ANALISIS DAN PERANCANGAN MANAJEMEN KEAMANAN INFORMASI DIREKTORAT SISTEM INFORMASI UNIVERSITAS TELKOM DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA AREA PENGELOLAAN ASET INFORMASI, TEKNOLOGI DAN KEAMANAN INFORMASI

ANALYSIS AND DESIGN OF INFORMATION SECURITY MANAGEMENT DIRECTORATE OF INFORMATION SYSTEMS OF TELKOM UNIVERSITY USING THE INFORMATION SECURITY INDEX (KAMI) IN THE AREA OF INFORMATION ASSET MANAGEMENT, TECHNOLOGY AND INFORMATION SECURITY

Rizky Cherthio Annisyah[1], Avon Budiono[2], Rokhman Fauzi[3]

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

[1] rizkycherthio@student.telkomuniversity.ac.id [2] avonbudi@telkomuniversity.ac.id [3] rokhmanfauzi@telkomuniversity.ac.id

Abstrak - Informasi merupakan aset yang sangat berharga bagi sebuah lembaga baik lembaga pemerintah maupun swasta termasuk dalam hal ini adalah Direktorat SISFO yang merupakan Direktorat pada salah satu institusi Perguruan Tinggi swasta. Maka dari itu pengamanan informasi harus dilakukan dengan sebaik mungkin. Sumber daya yang memadai dan cukup harus dialokasikan untuk melindungi aset informasi melalui penyelenggaraan kebijakan keamanan sistem informasi yang terukur sesuai dengan standard yang ada. Tujuan dari penelitian ini adalah sebagai kajian untuk mengetahui tingkat kesiapan pengamanan sistem informasi institusi berdasarkan Indeks KAMI yang merupakan sebuah alat untuk menganalisa tingkat kesiapan pengamanan informasi yang dibuat oleh Kemkominfo pada tahun 2011. Indeks KAMI merupakan suatu alat evaluasi yang digunakan untuk menganalisa tingkat kesiapan pengamanan informasi di organisasi. Evaluasi dilakukan terhadap beberapa area yang memenuhi aspek keamanan informasi yang didefinisikan dalam standar ISO/IEC 27001 yang merupakan suatu standard yang dipublikasikan oleh International Standard Organization dan International Electrotechnical Commission, standar tersebut menyediakan rekomendasi best practice terhadap manajemen keamanan informasi dan pemeliharaan ISMS pada organisasi. Hasil analisis penilaian indeks KAMI menunjukan bahwa kategori Sistem Elektronik tergolong tinggi dan status kesiapan pada area pengelolaan asset informasi, teknologi dan kemanan informasi dilevel II dengan hasil skor seluruh area 276 dari 645 total skor. Pada tingkatan ini menjelaskan kondisi dasar dari kerangka kerja penerapan keamanan informasi yang masih belum melakukan dokumentasi diseluruh area. Direktorat Sisfo belum memenuhi penerapan keamanan informasi sehingga diperlukan perbaikan dengan meningkatkan control keamanan yang terdokumentasi dan terstruktur.

Kata Kunci: Indeks KAMI, ISO/IEC 27001, *Information Security*, SMKI.

Abstract - Information on assets that is very valuable for an institution, both government and private, including in this case is the SISFO Directorate, which is a private university. Therefore, information security must be done as well as possible. Adequate and sufficient resources must be allocated to protect information assets through the implementation of a measurable information system security policy in accordance with existing standards. The purpose of this research is as an evaluation to monitor the level of information system security readiness made by a tool to analyze the level of information security readiness made by the Ministry of Communication and Information in 2011. The KAMI index is an evaluation tool used to analyze the level of information security readiness in organizations. Evaluation is carried out on several areas that meet the security aspects defined in the ISO / IEC 27001 standard which is a standard published by the International Standard Organization and International Electrotechnical Commission, the standard provides best practice recommendations for information management and ISMS maintenance in organizations. The results of our index analysis show that the category of Electronic Systems is high and the status of readiness in the area of management of information assets, technology and data information is level II with the results of a total score of 276 out of 645 total areas. At this level, it explains that the basic condition of the information application framework which is still not documented in all areas. The Sisfo Directorate has not fulfilled the implementation of information security so that improvements are needed by increasing documented and structured controls.

Keywords: KAMI Indeks, ISO/IEC 27001, Information Security, ISMS

1) Pendahuluan

Direktorat SISFO merupakan suatu departemen yang berada dibawah naungan Telkom University yang mengurus bidang akademik dan non-akademik pada sisi teknologi informasi. Direktorat SISFO membawahi wakil Rektor II melayani seluruh unit yang ada di Telkom University dengan ruang lingkup layanan dibagi berdasarkan struktur organisasi yaitu unit Layanan Operasional Sistem Informasi (LOPSI), unit Infrastrukture dan Content (INTEN) dan unit Riset dan Pengembangan Sistem Informasi (RISBANGSI).

Direktorat Sistem Informasi (Sisfo) berfungsi menjadi enabler yang menyediakan sarana pendukung pencapaian WCU tersebut dalam bidang *Information Technology*" (is.telkomuniversty.ac.id). Dalam hal ini Direktorat Sisfo memiliki peran aktif dalam mendukung aktivitas akademik dan non-akademik untuk dapat menyimpan, mengelola, dan mengekpos informasi atau data dengan baik dan benar maka dibutuhkannya manajemen yang baik untuk pengamanan informasi.

Untuk mengetahui keamanan terhadap informasi yang telah dilakukan oleh suatu instansi maka dibutuhkannya alat evaluasi yaitu Indek KAMI. Indeks KAMI merupakan alat evaluasi terhadap tingkat kesiapan (kelengkapan dan kematangan) untuk menerapkan keamanan informasi di sebuah organisasi sesuai dengan standar SNI ISO 27001 pada area tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan asset, dan aspek teknologi (bssn.go.id).

Oleh karena itu, dilakukanlah penilaian kondisi keamanan informasi menggunakan Indeks KAMI yang ada saat ini, untuk memperoleh nilai kesiapan untuk penerapan ISO 27001 dan melakukan perumusan strategi yang akan dilaksanakan kedepannya dari hasil analisis Indek KAMI, serta memberikan desain solusi yang meningkatkan keamanan informasi dari aspek struktur organisasi yang ada, alur proses bisnis yang terjadi, dan pada teknologi yang digunakan.

2) Landasan Teori

2.1 Keamanan Informasi

Menurut G.J. Simons keamanan informasi adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik (Purwanto, 2014).

Suatu organisasi yang berhasil harus memiliki keamanan yang baik yaitu pada:

1. *Physical security*
2. *Personal security*
3. *Operation security*
4. *Communication security*
5. *Network security*

Prinsip dasar dari Keamanan Informasi sebagai berikut, yaitu:

1. *Confidentiality*, Kerahasiaan menurut (Mokodompit & Nurlaela, 2017) informasi hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity*, Integritas artinya informasi dijaga agar selalu akurat untuk menjaga informasi tersebut maka informasi hanya boleh di ubah dengan izin pemilik informasi.
3. *Availability*, Ketersediaan adalah memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan (Mokodompit & Nurlaela, 2017).

2.2 Frameork untuk Keamanan Informasi

a. **ITIL Versi 3**

ITIL V3 singkatan dari *Information Thecnology Infrastructure Library* Versi 3 yang merupakan sebuah *framework* yang digunakan dalam mengelola layanan IT (IT *Service Management*). ITIL v 3 memiliki 5 domain yaitu

1. *service strategy,*
2. *service design,*
3. *service transition,*
4. *service operation*
5. *continual servce improvement*.

b. **Cobit 5 For Information Security**

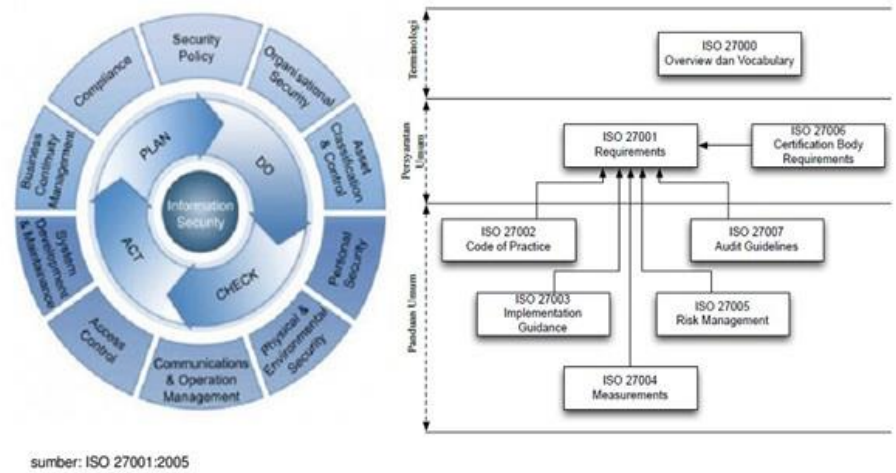
Berdasarkan (ISACA, 2012), COBIT 5 untuk Keamanan Informasi memberikan panduan spesifik yang berhubungan dengan semua enabler:

1. Kebijakan keamanan informasi, prinsip dan kerangka kerja
2. Proses, termasuk rincian dan aktivitas spesifik keamanan informasi
3. Struktur organisasi khusus keamanan informasi
4. Dalam hal budaya, etika dan perilaku, faktor penentu keberhasilan tata kelola dan pengelolaan keamanan informasi
5. Jenis informasi keamanan spesifik informasi untuk memungkinkan pengelolaan dan pengelolaan keamanan informasi di dalam perusahaan
6. Kemampuan layanan yang diperlukan untuk menyediakan keamanan informasi dan fungsi terkait ke suatu perusahaan
7. Orang, keterampilan, dan kompetensi khusus untuk keamanan informasi.

2.3 Standar Sistem Manajemen Keamanan Informasi (SMKI)

a. ISO/IEC 27001

ISO/IEC 27001 dirilis pada tahun 2005. Menurut (ISO/ IEC 27001, 2005) ini terus mengalami pembaharuan, ISO 27001: 2013 merupakan icon sertifikasi 27000 terbaru yang di rilis tahun 2013, sebuah dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) yang berisi tentang gambaran umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi atau enterprise dalam rangka mengimplementasikan konsep-konsep keamanan informasi.



sumber: ISO 27001:2005

Gambar 1 Siklus ISO 27001: 2005

Penjelasan dari model PDCA ISO 27001, sebagai berikut:

1. *Plan* (*Establish* ISMS)
   Menentukan kebijakan ISMS, sasaran, proses, dan prosedur yang sesuai untuk mengelola resiko dan meningkatkan keamanan informasi.
2. *DO* (*Maintain and improve the* ISMS)
   Dilakukannya kebijakan ISMS, control, dan proses prosedur yang telah direncanakan.
3. *Check* (*Monitor dan review the* ISMS)

Dilakukan pemantauan dan mengkaji kembali kinerja proses kebijakan, sasaran, dan akan melaporkan hasil untuk penilaian efektivitasnya.

4. *Act* (*Implement and operate the* ISMS)
   Dilakukan perbaikan dan pencegahan dari hasil evaluasi, audit internal dan tinjauan manajemen tentang ISMS agar dapat meningkatkan kinerja proses ang terjadi.

Pada (ISO/ IEC 27001, 2013) berisi 14 group (Klausa) yang membahas 113 kontrol keamanan informasi. Dengan menerapkan ISO/IEC 27001 akan meningkatkan kepercayaan publikterhadap informasi yang dihasilkan dan diproses oleh sebuah pihak pengguna serta meningkatkan jaminan kualitas dari sebuah informasi.

2.4 Sistem Manajemen Keamanan Infomasi / ISMS (*Infromation Security Management System*)

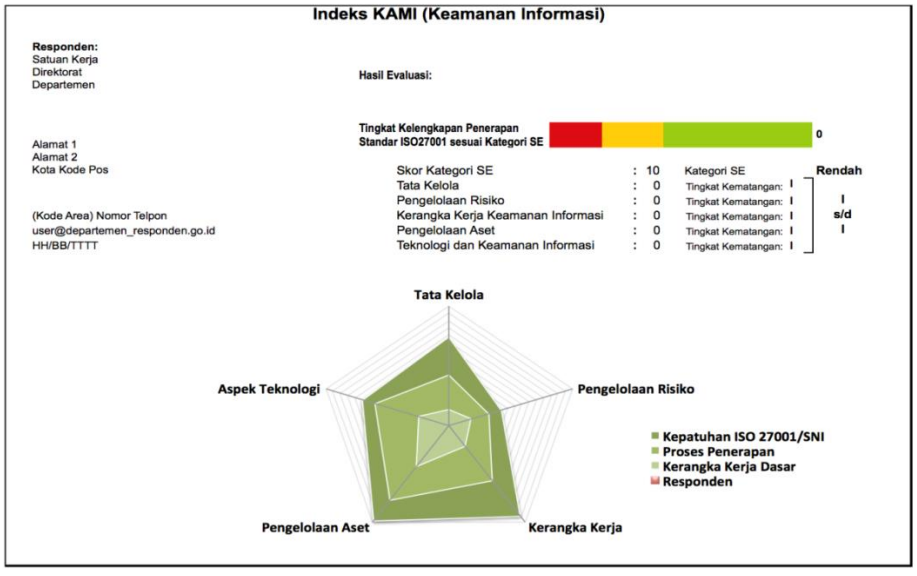
Menurut (Whitman dan Mattord,2014) ISMS harus didukung oleh hal-hal berikut yaitu :

1. Percanaaan : melakukan kegiatan yang meliputi proses perancangan, pembuatan dan implementasi untuk mencapai tujuan ISMS.
2. Kebijakan keamanan : kebijakan keamanan memberikan arahan dan dukungan sumber daya untuk mencapai tujuan ISMS. Program Pelatihan Keamanan Informasi : memberikan pengetahuan kepada pegawai mengenai keamanan informasi dan meningkatkan pemahaman keamanan informasi pekerja sehingga dicapai peningkatan keamanan informasi organisasi.
3. Penilaian Risiko : dengan penilaian risiko ini organisasi dapat memahami seberapa besar dampak yang akan diterima organisasi jika terjadi kejadian yang menyangkut keamanan informasi
4. Sumber Daya Manusia : manusia adalah pemgubung utama dalam program keamanan informasi, bisa meliputi keamanan personil secara individu saat bekerja dan keamanan personil dalam organisasi.
5. Tanggung Jawab: meliputi tanggung jawam manajemen, masing-masing individu organisai serta tanggung jawab untuk menjalankan dan memelihara ISMS.

2.5 Indeks KAMI

Menurut (Bssn.go.id), Indeks KAMI adalah suatu alat evaluasi untuk menganalis tingkat kesiapan pengamanan informasi di organisasi atau instansi pemerintah. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013.

Gambar dibawah ini tampilan Dari hasil evaluasi indeks KAMI akan menggambarkan tingkat kematangan dan kelengkapan untuk menerapkan SNI ISO/IEC27001 dan peta area yang dievaluasi indeks KAMI di suatu organisasi.



Gambar 2Tampilan *daskboard* hasil evaluasi Indeks KAMI

a. Metode Penilaian Indeks KAMI

Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009, pada (Keamanan Informasi, 2011) yang disusun kembali menjadi 5 (lima) area di bawah ini:

1) Tata Kelola Keamanan Informasi – Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

2) Pengelolaan Risiko Keamanan Informasi – Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

3) Kerangka Kerja Keamanan Informasi – Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

4) Pengelolaan Aset Informasi – Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

5) Teknologi dan Keamanan Informasi – Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

b. Proses penilaian kelengkapan dan kematangan Tata Kelola Keamanan Informasi

Proses penilaian dilakukan melalui 2 (dua) metode:

1. Jumlah (kelengkapan) bentuk pengamanan
2. Tingkat kematangan proses pengelolaan pengamanan informasi.

Metode pertama akan mengevaluasi sejauh mana instansi responden sudah menerapkan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Untuk kelima area evaluasi, yang dimaksud sebagai kontrol dijelaskan secara singkat di bawah ini:

1) Tata Kelola Keamanan Informasi Pengelolaan Risiko Keamanan Informasi

2) Kerangka Kerja Keamanan Informasi Pengelolaan Aset Informasi Teknologi dan Keamanan Informasi.

c. Penjelasan dan penilaian tingkat kematangan

Menurut (Keamanan Informasi, 2011)Pemetaan dan pemeringkatan akan dilakukan Tim yang ditetapkan Kementrian Komunikasi dan Informatika (Kominfo) dan menjadi dasar bagi pemberian opini Kominfo tentang kondisi tata kelola keamanan informasi di Kementrian/Lembaga terkait.

1. **Tingkat 0** - Tidak Diketahui(PASIF)

2. **Tingkat I** - Kondisi Awal (REAKTIF)

3. **Tingkat II** - Penerapan Kerangka Kerja Dasar (AKTIF)

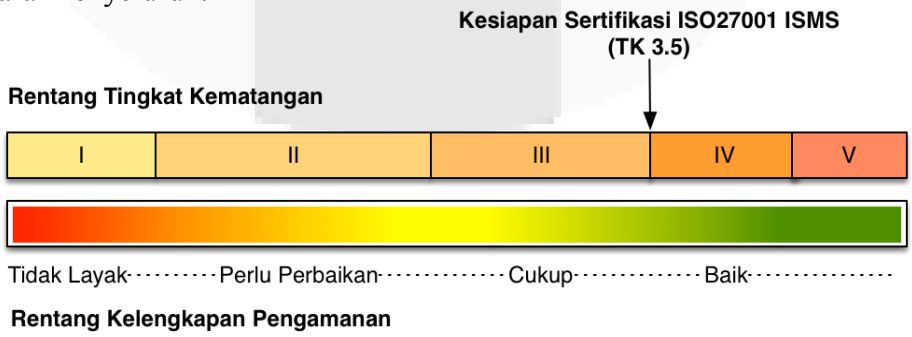
4. **Tingkat III** - Terdefinisi dan konsisten (PRO AKTIF)

5. **Tingkat IV** - Terkelola dan Terukur (TERKENDALI)

6. **Tingkat V** - Optimal (OPTIMAL)

Mekanisme penilaian dari Tingkat Kematangan Indeks KAMI:

1. **Tingkat Kematangan I**: Tidak ada ambang batas minimum – diasumsikan semua responden diberikan status ini pada saat dimulainya evaluasi.
2. **Tingkat Kematangan I+**: Mencapai minimal dimana hasil empat bentuk pengamanan TKII-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian" dan sisa jumlah pengamanan TKII-Tahap 1 yang ada dengan status "Sedang Direncanakan."
3. **Tingkat Kematangan II**: Mencapai minimal dimana hasil seluruh bentuk pengamanan TKII-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian" dan semua bentuk pengamanan TKII-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian."
4. **Tingkat Kematangan II+**: Mencapai minimal dimana hasil prasyarat Dasar TKII+, yaitu mencapai nilai total bentuk pengamanan Tingkat Kematangan II > (80% dari nilai seluruh bentuk pengamanan TKII-Tahap 1 & 2 dengan status "Diterapkan Secara Menyeluruh") dan semua bentuk pengamanan TKIII-Tahap 1 dengan status "Diterapkan Secara Menyeluruh", terdapat dua bentuk pengamanan TKIII-Tahap 2 dengan status "Sedang Direncanakan"; dan sisa jumlah pengamanan TKIII-Tahap 2 yang ada dengan status "Dalam Penerapan/Diterapkan Sebagian".
5. **Tingkat Kematangan III**: Mencapai minimal dimana hasil prasyarat Dasar TKII+, yaitu seluruh bentuk pengamanan TKIII-Tahap 1 dengan status "Diterapkan Secara Menyeluruh", terdapat Dua bentuk pengamanan TKIII-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian"; dan sisa jumlah pengamanan TKIII-Tahap 2 yang ada dengan status "Diterapkan Secara Menyeluruh" serta terdapat dua bentuk pengamanan TKIII-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian."
6. **Tingkat Kematangan III+**: Mencapai minimal dimana hasil prasyarat Dasar TKIII+ yaitu mencapai semua bentuk pengamanan TKIII-Tahap 1 dengan status "Diterapkan Secara Menyeluruh", tedapat satu bentuk pengamanan TKIII-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian"; dan sisa jumlah pengamanan TKIII-Tahap 2 yang ada dengan status "Diterapkan Secara Menyeluruh", dan terdapat satu bentuk pengamanan TKIII-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian" dengan sisa jumlah pengamanan TKIII-Tahap 3 dengan status "Diterapkan Secara Menyeluruh." Serta terdapat dua bentuk pengamanan TKIV-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian"; dan sisa jumlah pengamanan TKIV-Tahap 3 yang ada dengan status "Dalam Perencanaan."
7. **Tingkat Kematangan IV**: Mencapai minimal dimana hasil memenuhi prasyarat Dasar TKIII+; dan semua bentuk pengamanan TKIV-Tahap 3 dengan status "Diterapkan Secara Menyeluruh."
8. **Tingkat Kematangan IV+**: Mencapai minimal dimana hasil telah mencapai Tingkat Kematangan IV, dan terdapat satu bentuk pengamanan TKV-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian."
9. **Tingkat Kematangan V**: Mencapai minimal dimana hasil telah mencapai Tingkat Kematangan IV; dan semua bentuk pengamanan TKV-Tahap 3 dengan status "Diterapkan Secara Menyeluruh."



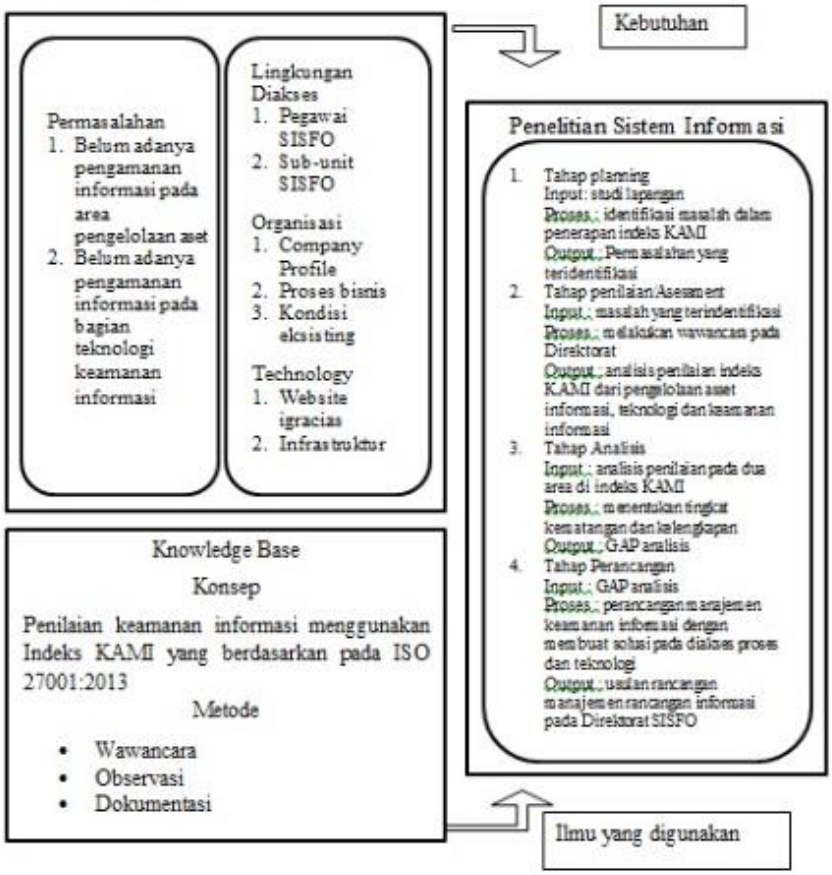
Gambar 3 Hubungan tingkat Kematangan dan kelengkapan

Sumber: *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Publik*

3) METODOLOGI PENELITIAN

3.1 Konseptual Model

Model Konseptual merupakan gambaran dari konsep yang akan digunakan dalam rangkaian pelaksanaan penilaian terhadap kesiapan keamanan informasi menggunakan Indeks KAMI pada Layanan Operasional Sistem Informasi Direktorat SISFO.



Gambar 4 Konseptual Model

1. Tahap Analisis penilaian
   Pada tahapan ini akan dilakukan pemetaan kategori sistem elektronik, melakukan penentuan tingkat kelengkapan kontrol untuk menerapkan ISO 27001, selanjutnya tentukan tingkat kematangan proses pengelolaan pengamanan informasi yang ada dilapangan. Kemudian lakukan analisis *gap* dari hasil yang didapat dilapangan, evaluasi akan dilakukan pada area yang telah ditetapkan agar dapat menentukan target perencananan selanjutnya.
2. Perancangan manajemen keamanan informasi
   Pada tahapan ini dilakukannya perancangan solusi dari hasil analisis yang telah dilakukan untuk membantu meningkatkan keamanan informasi yang ada di perusahaan. Desain solusi yang akan diberikan pada tahap ini dalam aspek *people*, *Process*, dan *Technology*. Memberikan rekomendasi kepada Direktorat SISFO berupa kebijakan dan SOP dari kontrol objective. Kemudian membuat kesimpulan dari hasil penelitian dengan menyesuaikan pada tujuan penelitian dan memberikan saran agar dapat dikembangkan pada penelitian selanjutnya. Saran yang diberikan sebaiknya sesuai dengan kondisi sistem keamanan informasi pada Direktorat SISFO berdasarkan hasil penilaian indeks KAMI.

Pada penelitian ini data yang akan digunakan disesuaian dengan tiap kategori dalam Indeks KAMI bersama penanggung jawab atau yang memiliki kredibilitas di Direktorat Sistem Informasi, kategori yang termasuk dalam Indeks KAMI adalah:

1) Sistem elektronik
2) Pengelolaan Aset informasi
3) Teknologi dan keamanan Informasi

4) Pengolahan dan Analisis Data

4.1 Hasil Penilaian Pengelolaan Aset Informasi

Berikut ini hasil matriks skor pada area Pengelolaan Aset Informasi:

Tabel 1 Skor Pengelolaan Aset Informasi

Pertanyaan Pengelolaaan Aset Informasi	Total Skor
Jumlah Pertanyaan status pengamanan tahap 1 ada 24 pertanyaan	44
Jumlah Pertanyaan status pengamanan tahap 2 ada 10 pertanyaan	32
Jumlah Pertanyaan status pengamanan tahap 3 ada 4 pertanyaan	0
Batas skor Min untuk skor status pengamanan tahap 3	88
Total skor status pengamanan tahap 1 dan 2	76
Status penilaian status pengamanan tahap 3	Tidak valid
Total evaluasi Pengelolaan Aset Informasi	76

Tabel diatas menunjukkan total skor status pengamanan tahap 1 dan 2 bernilai 76 skor, sedangkan status pengamanan tahap 3 dengan 4 pertanyaan memiliki skor 0. Syarat untuk skor min status pengamanan tahap 3 yaitu di mana seluruh pengamanan tahap 1&2 dalam kondisi "Dalam Penerapan/ Diterapkan Sebagian" dengan total skor 88 status pengamanan tahap 3 menunjukkan "Tidak Valid",berarti penerapan tahap 3 tidak memenuhi batas skor minimal.

4.2 Hasil penilaian Teknologi dan Keamanan Informasi

Pada teknologi dan keamanan informasi ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Terdapat 14 pertanyaan yang berkaitan pada tingkat kematangan II, ada 11 pertanyaan tingkat kematangan III, adan ada 1 pertanyaan terkait tingkat kematangan IV dengan total pertanyaan pada bagian ini ada 26 pertanyaan. Pada area teknologi mensyaratkan adanya strategi yang terkait dengan tingkatan risiko, dan tidak secara eksplisit menyebutkan teknologi atau merk pabrikan tersebut. Pada teknologi dan keamanan informasi pada indeks KAMI menunjukkan hasil sebagai berikut, ini hasil matriks skor padaarea Teknologi dan Keamanan Informasi:

Tabel 2 Skor Teknologi dan Keamanan Informasi

Pertanyaan Teknologi dan Keamanan Informasi	Total Skor
Jumlah Pertanyaan status pengamanan tahap 1 ada 14 pertanyaan	32
Jumlah Pertanyaan status pengamanan tahap 2 ada 10 pertanyaan	46
Jumlah Pertanyaan status pengamanan tahap 3 ada 2 pertanyaan	6
Batas skor Min untuk skor status pengamanan tahap 3	68
Total skor status pengamanan tahap 1 dan 2	78
Status penilaian status pengamanan tahap 3	Valid
Total evaluasi teknologi dan keamanan informasi	84

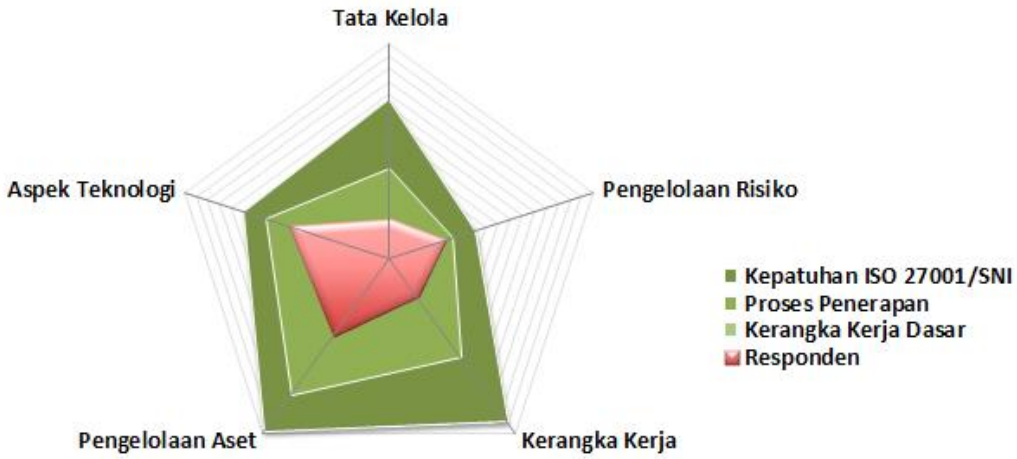
Tabel diatas menunjukkan total skor status pengamanan tahap 1 dan 2 bernilai 78 skor, sedangkan status pengamanan tahap 3 dengan 2 pertanyaan memiliki skor 6. Syarat untuk skor min status pengamanan tahap 3 yaitu di mana rata-rata pengamanan tahap 1&2 dalam kondisi "Dalam Penerapan/ Diterapkan Sebagian" dengan total skor 78, dan status pengamanan tahap 3 menunjukkan "Valid", berarti penerapan tahap 3 telah memenuhi batas skor minimal.

4.3 Hasil dari kajian Penilaian Indeks KAMI

Berdasarkan hasil evaluasi penilaian Indeks KAMI, tingkat kelengkapan penerapann standard ISO 27001 ditunjukkan pada gambar berikut,

Gambar 5 Tingkat Kelengkapan dan Kematangan SMKI

Pada Gambar 6, menunjukkan hasil tingkat kelengkapan penerapan SMKI berada pada area "Kuning" yaitu perlu perbaikan, di mana ketergantungan terhadap TIK dinilai Tinggi dan total jumlah nilai kelengkapan 276 skor, maka dasbor akan menampilkan hasil seperti yang ada di Gambar 6. Pada matriksperan TIK dan Status Kesiapan, pada tingkat ketergantungan tinggi memiliki syarat dalam pencapaian kelengkapan dengan hasil evaluasi batas max untuk warna "merah" dengan skor 272warna "kuning" dengan max skor 455, dan pada warna "hijau" dengan max skor 583. Oleh karena itu perlunya ditingkatkan pengamanan pada seluruh area yang dengan melakukan *self assessment* apabila telah melakukan peningkatan dalam salah satu area yang ada sehingga akan melengkapi kesiapan standard ISO 27001.
Berdasarkan diagram radar dapat dilihat sebagai berikut,



Gambar 6 Diagram Radar tingkat Kelengkapan Area Indeks KAMI

Berdasarkan diagram radar menunjukkan sejauh mana pengamanan yang dilakukan pada kondisi saat ini di Direktorat SISFO untuk mencapai tingkat kelengkapan yang diharapkan. Dalam diagram radar, yang menjadi latar belakang area menunjukkan batas tingkat kelengkapan (kategori) 1 s/d 3 (hijau muda s/d hijau tua), dan masing-masing area ditampilkan dalam area merah. Pada diagram ini Direktorat SISFO masih jauh untuk melengkapi kepatuhan dalam standard ISO 27001, akan tetapi pada direktorat SISFO sisfo sebagian besar sudah masuk pada kerangka kerja dasar pada kondisi saat ini, oleh karena itu direktorat perlu meningkatkan keamanan informasi yang mana tingkat kategori SE yang cukup tinggi dan diperlukannya prosedur ataupun kebijakan dalam mengatasi permasalahan yang berkaitan dengan keamanan informasi.

4.4 Gap Analysis

Gap analisis adalah kegiatan yang dilakukan dengan tujuan untuk membandingkan persyaratan standar ISO 27001 dengan kondisi direktorat SISFO saat ini baik pada aspek kerangka kerja (kebijakan dan prosedur) maupun penerapannya.

Tabel 3 Hasil GAP analisis

Area	Kategori tingkat kelengkapan	Persyaratan	Jawaban	temuan/ hasil wawancara	Bukti	GAP Analisis
Pengelolaan Aset Informasi	5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)	Dalam Penerapan / Diterapkan Sebagian	Sudah tersedia, tapi belum seluruhnya terdaftar, akurat dan terpelihara.	tertera pada dokumen No. Dok : 1. Tel_U-NA-WR2-DSI-KLC-API-IK-01 2. Tel_U-NA-WR2-DSI-KLC-API-IK-02	direktorat Sisfo melakukan dokumentasi terkait daftar inventaris aset yang ada akan tetapi belum ada pemeliharaan secara akurat pada seluruh aset yang terdaftar. Aset informasi perlu dijaga dengan baik dengan melakukan pemeliharaan secara rutin dan pengawasan secara berkala sesuai standar ISO 27001
	5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	Sudah tersedia, berdasarkan standar yang berlaku	pada dokumen Prosedur Pengendalian Informasi Terdistribusi	direktort Sisfo sudah melakukan penerapan dengan baik terkait definisi klasifikasi aset informasi sesuai dengan peraturan perundangan yang berlaku
	5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Dalam Penerapan / Diterapkan Sebagian	sudah tersedia karna sisfo telah mengklasifikasi aset informasi sesuai tingkat kepentingan aset. Tetapi belum menyeluruh di lakukan pengamanan terhadap asetnya.	Pada dokumen Katalog Layanan Aplikasi	direktorat sisfo menerapkan proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan aset
	5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut	Dalam Penerapan / Diterapkan Sebagian	Sudah dilakukan definisi tingkatan akses dari setiap klasifikasi aset informasi	terdapat pada dokumen Katalog layanan Aplikasi	direktorat sisfo sudah menerapkan terkait definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi aksesnya
	5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	Sudah tersedia, setiap perubahan proses bisnis selalu mengusulkan perubahannya di dokumen iso 20000, setiap ada perubahan proses bisnis dirapatkan dahulu, setelah menjadi keputusan dibuat draf perubahan bisnis proses dan diusulkan sesuai dengan alur sampai ke MR (menejemen representative) hingga di approve dan baru bisa digunakan perubahan tersebut.	Pada Dokumen Proses Manajemen Perubahan , No. Dok: Tel_U-UT-WR2-DSI-DI-DP-004	pada area ini direktorat sisfo telah melakukan proses pengelolaan perubahan terhadap sistem, proses bisnis, dan proses teknologi informasi yang dilakukan secara konsisten
	5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	Sudah tersedia konfigurasi standar keamanan sistem	Terdapat pada dokumen Proses Manajemen Perubahan , No. Dok: Tel_U-UT-WR2-DSI-DI-	pada area ini direktorat sisfo telah melakukan proses pengelolaan konfigurasi yang diterapkan sesuai standar keamanan sistem dan di telah didokumentasikan secara formal.
	5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Dalam Penerapan / Diterapkan Sebagian	ada proses perilisan suatu aset baru kedalam lingkungan operasional	pada dokumen Katalog Layanan Aplikasi	pada area ini direktorat sisfo menerapkan proses perilisan suatu aset baru kedalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
	5.8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Dalam Perencanaan	direktorat Sisfo akan melakukan sosialisasi terkait penjelasan mengenai tanggungjawab pengamanan informasi secara individu kepada seluruh karyawan dengan membuat kebijakan	tertera pada MoM Pembahasan persiapan Implementasi ISO 27000	pada area ini direktorat sisfo seharusnya mempunyai dokumen terkait definisi tanggungjawab pengamanan informasi secara individual untuk semua karyawan sehingga dapat meningkatkan kesadaran tentang pentingnya keamanan informasi
	5.9	Tata tertib penggunaan komputer, email, internet dan intranet	Dalam Penerapan / Diterapkan	Sudah ada tetapi masih diterapkan sebagian	perdapat pada dokumen Permintaan dan Penghapusan Layanan	pada area ini direktorat sisfo sudah mempunyai dokumen terkait tata tertib penggunaan komputer, email, intermet, dan intranet.
	5.10	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Dalam Perencanaan	Tidak ada tata tertib masih dalam tahap perencanaan, dan terkait HAKI hanya ada pada logo iGracias	tertera pada MoM Pembahasan persiapan Implementasi ISO 27000	pada area ini direktorat sisfo seharusnya mempunyai dokumen tata tertib pengamanan dan penggunaan aset terkait HAKI tidak hanya pada logo iGracias saja
	5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi	Tidak Dilakukan	belum ada peraturan terkai piranti lunak di aset		pada area ini direktorat sisfo seharusnya memiliki dokumentasi peraturan terkait instalasi piranti lunak di aset TI

A. Identifikasi Area yang tidak Terpenuhi

Identifikasi area yang tidak terpenuhi merupakan hasil dari suatu proses eksisting yang telah dilakukan analisis GAP pada Direktorat Sistem Informasi. Dari hasil identifikasi area yang tidakterpenuhi maupun yang belum dilakukan oleh direktorat akan di gunakan untuk mengetahui apa saja area yang belum memenuhi standar ISO. Dibawah ini merupakan hasil temuan yang telah diidentifikasi dengan meyesuaikan area dan persyaratan yang ada pada indeks KAMI.

Tabel 4Area yang tidak terpenuhi

no	Area Indeks Keamanan Informasi	Kategori Tingkat Kelengkapan	Temuan
1	Pengelolaan Aset Infromasi	5.8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di direktorat sisfomasi masih dalam perencanaan
2		5.10	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI masih dalam perencanaan
3		5.11	Direktorat SISFO belum memiliki peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan
4		5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian izin tertulis oleh pemilik data pribadi masih dalam perencanaan
5		5.16	Direktorat SISFO belum membuat ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya
6		5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi masih dalam perencanaan

7		5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya
8		5.20	direktorat sisfo belum melakukan Proses pengecekan latar belakang SDM
9		5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib masih dalam perencanaan
10	Pengelolaan Aset Informasi	5.26	Direktorat belum memiliki daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya
11		5.27	direktorat sisfo belum melakukan pengamanan akses yang berkaitan dengan pihak ketiga dan belum tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI
12		5.32	belum memiliki peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi/ diluar kantor
13		5.33	belum memiliki preosedur untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)
14		5.36	mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga dalam perancanaan oleh direktorat sisfo
15		5.38	belum tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan direktorat
16	teknologi dan keamanan Informasi	6.10	tidak semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)
17		6.21	rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware belum dimutakhirkan secara rutin dan sistematis dan masih dalam perencanaan
18	teknologi dan keamanan Informasi	6.26	Direktorat belum melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin

B. Hasil Kriteria Risiko

Pada penelitian ini hasil kriteria risiko diperoleh dari hasil penilaian hitungan nilai skala probability dan nilai impact yang menunjukkan kondisi yang terjadi saat ini pada direktorat SISFO. Tabel dibawah ini adalah hasil kreiteria risiko.

Tabel 5Hasil Kriteria Risiko

No	Syarat	Jawaban	Temuan	Assessment risk										
				Deskripsi risiko		Sebelum Penanganan								
				Ancaman	kerentanan	Pemilik risiko	Kontrol saat ini	kategori kontrol	tingkat kemungki	Penjelasan kemungkinan	tingkat dampak	Penjelasan Dampak	Skor risiko	Tingkat risiko
1	(5.8) Definisi tanggung jawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Dalam Perencanaan	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di direktorat sisfomasi masih dalam perencanaan	kurangnya awarness (kesadaran) dari pegawai dan kesulitan dalam mengetahui bertanggung jawab dari tiap personil atas pengamanan informasi yang ada pada direktorat sisfo	pengamanan suatu aset tidak optimal dan keamanan informasi yang dilakukan tidak sesuai dengan standar yang berlaku	Direktorat Sistem Informasi	Belum ada		2	Memungkinkan terjadinya human error saat melakukan pegamanan informasi	2	menimbulkan kelalaian pada tiap personil di direktorat Sisfo	4	Medium
2	(5.10) Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Dalam Perencanaan	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI masih dalam perencanaan	tidak ada pedoman mengenai pengamanan dan penggunaan aset terkait HAKI	kurangnya kesadaran organisasi dalam pengamanan dan penggunaan aset terkait HAKI	Direktorat Sistem Informasi	Belum ada		3	Memungkinkan terjadinya kesalahan penggunaan aset informasi terkait HAKI dan proses pengamanannya	4	menimbulkan kelalaian pada tiap personil di direktorat Sisfo dalam hal pengamanan dan penggunaan aset terkait HAKI	12	High
3	(5.11) Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Tidak Dilakukan	Direktorat Sisfo belum memiliki peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	tidak ada acuan langkah untuk instalasi piranti lunak di aset TI milik direktorat	kurang kesadaran organisasi terhadap aturan terkait instalasi piranti lunak di aset TI milik direktorat	Direktorat Sistem Informasi	Belum ada		3	kemungkinan terjadi kesalahan karena belum adanya acuan pegawai untuk instalasi piranti lunak	3	menimbulkan penundaan aktivitas karena belum adanya peraturan terkait instalasi piranti lunak pada direktorat Sisfo	9	Medium
4	(5.12) Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data	Dalam Perencanaan	Peraturan penggunaan data pribadi yang mensyaratkan pemberian izin tertulis oleh pemilik data pribadi masih dalam perencanaan	kebocoran data pribadi yang akan merugikan direktorat sisfo dalam berbagain aspek	disalah gunakan data pribadi yang tanpa pemberian ijin tertulis pemilik data pribadi	Direktorat Sistem Informasi	Belum ada		3	kemungkinan besar terjadi pada suatu kondisi yang sangat beresiko tinggi karena tidak adanya pengelolaan aset untuk penggunaan data pribadi dengan pemberian izin tertulis	4	menimbulkan hilangnya kepercayaan dari pemilik data pribadi	12	High
5	(5.16) Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak Dilakukan	Direktorat Sisfo belum membuat ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	tidak ada acuan / pedoman terkait pengamanan pertukaran data dengan pihak eksternal	penyalah gunaan aset informasi yang didapat oleh pihak eksternal	Direktorat Sisfo	Belum ada		3	kemungkinan terjadi penyalahguaan data saat pertukaran data dengan pihakl eksternal karena tidak adanya ketetapan keamanan pengelolaan aset dengan pihak eksternal.	4	menimbulkan penyalahgunaan data karena belum adanya Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya pada	12	High
6	(5.17) Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Perencanaan	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi masih dalam perencanaan	merusak data informasi yang ada , pencurian, dan pemalsuan data	meemungkinkan haker untuk meretas dan mengganggu aktivitas yang ada	Direktorat Sisfo	Belum ada		3	kemungkinan timbulnya kegagalan dalam proses pelaporan dan penanganan insiden.	3	menimbulkan permasalahan dengan pihak penggelolah keamanan informasi.	9	Medium
7	(5.19)Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Perencanaan	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya masih direncanakan	memungkinkan adanya pencurian data, kerusakan aset oleh pihak yang tidak berwenang	pihak yang tidak berkepentingan akan leluasa menggunakan aset yang ada tanpa keamanan kusus.	Direktorat Sisfo	Belum ada		3	kemukinan timbulnya ketidak sesuaian klasifikasi aset.	3	menimbulkan kerusakan fisik suatu aset dizona pengawasan yang mengakibatkan kerugian finansial	9	Medium
8	(5.20) Proses pengecekan latar belakang SDM	Tidak Dilakukan	direktorat sisfo belum melakukan Proses pengecekan latar belakang SDM	penempatan tugas yang diberikan ke pegawai tidak sesuai dengan latar belakang , kurangnya pengetahuan dalam posisi yang ditempati	tidak tercapainya tujuan perekrutan pegawai sesuai dengan posisi yangakan ditempatkan	Direktorat Sisfo	Belum ada		2	kemungkinan akan terjadi kurangnya rasa tanggung jawab dalam mengerjakan tugas yang diberikan	3	tidak tercapainya tujuan dalam perekrutan pegawai	6	Medium
9	(5.21) Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Dalam Perencanaan	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib masih dalam perencanaan	kesalahpahaman antar kedua belah pihak yang akan menimbulkan masalah baru yang lebih parah lagi	permasalahan yang dihadapi akan semakin bertambahan besar yang akan menyebabkan kerugian dalam waktu, pemeliharaan perangkat, hingga financial	Direktorat Sisfo	Belum ada		3	kemungkinan tidak ada penyelesaian terhadap insiden yang terjadi	4	akan terjadi gangguan terhadap kinerja operasional	12	High
10	(5.26) Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak Dilakukan	Direktorat belum memiliki daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya	insiden yang pernah terjadi atau sedang terjadi sewaktu–waktu akan terulang kembali akan berdampak pada efektifitas dan efisiensi pada perbaikan dan pemeliharaan suatu aset	masalah yang timbul akan terulang kembali, tidak sesuai dengan klasifikasinya	Direktorat Sisfo	Belum ada		3	Kemungkinan tidak ada bukti pelaksanaan keamanan imformasi sesuai dengan klasifikasinya	4	akan terjadi kurang optimalnya penanganan keamanan yang telah dilakukan	12	High
11	(5.27) Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/ vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Tidak Dilakukan	direktorat sisfo belum melakukan pengamanan akses yang berkaitan dengan pihak ketiga dan belum tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI	apabila terjadi kesalahan dalam menggunakan perangkat milik pihak ketiga tanpa memastikan aspek HAKI akan merusak hubungan baik antar kedua belah pihak sehingga hilangnya kepercayaan dari mitra kerja	hilangnya legalitas dari suatu aset data yang dimiliki oleh salah satu pihak	Direktorat Sisfo	Belum ada		2	kemungkinan besar terjadi karena belum adanya pedoman atau acuan pengamanan akses untuk pegawai dalam penggunaan perangkat pengolah informasi milik mitra kerja	3	Menimbulkan kerusakan fisik pada perangkat pengolah informasi milik pihak ketiga karna tidak pengamanan akses	6	Medium
12	(5.32) Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi/ diluar kantor	Tidak Dilakukan	belum memiliki peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi/ diluar kantor	tidak ada acuan dalam memangamankan perangkat komputasi milik direktorat pada saat digunakan diluar lokasi kerja	penyalah gunaan perangkat komputasi oleh karyawan saat berada diluar lokasi kerja	Direktorat Sisfo	Belum ada		3	kemungkinan besar terjadi karena belum adanya pedoman atau acuan pengamanan perangkat komputasi milik direktorat jika berada diluar lokasi kerja	3	menimbulkan kerusakan pada perangkat komputasi karena tidak ada pengamanan yang dilakukan	9	Medium
13	(5.33) Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya	Tidak Dilakukan	belum memiliki preosedur untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)	hilangnya nilai suatu aset apabila digunakan kembali saat terjadi perpindahan lokasi kerja/ tempat	kurangnya perhatian karyawan terhadap nilai aset yang dimilik apa bila terjadi perpindahan lokasi kerja	Direktorat Sisfo	Belum ada		3	kemungkinan besar terjadi karena belum adanya pedoman atau acuan pemindahan aset TIK dari lokasi yang telah ditetapkan	3	menimbulkan terjadi kesalahan dalam memindahan aset TIK dari lokasi yang sudah dialokasikan.	9	Medium
14	(5.36) Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak	Dalam Perencanaan	mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga dalam perancanaan oleh direktorat sisfo	kerusakan pada aset saat pengiriman	tidak acuan/ pedoman dalam pengamanan proses pengiriman suatu aset dengan pihak ketiga	Direktorat Sisfo	Belum ada		2	kesalahan mekanisme pengaman dalam pengiriman aset informasi kepihak ketiga.	4	kesalahan mekanisme pengiriman mengakibatkan aset yang diterima pihak ketiga tidak sesuai dengan permintaan	8	medium
15	(5.38) Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk	Tidak Dilakukan	belum tersedia proses untuk mengamankan lokasi kerja dari keberadaan/ kehadiran pihak ketiga yang bekerja untuk kepentingan direktorat	Kehilangan data, dan bocornya informasi penting milik direktorat jika tidak ada pedoman dalam mengamankan lokasi kerja dari kehadiran pihak ketiga	Data rahasia akan mudah bocor dan kurangya pengawasan langsung dari pegwai yang berkepentingan	Direktorat Sisfo	Belum ada		3	ketidak ketersedian pengamanan lokasi kerja yang dapat mengetahui keberadaan /kehadiran pihak ketiga.	4	akibat tidak ada keamanan dilokasi kerja maka akan menyulitkan untuk mengetahui keberadaan /kehadiran pihak ketiga.	12	High
16	(6.10) Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Perencanaan	tidak semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)	Data pribadi yang tersimpan di Direktorat akan dengan mudah mendapatkan pelanggaran karna kurangnya analisa pada semua log jika dilakukan audit oleh pihak eksternal	Data rahasia yang tidak terjagadengan baik yang sisebabkan karna akses yang tidak sah ke file dan folder yang ada, dan dapat menimbulkan pelanggaran terhdap keamanan.	Direktorat Sisfo	Belum ada		3	kemungkinan ada log yang tidak dianalisi secara berkala sehingga kepastian,akurasi dan validasi kelengkapan isi,untuk keperluan audit.	4	akibat kesalahan analisis tidak secara berkala akurasi dan validasi sehingga tidak semua log dapat teranalisis secara lengkap.	12	High
17	(6.21) Apakah ada rekaman dan hasil analisa (jejak audit – *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan	Dalam Perencanaan	rekaman dan hasil analisa (jejak audit – *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware belum dimutakhirkan secara rutin dan sistematis dan masih	Kurangnya bukti pada saat analisa audit yang dapat mengkonfirmasi bahwa antivirus/ antimalware telah dilakukan pemutakhiran secara sistematis dan rutin	Antivirus yang digunakan tidak sesuai sebagaimana mestinya, karna tidak ada rekaman analisa yang tepat untuk bukti audit.	Direktorat Sisfo	Belum ada		4	Kemungkinan tidak ada bukti hasil analisa yang mengkonfirmasi antivirus/ antimalware telah di mutakhirkan secara rutin sesuai dengan klasifikasinya	3	kurang optimalnya penanganan audit yang membutuhkan bukti analisis pemutakhiran antivirus/antimalware secara sistematis dan rutin	12	High
18	(6.26) Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi	Tidak Dilakukan	Direktorat belum melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin	Terjadi permasalahan pada pelanggaran hukum yang berlaku karna pengamanan yang belum teruji kehandalan keamanan informasinya.	Permasalahan akan merugikan direktorat dalam hal financial dikarenakan kurang handalnya keamanan informasi yang dimiliki	Direktorat Sisfo	Belum ada		3	memungkinkan kehandalan keamanan informasi tidak sesuai dengan standar yang berlaku karna tidak melibatkan pihak independen	4	keamanan informasi yang dilaksanakan tidak secara legal diterima oleh tim audit eksternal	12	High

5) PERANCANGAN KEAMANAN INFORMASI

Pada perancangan keamanan informasi ini akan menjadi salah satu usulan dari penulis untuk membantu Direktorat SISFO dalam mencapai target penerapan Standar ISO 27001 melalui penilaian dengan menggunakan Indeks KAMI yang telah mengacu pada standar tersebut. Dari hasil analisis yang telah dilakukan beberapa kontrol yang dapat diterapkan oleh direktorat SISFO sebagai pendukung dalam rekomendasi perancangan Indeks Keamanan Informasi. Perancangan yang diajukan pada penulisan ini yaitu pada perancangan *Process,diakses*, dan teknologi.

A. Perancangan Process

Perancangan proses merupakan salah satu rancangan usulan dalam alur proses bisnis berupa dokumen kebijakan, prosedur, dan dokumen lainnya. Kebijakan dan prosedur yang dibuat dengan memperhatikan rekomendasi kontrol sesuai standar area yang belum terpenuhi pada Indeks KAMI. Kebijakan ini akan menjadi acuan atau pedoman dalam pelaksanaan Aktivitas pada Direktorat SISFO. Perancangan kebijakan yang direkomendasikan adalah kebijakan pengelolaan aset keamanan informasi.

a. Perancangan Kebijakan Keamanan Informasi
b. Perancangan SOP (Standard Operasional Prosedure)

B. Perancangan Aspek People

Perancangan People adalah suatu rancangan yang dibuat dari hasil pengelolaan risiko dalam Indeks KAMI yang membutuhkan kontrol pada sumber daya manusia untuk dapat meningkatkan kinerja dari Direktorat SISFO. Pada perancangan ini akan ada beberapa usulan penambahan deskripsi kerja terhadap struktur organisasi Direktorat Sistem Informasi.

C. Perancangan Roadmap

Roadmap merupakan perencanaan pengamanan informasi berdasarkan jangka waktu pelaksanaan kegiatan yang akan dilakukan untuk dapat mencapai tujuan perusahaan. Perancangan roadmap di peroleh dari hasil analisis tingkat risiko yang tertinggi yang akan dilakukan dalam triwulan ke-3 dengan berkala ditiap kegiatan memiliki waktu yang berbeda.

6) KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian pada Direktorat Sistem Informasi yang dilakukan menggunakan Indeks KAMI, maka didapat penerapan SMKI sebagai berikut:

a) Penilaian Kategori Sistem Elektronik pada Direktorat Sistem Informasi menunjukkan total skor 29 point. Hal ini menjelaskan bahwa direktorat SISFO sebagai pengguna TIK sangat berperan penting sehingga tidak bisa dipisahkan dari proses bisnis yang berjalan. Tingginya nilai kategori sistem elektronik ini menegaskan bahwa data yang dikelola Direktorat SISFO secara mandiri ini tersimpan pada layanan yang dibangun oleh direktorat SISFO yaitu i-Gracias. I-Gracias ini digunakan oleh seluruh civitas yang ada di Universitas Telkom untuk segala aktivitas yang berhubungan dengan akademik maupun non akademik. Dampak yang akan dialami jika sistem elektronik tidak berjalan sebagaimana mestinya yaitu merusak alur proses bisnis yang sedang terjadi, timbulnya kerugian finansial, hingga memperlambat kerja adminstrasi dalam mengolah data yang ada.
b) Penilaian Indeks KAMI pada seluruh area memperoleh skor sebesar 276,di mana area pengelolaan aset memperoleh skor 76 dengan tingkat kematangan pada level kematangan II, dan

area teknologi dan keamanan informasi memperoleh skor 84 dengan tingkat kematangan pada level kematangan II. Dari hasil yang diperoleh direktorat Sisfo belum mencapai syarat tingkat kematangan standar ISO/IEC 27001:2013 dengan tingkat kematangan minimalnya III. Hal ini menjelaskan bahwa direktorat Sisfo perlu melakukan perbaikan pada area yang belum terpenuhi di penilaian sebelumnya dengan melakukan penerapan kontrol pada standar ISO 27001:2013 agar dapat mencapai target standar ISO 27001 dan juga dapat menjaga seluruh informasi yang ada pada Direktorat Sistem Informasi.

B. Saran

Saran yang diberikan penulis dari hasil penelitian Indeks KAMI sebagai berikut:

a) Direktorat Sisfo diharapkan melakukan penerapan kontrol pada standar ISO 27001:2013, dengan melaksanakan seluruh kebijakan dan prosedur yang telah dbuat terkait keamanan informasi dan melakukan evaluasi pada area pengolahan aset informasi dan teknologi keamanan infromasi.
b) Melakukan evaluasi keamanan informasi dengan menggunakan Indeks KAMI ini dua kali dalam satu tahun untuk meninjau ulang kesiapan keamanan informasi sekaligus mengukur keberhasilan pada perbaikan yang dilakukan.
c) Pada penelitian selanjutnya disarankan untuk dapat melakukan evaluasi dengan metode indeks KAMI dengan versi terbaru, agar dapat menyesuaikan perubahan pada saat melakukan evaluasi di Direktorat Sistem Informasi.

REFERENSI

[1] Akhirina, Tri Yani, dkk. (2016). Evaluasi Keamanan Teknologi Informasi pada PT Indotama Partner Logistics Menggunakan Indeks Keamanan Informasi (KAMI). Teknosi.Vol. 02, No. 02, Agustus 2016.

[2] Badan Siber dan Sandi Negara.(2018). Indeks KAMIDiakases pada tanggal 15september 2018.https://bssn.go.id/indeks-kami

[3] Candiwan, el al. (2015). Comparison Analysis Of Information Security Risks And Implementation Of ISO27001 On Higher Educational Institutions In Indonesia. Retrieved from International Journal of Basic and Applied Science, 4 (w2) : 40-52.

[4] Chazar, C. (2015). Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005. *Jurnal Informasi,VII*(2), 48–57.

[5] ISACA. (2012). *COBIT 5 for Information Security*.

[6] ISO/ IEC 27001, S. (2005). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements, *2005*. https://doi.org/10.1177/0011128708322943

[7] ISO/ IEC 27001, S. (2013). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements, *2013*. https://doi.org/10.1177/0011128708322943

[8] ISO/IEC 27000, S. (2014). INTERNATIONAL STANDARD ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary, *2014*, 1. Retrieved from papers3://publication/uuid/F41B7AE4-6A56-4A74-B71E-2739C41A3849

[9] Keamanan Informasi, T. D. (2011). Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik.

[10] Keamanan Informasi, T. D. (2017). Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informai (wIndeks KAMI).

[11] Manullang, A. F., Harsono, L. D., & Candiwan. (2017). Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) pada Institusi XYZ . *Journal Information Engineering and Educational Technology,01*, 73–82.

[12] 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

[13] OGC. (2007). ITIL v3 - Service Lifecycle - Introduction to ITIL.

[14] Purwanto, E. (2014). Keamanan Informasi. Retrieved from https://bpptik.kominfo.go.id/2014/03/24/404/keamanan-informasi/

[15] Rashid Ridho, M., Ghozali, K., & Cahyo Hidayanto, B. (2012). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi Dan Informatika Surabaya, *1*(1), 1–6.

[16] Sari, P. K., & Sebastian, J. (2014). Comparison Analysis of Information Security Risks and Implementation of ISO27001 on Higher Educational Institutions in Indonesia, (October), 40–52.

[17] Sugiyono. (2016). *Metode Penelitian Kuantitatif, Kualitatif, dan R & D.* Bandung: Alfabeta.