Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya

Firzah A Basyarahil, Hanim Maria Astuti, dan Bekti Cahyo Hidayanto
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jalan Arif Rahman Hakim, Surabaya 60111 Indonesia
e-mail: hanim@its-sby.edu bekticahyo@its-sby.edu

Abstrak— **DPTSI merupakan sebuah direktorat untuk menangani permasalahan teknologi informasi dan sistem informasi yang dimiliki oleh ITS. Menurut UU. No. 12 Tahun 12 Ttg. Perguruan Tinggi, misi mencari, menemukan, dan menyebarluaskan kebenaran ilmiah tersebut dapat diwujudkan apabila perguruan tinggi di kelola berdasarkan suatu Tata kelola perguruan tinggi yang baik (Good University Governance). Pengelolaan Informasi merupakan salah satu aspek dalam Good University Governance, termasuk kualitas dan keamanan pengelolaan informasi. Salah satu upaya yang dapat dilakukan untuk meningkatkan kualitas dari keamanan informasi, kementrian Kominfo membuat alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Penggunaan Indeks KAMI ini juga diikuti dengan penerapan ISO 27001 sebagai standar keamanan internasional yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif. Hasil dari penggunaan Indeks KAMI versi 3.1 di DPTSI ITS ini adalah tingkat ketergantungan penggunaan sistem elektronik sebesar 26 dari total skor 50 dan masuk kedalam kategori Tinggi dimana sistem elektronik adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 249 dari 645 dan berada pada kategori tidak layak. Dari hasil tersebut maka dibuat rekomendasi berdasarkan kontrol ISO 27002:2013 untuk pertanyaan-pertanyaan yang mendapat nilai kurang. Kemudian rekomendasi dari penelitian ini dapat dijadikan sebagai bahan pertimbangan dan evaluasi bagi pihak DPTSI ITS Surabaya dalam melakukan perbaikan yang berkaitan dengan mitigasi atau pencegahan kerentanan keamanan informasi, serta memastikan regulasi dapat dicapai dengan baik dan kebijakan keamanan institusi di masa yang akan datang.**.

***Kata Kunci*— Indeks KAMI, ISO 27001:2013, Keamanan Informasi, Manajemen Risiko.**

I. PENDAHULUAN

MENJAGA keamanan informasi berarti pula perlunya usaha dalam memperhatikan faktor-faktor keamanan dari seluruh piranti pendukung, jaringan, dan fasilitas lain yang terkait secara langsung maupun tidak langsung dalam proses pengolahan informasi [1]. Instansi pendidikan di Indonesia juga perlu menerapkan keamanan informasi untuk menghindari adanya pencurian data dan hilangnya data secara sengaja maupun tidak sengaja.

Hal ini juga perlu diterapkan dan diperhatikan di Institut Teknologi Sepuluh Nopemeber Surabaya. ITS membangun sebuah direktorat yang bernama DPTSI untuk menangani permasalahan teknologi informasi dan sistem informasi yang dimiliki. Semua kegiatan teknologi informasi dan sistem informasi dipusatkan dan dikembangkan di DPTSI ITS [2].

Data dari DPTSI menyatakan bahwa ditemukannya beberapa celah keamanan sistem informasi dan jaringan yang cukup berbahaya [3]. Gangguan keamanan informasi tersebut juga dirasakan oleh pihak civitas akademika ITS, seperti pembobolan data untuk Sistem Integra ITS dimana para mahasiswa tidak dapat login pada masing-masing akun yang dimiliki. Selain gangguan pada Sistem Integra ITS, hal serupa juga pernah terjadi untuk akun email ITS yang dibobol dan harus dilakukan reset password untuk menangani masalah tersebut.

Salah satu upaya yang dapat dilakukan oleh kementrian Kominfo untuk meningkatkan kualitas keamanan informasi pada suatu instansi adalah dengan membuat salah satu alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Indeks KAMI mengacu pada ISO 27001 yang berisi tentang keamanan informasi [4].

ISO 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi informasi dan pengelolaan aset yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif. Ada juga ISO 27002 yang berisi tentang kontrol keamanan yang dapat dijalankan oleh sebuah instansi yang telah mengimplementasikan ISO 27001. Hal ini termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas atas informasi yang dimiliki [1].

Pada tahun 2012 pernah dilakukan penerapan penilaian keamanan informasi dengan menggunakan indeks KAMI di DPTSI ITS [5]. Namun pada penelitian sebelumnya, hanya dilakukan pada sub bagian Keamanan & Jaringan saja dan tidak menyeluruh ke instansi yang bersangkutan [5],

sedangkan penerapan Indeks KAMI ini dilakukan untuk pengelolaan keamanan informasi di seluruh bagian instansi yang bersangkutan [6].

Penilaian keamanan informasi dengan menggunakan indeks KAMI hanya pernah dilakukan satu kali di DPTSI dan terbilang sudah cukup lama. Metode yang digunakan pada penilaian keamanan informasi DPTSI pada tahun 2012 juga menggunakan kuesioner penilaian (pertanyaan yang ada di Indeks KAMI) yang diisi oleh responden, sedangkan peneliti mencari temuan-temuan terkait dengan penilaian dan memastikan bahwa hasil temuan sesuai dengan nilai dari kuesioner tersebut. Setelah peneliti memastikan hasilnya, maka dilakukan pembenaran temuan sesuai dengan hasil kepatuhan [5].

Metode penilaian keamanan informasi pada penelitian kali ini akan dirubah, yaitu akan dilakukan penilaian oleh peneliti secara langsung. Peneliti akan mengumpulkan temuan-temuan pendukung untuk melakukan penilaian keamanan informasi sekaligus melakukan penilaian dengan mengisi nilai pada pertanyaan yang ada di Indeks KAMI.

Metode yang digunakan akan dirubah karena evaluasi ini dianjurkan untuk dilakukan oleh orang yang secara langsung bertanggung jawab & berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya [6]. Berhubung di DPTSI sendiri masih belum ada bagian khusus yang melakukan penilaian keamanan informasi menggunakan Indeks KAMI, maka tema ini akan diangkat menjadi sebuah penelitian dan peneliti sendiri yang akan melakukan penilain terhadap kelima area yang ada di Indeks KAMI.

Penilaian Indeks KAMI sebaiknya dilakukan secara periodik waktu tertentu sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu [7] [8]. Faktanya penilaian keamanan informasi di DPTSI terakhir kali dilakukan pada tahun 2012 dan belum dilakukan lagi sampai tahun 2016.

II. TINJAUAN PUSTAKA

A. *Keamanan Informasi*

Menurut Sarno dan Iffano, Keamanan informasi merupakan suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin akan timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resiko-resiko yang terjadi, dan mengoptimalkan pengembalian investasi. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing-kan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan (Sarno dan Iffano: 2009) [9].

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dalam sebuah organisasi. Jenis keamanan informasi dapat dibagi menjadi beberapa bagian berikut (Whitman & Mattord, 2013) [10]:

- Physical security
- Personal security
- Operational security
- Communications security
- Network security

B. *Sistem Manajemen Keamanan Informasi (SMKI)*

Sebuah organisasi harus menerapkan Sistem Manajemen Keamanan Informasi untuk menjamin keamanan aset teknologi informasi dan komunikasi (TIK). Sistem Manajemen Keamanan Informasi adalah kumpulan dari kebijakan dan prosedur untuk mengatur data sensitif milik organisasi secara sistematis. Tujuan dari SMKI sendiri adalah untuk meminimalisir risiko dan menjamin kelangsungan bisnis secara proaktif untuk membatasi dampak dari pelanggaran keamanan [11].

Sistem Manajemen Keamanan Informasi juga harus mengacu pada standar nasional atau internasional yang ada agar kualitas pengamanan yang diberikan tinggi dan mampu menanggulangi adanya masalah. Standar internasional yang telah direkomendasikan untuk penerapan SMKI adalah ISO/IEC 27001. Standar ini telah berjalan berbasis risiko sehingga mampu mengurangi ancaman dan menanggulangi masalah dengan cepat dan tepat [12].

C. *Manajemen Risiko Teknologi Informasi*

Manajemen risiko merupakan serangkaian aktivitas dalam menganalisis risiko. Risiko tersebut diidentifikasi, dinililai, dan selanjutnya disusun langkah strategis yang dapat digunakan dalam mengatasi risiko tersebut (Stoneburner, 2002) [13].

Tujuan utama dari dilaksanakannya manajemen risiko adalah memberikan pandangan terkait kemungkinan yang bisa terjadi sehingga perusahaan dapat menyusun langkah mitigasi dan evaluasi terkait risiko. Tahapan dalam manajemen risiko berdasarkan (Spremic, 2008) diantaranya [14]:

1. Mengidentifikasi dan mengklarifikasi risiko.
2. Setiap risiko dinilai.
3. Menyusun langkah penaggulangan risiko.
4. Pendokumentasian dan pengimplementasian dari langkah menanggulangi risiko.
5. Pendekatan portfolio risiko TI.
6. Monitoring berkala terhadap tingkat risiko TI dan audit.

Berikut ini adalah diagram alur dari proses manajemen risiko secara umum.

Gambar 1. Alur Manajemen Risiko (Budi,2013)

Pada alur proses pelaksanaan Manajemen Risiko, ketika memasuki tahapan penanganan atau aksi apa yang harus diambil, maka terdapat 4 pilihan penanganan terhadap risiko potensial tersebut, yaitu [15]:

1) Take

Jika risiko yang ada dirasakan cukup besar dan tidak dapat dihindari, maka perusahaan dapat mengalami dampak yang

mengganggu dan bersifat merusak secara alamiah dan seharusnya diambil tindakan take atau menerima risiko tersebut. Contoh risiko yang dapat ditangani dengan tindakan take adalah terjadinya bencana alam, yakni gempa bumi, banjir, badai, dan sebagainya. Sebab perusahaan tentunya tidak dapat melawan alam.

2) Treat

Jika risiko yang ada dirasakan dapat ditanggapi dengan tindakan untuk menurunkan tingkat risikonya, maka diambil tindakan Treat untuk mnegontrol risiko tersebut. Tindakan nyatanya adalah dengan menerapkan kontrol atau mitigasi terhadap risiko yang ada sehingga risiko tersebut dapat diturunkan levelnya.

3) Terminate

Jika risiko yang ada dirasakan terlalu besar (misalnya dalam rangka membuat suatu produk IT baru), maka dapat diambil tindakan "Terminate" terhadap risiko tersebut, artinya kita harus menghindar dan tidak mau mengambil risiko dengan membuat produk IT baru tersebut, sehingga tindakan nyatanya adalah membatalkan rencana pembuatan produk IT tersebut.

4) Transfer

Jika risiko yang ada dianggap akan lebih baik jika dialihkan ke pihak lain yang sesuai dengan bidang ahlinya, misalnya ke pihak asuransi, maka dapat diambil tindakan Transfer terhadap risiko tersebut.

D. ISO/IEC 27001 sebagai Standar SMKI

ISO 27001 ini merupakan sebuah standar yang dikeluarkan oleh International Organization for Standardization. ISO 27001 ini merupakan standar yang ditujukan dapat membantu perusahaan dalam melindungi keamanan aset perusahaan dan untuk melindungi sistem manajemen keamanan informasi (SMKI) [16].

SMKI merupakan sebuah pendekatan yang bersifat sistematis yang bertujuan untuk mengelola informasi penting maupun informasi perusahaan yang bersifat sensitif agar tetap aman. SMKI ini juga memberikan panduan untuk mengelola unsur yang termasuk dalam melakukan pengelolaan informasi penting seperti manusia, proses dan sistem Teknologi Informasi dengan menerapkan proses manajemen risiko yang telah sesuai standar.

E. Indeks Keamanan Informasi (KAMI) versi 3.1 sebagai Tools SMKI

Indeks KAMI versi 3.1 adalah sebuah tools yang digunakan untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan ISO/IEC 27001:2013 dan gambaran tata kelola keamanan informasi di sebuah organisasi. Indeks KAMI ini dibuat oleh pihak kementrian Kominfo [4]. Alat evaluasi ini tidak digunakan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat yang untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pemimpin instansi [6].

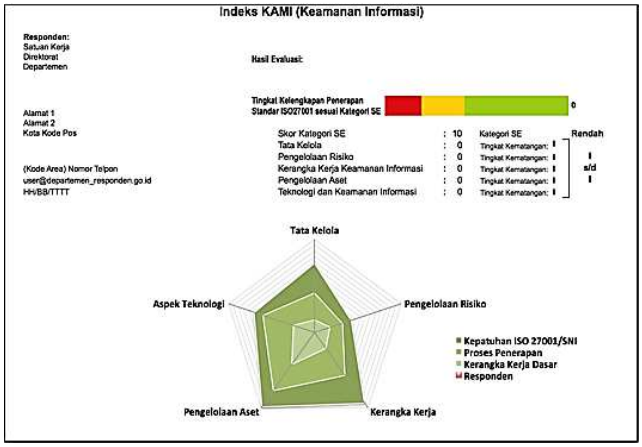
Alat evaluasi Indeks KAMI dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. Evaluasi yang dilakukan dengan menggunakan indeks KAMI ini mencakup 5 target area, yaitu [6] tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, dan teknologi & keamanan informasi.

Sebelum dilakukan proses penilaian secara kuantitatif, maka dilakukan proses klasifikasi terlebih dahulu terhadap kategori Sistem Elektronik. Responden diminta untuk mendeskripsikan Sistem Elektronik yang ada dalam satuan kerjanya secara singkat [6]. Tujuan dari penilaian kategori Sistem Elektronik ini adalah untuk mengelompokkan instansi kedalam ukuran tertentu yang akan ditampilkan dalam Gambar 2 [8] :

Rendah	
10	15
Tinggi	
16	34
Strategis	
35	50

Gambar 2. Nilai Kategori Sistem Elektronik

Setelah menklasifikasikan Peran SE di instansi terkait, maka akan dilakukan penilaian terhadap kelima area yang ada di Indeks KAMI versi 3.1. Hasil penilaian menggunakan Indeks KAMI versi 3.1 akan digambarkan kedalam diagram yang berbentuk jaring laba-laba (*spider chart*) dengan 5 area utama. Dalam jaring laba-laba tersebut juga akan dilihat tentang nilai Indeks KAMI dengan kepatuhan terhadap ISO/IEC 27001:2013 [8]. Hasil evaluasi menggunakan indeks KAMI versi 3.1 dapat dilihat melalui Gambar 3 :



Gambar 3. Dashboard Penilaian Indeks KAMI 3.1

Semakin tinggi ketergantungan sebuah instansi terhadap Peran SE, maka semakin banyak bentuk pengamanan yang diperlukan dan harus diterapkan sampai tahap tertinggi. Pada Gambar 4 dibawah ini akan menunjukkan skor akhir yang

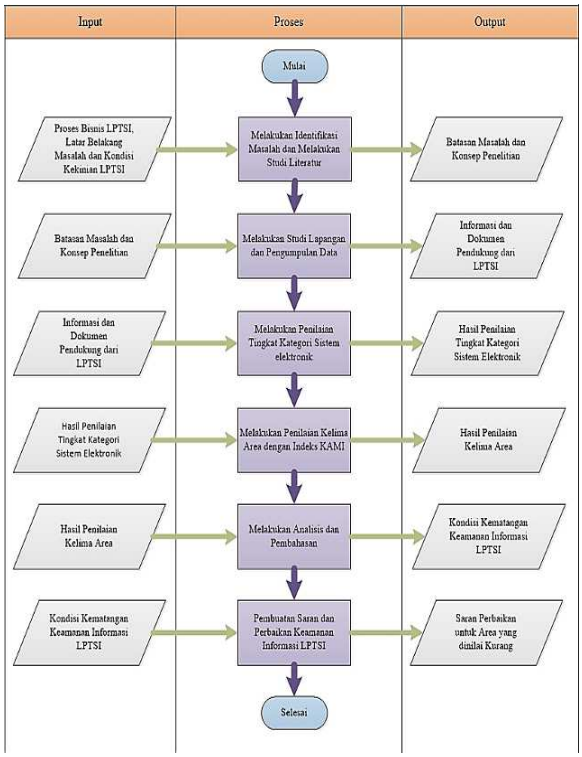
akan disesuaikan dengan status kesiapan instansi terkait mengenai keamanan informasinya [6].

KATEGORI SISTEM ELEKTRONIK				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	535	Cukup
		536	645	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	272	Tidak Layak
		273	455	Perlu Perbaikan
		456	583	Cukup
		584	645	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak Layak
		334	535	Perlu Perbaikan
		536	609	Cukup
		610	645	Baik

Gambar 4. Matriks Kategori SE dan Status Kesiapan Indeks KAMI 3.1

III. METODOLOGI

Pada bagian ini akan dijelaskan mengenai metodologi dalam melakukan penelitian, sehingga langkah-langkah pengerjaan menjadi lebih sistematis dan terorganisir lebih rapi. Berikut ini merupakan tahapan metodologi pengerjaan penelitian yang dilakukan:



Langkah-langkah yang dapat dilakukan untuk melakukan penelitian ini adalah sebagai berikut:

A. Melakukan Identifikasi Masalah & Studi Literatur
B. Melakukan Studi Lapangan & Pengumpulan Data dengan cara wawancara, observasi, dan review dokumen
C. Melakukan Penilaian Tingkat Kategori Sistem Elektronik
D. Melakukan Penilaian Kelima Area dengan Indeks KAMI
E. Melakukan Analisis dan Pembahasan
F. Pembuatan Saran dan Perbaikan berdasarkan ISO/IEC 27002:2013

IV. HASIL DAN PEMBAHASAN

A. Hasil Nilai Kepentingan Pengguna Sistem Elektronik di DPTSI ITS Surabaya

Dari hasil penilaian tingkat kepentingan penggunaan Sistem Elektronik di Direktorat Pengembangan Teknologi dan Sistem Informasi ITS telah didapatkan skor sebesar 26, sehingga dapat masuk kedalam kategori Tinggi sesuai dengan tabel tingkat kematangan Indeks KAMI dimana kategori **Tinggi** berkisar antara skor 16 sampai dengan 34.

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
	[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis	Status	Skor
#	Karakteristik Instansi		
1,1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar	C	1
1,2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar	B	2
1,3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional	B	2
1,4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik [A] Algoritma khusus yang digunakan Negara	C	1
1,5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna	A	5

Gambar 5. Hasil Penilaian Penggunaan Sistem Elektronik DPTSI ITS

Maksud dari kategori Tinggi disini yaitu kepentingan penggunaan sistem elektronik di DPTSI merupakan bagian yang tidak dapat terpisahkan dari proses kerja yang berjalan. Penggunaan sistem elektronik ini mendapat nilai ynag lumayan tinggi karena kewajiban kepatuhan terhadap Peraturan atau Standar Nasional, pengguna sistem elektronik juga lebih dari 5000 pengguna, keterhubungan data pribadi yang diolah terkait dengan data pribadi lainnya, dan dampak dari kegeglannya juga dapat berdampak pada tidak tersedianya layanan publik berskala nasional.

Menurut kepentingan penggunaan Sistem Elektronik di DPTSI ITS, maka hasil dari penilaian kelima area Indeks KAMI selanjutnya harus mendapatkan nilai diatas 583 untuk mendapatkan status Baik.

B. Menilai Kesiapan 5 Area Keamanan Informasi di DPTSI ITS Surabaya

Dalam penilaian kelima area tersebut akan terdapat beberapa warna yang berbeda dalam tabel penilaian. Warna tersebut menunjukkan tingkatan yang berbeda. Tabel 1 berikut akan berisikan keterangan dari tingkatan warna yang terdapat dalam penilaian lima area Indeks KAMI:

Tabel 1. Penjelasan Tingkatan Warna dalam Penilaian Indeks KAMI

`	Tingkat Kematangan Keamanan II
	Tingkat Kematangan Keamanan III
	Tingkat Kematangan Keamanan IV
	Tingkat Kematangan Keamanan V
Kategori Pengamanan	Kategori Kematangan Pengamanan I
	Kategori Kematangan Pengamanan II
	Kategori Kematangan Pengamanan III

Status Pengamanan		Tidak Dilakukan
		Dalam Perenanaan
		Dalam Penerapan/ Diterapkan Sebagian
		Diterapkan Secara Menyeluruh

Setiap kategori pertanyaan memiliki nilai skor yang berbeda. Gambar 6. berikut adalah pemetaan skor Indeks KAMI berdasarkan masing-masing kategori:

	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 6. Hasil Pemetaan Skor Indeks KAMI

Berikut adalah salah satu contoh tabel dari penilaian dengan menggunakan Indeks KAMI yang telah dilakukan pada DPTSI ITS

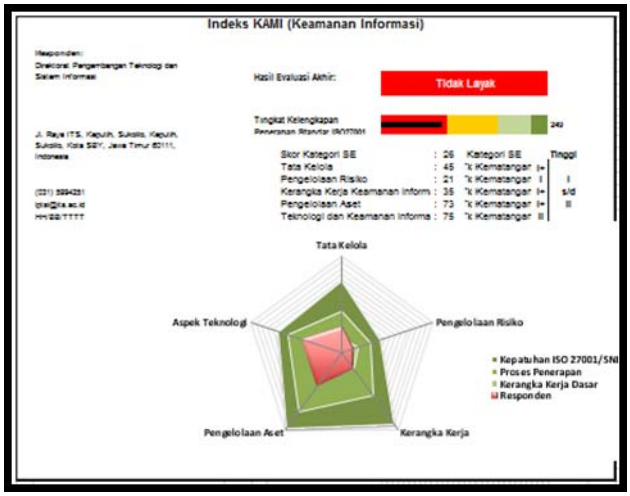
Tabel 2. Hasil Penilaian Tata Kelola Keamanan Informasi

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			**Status**	Skor
#	**Fungsi/Instansi Keamanan Informasi**			
2,1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Diterapkan Secara Menyeluruh	3
2,2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
2.22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan	0
			Total Nilai Evaluasi Tata Kelola	**45**	

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Tata Kelola yaitu 48. Didapat bahwa jumlah skor pada tahap penerapan 1 dan 2 adalah 45 sehingga dapat disimpulkan skor tidak melebihi Tahapan Penerapan 3. Maka dari itu bagian Tata Kelola disimpulkan masih menduduki Tingkat Kematangan I+.

c. Analisis Hasil Akhir Penilaian Indeks KAMI

Bagian ini akan menjelaskan hasil dari penilaian indeks KAMI pada Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya. Berikut ini adalah tampilan dari dashboard indeks KAMI yang dihasilkan:



Gambar 7. Hasil Dashboard Indeks KAMI DPTSI ITS

Dashboard diatas merupakan gambaran secara keseluruhan dari penilaian yang telah dilakukan dengan menggunakan indeks KAMI versi 3.1. Dari dashboard diatas, dapat dilihat bahwa tingkat kematangan keamanan informasi di DPTSI ITS Surabaya masih sangat kurang, yaitu tingkat II dengan nilai sebesar 249. Dapat dilihat pada radar chart dashboard tersebut bahwa hampir seluruh area yang dinilai dalam indeks KAMI belum terpenuhi dan sesuai dengan ISO 27001. Jika dilihat dibagian radar chart dashboard, hasil yang didapat hanya sebatas sampai kategori kerangka kerja dasar dan sebagian pada proses penerapan.

Gambar 8. Hasil Evaluasi Indeks KAMI di DPTSI ITS Surabaya

Untuk tingkat kematangan setiap area yang telah dinilai dalam indeks KAMI versi 3.1 masih sangat kurang. Berikut ini adalah uraian dari tingkat kematangan kelima area yang telah dinilai sebelumnya:

Tabel 3 Tingkat Kematangan Kelima Area

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

Urutan tingkat kematangan dari yang terendah hingga yang tertinggi adalah I – V. Batasan minimal yang harus dicapai agar dapat melakukan sertifikasi ISO adalah III+, sedangkan untuk saat ini tingkat kematangan dari DPTSI ITS Surabaya hanya dibatas I - II. Tingkat kematangan ini menunjukkan posisi DPTSI ITS Surabaya sebagai berikut ini:

Tabel 4. Tingkatan Kondisi DPTSI ITS

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

D. Saran Perbaikan 5 Area Keamanan Informasi

Setelah melakukan penilaian dengan indeks KAMI versi 3.1 dan mengetahui hasil dari setiap area yang terdapat dalam indeks KAMI versi 3.1, maka tahap selanjutnya adalah membuat saran perbaikan pada setiap bagian yang masih kurang baik. Berikut ini adalah saran perbaikan yang dibuat per masing-masiang area yang ada dengan tabel berisikan pertanyaan, status, nilai, dan saran perbaikan.

Tabel 5. Saran Perbaikan Sesuai ISO 27002:2013

No	Pertanyaan	Status	Nilai
2,4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan	0
	Saran Perbaikan **Control 12.1.3 Capacity management** Alokasi sumber daya harus dipantau dan diproyeksikan untuk menyesuaikan dengan kebutuhan dimasa mendatang. Kebutuhan kapasitas harus diidentifikasi dengan mempertimbangkan kekritisan bisnis dari sistem yang bersangkutan. Untuk proyeksi kebutuhan kapasitas dimasa mendatang juga dapat mempertimbangkan persyaratan sistem baru dan tren saat ini dan diproyeksikan dalam kemampuan pemrosesan informasi organisasi. Menyediakan kapasitas yang cukup juga dapat dicapai dengan meningkatkan kapasitas atau dengan mengurangi permintaan dengan cara: - Menghapus data yang sudah usang (*disk space*) - Dekomisioning aplikasi, sistem, dan database - Mengoptimalkan proses pengelompokan dan penjadwalan - Mengoptimalkan penggunaan logika aplikasi dan *query* database - Membatasi bandwidth untuk layanan yang tidak penting terkait bisnis (misal *streaming* film dan video) Dibuat dokumen terkait rencana pengelolaan kapasitas yang harus mempertimbangkan sistem yang penting/ kritis.		
2,5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan	0
	Saran Perbaikan **Control 16.1.2 Reporting information security events** Untuk segregasi kewenangan harus diurus agar tidak ada satu orang yang dapat mengakses, memodifikasi, atau menggunakan aset tanpa adanya otorisasi. Jika sulit untuk memisahkan kewenangan, maka dapat menerapkan kontrol lain seperti melakukan monitoring kegiatan, melakukan audit dan pengawasan manajemen. Segregasi kewenangan ini merupakan sebuah cara untuk mengurangi risiko penyalahgunaan terhadap aset organisasi. Dapat dibuat dokumen yang berisikan peran dari para pelaksana pengamanan informasi dan persyaratan terkait kewenangan masing-masing pihak.		

V. KESIMPULAN

Kesimpulan yang dapat diperoleh dari penelitian ini terkait penilaian manajemenen keamanan informasi di Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya dnegan menggunakan Indeks Keamanan Informasi (KAMI) adalah sebagai berikut:

1. Hasil dari penilaian tingkat penggunaan Sistem Elektronik adalah sebesar 26 dari jumlah total keseluruhan sebesar 50. Hal ini menunjukkan bahwa DPTSI ITS Surabaya sudah tinggi dalam kebutuhan penggunaan sistem elektronik yang artinya penggunaan sistem elektronik adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan
2. Hasil keseluruhan dari penilaian kelima area dalam Indeks KAMI adalah sebesar 249 dari jumlah total

keseluruhan sebesar 645 dan berada pada level I-II dimana level ini masih berada pada kondisi awal penerpan keamanan informasi dan kondisi penerapan kerangka kerja dasar penerapan keamanan informasi

3. Tingkat kematangan per-area akan dijabarkan sebagai berikut: Area Tata Kelola Keamanan Informasi berada pada tingkat I+, area Pengelolaan Risiko Keamanan Informasi pada tingkat I, area Kerangka kerja Pengelolaan Keamanan Informasi pada tingkat I+, area Pengelolaan Aset Informasi pada tingkat I+, dan area Teknologi & Keamanan Informasi pada tingkat II.
4. Poin nilai paling tinggi yang diperoleh dari kelima area tersebut adalah pada area Teknologi & Keamanan Informasi dengan nilai 75 poin. Poin ini diperoleh karena dari 26 pertanyaan, terdapat 6 pertanyaan yang tidak dilakukan dan 2 pertanyaan yang diterapkan sebagian. Untuk 18 pertanyaan yang lain sudah diterapkan secara keseluruhan oleh pihak DPTSI ITS Surabaya
5. Poin nilai paling rendah yang diperoleh dari kelima area tersebut adalah pada area Pengelolaan Risiko Keamanan Informasi dengan nilai 24 poin. Poin ini diperoleh karena dari 16 pertanyaan, terdapat 10 pertanyaan yang tidak dilakukan dan 6 pertanyaan yang lain sudah diterapkan secara keseluruhan oleh pihak DPTSI ITS Surabaya
6. Hasil penilaian kelima area yang menunjukkan nilai sebesar 252, dengan hasil nilai tingkat penggunaan sistem elektronik sebesar 26 maka DPTSI ITS Surabaya belum dapat dikatakan matang dan sesuai dengan standar ISO 27001:2013 karena belum mencapai level III+ dimana penerapan keamanan informasi telah terdefinisi dan konsisten.

DAFTAR PUSTAKA

[1] "Keamanan Informasi," 04 09 2012. [Online]. Available: https://keamananinformasi.wordpress.com/2012/09/04/definis-keamanan-informasi/. [Accessed 10 09 2016].

[2] "LPTSI," ITS, 2016. [Online]. Available: http://lptsi.its.ac.id/?page_id=150. [Accessed 11 09 2016].

[3] A. Affandi, "Memorandum Akhir Jabatan Ketua LPTSI ITS," LPTSI ITS, Surabaya, 2016.

[4] "Indeks Keamanan Informasi (KAMI)," Kementerian Komunikasi dan Informatika RI, 23 10 2013. [Online]. Available: https://kominfo.go.id/index.php/content/detail/3326/Indeks-Keamanan-Informasi--KAMI-/0/kemanan_informasi. [Accessed 10 09 2016].

[5] L. Ulinnuha, Evaluasi Pengelolaan Keamanan Jaringan di ITS Dengan Menggunakan Standar Indeks Keamanan Informasi (KAMI) Kemenkominfo RI, Surabaya: Sistem Informasi ITS, 2013.

[6] T. D. K. Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik," Jakarta, Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, 2012, pp. 34 - 58.

[7] K. K. d. Informasi, Writer, Indeks KAMI versi 2.3. [Performance]. 2012.

[8] K. K. d. Informasi, Writer, Indeks KAMI versi 3.1. [Performance]. 2015.

[9] S. R and I. I, "Sistem Manajemen Kemananan Informasi," 2009.

[10] W. M and M. H, Principles of Information Security Fifth Edition, Boston: Cengage Learning, 2014.

[11] M. Rouse, "Information Security Management System (ISMS)," 2011. [Online]. Available: http://whatis.techtarget.com/definition/information-security-management-system-ISMS. [Accessed 5 Oktober 2016].

[12] "Mengenal Sistem Manajemen Keamanan Informasi," Lembaga Sandi Negara, 10 Desember 2015. [Online]. Available: http://www.lemsaneg.go.id/index.php/2015/12/10/mengenal-sistem-manajemen-keamanan-informasi/. [Accessed 5 Oktober 2016].

[13] S. G, Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce: National Institute of Standards and Technology, 2010.

[14] S. M, IT Governance and IT Risk Management Principles and Methods for Supporting 'Always-on'Enterprise Information Systems, 2010.

[15] M. T and A.-T. F, Corporate Risk Management 2nd Edition, 2008.

[16] ISO, "ISO?IEC 27001- Information Security Management," 2013. [Online]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. [Accessed 11 09 2016].