baik kepada masyarakat dan memenuhi aspek kerahasiaan *(confidentiality),* keutuhan *(integrity)* dan ketersediaan *(availability).* Berdasarkan data dari GovCert terkait data statistik serangan terhadap domain .go.id pa-da tahun 2017 86,3% serangan ke domain .go.id adalah berupa serangan Web defacement, Phising sebesar 6,7%, Spam 5,5%, Brute Force 0,4%, dan Malware 0,1%[1]. Dengan jumlah seperti disebutkan diatas, Pemerintah perlu melakukan pengukuran untuk mengetahui tingkat kesiapan keamanan informasi dari teknologi *e-Government* yang digunakan. Karena informasi yang berada didalamnya merupkan aset yang paling berharga dalam memberikan pelayanan kepada masyarakat.

Pemerintah Kota Kediri merupakan Institusi yang menerapkan teknologi informasi dalam pelayanan dan pemberian informasi kepada masyarakat. Layanan teknologi informasi adalah berupa aplikasi *e-Government* yang didalamnya berisi aplikasi web, email, ataupun aplikasi yang lain yang bertujuan untuk memberikan layanan kepada masyarakat. Dalam pelaksanaannya pelayanan berbasis teknologi informasi dibutuhkan sebuah standar keamanan yang baik untuk dapat memenuhi unsur kerahasiaan *(confidentiality),* keutuhan *(integrity)* dan ketersediaan *(availability).* Agar standarisasi dapat berjalan dengan baik diperlukan Analisa tingkat kesiapan penerapan keamanan teknologi informasi dari layanan yang diberikan sehingga mendapatkan gambaran mengenai ke-siapan dan kematangan *(maturity)* menggunakan Indeks Keamanan Infor-masi [2]

Indeks KAMI sebagai alat yang disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika untuk mengukur dan meng-analisis tingkat kesiapan atau kematangan pengamanan informasi yang ada di suatu instansi [2]. Hasil pengukuran ini akan menghasilkan tingkat kematangan keamanan informasi di Pemerintah Kota Kediri, yang nantinya akan dievaluasi dan digunakan sebagai referensi untuk meningkatkan tingkat keamanan informasi Pemerintah Kota Kediri. Indeks KAMI dilaksanakan sebelum pengukuran menggunakan ISO 27001 dilaksanakan. Pengukuran menggunakan indeks KAMI diamanatkan berdasarkan Peraturan Menteri Komunikasi dan Informatika No 4 Tahun 2016 terkait Sistem Manajemen Pengamanan Informasi

LANDASAN TEORI

1. Keamanan sistem informasi

Keamanan sistem informasi merupakan hal yang perlu mendapat perhatian saat membangun sebuah sistem informasi. Bayangkan kita membuat sebuah rumah yang lengkap dengan jendela dan pintu, tetapi kita tidak membuat kunci untuk pintu dan jendela. Hal ini dapat menyebabkan seseorang bisa dengan mudah memasuki rumah kita, bahkan mungkin melakukan pencurian. Sama halnya dengan membangun sistem informasi, keamanan sistem informasi digunakan untuk menghindari seseorang yang tidak memiliki akses untuk dapat masuk ke dalam sistem.

Menurut G. J. Simons, keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan *(cheating)* atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik [3]. Menurut John D. Howard dalam bukunya "*An Analysis of Security Incidents on The Internet"* menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab [3].

2. Aspek Keamanan Informasi

Informasi merupakan salah satu aset penting dari perusahaan. Perusahaan melakukan pengolahan terhadap informasi, kemudian hasilnya disimpan dan dibagikan[6]. Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut ini:

1. *Confidentiality* (Kerahasiaan) Aspek yang menjamin kerahasian data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasian data yang dikirim, diterima dan disimpan [3].
2. *Integrity* (Integritas) Aspek yang menjamin bahwa data tidak diubah tanpa ada ijin pihak yang berwenang *(authorized),* menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini [3].
3. *Availability* (Ketersediaan) Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan *user* yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan) [3].

Sumber lain menyebutkan bahwa aspek keamanan sistem informasi melingkupi 4 aspek. Grafinkel mengemukakan bahwa keamanan komputer melingkupi 4 aspek, yaitu *privasi, integrity, authentication dan availability* [7]. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce,* yaitu *access control* dan *non-repudiation* [7].

3. Indeks Keamanan Informasi (KAMI)

Menurut Badan Siber dan Sandi Negara (BSSN) Keamanan informasi pada suatu organisasi merupakan hal yang sangat penting dan harus menjadi perhatian utama. Namun apakah kriteria penerapan keamanan informasi di organi-

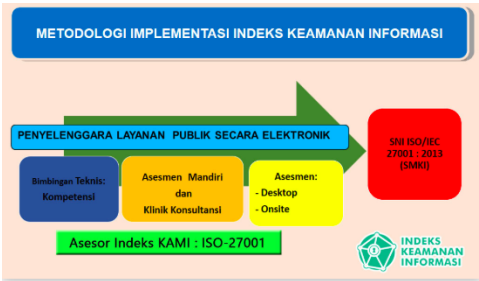
sasi anda telah memenuhi kelengkapan dan kematangan yang sesuai dengan standar[4]

Indeks KAMI (Keamanan Informasi) merupakan aplikasi yang digunakan sebagai alat bantu untuk menganalisa dan mengevalusi tingkat kesiapan (kelengkapan dan kematangan) penerapan keamanan informasi di sebuah organisasi sesuai dengan kriteria pada SNI ISO/IEC 27007, yaitu :

1. Tata Kelola
2. Pengelolaan Risiko
3. Kerangka Kerja
4. Pengelolaan Aset
5. Aspek Teknologi

Gambar 1 Area Indeks KAMI

Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada Pimpinan Instansi. Implementasi Indeks KAMI dilakukan oleh penyelenggara layanan publik secara elektronik melalui Bimbingan Teknis, Asesmen, dan Konsultasi.



Gambar 2 Metodologi Implementasi Indeks KAMI

Bentuk evaluasi yang diterapkan dalam Indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan potret indeks kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya[5].

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 kepada pihak yang terkait (stakeholders). Penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggung-jawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di instansi pemerintah. Pertukaran informasi dan diskusi dengan instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari *lesson-learned* yang sudah dilalui.

METODE PENELITIAN

Tempat dan waktu penelitian dilakukan di Di Pemerintah Kota Kediri, dimulai dari bulan September 2018 hingga November 2018. Dalam melakukan penelitian ini, penulis melakukan langkah-langkah penelitian yang dapat digambarkan pada gambar :

Gambar 3 Langkah Penelitian

a. Mendefinisikan Ruang Lingkup
   Langkah pertama yang harus dilakukan adalah mendefinisikan ruang lingkup penilaian. Ruang lingkup dapat dipilih sesuai dengan kepentingan penilaian Indeks KAMI, dan dapat dipilih sebagai suatu satuan

kerja (di tingkat apapun) ataupun suatu sistem informasi

b. Menetapkan Peran dan Tingkat kepentingan TIK di Instansi
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

c. Menilai Kelengkapan 5 Area
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 informasimasuk 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 :
   - Tidak dilakukan ;
   - Dalam Perencanaan : Dalam Penerapan atau Diterapkan Sebagian ;
   - Diterapkan Secara Menyeluruh.

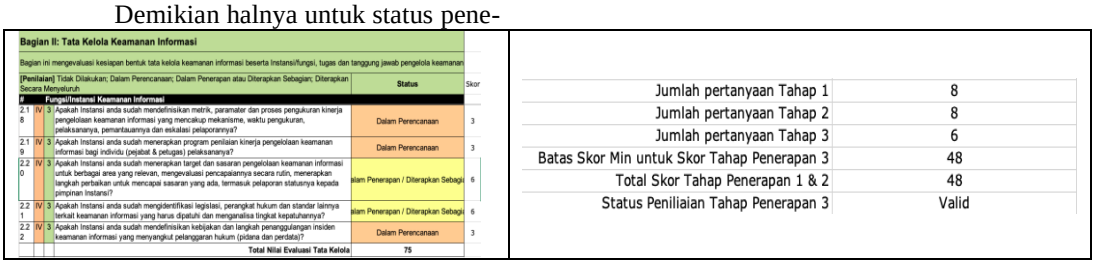
   Setiap jawaban akan diberikan skor yang nilainya disesuaikan dengan tahapan penerapan (kategori) bentuk pengamanan. Untuk tahapan awal nilainya akan lebih rendah dibandingkan tahapan berikutnya. Demikian halnya untuk status penerapannya, penerapan yang sudah berjalan secara menyeluruh memberikan nilai yang lebih tinggi dibandingkan bentuk penerapan lainnya.

d. Mengkaji Tingkat Kelengkapan dan Tingkat Kematangan Indeks KAMI.
   Hasil dari penjumlahan skor untuk masing-masing *area* ditampilkan dalam 2 (dua) instrumen di dasbor:
   1. Tabel nilai masing-masing *area*;
   2. Radar Chart dengan 5 (lima) sumbu sesuai dengan area pengamanan.

HASIL DAN PEMBAHASAN

Analisa Indeks KAMI di Pemerintah Kota Kediri, menggunakan Indeks KAMI versi 3.1. terdapat 141 (seratus tiga puluh satu) pertanyaan yang dibagi menjadi 6 bagian, versi 3.1 lebih banyak 10 pertanyaan dari versi sebelumnya 2.3. Pada Bagian I, informan diminta untuk mendefinisikan Peran TIK (Tingkat Kepentingan TIK) di unit masing-masing. Selain itu, informan juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Bagian II s.d. Bagian VI berisikan sejumlah pertanyaaan terkait Tingkat Kematangan keamanan informasi.

Bagian pertama dari indeks KAMI adalah penilaian kategori sistem elektronik, terdapat 10 pertanyaan, dan jawaban yang diberikan oleh Pemkot Kediri seluruhnya adalah bernilai 2 atau jawaban B, sehingga memiliki skor 20. Skor tersebut memiliki arti bahwa sistem elektronik memiliki kategori tinggi. Tinggi memiliki arti bahwa di Pemkot Kediri teknologi informasi dan komputer merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan.



Bagian II: Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas dan tanggung jawab pengelola keamanan

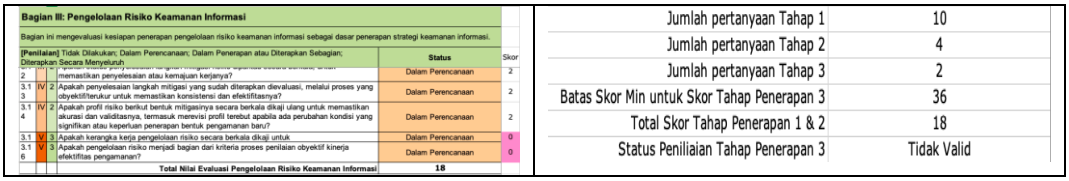
#			[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	Status	Skor
II			Fungsi/Instansi Keamanan Informasi		
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Dalam Perencanaan	3
2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Perencanaan	3
2.20	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?	alam Penerapan / Diterapkan Sebagi	6
2.21	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	alam Penerapan / Diterapkan Sebagi	6
2.22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Perencanaan	3
			Total Nilai Evaluasi Tata Kelola	**75**	

Jumlah pertanyaan Tahap 1	8
Jumlah pertanyaan Tahap 2	8
Jumlah pertanyaan Tahap 3	6
Batas Skor Min untuk Skor Tahap Penerapan 3	48
Total Skor Tahap Penerapan 1 & 2	48
Status Peniliaian Tahap Penerapan 3	Valid

Gambar 4 Hasil Penilaian Tata Kelola Keamanan Informasi

Penilaian kedua adalah penilaian tata kelola keamanan informasi bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi tugas dan tanggung jawab pengelola keamanan informasi. Dari 22 pertanyaan yang ditanyakan Pemkot Kediri menjawab 19 pertanyaan dengan jawaban dalam penerapan/penerapan sebagian dan menjawab 3 pertanyaan dengan jawaban dalam perencanaan,

skor untuk proses penilaian tata kelola keamanan informasi adalah 75. Skor rekapitulasi tahap I dan tahap II adalah 48 sedangkan skor validasi ke tahap III adalah 48 sehingga dapat dikategorikan valid (Gambar 4).



Bagian III: Pengelolaan Risiko Keamanan Informasi

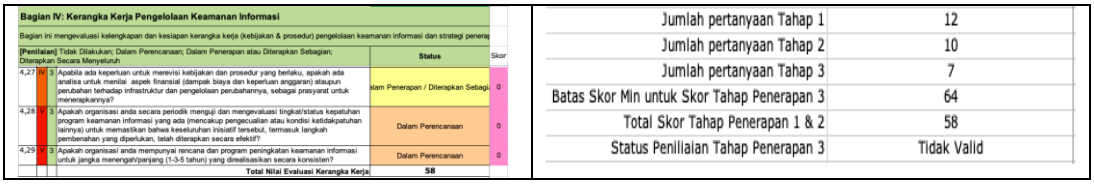
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
2			memastikan penyelesaian atau kemajuan kerjanya?	Dalam Perencanaan	2
3.1 3	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektifiterukur untuk memastikan konsistensi dan efektifitasnya?	Dalam Perencanaan	2
3.1 4	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Dalam Perencanaan	2
3.1 5	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk	Dalam Perencanaan	0
3.1 6	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Dalam Perencanaan	0
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	**18**	

Jumlah pertanyaan Tahap 1	10
Jumlah pertanyaan Tahap 2	4
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	36
Total Skor Tahap Penerapan 1 & 2	18
Status Peniliaian Tahap Penerapan 3	Tidak Valid

Gambar 4. Hasil Penilaian Pengelolaan Resiko

Bagian ketiga adalah penilaian pengelolaan resiko keamanan informasi, bagian ini mengevaluasi tingkat kesiapan penerapan pengelolaan resiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. terdapat 16 pertanyaan dengan jawaban yang diberikan oleh pemkot kediri adalah seluruh pertanyaan dengan jawaban dalam perencanaan. Total skor adalah 18 dan skor penerapan tahap I dan tahap II pada bagian keempat ini adalah 18, sedangkan untuk validasi ke tahap III adalah 36 sehingga untuk bagian ketiga penilaian pengelolaan resiko memiliki status tidak valid (Gambar 5).



Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

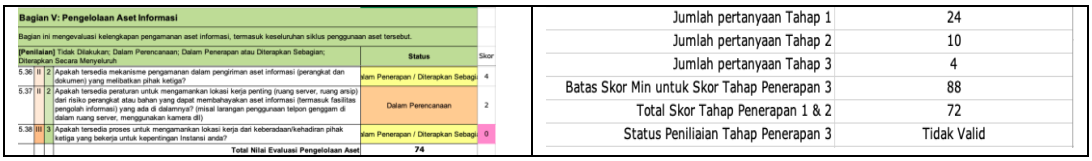
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penera

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
4,27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	lam Penerapan / Diterapkan Sebagi	0
4,28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Dalam Perencanaan	0
4,29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Dalam Perencanaan	0
			Total Nilai Evaluasi Kerangka Kerja	**58**	

Jumlah pertanyaan Tahap 1	12
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	7
Batas Skor Min untuk Skor Tahap Penerapan 3	64
Total Skor Tahap Penerapan 1 & 2	58
Status Peniliaian Tahap Penerapan 3	Tidak Valid

Gambar 5 Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian keempat adalah penilaian kerangka kerja pengelolaan keamanan informasi. Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (Kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Terdapat 29 pertanyaan, dan Pemkot Kediri memberikan jawaban 19 jawaban dalam penerapan/penerapan sebagian dan 10 pertanyaan dalam perencanaan, sehingga skor total adalah 58, sedangkan tahap I dan tahap II adalah 58. Skor minimum bagian keempat untuk kategori SE tinggi pada tahapan I dan II adalah 64. Sehingga Pemkot Kediri dapat dikategorikan tidak valid (Gambar 6)



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				Status	Skor
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	lam Penerapan / Diterapkan Sebagi	4
5.37	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Dalam Perencanaan	2
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	lam Penerapan / Diterapkan Sebagi	0
			Total Nilai Evaluasi Pengelolaan Aset	**74**	

Jumlah pertanyaan Tahap 1	24
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	4
Batas Skor Min untuk Skor Tahap Penerapan 3	88
Total Skor Tahap Penerapan 1 & 2	72
Status Peniliaian Tahap Penerapan 3	Tidak Valid

Gambar 6 Hasil Penilaian Pengelolaan Aset

Bagian kelima adalah pengeloaan aset. Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Terdapat 38 pertanyaan, dan Pemkot Kediri memberikan jawaban 27 jawaban dalam penerapan/penerapan sebagaian dan 11 pertanyaan dalam perencanaan. Total skor adalah 74 dan skor tahapan I dan tahapan II adalah 72. Skor minimum validasi untuk tahap III adalah 88. Sehingga Pemkot Kediri dapat dikategorikan tidak valid (Gambar 7).

Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

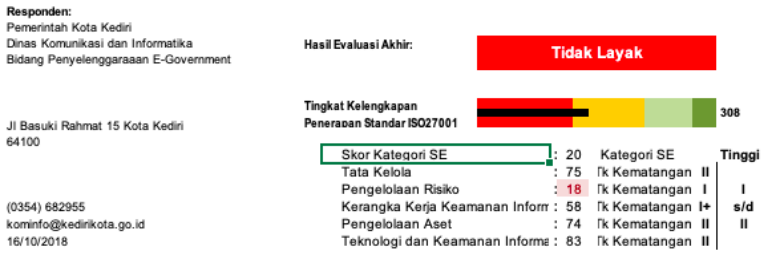
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
6.25	III	3	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	lam Penerapan / Diterapkan Sebagi	6
6.26	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	lam Penerapan / Diterapkan Sebagi	6
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**83**	

Jumlah pertanyaan Tahap 1	14
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	68
Total Skor Tahap Penerapan 1 & 2	71
Status Peniliaian Tahap Penerapan 3	Valid

Gambar 7 Teknologi Informasi

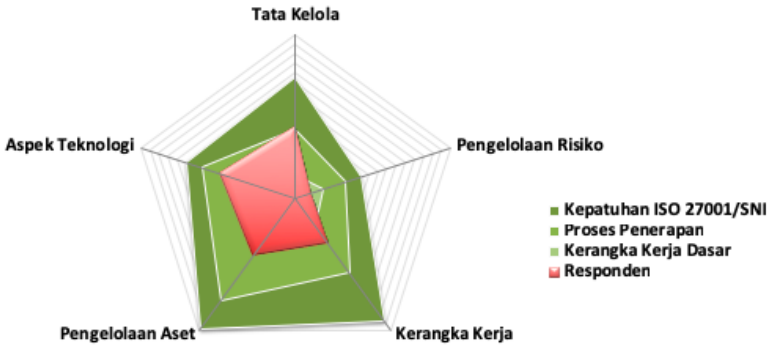
Bagian keenam adalah teknologi informasi, bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Terdapat 26 pertanyaan, dan Pemkot Kediri memberikan jawaban 3 jawaban sudah diterapkan keseluruhan, 22 jawaban dalam penerapan/penerapan sebagaian dan 1 pertanyaan dalam perencanaan. Total skor 83, skor untuk tahapan I dan tahapan II adalah 71. Skor minimum bagian keenam pada tahapan I dan II untuk validasi tahap III adalah 68. Sehingga Pemkot Kediri dapat dikategorikan valid (Gambar 8).

Rekapituasi dan pengolahan data hasil observasi dapat dilihat pada gambar 9 dibawah. Terlihat hasil penilaian dari indeks KAMI dari masing masing bagian. Skor kategori sistem elektronik (SE) adalah 20, untuk penilaian tata kelola skornya adalah 75, pengelolaan resiko skornya 18, kerangka kerja keamanan informasi nilainya 58, pengelolaan asset 74, dan penerapan teknologi keamanan dan informasi memiliki nilai 83 :



Gambar 8 Hasil Penilaian Indeks KAMI

Tingkat penerapan Sistem elektronik di Pemerintah Kota Kediri masuk dalam kategori tinggi, hal ini dilihat dari posisi kategori ada di kategori I dan II. Namun hasil evaluasi dengan kategori yang tinggi sistem elektronik di Pemkot ketegori mendapatkan hasil evaluasi yang tidak layak dengan nilai tingkat kelengkapan penerapan standar ISO 27001 di nilai 308.



Gambar 9 Radar hasil Sistem Managemen Keamanan Informasi

Gambar 10 menunjukkan hasil radar sejauh mana respon Pemkot Kediri (warna merah muda) terhadap penerapan system manajemen kemanan informasi (SMKI). Dari lima kategori terlihat aspek teknologi dan tata kelola lebih baik dibandingkan aspek pengelolaan resiko, pengelolaan asset, dan kerangka kerja.

SIMPULAN

Penerapan atau tingkat kematangan keamanan sistem di Pemerintah Kota Kediri masuk ke dalam katagori tidak layak, terutama di bidang pengelolaan resiko dengan nilai 18. Skor Maksimal dari Indeks KAMI ada-lah 588 dan Pemerintah Kota kediri bera-da di Skor 308. Dengan tingkat penggunaan Sistem Elektronik yang berada di level Tinggi. Dapat dikatakan sistem Keamanan yang digunakan di Pemerintah Kota Kediri tidak memadai.

DAFTAR PUSTAKA

[1] Noname, https://govcsirt.kominfo.go.id/wp-content/uploads/2018/02/statistik-2017_upload.pdf, Diakses 20 November 2018

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

[3] Harliana P, Perdana A, Prasetyo RMK: Sniffing dan Spoofing Pada Aspek Keamanan Komputer. https://www.academia.edu/5088063/JurnalKeamanan-Komputer, diakses pada 20 November 2018

[4] No Name, https://bssn.go.id/indeks-kami/ , diakses pada tanggal 20 November 2018

[5] Faturachman Husein, "Implementasi Indeks KAMI di Universitas Sam Ratulangi" , E-Journal Teknik Informatika Vol. 12 No. 1 (2017) ISSN: 2301-8364

[6] I Gede Putu Krisna Juliharta, "Investigasi Keamanan Aplikasi Teknologi Informasi dengan Teknik Packet Sniffing", Seminar Nasional Informatika Vol.1 No.2, Universitas Pembangunan Nasional "Veteran" Yogyakarta, 2016.

[7] I Gede Putu Krisna Juliharta, "Bussiness Impact Analysis Aplikasi Jaringan Komputer Dengan Teknik Packet Sniffing", Jurnal Sistem dan Informatika Vol. 10 No. 1 ISSN 2460:3732, STMIK STIKOM Bali, 2015

[8] Insecure.org. 2009. "Free Security Scanner For Network Exploration & Security Audits" diakses pada tanggal 20 oktober 2018