Jurnal CoreIT, Vol.4, No.2, Desember 2018
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X

Thoyyibah. T
Teknik Informatika, Universitas Pamulang
Jalan Surya Kencana No. 1 Pamulang – Tangerang Selatan Banten
dosen01116@unpam.ac.id

Abstrak **– Perguruan tinggi merupakan sebuah lembaga yang mengelola generasi penerus melalui berbagai data olahan yang tersimpan. Data yang tersimpan diolah menggunakan sebuah sistem yaitu sistem informasi akademik atau sering disebut pusat informasi sebagai pangkalan data. Sebuah sistem informasi seharusnya memiliki perlindungan agar terbebas dari berbagai ancaman dan bahaya. Dengan adanya permasalahan tersebut maka perlu evaluasi terhadap keamanan informasi yang ada. Evaluasi digunakan pada pangkalan data untuk mengetahui seberapa baik tingkat keamanan pada Sistem Informasi. Penelitian ini menggunakan metode pengumpulan data secara kuesioner yaitu indeks KAMI versi 3.1. berdasarkan ISO 27001:2013. Melalui penelitian ini juga dilakukan untuk menambah wawasan dan pengetahuan tentang keamanan pada Sistem Informasi. Hasil penelitian ini berupa skor pengukuran SE (Sistem Elektronik) pada sistem informasi akademik perguruan tinggi X adalah 22, yang termasuk kedalam kategori tinggi. Jumlah total semua skor dari 5 area indeks KAMI yang diiukur adalah 577, dengan arti bahwa indeks keamanan informasi pada pustipanda adalah cukup baik. Rincian area indeks KAMI sebagai berikut, Tata kelola III+, Pengelolaan Risiko IV+, Kerangka Kerja Keamanan Informasi II, Pengelolaan Aset III dan Teknologi dan Keamanan Informasi III. Hasil penilaian kelima area yang menunjukkan nilai sebesar 577, dengan hasil nilai tingkat penggunaan sistem elektronik sebesar 22 maka perguruan tinggi X sudah dapat dikatakan matang dan sesuai dengan standar ISO 27001:2013 karena sudah mencapai level IV+.**

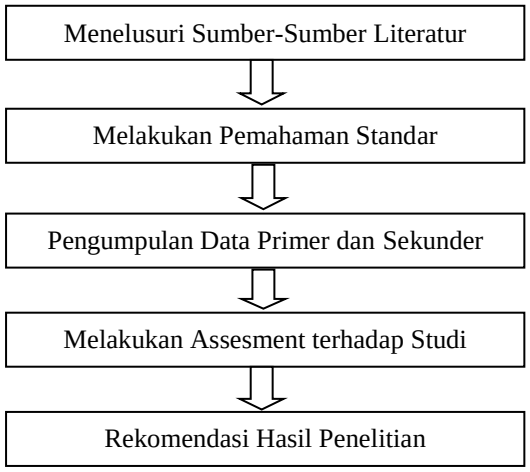
Kata Kunci – Indeks KAMI, ISO 27001:2013, Keamanan Informasi

PENDAHULUAN

Sistem merupakan suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan [1]. Sebuah sistem informasi biasanya sudah dirancang dengan memiliki perangkat pengamanan yang bertujuan untuk melindungi informasi yang terdapat didalam sistem informasi tersebut agar aman dan terbebas dari ancaman dan bahaya. Selain itu, keamanan sistem informasi juga digunakan untuk mendeteksi dan memperbaiki akibat dari segala kerusakan sistem. Pentingnya keamanan informasi kadang terabaikan dan baru disadari setelah terjadi bencana. Mengingat kerugian sebagai akibat dari sebuah serangan terhadap sistem informasi sangat besar, maka sistem manajemen informasi harus dapat melindungi kerahasiaan, integritas dan ketersediaan informasi [2]. Evaluasi terhadap keamanan sistem informasi dilakukan bertujuan untuk menjaga kesesuaian antara sistem manajemen keamanan informasi dan kebutuhan organisasi. Walaupun sebuah sistem informasi sudah dilengkapi dengan perangkat pengamanan tetap saja diperlukan adanya monitoring dan evaluasi. Evaluasi ini diperlukan karena mengingat ancaman serangan keamanan yang dapat terjadi kapan saja menyerang sistem informasi. Salah satu standar penilaian untuk sistem informasi manajemen keamanan informasi yang telah diakui secara internasional adalah ISO 27001:2013. Hasil evaluasi dengan menggunakan indeks KAMI yang mengacu pada ISO 27001:2013 dapat menunjukkan seberapa baik atau seberapa buruk keamanan informasi yang diterapkan oleh suatu organisasi atau perusahaan. Penerapan keamanan informasi juga diperlukan pada sebuah perguruan tinggi terutama di Indonesia guna menghindari pencurian data secara sengaja ataupun tidak sengaja [3].

METODE PENELITIAN

Metode penelitian pada Gambar 1 terdiri dari beberapa tahap yaitu menelusuri sumber-sumber informasi, melakukan pemahaman standar, pengumpulan data primer dan sekunder, melakukan *assesment* terhadap studi serta rekomendasi hasil penelitian. Metode penelitian yang digunakan penulis mengacu pada Evaluasi Keamanan Informasi Menggunakan Indeks KAMI SNI ISO/IEC27001:2009 Studi Kasus Perguruan Tinggi X [4].



HASIL DAN PEMBAHASAN

Indeks KAMI yang digunakan dalam penelitian ini adalah indeks kami versi 3.1. Tools ini digunakan untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan ISO/IEC 27001:2013 dan gambaran tata kelola kemanan informasi di sebuah organisai. Alat evaluasi indeks KAMI dianjurkan dilakukan oleh orang yang berwenang langsung untuk mengelola keamanan sistem informasi. Pada penelitian ini, kami mewawancarai staff data center Perguruan tinggi X.

Evaluasi yang dilakukan dengan menggunakan indeks KAMI mencakup 5 target area, yang terdiri dari tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, dan teknologi & keamanan informasi. Sebelum mengukur ke 5 target diatas, perlu dilakukan proses klasifikasi terhadap sistem elektronik pada organisasi. Tujuan dari klasifikasi ini adalah, untuk mengelompokan instansi kedalam ukuran nilai kategori sistem elektronik seperti Gambar 2 berikut :

Rendah	
10	15
Tinggi	
16	34
Strategis	
35	50

Gambar 2. Ukuran nilai kategori sistem elektronik

Dari hasil penilaian tingkat kepentingan penggunaan Sistem Elektronik di PT. X telah didapatkan skor sebesar 22, sehingga dapat masuk kedalam kategori Tinggi sesuai dengan tabel tingkat kematangan Indeks KAMI dimana kategori Tinggi berkisar antara skor 16 sampai dengan 34. Kategori ini menandakan kepentingan penggunaan sistem elektronik di PT. X merupakan bagian yang tidak dapat terpisahkan dari proses kerja yang berjalan. Semakin tinggi ketergantungan sebuah instansi terhadap Peran SE, maka semakin banyak bentuk pengamanan yang diperlukan dan harus diterapkan sampai tahap tertinggi.

Setelah tahap penilaian kategori sistem elektronik, kita dapat menilai kesiapan 5 area Keamanan Informasi di PT. X. Gambar 3 berikut adalah penjelasan tingkatan warna dalam penilaian indeks KAMI.

Gambar 3. Penilaian Indeks KAMI

Setiap kategori pertanyaan memiliki nilai skor yang berbeda. Gambar 4 berikut adalah pemetaan skor Indeks KAMI berdasarkan masing-masing kategori. Berikut adalahtable-tabel dari penilaian dengan menggunakan Indeks KAMI yang telah dilakukan. Pada Gambar 4 setiap kategori pertanyaan memiliki nilai skor yang berbeda.

	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 4. Kategori Pengamatan

A. Tata Kelola Keamanan Informasi

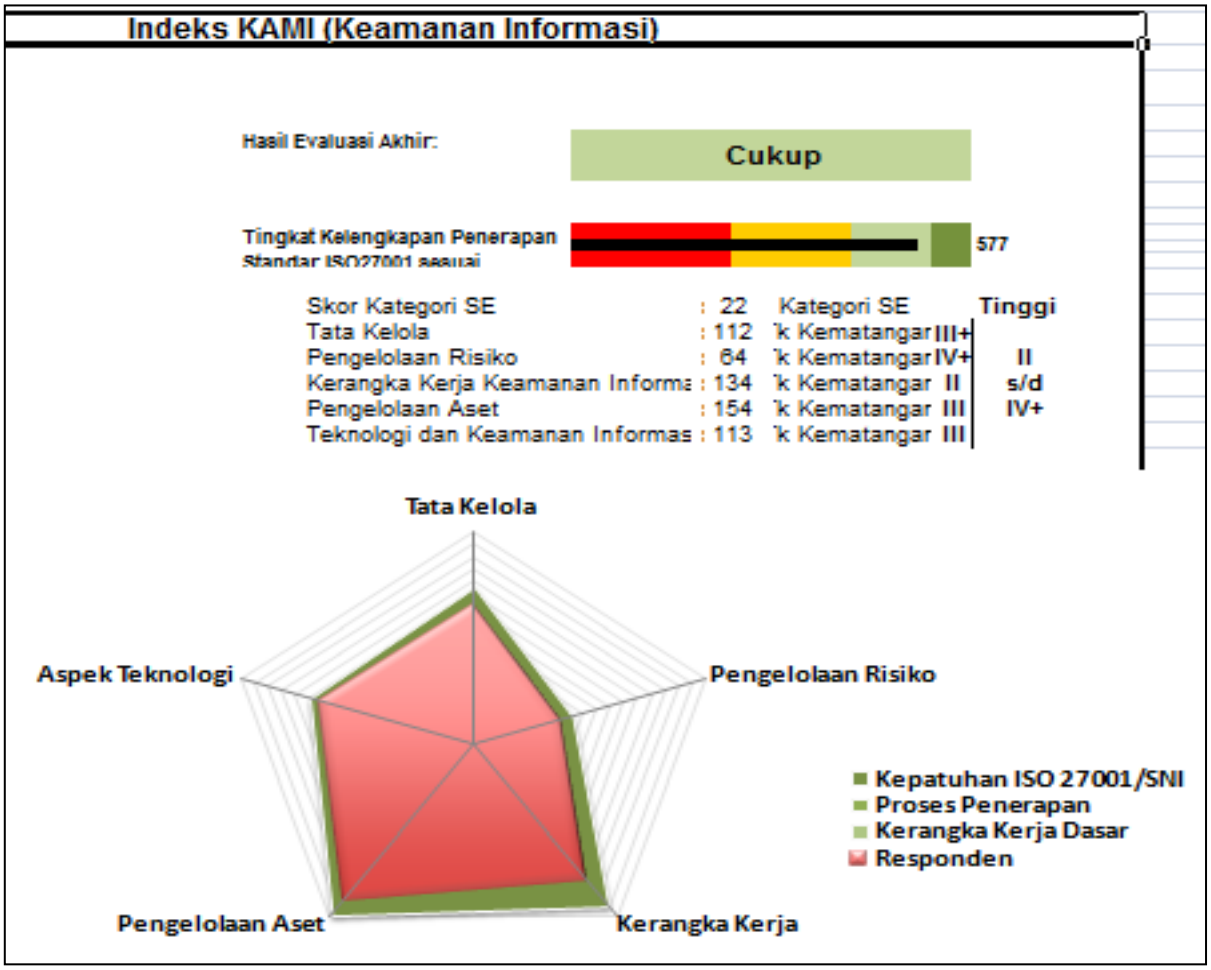
Berikut ini merupakan tabel penilaian tata kelola keamanan informasi pada PT. X. Total nilai evaluasi tatakelola sebanyak 112. Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta fungsi dan tanggung jawab keamanan informasi.

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**
#			**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
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
2,3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh
2,4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Perencanaan
2,5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Diterapkan Secara Menyeluruh
2,6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh
2,7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Diterapkan Secara Menyeluruh
2,8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Diterapkan Secara Menyeluruh
2,9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Diterapkan Secara Menyeluruh
2.11	II	2	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Diterapkan Secara Menyeluruh
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Diterapkan Secara Menyeluruh
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Penerapan / Diterapkan Sebagian
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Diterapkan Secara Menyeluruh
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Diterapkan Secara Menyeluruh
2.17	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Diterapkan Secara Menyeluruh
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Diterapkan Secara Menyeluruh
2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Penerapan / Diterapkan Sebagian
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?	Diterapkan Secara Menyeluruh
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?	Dalam Penerapan / Diterapkan Sebagian
2.22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Diterapkan Secara Menyeluruh
			Total Nilai Evaluasi Tata Kelola	**112**

Gambar 5. Hasil tata kelola keamanan informasi

B. Analisis Hasil akhir penilaian indeks KAMI

Gambar 6 menjelaskan hasil dari penilaian indeks KAMI pada PT X. Tampilan dari dashboard indeks KAMI yang dihasilkan yaitu skor kategori SE, tata kelola, pengelolaan resiko, kerangka kerja kemanan informasi, pengelolaan aset dan teknologi keamanan informasi.



Gambar 6. Hasil menggunakan indeks KAMI

Dari hasil ke-6 indeks KAMI diatas, dapat diambil kesimpulan bahwa keamanan sistem informasi pada sistem akademik PT. X berada pada tingkatan "cukup" dengan jumlah skor 577. Dapat dilihat pada radar *chart dashboard* tersebut bahwa hampir seluruh area yang dinilai dalam indeks KAMI sudah hampir terpenuhi dan sesuai dengan ISO 27001. Dari ke-5 klausal diatas rentang nilai kematangan indeks yaitu II s/d IV+.

KESIMPULAN DAN SARAN

Kesimpulan yang dapat diambil dari penelitian dengan menggunakan ISO 27001:2013 dengan indeks KAMI versi 3.1 diperoleh kesimpulan bahwa, sistem informasi pada PT. X sebagai berikut :

1. Hasil skor pengukuran SE (Sistem Elektronik) pada sistem informasi akademik perguruan tinggi PT. X adalah 22, yang termasuk kedalam kategori tinggi.
2. Jumlah total semua skor dari 6 area indeks KAMI yang diiukur adalah 577, dengan arti bahwa indeks keamanan informasi pada pustipanda adalah cukup baik.
3. Rincian area indeks KAMI sebagai berikut, Tata kelola III+, Pengelolaan Risiko IV+, Kerangka Kerja Keamanan Informasi II, Pengelolaan Aset III dan Teknologi dan Keamanan Informasi III.
4. Hasil penilaian kelima area yang menunjukkan nilai sebesar 577, dengan hasil nilai tingkat penggunaan sistem elektronik sebesar 22 maka PT. X sudah dapat dikatakan matang dan sesuai dengan standar ISO 27001:2013 karena sudah mencapai level IV+.
5. Perlunya pendokumentasian yang jelas (terdefenisi) terhadap kerangka kerja (kebijakan dan prosedur) keamanan informasi serta melakukan uji coba dan monitoring kerangka kerja keamanan secara berkelanjutan

REFERENSI

[1] Jogiyanto,HM. 2003. Sistem Teknologi Informasi, Yogyakarta: Andi

[2] Mokodompit, M. P., & Nurlaela, N. (2017). Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X). Jurnal Sistem Informasi Bisnis, 6(2), 97. https://doi.org/10.21456/vol6iss2pp97-104

[3] Basyarahil FA, Astuti HM, Hidayanto BC. (2017). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan informasi (KAMI) berdasarkan ISO/IEC27001:2013 Pada Direktorat Pengembangan Teknologi Sistem Informasi (DPTSI)ITS Surabaya. Jurnal Teknis ITS. Vol. 6 No. 1: 2337-3539.

[4] Afrianto I, Suryana T, Sufa'atin. (2015). Evaluasi Keamanan Informasi Menggunakan Indeks KAMI SNI ISO/IEC27001:2009 Studi Kasus Perguruan Tinggi X. Jurnal Ultima InFoSys. Vol. VI No. 1: 2085-4579.