ANALYSIS OF GOVERNANCE SECURITY MANAGEMENT INFORMATION SYSTEM USING INDEX KAMI IN CENTRAL GOVERNMENT INSTITUTION

Hambali, Purnawarman Musa
Magister Manajemen Sistem Informasi
Universitas Gunadarma
08mi071@gmail.com, p_musa@staff.gunadarma.ac.id

Abstract

Information security is very vulnerable to institutions if there is interference from other parties outside the organization or institution as a supply chain of services that can pose an information security risk. Based on the Regulation of the Minister of Communication and Information Technology number 4 of 2016, the Electronic System organizers that operate Low Electronic Systems must apply the Information Security Index guidelines. Index KAMI are a tool in analyzing and evaluating the level of information security based on the criteria in organizations or in government institutions. The research objective is to measure the level of information security readiness that meets the requirements of the ISO/IEC27001: 2013 standard at the Central Government Institution Unit X. The results of the assessment with the index KAMI obtained an electronic system category score of 30, for the assessment of governance the score is 84, the risk management score is 35, the framework information security work value is 61, asset management 128, and the application of security and information technology has a value of 100, the level of information security maturity is level II+ with a value of 408, the results obtained up to the Compliance of the Basic Framework.

***Keywords**: ISO / IEC 27001:2013, Index KAMI, Information Security.*

Abstrak

Keamanan informasi sangat rentan terjadi pada instansi jika ada campur tangan pihak lain diluar organisasi/institusi sebagai rantai pasok (*supply chain*) layanan yang dapat menimbulkan risiko keamanan informasi. Berdasarkan Peraturan Menteri Komunikasi dan Informatika nomor 4 tahun 2016, penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik rendah harus menerapkan pedoman Indeks Keamanan Informasi. Indeks KAMI merupakan alat bantu dalam menganalisa dan mengevalusi tingkat keamanan informasi di organisasi atau di institusi pemerintah. Tujuan penelitian adalah mengukur tingkat kesiapan keamanan informasi yang memenuhi persyaratan standar ISO/IEC 27001:2013 di Unit Kerja X Instansi Pemerintah Pusat. Hasil penilaian dengan indeks KAMI didapatkan skor kategori sistem elektronik adalah 30, untuk penilaian tata kelola dengan skor 84, pengelolaan resiko skornya 35, kerangka kerja keamanan informasi nilainya 61, pengelolaan aset 128, dan penerapan teknologi keamanan dan informasi memiliki nilai 100, tingkat kematangan keamanan informasi yaitu tingkat II+ dengan nilai sebesar 408, hasil yang didapat sampai Pemenuhan Kerangka Kerja Dasar.

Kata Kunci : ISO/IEC 27001:2013, Indeks KAMI, Keamanan Informasi.

1. Latar Belakang

Keamanan informasi merupakan salah satu hal penting saat ini, terutama terhadap organisasi yang menggunakan Teknologi Informasi (TI) sebagai pendukung proses bisnisnya. Dengan terbitnya Peraturan Menteri Komunikasi dan Informatika (Kominfo) nomor 4 tahun

2016 tentang Sistem Manajemen Pengamanan Informasi [1], maka keharusan untuk memiliki dan menerapkan SMKI lebih ditekankan kembali bagi pelayanan publik khususnya yang berkategori "Tinggi" dan "Strategis".

ISO/IEC 27001 merupakan standar SNI (Standar Nasional Indonesia) dalam mengelola keamanan informasi untuk semua organisasi di Indonesia oleh Badan Standarisasi Nasional (BSN) yang mencakup seluruh tipe organisasi, seperti perusahaan komersil, pemerintahan dan organisasi *non*-profit, bahkan semua ukuran dari bisnis mikro sampai multi-nasional. Standar ini bersifat indefenden terhadap produk TIK (Teknologi Informasi dan Komunikasi) yang tidak bergantung pada produk tertentu. ISO/IEC 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 sesuai dengan SNI. Ada pun ISO/IEC 27002 yang berisi tentang kontrol keamanan yang dapat dijalankan oleh sebuah instansi yang telah mengimplementasikan ISO/IEC 27001. Hal ini termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas atas informasi yang dimiliki [2].

Pusat Data dan Teknologi Informasi Instansi Pemerintah Pusat merupakan organisasi pemerintahan yang menggunakan TI untuk mendukung proses bisnisnya. Penggunaan TI di Unit Kerja X Instansi Pemerintah Pusat bertujuan untuk meningkatkan kualitas pelayanan yang diberikan kepada pihak internal Instansi Pemerintah Pusat maupun pihak eksternal Instansi Pemerintah Pusat. Bentuk dukungan keamanan informasi yang diterapkan Unit Kerja X adalah dengan adanya tata kelola TI dengan memasukkan unsur keamanan informasi agar risiko dan ancaman keamanan dapat dipetakan guna mengurangi atau menghindari risiko. Keamanan informasi merupakan aspek penting dari tata kelola organisasi, kinerja TI akan terganggu jika keamanan informasi mengalami masalah terkait kerahasiaannya, keutuhannya, dan ketersediaannya. Keamanan informasi secara tidak langsung akan mempengaruhi kegiatan operasional yang dilakukan Unit Kerja X Instansi Pemerintah Pusat. Oleh karena itu pentingnya organisasi dapat melindungi dan memelihara kerahasiaan, integritas, dan ketersediaan informasi dan untuk mengelola serta mengendalikan risiko keamanan informasi pada organisasi.

Salah satu tugas pokok Unit Kerja X Instansi Pemerintah Pusat sesuai adalah pengendalian mutu sistem dan teknologi informasi. Dalam pengendalian mutu sistem dan teknologi informasi, keamanan informasi merupakan salah satu unsur yang dievaluasi dalam rangka pelaksanaan pengendalian mutu sistem. Unit Kerja X akan menerapkan sertifikasi Sistem Manajemen Keamanan Informasi (SMKI) pada layanan publik. Sebelum melakukan penerapan sertifikasi SMKI pada layanan publik, akan dilakukan evaluasi internal atau pemantauan ulang dalam bentuk audit internal, kesenjangan operasional Klausul-klausul berdasarkan *assessment* ISO/IEC 27001:2013 yang berhubungan dengan SMKI sesuai persyaratan standar ISO/IEC 27001:2013 agar dapat mengantisifasi ancaman yang mengganggu keamanan informasi yang bersifat merusak dan dapat merugikan bisnis proses yang ada di lingkungan Instansi Pemerintah Pusat khususnya unit organisasi Unit Kerja X, seperti pelanggaran privasi dan pencarian informasi yang berorientasi *profit* (keuntungan). Penelitian ini juga dilakukan untuk menambah wawasan dan pengetahuan tentang keamanan pada Sistem Informasi.

Ada beberapa alat penilaian yang dapat digunakan untuk meningkatkan kualitas dari keamanan informasi, misalnya dengan menggunakan ISO 27001:2013, gabungan antara COBIT 4.1[3], ITIL v.3, dan Indeks KAMI [4]. Penelitian ini melakukan pengukuran tingkat keamanan informasi dengan menggunakan alat bantu yang telah dikembangkan oleh Kementerian Komunikasi dan Informasi (Kominfo) untuk mengukur tingkat kematangan dan

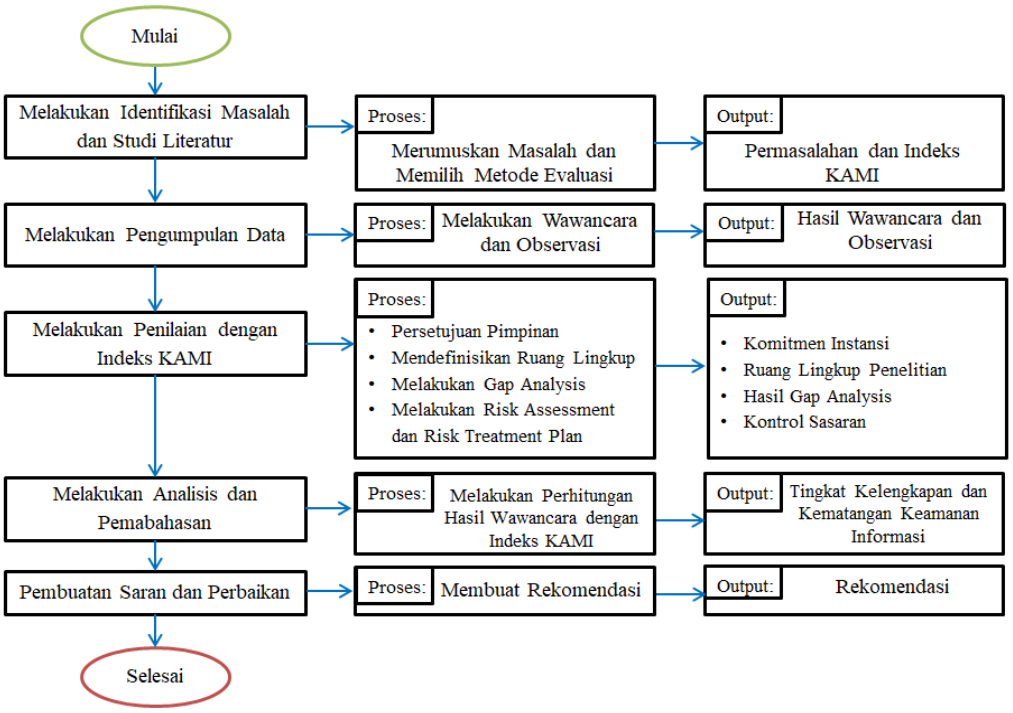
kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Hasil pengukuran dalam penelitian ini akan menghasilkan tingkat kematangan keamanan informasi di Unit Kerja X, yang nantinya akan dievaluasi dan digunakan sebagai referensi untuk meningkatkan tingkat keamanan informasi Instansi Pemerintah Pusat. Indeks KAMI mengacu pada standar ISO 27001 yang berisi tentang keamanan informasi [5].

Dasar penelitian yang mendasari dilakukkannya pengukuran tingkat keamanan informasi menggunakan Indeks KAMI yaitu Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektroknik (ITE), Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri KOMINFO No. 04 Tahun 2016 Pasal 10 tentang Sistem Manajemen Pengamanan Informasi.

Dalam melakukan penelitian terdapat beberapa referensi yang digunakan dalam evaluasi keamanan informasi ini. Salah satunya adalah "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya", yang ditulis oleh Firzah A Basyarahil dkk. Didalam penelitian tersebut hasil yang didapatkan bahwa keamanan informasi dari DPTSI ITS Surabaya berada dalam kategori tidak layak, dimana peneliti memberikan rekomendasi berdasarkan ISO 27001 untuk dijadikan bahan pertimbangan dan evaluasi kepada pihak DPTSI untuk melakukan perbaikan dalam keamanan informasi.

2. Metodologi Penelitian

Metodologi penelitian merupakan suatu kerangka dan asumsi yang ada dalam melakukan elaborasi penelitian sedangkan metode penelitian memerlukan teknik atau prosedur untuk menganalisa data yang ada [6]. Tahapan metodologi yang dilakukan untuk melakukan dapat dilihat pada gambar 1.



Gambar 1. Diagram Alir Penelitian

2.1 Melakukan Identifikasi Masalah dan Studi Literatur

Proses identifikasi masalah dapat dilakukan dengan mendeteksi permasalahan sistem manajemen keamanan informasi yang ada di Unit Kerja X. Setelah menemukan masalah

yang akan dijadikan topik penelitian, maka akan dilakukan pengambilan langkah untuk mengetahui lebih lanjut dengan melakukan observasi, membaca literatur atau studi literatur. Studi Literatur dilakukan dengan meninjau penelitian sebelumnya yang mana relevan dengan penelitian yang akan dilakukan serta mempelajari dan memahami teori-teori yang digunakan. Pada tahap ini dilakukan pencarian literatur berupa buku, jurnal, artikel, Peraturan Perundangan yang berlaku seperti Peraturan Menteri Kominfo nomor 4 tahun 2016 sebagai petunjuk teknis tentang Sistem Manajemen Keamanan Informasi.

2.2 Melakukan Pengumpulan Data

Pada tahap ini akan dilakukan pengumpulan data-data terkait dengan penelitian yang akan dikerjakan. Data yang didapat ini berasal dari Unit Kerja X Instansi Pemerintah Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI). Data yang akan diperoleh dengan melakukan wawancara dan observasi secara langsung adalah bukti pendukung berupa dokumen-dokumen yang dapat memperkuat pernyataan dari pihak yang diwawancara.

2.3 Melakukan Penilaian dengan Indeks KAMI

Indeks KAMI versi 4.0 adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di Instansi Pemerintah yang bertujuan untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Penilaian pada area yang ada di Indeks KAMI versi 4.0 bertujuan untuk menentukan nilai kematangan dari keamanan informasi yang ada di Unit Kerja X. Secara garis besar, Tahapan penerapan penilaian SMKI dapat dengan indeks KAMI versi 4.0 digambarkan sebagai berikut [5]:

a. Persetujuan dari pimpinan terhadap rencana penerapan SMKI.
b. Mendefinisikan ruang lingkup, dapat meliputi: proses, layanan dan kegiatan Pusat Pengelolaan dan Layanan Portal WEB, Pusat Pengembangan Sistem Informasi, dan Pusat Infrastruktur Teknologi Informasi yang dilakukan pada Unit Kerja X Instansi Pemerintah Pusat.
c. Melakukan gap *analysis* yang bertujuan untuk membandingkan seberapa jauh persyaratan klausul-klausul ISO 27001 telah terpenuhi, baik aspek kerangka kerja maupun aspek penerapannya. *Gap Analysis* yang digunakan dalam penelitian ini adalah *checklist* Indeks KAMI untuk kegiatan *gap analysis* ISO 27001
d. Melakukan Risk Assessment dan Risk Treatment Plan

2.4 Melakukan Analisis dan Pembahasan

Pada tahap ini akan dilakukan analisis dan pembahasan dari hasil nilai yang didapatkan. Penarikan kesimpulan tentang kesiapan Unit Organisasi Unit Kerja X untuk keamanan informasi yang ada juga akan dilakukan pada tahap ini. Pengambilan keputusan juga belum berhenti pada tahap ini, karena masih ada tahap selanjutnya untuk memberikan saran perbaikan yang dapat dilakukan oleh pihak Unit Kerja X.

2.5 Pembuatan Saran dan Perbaikan

Setelah melakukan pembahasan dari hasil penilaian keamanan informasi di Unit Organisasi Unit Kerja X, maka akan diberikan saran perbaikan yang sesuai untuk Unit Kerja X. Saran perbaikan dapat berupa saran yang lebih cocok untuk meningkatkan nilai di semua area keamanan informasi di Unit Kerja X agar dapat memenuhi kesiapan dalam penerapan SMKI berdasarkan standar ISO/IEC 27001:2013.

3. Hasil dan Pembahasan

Analisis sistem manajemen keamanan informasi di Unit kerja X Instasi Pemerintah Pusat, menggunakan Indeks KAMI versi 4.0 terdapat 141 (seratus empat puluh satu) pertanyaan yang dibagi menjadi 6 (enam) bagian, dan terdapat area modul suplemen dengan 53 pertanyaan. Berikut adalah penjelasan hasil penilaian dari area indeks KAMI:

3.1 Peggunaan Sistem Elektronik di Unit Kerja X Instansi Pemerintah Pusat

Bagian pertama dari indeks KAMI adalah Penilaian kategori sistem elektronik, terdapat 10 (sepuluh) pertanyaan, Setiap pertanyaan akan mempunyai 3 kriteria penilaian, yaitu A dengan nilai 5, B dengan nilai 2, dan C dengan nilai 1. Hasil dari penilaian tingkat kepentingan penggunaan Sistem Elektronik di Unit kerja X Instansi Pemerintah Pusat didapatkan skor sebesar 30, sehingga dapat masuk ke dalam kategori tinggi sesuai dengan tabel tingkat kematangan Indeks KAMI dimana kategori **Tinggi** berkisar antara skor 16 sampai dengan 34, sebagai panduan penilaian dapat dilihat pada tabel 1 berikut ini:

Tabel 1 Korelasi Antara Kategori Sistem Elektronik

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

(Sumber: Buku Panduan Penerapan Indeks KAMI Kominfo, 2017)

3.2 Tata Kelola Keamanan Informasi

Penilaian Tata Kelola Keamanan Informasi yang ada pada Unit Kerja X Instansi Pemerintah Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Tata Kelola Keamanan Informasi sebesar 84 dari 22 pertanyaan dengan status tingkat kematangan II.

Tabel 2. Tingkat Kelengkapan Tata Kelola Keamanan Informasi

Kategori (Tahapan)	Pertanyaan Tata Kelola	Nilai
1	8	18
2	8	42
3	6	24
Total	22	84

Tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+, namun hasil tata kelola keamanan informasi hanya valid ditingkat kematangan II, yang artinya dalam kondisi tingkat Penerapan Kerangka Kerja Dasar (Aktif), pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

3.3 Pengelolaan Risiko Keamanan Informasi

Penilaian Pengelolaan Risiko Keamanan Informasi yang ada pada Unit Kerja X Instansi Pemerintah Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana

didapatkan total nilai evaluasi Pengelolaan Risiko Keamanan Informasi sebesar 35 dari total 71, dengan 16 pertanyaan dengan status tingkat kematangan I+.

Tabel 3. Tingkat Kelengkapan Pengelolaan Risiko Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Pengelolaan Risiko	Nilai
1	10	19
2	4	16
3	2	0
Total	16	35

Pada area Pengeloaan Risiko Keamanan informasi hanya valid ditingkat kematangan I+ yang artinya dalam kondisi awal (Reaktif), sudah adanya pemahaman mengenai perlunya pengelolaan keamanan informasi.

3.4 Kerangka Kerja Pengelolaan Keamanan Informasi

Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi yang ada pada Unit Kerja X Instansi Pemerintah Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Kerangka Kerja Pengelolaan Keamanan Informasi sebesar 61, dengan 29 pertanyaan dengan status tingkat kematangan II.

Tabel 4 Tingkat Kelengkapan Pengelolaan Kerangka Kerja Keamanan Informasi

Kategori Kontrol(Tahapan)	Pertanyaan Kerangka Kerja	Nilai
1	12	23
2	10	38
3	7	0
Total	29	61

Pada area Kerangka Kerja Keamanan informasi hanya valid ditingkat kematangan II yang artinya dalam kondisi tingkat Penerapan Kerangka Kerja Dasar (Aktif)), pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

3.5 Pengelolaan Aset Informasi

Penilaian Pengelolaan Aset Informasi yang ada pada Unit Kerja X Instansi Pemerintah Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Pengelolaan Aset sebesar 128, dengan 38 pertanyaan dengan status tingkat kematangan II.

Tabel 5 Tingkat Kelengkapan Pengelolaan Aset Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Pengelolaan Aset	Nilai
1	24	55
2	10	46
3	4	27
Total	38	128

Pada area Pengelolaan Aset informasi hanya valid ditingkat kematangan II yang artinya dalam kondisi tingkat Penerapan Kerangka Kerja Dasar (Aktif), pengamanan sudah

diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

3.6 Teknologi dan Keamanan Informasi

Penilaian Teknologi dan Keamanan Informasi yang ada pada Unit Kerja X Instansi Pemerintah Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Telnologi dan Keamanan Informasi sebesar 100, dengan 26 pertanyaan dengan status tingkat kematangan II.

Tabel 6. Tingkat Kelengkapan Teknologi dan Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Teknologi dan Keamanan Informasi	Nilai
1	14	35
2	10	50
3	2	15
Total	26	100

Pada area Teknologi dan Keamanan informasi hanya valid ditingkat kematangan II yang artinya dalam kondisi penerapan kerangka kerja dasar (Aktif), pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

3.7 Penilaian Area Modul Suplemen Pada Unit Kerja X Instansi Pemerintah Pusat

Untuk mengetahui kesiapan pengamanan dalam bentuk persentase pada Unit Kerja X Instansi Pemerintah Pusat dalam mengelola risiko di 3 (tiga) area modul suplemen yaitu Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur Awan dan Perlindungan Data Pribadi dapat dilihat pada tabel 7. Syarat pemenuhan kesiapan pengamanan pada modul suplemen adalah 100% semua area terpenuhi.

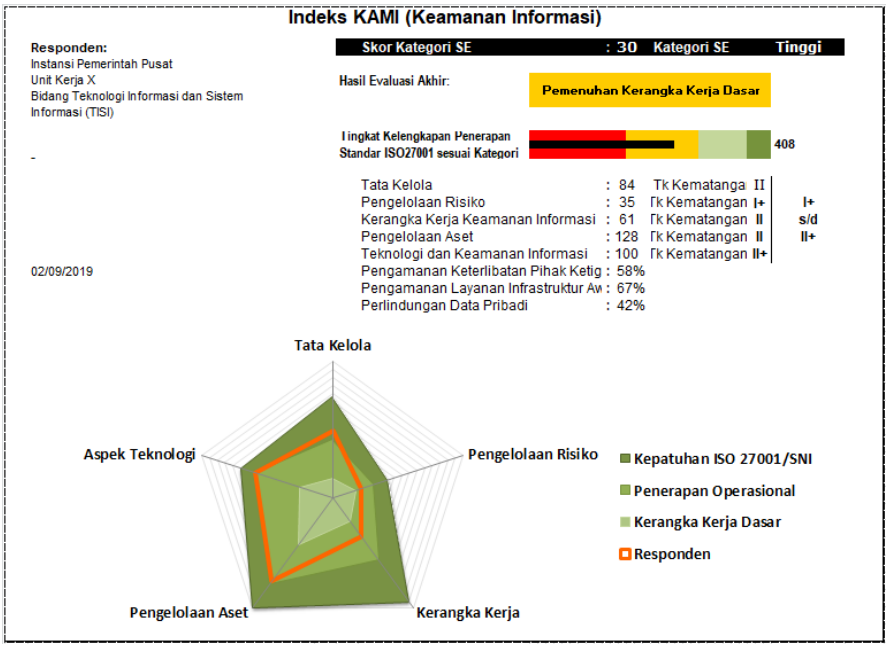
Tabel 7. Hasil Persentase Penilaian Area Modul Suplemen

Area Modul Suplemen	Pertanyaan Area Modul Suplemen	Nilai	Persentase
Pengamanan Keterlibatan Pihak Ketiga	27	1,74	58%
Pengamanan Layanan Infrastrukutur Awan	10	2	67%
Perlindungan Data Pribadi	16	1,25	42%

Pada modul suplemen area Pengamanan Keterlibatan Pihak Ketiga dengan nilai 1,74, jika dipersentasikan menjadi 58%, area Pengamanan Layanan Infrastruktur Awan dengan nilai 2, jika dipersentasikan menjadi 67%, dan area Perlindungan Data Pribadi dengan nilai 1,25, jika dipersentasikan menjadi 42%, diantara ke 3 (tiga) area modul suplemen tidak ada yang mencapai 100%, sehingga dapat disimpulkan bahwa Unit Kerja X Instansi Pemerintah Pusat belum memenuhi syarat kesiapan pengamanan pada modul suplemen karena nilai persentase masih berada di bawah 100%.

3.8 Analisis Hasil Akhir Penilaian Indeks KAMI

Gambaran secara keseluruhan dari penilaian yang telah dilakukan dengan menggunakan indeks KAMI versi 4.0 dapat dijelaskan bahwa tingkat kematangan keamanan informasi di Unit Kerja X Instansi Pemerintah Pusat yaitu tingkat II+ dengan nilai sebesar 408. Dapat dlihat pada *radar chart dashboard,* bahwa hampir seluruh area yang dinilai dalam indeks KAMI belum terpenuhi dan belum sesuai denga ISO 27001. Jika dilihat pada bagian *radar chart dashboard*, hasil yang didapat sampai Pemenuhan Kerangka Kerja Dasar.



Gambar 2. *Dashboard* Hasil Indeks KAMI Unit Kerja X Instansi Pemerintah Pusat

Nilai yang didapatkan masih dikatakan tahap Pemenuhan Kerangka Kerja Dasar karena nilai yang dicapai tidak sesuai dengan kepentingan penggunaan sistem elektronik yang digunakan pada Unit Kerja X Instansi Pemerintah Pusat, yaitu mencapai tingkat **Tinggi**. Untuk tingkat kematangan setiap area yang telah dinilai dalam indeks KAMI versi 4.0 masih kurang. Berikut ini adalah uraian dari tingkat kematangan kelima area yang telah dinilai sebelumnya:

Tabel 8. Tingkat Kematangan Kelima Area

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

Tingkat kematangan dari yang terendah hingga yang tertinggi adalah I – V. Batasan minimal yang harus dicapai agar dapat melakukan sertifikasi ISO 27001 adalah III+, sedangkan untuk saat ini tingkat kematangan dari Unit Kerja X hanya dibatas I+ - II+, dan tingkat keamanan sistem informasi berada pada tingkat "Penerapan Kerangka Kerja Dasar".

Setelah melakukan penilaian dengan indeks KAMI versi 4.0 dan mengetahui hasil dari setiap area yang terdapat dalam indeks KAMI versi 4.0, maka tahap selanjutnya adalah membuat rekomendasi berupa saran perbaikan pada area keamanan informasi setiap bagian yang memiliki hasil status penilaian masih kurang. Rekomendasi saran perbaikan pada area

tata kelola keamanan informasi, berisi saran perbaikan untuk pertanyaan yang memiliki nilai 0 (nol) atau statusnya tidak dilakukan oleh Unit Kerja X Instansi Pemerintah Pusat. Rekomendasi saran perbaikan mengacu pada ISO/IEC 27001:2013. Berikut ini adalah salah satu saran perbaikan yang dibuat per masing-masing area yang ada dengan tabel berisikan pertanyaan, status, kontrol ISO, dan saran perbaikan:

Tabel 9. Rekomendasi Saran Perbaikan Area Tata Kelola Keamanan Informasi

No	Pertanyaan	Status	Kontrol ISO
2.4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan	12.1.3
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 yang diproyeksikan dengan kemampuan pemrosesan informasi organisasi. Menyediakan kapasitas yang dapat menampung data dengan meningkatkan kapasitas atau dengan mengurangi permintaan dengan cara: - Menghapus data yang sudah usang (*disk space*) - Dekomisioning (menghentikan beroprasinya) aplikasi, sistem, dan database yang tidak digunakan lagi - 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) Membuat dokumen terkait rencana pengelolaan kapasitas yang harus mempertimbangkan sistem yang penting atau kritis.			

4. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan pada Instansi Pemerintah Pusat dengan Indeks KAMI versi 4.0 berdasarkan standar ISO 27001:2013 diperoleh kesimpulan sebagai berikut:

1. Hasil skor pengukuran SE (Sistem Elektronik) pada Instansi Pemereintah Pusat adalah 30 dari total skor 50, yang artinya peran dan tingkat kepentingan TIK termasuk kedalam kategori tinggi. Hasil penilaian kelima area yang yang telah dilakukan adalah sebesar 408, berada pada rentang tingkat kematangan level I+ - II+ dimana level ini berada pada kondisi Pemenuhan Kerangka Kerja Dasar penerapan keamanan informasi, yang artinya kondisi tingkat pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
2. Rincian area indeks KAMI sebagai berikut, Tata kelola II skor 84, Pengelolaan Risiko I+ skor 35, Kerangka Kerja Keamanan Informasi II skor 61, Pengelolaan Aset II skor 128, dan Teknologi dan Keamanan Informasi II+ skor 100. Hasil skor area modul suplemen

pada 3 (tiga) area yaitu Pengamanan Keterlibatan Pihak Ketiga dengan nilai persentase 58%, Pengamanan Layanan Infrastruktur Awan dengan nilai persentase 67%, dan Perlindungan Data Pribadi dengan nilai persentase 42%, diantara ke 3 (tiga) area modul suplemen tidak ada yang mencapai 100%, sehingga dapat disimpulkan bahwa Unit Kerja X Instansi Pemerintah Pusat belum memenuhi syarat kesiapan pengamanan pada modul suplemen.

3. Perlunya pendokumentasian yang jelas (terdefenisi) terhadap kerangka kerja (kebijakan dan prosedur) keamanan informasi serta melakukan uji coba dan monitoring kerangka kerja keamanan secara berkelanjutan.
4. Status dan perkembangan kegiatan implementasi SMKI harus dikomunikasikan secara berkala kepada pimpinan agar setiap masalah yang memerlukan pengambilan keputusan pimpinan dapat diselesaikan secara cepat dan tepat.
5. Dengan adanya evaluasi menggunakan Indeks KAMI versi 4.0, memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi di Unit Kerja X, untuk menganalisis tingkat kesiapan pengamanan informasi, sehingga dapat dilakukan perbaikan yang tidak sesuai pada pertanyaan-pertanyaan di dalam Indeks KAMI berdasarkan standar ISO/IEC 27001:2013.

Daftar Pustaka

[1] Peraturan Menteri Komunikasi Dan Informatika Nomor 4 Tahun 2016 *Sistem Manajemen Pengamanan Informasi*. 8 April 2016. Menteri Komunikasi Dan Informatika. Jakarta.

[2] Basyarahil, F. A., Astuti, H. M., & Hidayanto, B. C. (2017). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. Jurnal Teknik ITS, 6(1), 116-121.

[3] Sari, P. K., & Nurshabrina, N. (2016). *Assessment of Information Security Management on Indonesian Higher Education Institutions*. In *Advanced Computer and Communication Engineering Technology* (pp. 375-385). Springer, Cham.

[4] Septanto, H. (2017). Penilaian Tata Kelola *Elearning* Kelas *Shift* Dengan Menggunakan Kriteria Standar Indeks KAMI Di STMIK Bina Insani Bekasi. 4(1), 67-72.

[5] Kementerian Komunikasi Dan Informatika RI. (2017). Panduan Penerapan SMKI Berbasis Indeks KAMI. Volume 1. Direktorat Jenderal Aplikasi Informasi. Bagian Keamanan Informasi. Jakarta.

[6] Zainal, A. (2007). Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi; Konsep, Teknik, dan Aplikasi.