ANALISIS DAN PERANCANGAN MANAJEMEN KEAMANAN INFORMASI PADA DIREKTORAT SISTEM INFORMASI UNIVERSITAS TELKOM DENGAN INDEKS KEAMANAN INFORMASI (KAMI) PADA AREA TATA KELOLA KEAMANAN INFORMASI, PENGELOLAAN RISIKO KEAMANAN INFORMASI DAN KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI

ANALYSIS AND DESIGN OF INFORMATION SECURITY MANAGEMENT IN THE DIRECTORATE OF TELKOM UNIVERSITY INFORMATION SYSTEMS WITH INFORMATION SECURITY INDEX (US) IN SECURITY GOVERNANCE AREA OF INFORMATION, RISK MANAGEMENT OF INFORMATION SECURITY AND INFORMATION FRAMEWORK FOR INFORMATION SECURITY MANAGEMENT

Dhuwi Ambar Wati[1], Avon Budiono[2], Rokhman Fauzi[3]

[1,2,3]Program Studi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

[1]dhuwiambar@student.telkomuniversity.ac.id [2]avonbudi@telkomuniversity.ac.id,

[3]rokhmanfauzi@telkomuniversity.ac.id

Abstrak – Pada era globalisasi digital Teknologi Informasi semakin pesat. Hal tersebut dapat mempermudah dan memperlancar Institusi dalam menjalankan tugas dan fungsinya. Institusi harus dapat menjaga keamanan asset informasi. Direktorat Sistem Informasi (SISFO) sudah menerapkan teknologi informasi untuk menunjang kegiatan dan pengolahan data setiap hari, namun informasi yang dimiliki belum dilindungi dengan baik. Maka akan muncul risiko keamanan informasi yang dapat mengancam keamanan asset informasi, sehingga perlu dilakukan evaluasi keamanan informasi pada Direktorat Sisfo. Standar yang digunakan dalam penelitian ini menggunakan Indeks Keamanan Informasi (KAMI) yang mengacu pada ISO 27001 yaitu alat evaluasi yang dapat menganalisa gambaran kondisi kesiapan progam kerja keamanan informasi. Hasil penilaian Indeks KAMI Direktorat Sisfo dengan Kategori Sistem Elektronik tergolong tinggi dan status kesiapan untuk area tata kelola, pengelolaan risiko dan kerangka kerja pengelolaan keamanan informasi berada pada level II dimana bernilai 111 dari 357 dimana merupakan kondisi dasar penerapan kerangka kerja dimana proses pengamanan berjalan tanpa dokumentasi atau dokumen resmi. Dan merupakan kondisi dasar penerapan kerangka kerja dimana proses pengamanan berjalan tanpa dokumentasi atau dokumen resmi. Direktorat Sisfo belum siap dalam penerapan sistem manajemen keamanan informasi sehingga Direktorat harus melakukan perbaikan dengan peningkatan kontrol keamanan yang terdokumentasi untuk penerapan sistem manajemen keamanan informasi yang efektif dan efisien.

Kata kunci : Indeks Keamanan Informasi (KAMI), ISO/IEC 27001, Tingkat Kematangan, Direktorat Sistem Informasi.

Abstract -- I*n the era of digital globalization, Information Technology is getting faster. This can facilitate and facilitate the Institution in carrying out its duties and functions. Institutions must be able to maintain the security of information assets. The Directorate of Information Systems (SISFO) has implemented information technology to support activities and data processing every day, but the information that is owned is not well protected. Then an information security risk will emerge that can threaten the security of information assets, so that it is necessary to evaluate information security at the Sisfo Directorate. The standard used in this study uses the Information Security Index (US) which refers to ISO 27001, an evaluation tool that can analyze the picture of the condition of information security work program readiness. The results of our assessment of the Sisfo Directorate with the Electronic System Category are high and the readiness status for the area of governance, risk management and information security management framework is at level II worth 111 from 357 which is the basic condition for implementing a framework where the security process runs without official documentation or documents. The Sisfo Directorate is not yet ready for the implementation of an information security management system so that the Directorate must make improvements with documented security control improvements for the implementation of an effective and efficient information security management system.*

Keywords: *Keamanan Informasi (KAMI) Index, ISO/IEC 27001, maturity level, Directorate Information Systems*

1) Pendahuluan

Perkembangan teknologi informasi pada era globalisasi digital saat ini semakin pesat. Pada pemanfaatan teknologi informasi kerawanan akibat pesatnya kemajuan dunia Teknologi Informasi dan Komunikasi (TIK) menyebabkan munculnya berbagai bentuk serangan dan insiden yang sering terjadi, diperkirakan banyak menggunakan serangan *Cyberspace* yang dapat menyerang komputer tentunya memberikan dampak kerugian bagi institusi maupun perusahaan.

Segala ancaman dan insiden yang terjadi mengakibatkan dibutuhkannya suatu keamanan informasi untuk melindungi informasi dan infrastruktur. Salah satu kebijakan yang dapat diambil oleh organisasi untuk mengatasi gangguan keamanan informasi adalah dengan menerapkan Sistem Manajemen Kemanan Informasi (SMKI). SMKI merupakan penerapan keamanan informasi terhadap asset informasi dari ancaman dan gangguan yang mungkin terjadi.pada kegiatan tata kelola keamanan informasi perlu dilakukan untuk mencegah kemungkinan risiko terjadi gangguan pada Institusi ataupun Instansi. Salah satu upaya untuk meningkatkan kualitas keamanan informasi pada Institusi maupun Instansi, Kementrian Dinas Komunikasi dan Informasi membuat alat bantu untuk mengetahui gambaran kondisi, tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Keamanan Informasi (KAMI). Indeks KAMI dibuat pada penerapan keamanan informasi pada Institusi maupun Instansi Pemerintahan dengan acuan ISO 27001. Dalam area keamanan informasi mengacu pada kerangka kerja standar internasional yaitu ISO 27001.

Direktorat Sistem Informasi (Direktorat Sisfo) merupakan sebuah Direktorat yang bertanggung jawab untuk mengelola data dan informasi yang ada pada Universitas Telkom. Direktorat Sisfo dibagi menjadi tiga unit yaitu Layanan Operasional Sistem Informasi (LOPSI), Infrastruktur dan Konten (INTEN), Riset dan Pengembangan Sistem Informasi (RISBANGSI). Data dan Informasi merupakan hal yang sangat berisiko dalam bidang keamanan informasi. Beberapa aplikasi telah berhasil diciptakan oleh Direktorat Sisfo, dan beberapa aplikasi tersebut diintegrasikan dengan sebuah sistem aplikasi yang bernama iGracias. Setelah melakukan observasi dan wawancara kepada Direktur Sisfo, Direktorat Sisfo belum mempunyai pengkajian mengenai keamanan informasi serta belum tersusunnya keragka kerja keamanan infoemasi. Oleh sebab itu dilakukan proses perancangan system manajemen keamanan informasi sebagai langkah awal untuk mengamankan informasi dengan memberikan gambaran kondisi keamanan informasi pada Direktorat Sisfo.

Indeks KAMI dapat digunakan mengevalyasi tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001 serta pada area tata kelola keamanan sistem informasi di suatu instansi pemerintah maupun Institusi. Yang dapat membantu institusi maupun Instansi dalam mencapai tujuan dan menghasilkan nilai tata kelola dan manajemen teknologi informasi yang efektif.

2) Landasan Teori

2.1 Keamanan Informasi

Keamanan informasi itu sendiri merupakan bentuk bagian yang harus dijalankan agar sistem tersebut terhindar dari segala ancaman dan risiko. Sistem Informasi harus mempunyai pengamanan dan pengendalian agar dapat meminimalisir terjadinya pencurian dan penyalahgunaan terhadap data data yang dapat merugikan sebuah organisasi Beragam ancaman mencakup berbagai jenis perilaku karyawan seperti ketidaktahuan karyawan, ketidakpatuhan, memberikan password kepada karyawan lain. Pada ancaman eksternal, yaitu virus. dan serangan *spyware, hacker,* dan penyusup di tempatmerupakan gambar sebuah struktur organisasi yang terdiri atas berbagai macam komponen pendukung dan relasinya.

2.2 Sistem manajemen Keamanan Informasi (SMKI)

Sistem manajemen Keamanan Informasi (SMKI) merupakan proses yang dibuat berdasarkan pendekatan resiko bisnis untuk merencanakan (*Plan*), memonitoring dan meninjau (*Check*), serta memelihara dan meningkatkan atau mengembangkan (*Act*) terhadap keamanan informasi perusahaan. SMKI sangat penting dalam pengelolaan informasi dalam perusahaan maupun organisasi. Keamanan informasi ditunjukan menjaga aspek kerahasiaan (*confidentiality*), keutuhan (*Integrity*), dan ketersediaan (*Availability*) dari informasi. Dalam penerapan keamanan informasi aspek SMKI dan teknologi keamanan informasi tidak dapat terpisahkan

Plan (merencanakan SMKI)	Menetapkan kebijakan SMKI, sasaran, proses, dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi.
Do (menerapkan dan menjalankan SMKI)	Menerapkan dan mengoperasikan kebijakan SMKI, control, proses, dan procedure-prosedure yang lainnya.
Check (memantau peninjauan ulang SMKI)	Mengukur kinerja proses terhadap kebijakan, sasaran, praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau ulang efektivitasnya.
Act (memelihara dan meningkatkan SMKI)	Melakukan perbaikan dan pencegahan, memanajemen tentang SMKI untuk mencapai peningkatan yang berkelanjutan.

Tabel 1 PDCA pada ISO/IEC 27001

2.3 *Information Security Awarness*

Kesadaran keamanan informasi berfungsi untuk menanamkan rasa tanggung jawab yang menangani dan mengelola system informasi, serta mengarahkan karyawan akan lebih peduli lingkungan pekerjaan mereka. Tujuan kesadaran keamanan informasi yaitu untuk meningkatkan keamanan dengan melakukan hal sebagai berikut:

1) Memahami dan bertanggung jawab terhadap system keamanan informasi.
2) Mengembangkan kemampuan terhadap keamanan informasi yang dapat melakukan pekerjaan mereka dengan aman.
3)Merancang,mengimplementasikan, mengoperasikan progam pembinaan kesadaran keamanan informasi untuk organisasi.

2.4 Indeks Keamanan Informasi (KAMI)

Indeks KAMI merupakan alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di Instansi pemerintah maupun organisasi, berdasarkan buku panduan yang dikeluarkan oleh Kementrian Informasi dan Komunikasi. Indeks KAMI tidak diperuntukan Untuk menganalisis kelayakan atau efektivitas bentuk pengamanan, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan pimpinan instansi. keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001, yaitu:

1. Tata kelola Keamanan Informasi
   Metode ini untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas dan tanggung jawab pengelolaan keamanan informasi.
2. Pengelolaan Risiko Keamanan Informasi
   Metode ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
3. Kerangka Kerja Keamanan Informasi
   Metode ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
4. Pengelolaan Aset
   Metode ini mengevaluasi kelengkapan pengamanan terhadap asset informasi, termasuk keseluruhan siklus penggunaan asset tersebut.
5. Teknologi dan Keamanan Informasi
   Metode ini mengevaluasi kelengkapan, konsisten dan efektivitas penggunaan teknologi dalam pengamanan asset informasi.

Dalam setiap area, proses evaluasi Indeks KAMI membahas mengenai aspek untuk mencapai tujuan untama dari pengamanan area tersebut. Bentuk pengamanan dengan kesiapan minimum dipersyarakat untuk proses sertifikasi standar SNI ISO/IEC 27001:2013. Berikut table pemetaan skor untuk penilaian mandiri dan membentuk matriks antar status kategori pengamanan.

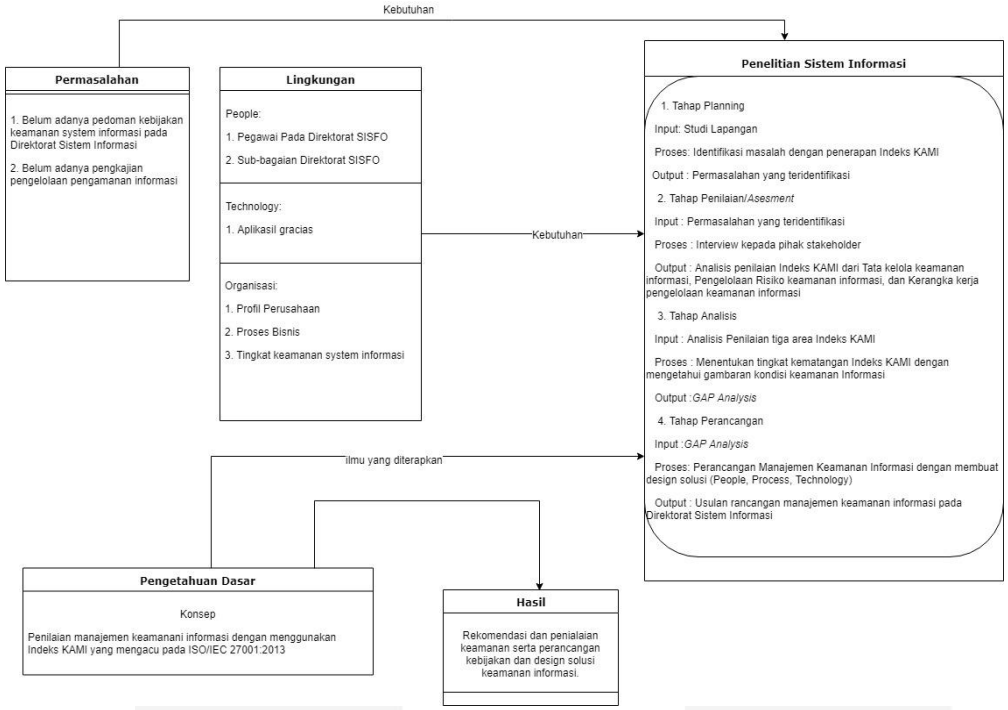
	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagaian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Tabel 2 Kategori Pengamanan Indeks KAMI

Untuk keseluruhan area pengamanan, pertanyaan dengan pengisian kategori "3" hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan kategori "1" dan "2" sudah terisi dengan minimal status "dalam penerapan atau diterapkan sebagaian".

3) Metodologi Penelitian

Model konseptual merupakan kerangka berfikir dalam melakukan penelitian yang menjelaskan mengenai konsep dalam pemecahan secara ringkas dan menghasilkan *output* yang sesuai dengan tujuan penelitian. Dengan adanya model konseptual dapat membantu dalam penataan masalah, mengidentifikasi faktor-faktor yang releavan, memberikan gambaran dalam merumuskan masalah penelitian. Metode konseptual dalam tugas akhir ini menggunakan Indeks KAMI yang mengacu pada ISO/IEC 27001. Model konseptual dari penelitian ini dapat digambarkan sebagai berikut:



Gambar 1 Model Konseptual

Dalam gambar model konseptual terbagi menjadi 3 (tiga) yang menggambarkan alur penelitian analisis asessment Indeks KAMI pada Direktorat Sistem Informasi

1. Dalam model konseptual penelitian ini adalah permasalahan lingkungan yang ada Direktorat Sisfo yaitu belum adanya keamanan sistem informasi serta belum adanya pedoman kebijakan keamanan informasi yang di terapkan pada Direktorat Sisfo itu sendiri. Keamanan sistem informasi pada Intansi sangat dibutuhkan untuk melindungi data data pada Instansi tersebut.
2. Pada bagian lingkungan beberapa kategori yaitu pada People terdapat Bagian unit, pegawai Direktorat Sisfo. Pada Technologi terdapat Aplikasi Igracias, konten dan infrastruktur. Kemudian organisasi ada profil perusahaan, proses bisnis dan tingkat keamanan informasi. Dari permasalahan limgkungan tersebut kebutuhan untuk penelitian sistem informasi diperlukan untuk menggambarkan pedoman yang dibutuhkan untuk memberikan solusi pada permaslahan yang ada. Dan pedoman untuk memberikan gambaran kondisi keamanan informasi saat ini pada Direktorat Sisfo.
3. Pada penelitian ini ilmu yang diterapkan terdapat konsep yang akan diterapkan untuk menjadi pedoman yaitu Indeks KAMI yang mengacu pada ISO/IEC 27001. Pada Indeks KAMI dilakukan analisis gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi.

4) Hasil dan Analisis

4.1 Hasil Penilaian Tata Kelola Keamanan Informasi

Tabel 3 Penilaian Tata Kelola Keamanan Informasi

Jumlah Pertanyaan Pengelolaan Risiko Keamanan Informasi	Skor
Jumlah pertanyaan status pengamanan 1 ada 8 Pertanyaan	15
Jumlah pertanyaan status pengamanan 2 ada 8 Pertanyaan	24

Jumlah pertanyaan status pengamanan 3 ada 6 Pertanyaan	0
Batas Skor Min untuk Skor status pengamanan Penerapan 3	48
Total Skor status pengamanan Penerapan 1 & 2	39
Status Peniliaian status pengamanan Penerapan 3	Tidak Valid
Total evaluasi Tata Kelola Keamanan Informasi	39

Pada Tabel diatas total skor tata kelola keamanan informasi yaitu 39 dimana dalam kategori 3 sebanyak 6 pertanyaan memiliki skor 0. Persyaratan skor untuk kategori penerapan 3 minimal 48 sedangkan hasil penilaian kategori penerapan 3 untuk bagian tata kelola yaitu "tidak valid", maka penilaian penerapan 3 tidak memenuhi nilai minimal yang dipersyaratkan. Total nilai tata kelola keamanan informasi mendapat poin 39 dari 126 (untuk keseluruhan poin yang dipersyaratkan pada area tata kelola) dimana poin tersebut rendah. Dapat disimpulkan bahwa sebagaian besar tugas dan tanggung jawab pengelolaan keamanan informasi belum diterapkan secara menyeluruh dan masih dalam tahap perencanaan.

4.2 Hasil Penilaian Pengelolaan Risiko Keamanan Informasi

Tabel 4 Penilaian Pengelolaan Risiko Keamanan Informasi

Jumlah Pertanyaan Pengelolaan Risiko Keamanan Informasi	Skor
Jumlah pertanyaan Tahap 1 ada 10 pertanyaan	21
Jumlah pertanyaan Tahap 2 ada 4 pertanyaan	16
Jumlah pertanyaan Tahap 3 ada 2 pertanyaan	3
Batas Skor Min untuk Skor Tahap Penerapan 3	36
Total Skor Tahap Penerapan 1 & 2	37
Status Peniliaian Tahap Penerapan 3	Valid
Total area evaluasi pengelolaan risiko keamanan informasi	40

Pada Tabel diatas total skor pengelolaan risiko keamanan informasi yaitu 40. Persyaratan skor untuk kategori penerapan 3 minimal 36 sedangkan hasil penilaian kategori penerapan 3 untuk bagian pengelolaan risiko yaitu "valid", maka penilaian penerapan 3 telah memenuhi nilai minimal yang dipersyaratkan. Total penilaian area evaluasi pengelolaan risiko keamanan informasi mendapat poin 40 dari total keseluruhan poin 72, dimana poin tersebut terbilang *high* atau tinggi karena pada Direktorat Sisfo sudah melakukan proses pengelolaan keamanan informasi yang merupakan dasar penerapan strategi keamanan informasi. Pada tahap ini Direkotarat Sistem informasi masih menerapkan sebagaian pengelolaan risiko terhadap keamanan informasi.

4.3 Hasil Penilaian Kerangka Kerja Keamanan Informasi

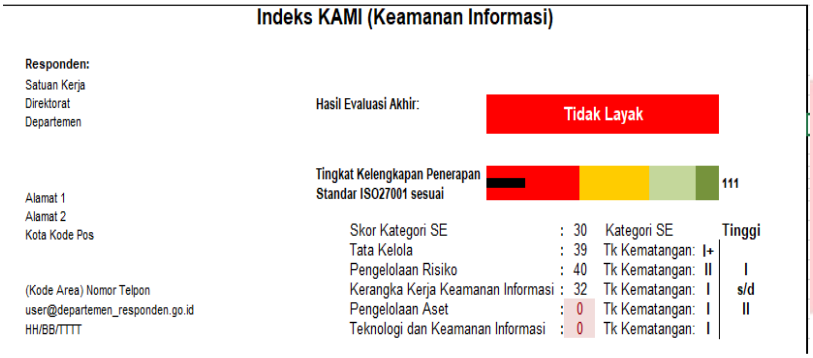
Tabel 5 Penilaian Kerangka Kerja Keamanan Informasi

Jumlah Pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi	Skor
Jumlah pertanyaan Tahap 1 ada 12 pertanyaan	14
Jumlah pertanyaan Tahap 2 ada 10 pertanyaan	18
Jumlah pertanyaan Tahap 3 ada 7 pertanyaan	0
Batas Skor Min untuk Skor Tahap Penerapan 3	64
Total Skor Tahap Penerapan 1 & 2	32
Status Peniliaian Tahap Penerapan 3	Tidak Valid

Pada Tabel diatas total skor kerangka kerja pengelolaan keamanan informasi yaitu 32 dimana dalam kategori 3 sebanyak 7 pertanyaan memiliki skor 0. Persyaratan skor untuk kategori penerapan 3 minimal 64 sedangkan hasil

penilaian kategori penerapan 3 untuk bagian kerangka kerja pengelolaan yaitu “tidak valid”, maka penilaian penerapan 3 tidak memenuhi nilai minimal yang dipersyaratkan. Total penilaian area evaluasi kerangka kerja pengelolaan keamanan informasi mendapat poin 32 dari total keseluruhan poin 159, dimana poin tersebut terbilang rendah dikarenakan pada Direktorat Sisfo belum melakukan strategi pengamanan terhadap kerangka kerja pengelolaan keamanan informasi yang merupakan bagian keamanan informasi. Direktorat Sistem Informasi belum adanya kerangka kerja dalam pengelolaan kelengkapan dan kesiapan baik itu kebijakan dan prosedur terhadap pengelolaan keamanan informasi dan strategi keamanan informasi masih dalam tahap perencanaan.

4.4 Hasil Kajian Indeks KAMI



Gambar 2 Hasil Tingkat Kelengkapan Indeks KAMI

Dalam assessment Indeks KAMI untuk area tata kelola, pengelolaan risiko dan kerangka kerja pengelolaan keamanan informasi berada di warna merah yang masih dalam status kesiapan “Tidak Layak” berdasarkan cakupan Kategori Sistem Elektronik pada Direktorat Sistem Informasi yang memiliki kategori tinggi tetapi belum didukung oleh bentuk penerapan yang dibutuhkan karena semakin tinggi tingkat ketergantungan Sistem Elektronik makan semakin penting peranan Sistem Elektronik terhadap area kerja Direktorat Sistem Informasi. Maka proses pengamanan keamanan informasi di lingkungan Direktorat harus dikelola dengan mulai melakukan penilaian *self assessment.* Hasil penilaian Indeks KAMI Direktorat Sisfo dengan Kategori Sistem Elektronik yang tergolong tinggi dan status kesiapan untuk area tata kelola, pengelolaan risiko dan kerangka kerja pengelolaan keamanan informasi berada pada level II bernilai 111 dari 357 dimana merupakan kondisi dasar penerapan kerangka kerja dimana proses pengamanan berjalan tanpa dokumentasi atau dokumen resmi.

4.5 *Gap Analysis*

Setelah melakukan penilaian dan menentukan tingkat kematangan Indeks KAMI, tahap selanjutnya melakukan *gap analysis*, yang merupakan perbandingan fakta lapangan dengan kondisi ke depannya atau kondisi ideal dengan mengacu pada Indeks KAMI standar ISO 27001:2013.

A. Identifikasi Area yang tidak terpenuhi

Identifikasi area yang tidak terpenuhi merupakan hasil dari proses *ekstisting* Direktorat Sistem Informasi yang telah dianalisis. Area yang tidak terpenuhi atau belum dilakukan akan diidentifikasi untuk mendapatkan *output* atau keluaran yang dihasilkan dari area yang tidak terpenuhi. Berikut Tabel merupakan temuan yang telah diidentifikasi berdasarkan area dan persyaratan area.

Tabel 6 Hasil area yang tidak terpenuhi

No	Area Indeks Keamanan Informasi	Kategori Tingkat Kelengkapan	Temuan
1.	Tata Kelola Keamanan Informasi	2.18	Direktorat Sisfo belum mempunyai parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup waktu pengukuran, pelaksanaannya, dan ekskalasi pelaporannya.
2.	Pengelolaan Risiko Keamanan Informasi	3.15	Direktorat Sisfo belum melakukan peninjauan terhadap mengenai analisis risiko dari setiap aset utama.
3.	Kerangka kerja pengelolaan keamanan informasi	4.1	Direktorat Sisfo belum mempunyai kebijakan dan SOP keamanan informasi untuk pengamanan aset informasi yang terkelola dengan pihak yang diberikan wewenang untuk menerapkannya
		4.5	Direktorat Sisfo belum mempunyai kebijakan dan SOP mengenai pengelolaan kajian risiko
		4.8	Direktorat Sisfo belum memiliki dokumen kebijakan mengenai konsekwensi dari pelanggaran keamanan informasi
		4.9	Direktorat Sisfo belum adanya SOP mengenai tindak lanjut konsekwensi terhadap penerapan keamanan informasi
		4.14	Direktorat Sisfo belum mempunyai kebijakan dan SOP mengenai mengenani penanggulangan terjadinya ketidakpatuhan terhadap kebijakan yang ada.
		4.19	Direktorat Sisfo belum melakukan perbaikan secara berkala mengenai evaluasi terhadap kebijakan dan SOP
		4.27	Direktorat Sisfo belum menjalankan inisiatif Analisa kajian risiko keamanan informasi secara struktur terhadap asset informasi yang ada.
		4.28	Direktorat Sisfo belum memiliki kebijakan dan SOP keamanan informasi untuk pengamanan aset informasi yang terkelola dan kepatuhan terhadap progam keamanan informasi.

B. Hasil Kriteria Risiko

Dari Gap Analyisis terdapat macam ancaman dan kerentanan dari setiap area. Hasil dari kriteria risiko merupakan hasil yang didapatkan berdasarkan nilai *impact* dan nilai *probability* yang terjadi pada Direktorat Sisfo. Berikut tabel dari hasil kriteria risiko.

Tabel 7 Hasil kriterio Risiko

No	Area	Pertanyaan Indeks KAMI	Jawaban	Temuan	Deskripsi Risiko		Pemilik Risiko	Sebelum Penanganan							Tingkat Risiko
					Ancaman	Kerentanan (bahaya yang terjadi yang menimbulkan bencana)		Kontrol saat ini	Kategori Kontrol	Tingkat kemungkinan / Probability	Penjelasan Kemungkinana	Tingkat dampak	Penjelasan Dampak	Skor Risiko	
1	Bagaimana fungsi Keamanan Informasi di Direktorat Sisfo?	Apakah Direktorat Sisfo sudah mendefinisikan metrik, parameter, dan proses pengukuran pengelolaan keamanan informasi?	Tidak dilakukan	Direktorat Sisfo belum mendefinisikan metrik, parameter, serta proses pengelolaan keamanan informasi	Proses pengukuran pengelolaan keamanan informasi yang belum didefinisikan akan mengalami gangguan keamanan seperti serangan spam (malware) oleh hacker	Belum adanya pengelolaan keamanan informasi yang terdifinisikan sesuai standar parameter	Direktorat Sistem Informasi	Belum ada		3	Memungkinkan terjadinya gangguan keamanan dapat terjadi dalam jangka waktu yang relatif lama (3-5 tahun), yang sebagaian dapat di mitigasi dan dibuatlah prosedur	5	Menimbulkan penundaan aktivitas pengelolaan keamanan informasi akibat gangguan pada proses hingga lebih dari sebulan	15	High
		(3.15) Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak dilakukan	Direktorat Sisfo belum melaksanakan dan merencanakan tangkah mitigasi dan penanggulangan risiko secara berkala untuk memastikan akurasi dan validitasnya	Belum bisa meningkatkan efektifitas mutu pengelolaan risiko	Belum adanya awamess (kesadaran) terhadap pengamanan informasi terhadap pengelolaan risiko berdasarkan area persyaratan Indeks KAMI	Direktorat Sistem Informasi	Belum ada		3	Kemungkinan besar terjadi beberapa kali karena belum adanya pengelolaan risiko secara berkala	3	Menimbulkan lambatnya proses pengelolaan risiko keamanan informasi atau penundaan	9	Medium
3	Bagaimana penyusunan dan pengelolaan kebijakan & prosedur keamanan informasi di Direktorat Sisfo?	(4.1) Apakah kebijakan dan prosedur atau dokumen lainnya diperlukan terkait keamanan informasi sudah disusun dan dinaikan dengan jelas pihak-pihak yang diberikan wewenang untuk menerapkannya?	sudah kebijakan 2018, hanya standar yang mengelolanya saja, SOP belum ada	Dokuasen kebijakan dan SOP keamanan informasi sudah disusun namun belum dinaikan dengan jelas pihak yang diberikan wewenang untuk menerapkannya	Kurangnya awamess (kesadaran) pegawai mengenai prosedur dan kebijakan sesuai tanggung jawab	Tidak adanya acuan dalam kegiatan terkait keamanan informasi	Direktorat Sistem Informasi hanya untuk kebijakan ke pak dadang dan buans	Dilakukan pembahasan terkait kebijakan keamanan informasi bersama YPT saat rapat pimpinan	Process	4	Kemungkinan besar terjadi karena belum adanya pedoman atau acuan pegawai untuk pengelolaan keamanan informasi	3	Menimbulkan penundaan aktivitas kegiatan keamanan informasi karena belum adanya acuan kebijakan untuk setiap pihak pihak yang berwenang dalam pengelolaan keamanan informasi	12	Medium
		(4.5) Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	Tidak dilakukan	Dokumen kebijakan dan SOP keamanan informasi sudah disusun namun belum lengkap dan belum terdapat kebutuhan mitigasi dari hasil kasijan risiko	Tidak adanya acuan langkah untuk mitigasi kajian risiko	Kurangnya kesadaran organisasi dalam pendokumentasian serta pengimplementasikan kontrol dan prosedur dalam mitigasi dan penanggulangan risiko	Direktorat Sistem Informasi	Belum ada		4	kemungkinan besar terjadi terus dalam berbagai kondisi untuk penanggulang risiko karena belum adanya acuan dalam kebijakan keamanan informasi	4	Menimbulkan terhambatnya proses penanggulangan risiko dan hasil kajian risiko	16	High
		(4.8) Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegaskan?	Tidak dilakukan	Dokumen kebijakan dan SOP keamanan informasi sudah dipetakan namun belum lengkap termasuk konsekwensi pelanggaran kebijakan	Tidak adanya pedoman atau acuan langkah untuk konsekwensi pelanggaran kebijakan keamanan informasi	Kurangnya kesadaran organisasi dalam pendokumentasian kebijakan serta pengimplementasikan kontrol dan prosedur dalam mitigasi dan konsekensi dari pelanggaran kebijakan keamanan informasi	Direktorat Sistem Informasi	Belum ada		3	kemungkinan besar terjadi berbagai kondisi apabila dalam pengimplentasikan kontrol dan prosedur dalam mitigasi dan konsekens	3	Menimbulkan penundaan aktivitas karena belum adanya konsekensi pelanggaran keamanan informasi	9	Medium
		(4.9) Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?	Tidak dilakukan	Dokumen kebijakan dan SOP keamanan informasi sudah dipetakan namun belum lengkap konsekwensi pelanggaran dan proses untuk menindak lanjuti	Tidak adanya pedoman atau acuan langkah untuk konsekwensi pelanggaran kebijakan keamanan informasi	Kurangnya kesadaran organisasi dalam pendokumentasian kebijakan serta pengimplementasikan kontrol dan prosedur dalam mitigasi dan konsekensi dari pelanggaran kebijakan keamanan informasi	Direktorat Sistem Informasi	Belum ada		4	Kemungkinan besar terjadi berbagai kondisi apabila proses untuk menindaklanjuti konsekwekwensi tidak dilakukan. Dan kejadian tersebut akan terus berulang	4	Menimbulkan penundaan aktivitas karena belum adanya konsekensi pelanggaran keamanan informasi	16	High
		(4.14) Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru?	Tidak dilakukan	Belum adanya proses untuk penanggulangan risiko terhadap pengembangan sistem baru, misalnya pada aktivitas Deployment Aplikasi yaitu pada perisitiva server development dan production berada dalam satu sever yang sama	Terjadinya risiko baru atau ketidakpatuhan terhadap kebijakan yang ada dan dampak langsung aplikasi terpublish secara tidak sengaja ke user	Kurangnya kesadaran organisasi dalam pendokumentasian serta pengimplementasikan kontrol dan prosedur dalam penanggulangan risiko terhadap pengamanan baru	Direktorat Sistem Informasi	Belum ada		4	Kejadian aktivitas kebiasaneng terulang mengenai deployment server	4	Menimbulkan kegagalan kurang lebih 60 % fungsi operasional pengelolaan untuk menjalankan aktivitas	16	High
		(4.19) Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak dilakukan	Dokumen kebijakan dan SOP belum disusun dan belum dilakukan perbaikan secara berkala	Tidak adanya pedoman dan prosedur keamanan informasi serta tidak adanya peningkatan dan efektifitas terhadap pengamanan informasi	Belum adanya peningkatan efektifitas pengamanan informasi dan rentan akan pengelolaan keamanan informasi	Direktorat Sistem Informasi	Belum ada		4	Kemungkinan besar terjadi pada suatu kondisi sangat riskan karena tidak adanya evaluasi kebijakan dan sop keamanan informasi	4	Menimbulkan tidak adanya peningkatan efektifitas kebijakan dan sop keamanan informasi	16	High
	Bagaimana Direktorat Sisfo melakukan pengelolaan strategi dan program keamanan informasi?	(4.27) Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai pensyarat untuk menerapkannya?	infrasruktur ada yaitu layanan tune	Dokumen kebijakan dan SOP belum disusun dan belum dilakukan perbaikan dan pengelolaan secara berkala	Tidak adanya pedoman kebijakan maka akan terjadi kesalahan penggunaan untuk melakukan analisa untuk menilai aspek perubahan terhadap infrastruktur	Belum adanya pedoman dan acuan sesuai standar keamanan informasi serta belum adanya peningkatan efektifitas pengamanan yang berlaku	Direktorat Sistem Informasi	Belum ada		3	Kemungkinan besar terjadi pada suatu kondisi sangat riskan karena tidak adanya evaluasi kebijakan dan sop keamanan informasi	4	Menimbulkan tidak adanya peningkatan efektifitas kebijakan dan sop keamanan informasi	12	medium
		(4.28) Apakah Direktorat Sisfo secara periodik menguji dan mengevaluasi tingkat kepatuhan program keamanan informasi yang ada untuk memastikan bahwa kesesuaian insiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Tidak dilakukan	Direktorat Sisfo secara berkala belum melakukan evaluasi dan menguji tingkat kepatuhan keamanan informasi yang ada.	Kesulitan melakukan pengujian dan evaluasi untuk merencanakan peningkatan kepatuhan progam keamanan informas	Belum adanya pedoman dan acuan sesuai standar keamanan informasi untuk menganalisa tingkat kepatuhan secara efektif	Direktorat Sistem Informasi	Belum ada		4	Kemungkinan besar terjadi cukup sering pada suatu kondisi karena belum adanya evaluasi berkala mengenai kepatuhan keamanan informasi	3	menimbulkan tidak adanya peningkatan efektifitas kepatuhan keamanan informasi	12	medium

4.6 Perancangan Keamanan Informasi

Perancangan pada keamanan informasi merupakan salah satu usulan atau target untuk mengatur proses keamanan informasi pada Direktorat Sisfo. Setelah melakukan penilaian dengan Indeks KAMI yang mengacu pada ISO/IEC 27001 serta control *Annex* sebagai pendukung dalam rekomendasi perancangan Indeks Keamanan Informasi. Perancangan yang diajukan penulis berupa perancangan *process*, *people* dan *technology*. Berikut penjelasan dibawah ini:

A. Perancangan *Process*

Perancangan *process* merupakan perancangan yang diusulkan berupa dokumen kebijakan, prosedur, dan dokumen lainnya untuk pemenuhan persyaratan Indeks KAMI. Perancangan *process* dilakukan berdasarkan penilaian dari hasil pengelolaan risiko. Pada usulan ada *Standar Operational Procedure* (SOP) rekomendasi berdasarkan standar area yang belum terpenuhi dari Indeks KAMI, sedangkan kebijakan merupakan pedoman umum atau acuan dalam melakukan proses kerja pada Direktorat Sisfo.

1. Kebijakan Sistem Manajemen Keamanan Informasi
    a) Kebijakan Organisasi Keamanan Informasi
    b) Kebijakan Penanggulangan Risiko
    c) Kebijakan mengenai pelanggaran kebijakan keamanan informasi.
    d) Kebijakan pengecualian terhadap penerapan keamanan informasi
    e) Kebijakan kepatuhan terhadap kebijakan yang ada
2. Perancangan SOP (*Standard Operational Procedure*)
    a) Prosedure Mitigasi Hasil Kajian Risiko
    b) Prosedure penanganan insiden Keamanan Informasi.

B. Perancangan Aspek *People*

Perancangan *People* merupakan perancangan yang didapat dari hasil pengelolaan risiko dalam Indeks KAMI. Perancangan *People* dapat menghasilkan rekomendasi kompetensi keahlian sumber daya manusia yang harus dimiliki pada struktur organisasi.

C. Perancangan *Roadmap*

Roadmap merupakan dokumen perencanaan pengamanan informasi berbasis jangka waktu pelaksanaan kegiatan yang harus dilakukan untuk mencapai target perusahaan. Perancangan *roadmap* ni berdasarkan hasil analisis dari tingkat risiko high yang dilaksanakan pada triwulan ke-3 secara berkala dan masing-masing kegiatan berbeda waktu.

5. Kesimpulan dan Saran

a) Kesimpulan

Penilaian Kategori Sistem Elektronik pada proses kerja pada Direktorat Sistem Informasi yaitu dengan skor 30. Dimana penggunaan TIK pada Direktorat Sisfo sangat berperan penting dan tidak dapat terpisahkan untuk mendukung proses kerja yang berjalan. Dalam proses assessment ketiga area dalam Indeks KAMI memperoleh skor sebesar 111 dari total keseluruhan nilai dari kelima area sebesar 645, dalam ketiga area yang berada pada level kematangan II dimana kondisi terseut merupakan kondisi dasar penerapan kerangka kerja dimana proses pengamanan berjalan tanpa dokumentasi atau dokumen resmi. Dan hal ini belum layak dalam penerapan sistem manajemen keamanan informasi untuk melindungi aset pengamanan informasi sehingga masih rentan terhadap kejahatan computer yang dapat mengakibatkan pelayanan sistem informasi di Direktorat Sistem Informasi.

b) Saran

- Direktorat Sistem Informasi perlu menerapkan semua obyektif control yang ada pada ISO 27001:2013 serta sebaiknya menerapkan salah satu sub klausul pada Organisasi Keamanan Informasi, agar Direktorat Sistem Informasi dapat mencapai target yang diharapka, dan dapat membantu proses bisnis perusahaan.
- Diretorat Sistem Informasi harus menerapkan kerangka kerja pengamanan informasi dengan penilaian mandiri (self assessment) Indeks KAMI secara berkala untuk menyiapkan standarisasi ISO 27001:2013.

DAFTAR PUSTAKA

[1] Hasin, M. F., Wowon, H. F., & Karouw, S. D. (2017). Implementasi Indeks KAMI di Universitas Sam Ratulangi. *E-Journal Teknik Informatika Vol 12, No. 1, ISSN: 2301- 8364*.

[2] *https://bssn.go.id/indeks-kami/*. (2018, Januari 2). Retrieved from Badan Siber dan Sandi Negara: https://bssn.go.id/indeks-kami/

[3] Manullang, A. F., Candiwan, & Harsono, L. D. (2017). Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Institusi XYZ. *JIEET: Volume 01 Nomer 02, ISSN: 2549-869X*, 73-81.

[4] *Tingkatkan Koordinasi Proteksi Keamanan Siber Indonesia*. (2018, September 25). Retrieved from Proteksi Keamanan Siber Indonesia: https://kominfo.go.id/index.php/content/detail/14605/ciip-id-summit-2018-tingkatkan-koordinasi-proteksi-keamanan-siber-indonesia/0/sorotan_media

[5] Ferdinand Aruan. (2003). Tugas Keamanan Jaringan Informasi (Dosen. Dr. Budi Rahardjo) Tinjauan Terhadap ISO 17799 - Program Magister Teknik Elektro Bidang Khusus Teknologi Informasi Institut Teknologi Bandung

[6] Indeks Keamanan Informasi. *[online]*. *https: https://bssn.go.id/indeks-kami/* [27 Oktober 2018]
Paryati. (2008). *Keamanan Sistem Informasi Seminar Nasional Informatika.* ISSN: 1979-2328 UPN "Veteran" Yogyakart

[7] The Open Group. 2011. *Open Book Standard - Open Information Security Management Maturity Model (O-ISM3).* United Kingdom: The *Open Group*.

[8] (2016, 12 19). Retrieved from BMC (The multi-Cloud Management Company): http://www.bmc.com/guides/itil-information-security-management.html

[9] Indonesia, I. G. (2016, Desember 7). Retrieved from ITG.ID (IT Governance Indonesia): https://itgid.org/pengertian-cobit-5/

[10] Whitman, M, and Mattord H. (2004). *Management Of Information Security* : Canada : Thomson Learning

[11] D. Willet Keith, Arnason Sigurjon Thor. (2008). How to achieve 27001 certification: an example of applied compliance managemen. Taylor & Francis Group, LLC.

[12] Cahyani Dini Indra. (2018). Sistem Manajemen Pengamanan Informasi ISO 27001:2013 berdasarkan PDCA Klausul 8-10 mengenai operasi, evaluasi kinerja dan peningkatan dan kontrol annex (Studi Kasus : Diskominfo Jabar)

[13] Kementrian Komunikasi dan Informatika. (2017). Diambil kembali dari http://fikom umi.id/po-content/uploads/tot/Panduan%20Penerapan%20SMKI%20Berbasis%20%20Indeks%20KAMI_2017_tanpa%20Cover.pdf