AICOMS
Applied Information Technology and Computer Science
e-ISSN: 2964-7703
Vol. 2 No. 1, Juni-2023, pp. 15-22

Audit Manajeman Keamanan Informasi Untuk Kelayakan Keamanan Sistem Informasi (Studi Kasus : Politeknik Lamandau, Kalimantan Tengah)

Rahmat Hidayat[1,*], Ariana Febriani[2], Kurnia Ayu Nilam Sari[3], dan Riska Puji Rahayu[4]

[1] Jurusan Teknologi Rekayasa Komputer, Politeknik Lamandau; rahmathidayat@polilaman.ac.id; 1arianafebriani1902@gmail.com; kurniaayunilamsari@gmail.com; rriskapuji@gmail.com
* Korespondensi: rahmathidayat@polilaman.ac.id

Info Artikel:
Dikirim: 15 Februari2023
Direvisi: 10 Mei 2023
Diterima: 20 Mei 2023

Intisari: Harus ditulis dalam satu paragraf yang terdiri atas maksimum 200 kata. Untuk artikel ilmiah, abstrak harus memberikan gambaran terkait hal yang dikerjakan. Kami sangat menyarankan penulis untuk menggunakan gaya abstrak terstruktur berikut, tetapi tanpa judul: (1) Latar Belakang: Tempatkan pertanyaan dalam konteks yang luas dan menyoroti tujuan penelitian; (2) Metode: jelaskan secara singkat metode atau perlakuan utama yang diterapkan; (3) Hasil: merangkup temuan utama artikel; (4) Kesimpulan: menunjukkan kesimpulan utama atau interpretasi. Abstrak harus merupakan representasi objektif dari artikel dan tidak boleh berisi hasil yang tidak disajikan dan dibuktikan dalam teks utama dan tidak boleh melebih-lebihkan kesimpulan utama.

Kata Kunci: ISMS; Politeknik Lamandau; index KAMI; ISO2700:2009

1. Pendahuluan

Politeknik Lamandau di Kalimantan Tengah telah mengimplementasikan sistem elektronik sebagai sarana untuk memberikan pelayanan kepada masyarakat, terutama kepada civitas akademik. Namun, sebagai penyelenggara pelayanan publik, Politeknik Lamandau harus memastikan bahwa sistem elektronik yang digunakan beroperasi dengan tingkat keamanan yang tinggi. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia telah menetapkan bahwa setiap penyelenggara sistem elektronik untuk pelayanan publik wajib menjalankan sistem elektronik dengan tingkat keamanan yang tinggi, dan audit manajemen keamanan sistem elektronik juga diperlukan untuk memastikan keamanan yang sesuai.

Karena data yang dikelola oleh Politeknik Lamandau sangat penting dan dianggap sebagai aset utama, penting untuk menjamin kerahasiaan, keutuhan, dan ketersediaan informasi tersebut. Politeknik Lamandau telah melakukan identifikasi terhadap potensi ancaman yang mungkin terjadi, baik yang disengaja seperti serangan dari individu atau organisasi kriminal, maupun yang tidak disengaja seperti kemungkinan kerusakan perangkat komputer atau bencana alam seperti gempa bumi dan kebakaran.

Sebelum menerapkan standardisasi keamanan informasi, evaluasi sistem keamanan informasi di Politeknik Lamandau perlu dilakukan untuk mendapatkan gambaran kondisi kesiapan dan kematangan manajemen keamanan informasi. Dalam penelitian ini, akan dilakukan pengukuran tingkat kematangan manajemen keamanan informasi di Politeknik Lamandau menggunakan model yang disiapkan oleh Kementerian Komunikasi dan Informatika Republik Indonesia pada tahun 2008, yaitu Indeks KAMI. Indeks KAMI dibuat dengan mengacu pada standar ISO 27001:2009 yang mengatur keamanan informasi. Standar ini mencakup berbagai aspek keamanan informasi, termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas.

Penelitian sebelumnya, seperti "Information Security Readiness of Government Institution in Indonesia", telah memberikan gambaran tentang status keamanan informasi di sektor pemerintah Indonesia. Hasil penelitian tersebut menunjukkan bahwa sebagian besar instansi pemerintah masih membutuhkan perbaikan dalam memenuhi standar

keamanan informasi. Oleh karena itu, penting untuk melakukan evaluasi dan perbaikan keamanan informasi di lembaga pendidikan seperti Politeknik Lamandau.

Penelitian lainnya, seperti "Analysis of Information Security through Asset Management in Academic Institutes of Pakistan", juga menekankan pentingnya standar praktik keamanan terbaik, termasuk standar ISO 27001, dalam memastikan keamanan informasi. Aset utama suatu organisasi adalah informasi yang disimpan dalam berbagai komponen, baik dalam bentuk elektronik maupun perangkat keras. Manajemen aset yang efektif merupakan kunci untuk mencapai tujuan organisasi dan menjaga keamanan informasi.

Dalam konteks lembaga akademik, untuk mencapai tujuan yang diharapkan, penting bagi mereka untuk mematuhi standar ISO 27001 yang bersertifikasi. Standar ini memberikan kebijakan, prosedur, dan pedoman terkait semua aspek keamanan informasi, termasuk keamanan fisik dan keamanan jaringan. Melakukan survei di lembaga akademik dapat membantu memeriksa tingkat keamanan sesuai dengan aspek-aspek tersebut dan memberikan pemahaman yang jelas tentang tindakan yang dilakukan dan perbaikan yang harus dilakukan.

Dengan mempertimbangkan konteks ini, penelitian ini bertujuan untuk mengukur tingkat kematangan manajemen keamanan informasi di Politeknik Lamandau dengan menggunakan Indeks KAMI sebagai alat untuk mengevaluasi keamanan informasi. Melalui penelitian ini, diharapkan dapat diberikan rekomendasi dan pedoman bagi pihak manajemen Politeknik Lamandau dalam meningkatkan keamanan sistem informasi mereka dan melindungi aset informasi yang penting.

A. Indeks KAMI

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di Instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi [4]. 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 27001:2009. Pengukuran dalam Indeks KAMI dapat dilakukan dengan alur proses berikut : a. Mendifinisikan Ruang Lingkup

b. Menetapkan Peran atau Tingkat Kepentingan TIK di Instansi
c. Menilai Kelengkapan Pengamanan 5 Area
d. Mengkaji Hasil Indeks KAMI disertai dengan menetapkan langkah-langkah perbaikan

B. Penggunaan Indeks KAMI

Sebelum proses penilaian dilakukan secara kuantitatif, proses klasifikasi dilakukan terlebih dahulu terhadap peran TIK dalam instansi atau cakupan evaluasinya. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik kepentingan TIK yang sama. Dapat dilihat pada gambar 1. Memberikan ilustrasi tampilan evaluasi peran TIK berikutpilihannya[Minim (0);

Rendah (1); Sedang (2); Tinggi (3); Kritis (4)] dan tabel pemetaan hasil penjumlahan menjadi 4 (empat) klasifikasi (Rendah; Sedang; Tinggi; Kritis).

Data yang digunakan dalam evaluasi ini nantinya akan memberi snapshot indeks kesiapan (kelayakan) dan kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding menyusun langkah-langkah perbaikan dan penetapan prioritasnya.

Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status
6.9	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Perencanaan
6.10	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Tidak Dilakukan
6.11	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan
6.12	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Tidak Dilakukan
6.13	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Dalam Perencanaan
6.14	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Tidak Dilakukan
6.15	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Tidak Dilakukan
6.16	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Tidak Dilakukan
6.17	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Tidak Dilakukan
6.18	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Tidak Dilakukan
6.19	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Dalam Perencanaan

Gambar 1. Penggunaan Indeks KAMI pada Teknologi dan Keamanan Informasi

Penggunaan dan publikasi hasil evaluasi indeks KAMI merupakan bentuk tanggung jawab dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi. Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan atau kematangan kepada pihak yang terkait (stakeholders). Untuk peran TIK di instansi memiliki penilaian yang berbeda dari beberapa bagian lainnya dikarenakan Peranan TIK di instansi ini diharapkan untuk mendapatkan nilai dari ketergantungan instansi itu sendiri akan perananan teknologi dan sistem informasinya. Skor penilaian untuk peran TIK di instansi dapat dilihat pada tabel 1

Tabel 1. Skor Penilaian TIK di Instansi

Skor Peran TIK	
Minim	0
Rendah	1
Sedang	2
Tinggi	3
Sangat Tinggi / kritis	4

Akan tetapi untuk untuk bagian-bagian lainnya seperti tata kelola keamanan informasi, pengelolaan resiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, serta teknologi dan keamanan informasi, memiliki penilain yang berbeda dari tiap pertanyaan yang diajukannya. Seluruh pertanyaan yang ada dalam setiap area dikelompokkan menjadi 3 (tiga) kategori pengamanan, sesuai dengan tahapan dalam penerapan standar ISO/IEC 27001. Pertanyaan yang terkait dengan kerangka kerja dasar keamanan informasi masuk dalam kategori "1", untuk efektivitas dan konsistensi penerapannya didefinisikan sebagai kategori "2", dan hal-hal yang merujuk pada kemampuan untuk selalu meningkatkan kinerja keamanan informasi adalah kategori "3".

Responden kemudian diminta untuk menjawab setiap pertanyaan dengan pilihan Status Penerapan:

a. Tidak Dilakukan
b. Dalam Perencanaan
c. Dalam Penerapan atau Diterapkan Sebagian
d. Diterapkan Secara Menyeluruh.

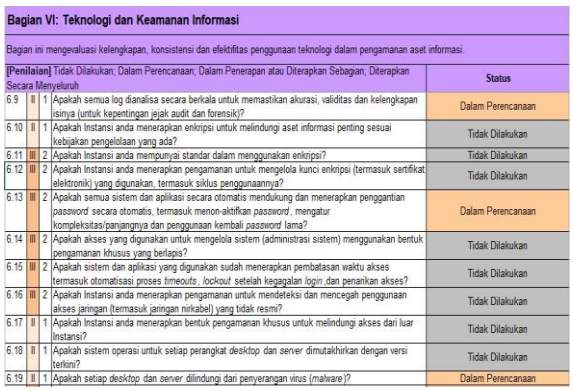
Setiap jawaban akan diberikan skor yang nilainya disesuaikan dengan tahapan penerapan (kategori) bentuk pengamanan. Untuk tahapan awal nilainya akan lebih rendah dibandingkan tahapan berikutnya. Demikian halnya untuk status penerapannya, penerapan yang sudah berjalan secara menyeluruh memberikan nilai yang

lebih tinggi dibandingkan bentuk penerapan lainnya.Tabel pemetaan skor dapat dilihat pada Tabel 2. Tabel ini merangkum seluruh jumlah jawaban penilaian mandiri dan membentuk matriks antara status pengamanan dan kategori.

Tabel 2. Skor Tahap Pengamanan

Status Pengamanan	**Tingkat Kematangan**		
	1	2	3
Tidak dilakukan	0	0	0
Dalam perencanaan	1	2	3
Dalam penerapan atau diterapkan sebagian	2	4	6
Diterapkan secara menyeluruh	3	6	9

Nilai untuk kategori pengamanan yang tahapannya lebih awal, lebih rendah dibandingkan dengan nilai untuk tahapan selanjutnya. Hal ini sesuai dengan tingkat kompleksitas yang terlibat dalam proses penerapannya. Catatan: untuk keseluruhan area pengamanan, pengisian pertanyaan dengan kategori "3" hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan kategori "1" dan "2" sudah di isi dengan status minimal "Diterapkan Sebagian". Dapat di lihat pada gambar 2 berikut



Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status
6.9	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Perencanaan
6.10	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Tidak Dilakukan
6.11	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan
6.12	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Tidak Dilakukan
6.13	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Dalam Perencanaan
6.14	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Tidak Dilakukan
6.15	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Tidak Dilakukan
6.16	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Tidak Dilakukan
6.17	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Tidak Dilakukan
6.18	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Tidak Dilakukan
6.19	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Dalam Perencanaan

Gambar 2. Ilustrasi kesiapan dan kematangan keamanan informasi

Keterangan Ilustrasi:
1. Kolom yang menunjukkan kategori kematangan terkait pertanyaan yang dibahas
2. Kolom yang menunjukkan kategori tahap penerapan
3. Daftar pertanyaan
4. Pilihan jawaban

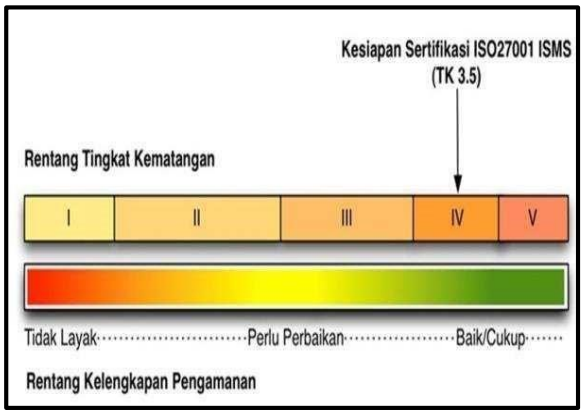
Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan kondisi penerapan keamanan informasi sesungguhnya. Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan azas keterbukaan dan kejujuran. Jika sudah mendapatkan hasil dari penilaian atas penerapan dari tiap-tiap bagian yang ada, maka pimpinan instansi dapat melihat kebutuhan pembenahan yang diperlukan dan korelasi antara berbagai area penerapan keamanan informasi. Adapun korelasi antara peran atau tingkat kepentingan TIK dalam instansi didefinisikan melalui tabel 3 berikut ini

Tabel 3. Matriks peran TIK dan status kesiapan

Peran TIK				
Rendah		Indeks (SkorAkhir)		Status Kesiapan
0	12	0	124	TidakLayak
		125	272	PerluPerbaikan
		273	588	Baik/Cukup
Sedang		SkorAkhir		Status Kesiapan
13	24	0	174	TidakLayak
		175	312	PerluPerbaikan
		313	588	Baik/Cukup
Tinggi		SkorAkhir		Status Kesiapan
25	36	0	272	TidakLayak
		273	392	PerluPerbaikan
		393	588	Baik/Cukup
Kritis		SkorAkhir		Status Kesiapan
37	48	0	333	TidakLayak
		334	453	PerluPerbaikan
		454	588	Baik/Cukup

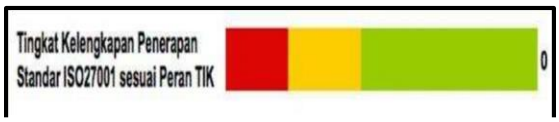
Pengelompokan kedua dilakukan berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan di institusi seperti pada gambar 3. Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefiisikan sebagai berikut:

a. Tingkat I – Kondisi Awal
b. Tingkat II Penerapan Kerangka Kerja Dasar
c. Tingkat III – Terdefiisidan Konsisten
d. Tingkat IV – Terkelola dan Terukur
e. Tingkat V – Optimal



Gambar 3. Tingkat kematanagn Dalam Indeks KAMI

Status Kesiapan atau Kelengkapan dapat ditampilkan dengan instrumen Bar Chart atau diagram batang seperti terlihat pada gambar 4



Gambar 4. Bar Chart Tingkat Kelengkapan Penerapan Standar ISO2700

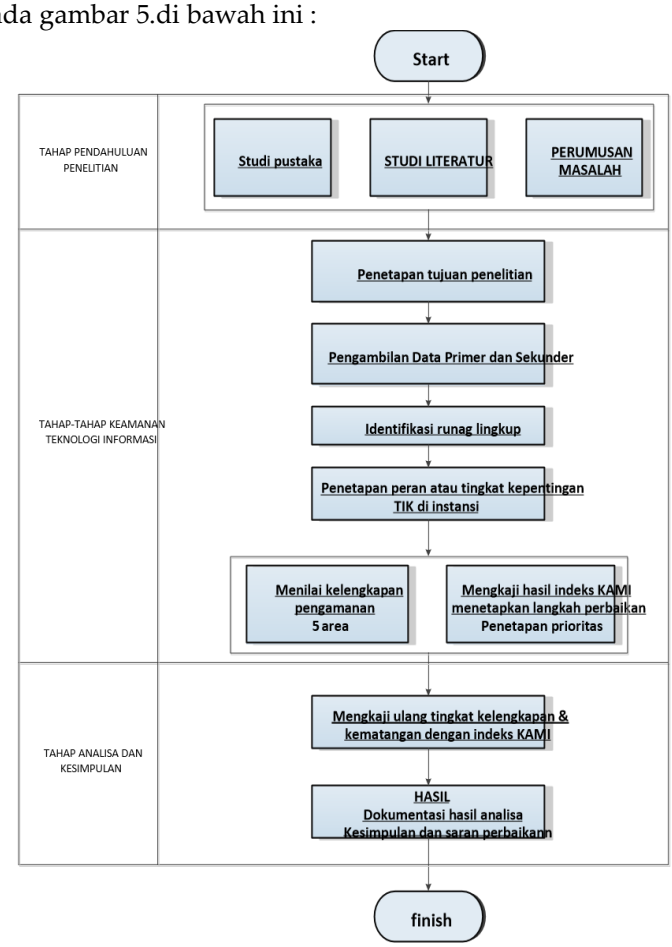
2. METODE PENELITIAN

Metodologi penelitian merupakan suatu metode yang digunakan untuk menentukan langkah-langkah yang harus dilakukan dalam sebuah penelitian. Metode penelitian yang digunakan adalah metode deskriptif dengan pendekatan penelitian kualitatif dan kuantitatif.

a. Perumusan masalah : mengumpulkan permasalahan yang ditemukan dan disatukan dalam suatu research question. Selanjutnya research question ini digunakan sebagai pedoman, penentu arah atau fokus dari penelitian.
b. Studi literarur : Melakukan review, pembandingan dan melihat literarur yang terkait dengan penelitian.
c. Pengumpulan data : Pada tahapan ini dilakukan pengumpulan data secara kualitatif dengan melakukan wawancara, observasi dan kuisioner.
d. Mendefinisikan ruang lingkup variabel evaluasi
e. Analisa data dan Pembuatan indeks penilaian merujuk pada penggunaan Indeks KAMI.
f. Melakukan verifikasi pada tingkat kematangan pada sistem manajemen keamanan informasi di Politeknik Lamandau
g. Kesimpulan dan saran : penarikan kesimpulan berdasarkan hasil penelitian

2.1. Alur Penelitian

Agar penelitian ini berjalan dengan sistematis dan terstruktur maka peneliti harus membuat alur penelitian seperti yang tercantum pada gambar 5.di bawah ini :



Gambar 5. Alur Penelitian

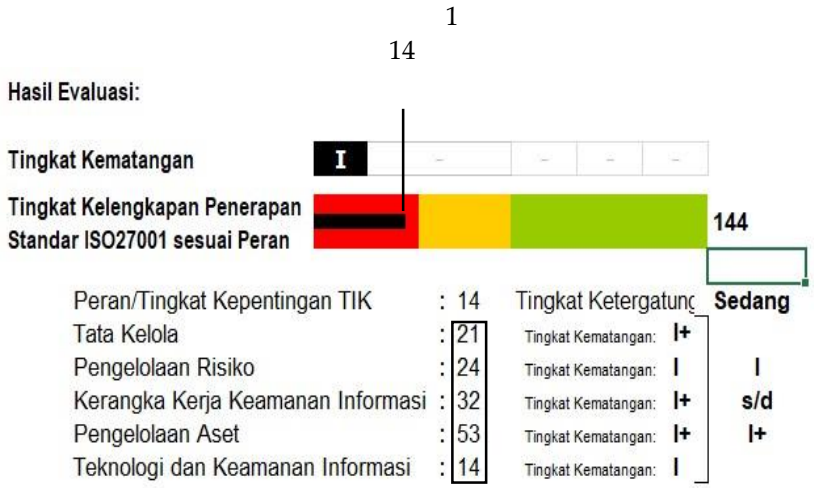
4. Hasil Penelitian

Langkah pertama penggunaan indeks KAMI adalah dengan menjawab pertanyaan terkait kesiapan pengamanan informasi, dalam hal ini responden di minta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis.Setelah itu dilakukan menjawab pertanyaan atau kuisioner terkait pengukuran kesiapan keamanan informasi pada bagian Teknologi Keamanan Informasi, hasilnya pada tabel 4 berikut ini :

Tabel 4. Pengukuran Hasil Teknologi Keamanan Informasi

Bagian VI : Teknologi dan Keamanan Informasi							
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi							
Jumlah Pertanyaan	TP1	TP2	TP3	Total			
	13	10	1	24 butir			
Hasil Jawaban Responden Bagian VI							
Sistem Pengamanan	Tingkat Kematangan						
	TP 1	SKOR TP 1	TP 2	SKOR TP 2	TP 3	SKOR TP 3	Total
Tidak Dilakukan	5	0	7	0	1	0	0
Dalam Perencanaan	8	8	3	6	0	0	14
Dalam Penerapan atau Diterapkan Sebagian	0	0	0	0	0	0	0
Diterapkan Secara Menyeluruh	0	0	0	0	0	0	0
Total Nilai Evaluasi Teknologi dan Keamanan Informasi di Politeknik Lamandau, Kalimantan Tengah							14

Berdasarkan hasil perhitungan total skor kesiapan keamanan informasi pada bagian Teknologi Keamanan Informasi di Politeknik Lamandau pada gambar 5 tingkat kematangan berada level I, dimana hasil evaluasi pada bagian Teknologi Keamanan Informasi berada pada tingkat 14 yang berarti kondisi persiapan peran TIK di Politeknik Lamandau masih berstatus sedang akan tetapi tidak layak. Pada tingkat kematangan level I yaitu tidak ada ambang batas minimum yang diasumsikan semua responden diberikan status ini pada saat dimulainya evaluasi



Gambar 5. Hasil evaluasi

Tabel 5. Kesiapan SMKI di Politeknik Lamandau

Peran TIK				
Rendah		Indeks (SkorAkhir)		Status Kesiapan
0	12	0	124	TidakLayak
		125	272	PerluPerbaikan
		273	588	Baik/Cukup
Sedang		SkorAkhir		Status Kesiapan
13	24	0	174	TidakLayak
		175	312	PerluPerbaikan
		313	588	Baik/Cukup
Tinggi		SkorAkhir		Status Kesiapan
25	36	0	272	TidakLayak
		273	392	PerluPerbaikan
		393	588	Baik/Cukup
Kritis		SkorAkhir		Status Kesiapan
37	48	0	333	TidakLayak
		334	453	PerluPerbaikan
		454	588	Baik/Cukup

5. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa :

a. Tingkat kelengkapan dan kematangan
SMKI pada bagian Teknologi Keamanan Informasi di Politeknik Lamandau, Kalimantan Tengah dengan menggunakan model indeks KAMI masih berada pada level I, berarti tidak ada ambang batas minimum yang diasumsikan semua responden diberikan status ini pada saat dimulainya evaluasi.

b. Nilai hasil evaluasi tingkat kesiapan penerapan pada bagian Teknologi Keamanan Informasi medapat skor 14, dengan total keseluruhan evaluasi 114. Maka dalam matriks peran TIK dan Status kesiapan berada pada tingkat sedang dengan kondisi "Tidak Layak" karena semakin tinggi ketergantungan terhadap TIK atau semakin penting peran TIK maka harus semakin banyak bentuk pengamanan yang di perlukan dan harus di terapkan sampai tahap tertinggi.

Untuk mendapatkan SMKI yang standard ISO27001:2009/SNI maka yang harus di lakukan terkait penerapan SMKI di Politeknik Lamandau, Kalimantan Tengah. Peneliti menyarankan sejumlah hal sebagai berikut:

1. Melaksanakan sejumlah program peningkatan awareness pimpinan dan pejabat tentang arti penting SMKI, baik dari sisi aturan maupun penerapannya, seperti program sosialisasi, internalisasi, workshop, seminar dan pelatihan terkait keamanan informasi dengan melibatkan pihak yang pimpinan instansi dan pihak yang terlibat dengan harapan bahwa pengembangan SMKI dapat menjadi bagian dari Rencana Strategis
Politeknik Lamandau
2. Melakukan evaluasi secara berkala terhadap kerangka kerja keamanan informasi sehingga bisa melihat adanya perubahan kondisi keamanan informasi yang sedang diterapkan.
3. Meningkatkan kematangan pada Teknologi Keamanan Informasi agar tingkat kesiapan di Politeknik Lamandau agar semakin lebih baik.

Daftar Pustaka

[1] Badan Sertifikasi Nasional. (2009) Standar Nasional Indonesia (SNI)–ISO/IEC 27001:2009), Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan informasi – Persyaratan. Jakarta.

[2] Direktorat Keamanan Informasi, Kementerian Komunikasi dan Informatika. (2011) Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Jakarta.

[3] Kautsarina. et al. (2014) Information Security Readiness of Government Institution in Indonesia, 978-1-4799-3580 2/14/$31.00©2014 IEEE.

[4] Marco. R. (2016) Indeks Penilaian Tingkat Kematangan (Maturity) It Governance pada Manajemen Keamanan Layanan Teknologi Informasi, Jurnal DASI vol. 17 no. 2. Pp 7682, ISSN: 1411-3201.

[5] Nadia. M. (2015) Analysis of Information Security through Asset Management in Academic Institutes of Pakistan, 10.1109/ICICT.2015.7469581 IEEE.