Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) pada Institusi Xyz

Astri F. Manullang[1], Candiwan[2], Listyo Dwi Harsono[3]

[1,2,3] Program Studi S1 Manajemen Bisnis Telekomunikasi dan Informatika, Universitas Telkom
[1]astrimanullang60@gmail.com
[2]candiwan@telkomuniversity.ac.id
[3]listyo@telkomuniversity.ac.id

***Abstrak*— Perkembangan teknologi informasi memberikan kemudahan bagi setiap institusi dalam menjalankan tugas dan fungsinya. Institusi yang menerapkan teknologi informasi harus menjaga keamanan informasi yang dimiliki agar pengelolaanya dapat dilakukan dengan cepat dan akurat sehingga dapat menghindari terjadinya kegagalan atau pelanggaran. Institusi XYZ pada saat ini telah menerapkan teknologi informasi, tetapi informasi yang dimiliki belum dilindungi dengan baik. Pada institusi XYZ terdapat akses kontrol yang belum dilaksanakan dengan baik diantaranya kurang keamanan atau pengawasan lokasi kerja penting (ruang server, ruang arsip) sehingga siapa saja bebas untuk melakukan akses, kemudian pada institusi XYZ belum menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel). Oleh karena itu penting melakukan asesmen terhadap institusi XYZ untuk mengetahui tingkat kematangan dan kelengkapan keamanan informasinya. Asesmen dilakukan menggunakan Indeks Keamanan Informasi (KAMI) yang dikeluarkan oleh Departemen Komunikasi dan Informasi yang telah memenuhi syarat dan aspek keamanan informasi yang mengacu pada ISO 27001. Metode yang digunakan adalah metode kualitatif yaitu Indeks KAMI sebagai alat ukur untuk menilai sistem manajemen keamanan informasi institusi XYZ. Hasil penilaian Indeks KAMI pada Institusi XYZ menunjukkan tingkat ketergantungan terhadap Sistem Elektronik tergolong tinggi dan status kesiapan dalam manajemen keamanan informasi tidak layak dan berada pada level I-I+ dimana level ini masih berada pada kondisi awal penerapan keamanan informasi. Sehingga Institusi XYZ harus melakukan perbaikan dan peningkatan kontrol keamanan dengan pembuatan kebijakan dan prosedur keamanan informasi yang sesuai dengan kondisi TI/SI dengan memperhatikan kesiapan, sumber daya yang dimiliki untuk mendapatkan penerapan sistem manajemen keamanan informasi yang efektif dan efisien.**

***Kata Kunci*— asesmen, indeks KAMI, keamanan informasi**

I. PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi pada era digital saat ini semakin pesat. Seiring dengan perkembangan teknologi informasi tersebut institusi - institusi di indonesia menerapkan teknologi informasi dalam institusi mereka untuk mempermudah dan melancarkan kegiatan yang mereka lakukan. Teknologi informasi dimanfaatkan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan pemerintahan dan merupakan informasi yang strategis untuk mengambil keputusan.

Informasi yang diolah oleh setiap institusi harus dijaga kerahasiaan dan keamanannya, karena informasi atau data – data yang dimiliki oleh sebuah institusi merupakan aset yang sangat berharga dan sangat rentan terhadap tindakan kejahatan yang dilakukan oleh pihak – pihak yang tidak bertanggung jawab. Apabila data yang dimiliki oleh suatu institusi dicuri atau disalahgunakan akan memberikan dampak kerugian bagi institusi tersebut. Pada tahun 2017 di indonesia terdapat serangan cyber yang disebut dengan nama Ransomware *WannaCry*. *Ransomware WannaCry* adalah bentuk malware yang mengenkripsi dokumen pada PC atau bahkan jaringan, sehingga data yang dimiliki oleh institusi tidak dapat diakses.

Serangan *Cyber* yang menyerang komputer tentunya memberikan dampak kerugian bagi institusi yang ada.Hal tersebut dapat menurunkan citra dari institusi tersebut, dimana dengan terjadinya serangan terhadap sistem yang dimiliki akan menyebabkan terkendalanya sistem yang ada dalam instutisi tersebut dan dapat menimbulkan kerugian dari sisi materil.

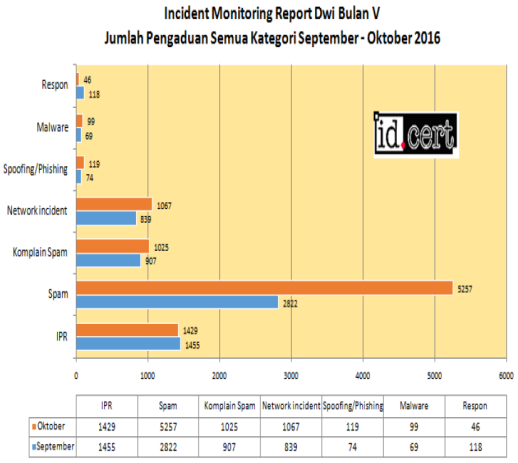
Menurut Symantec Corporation dalam *Internet Security Threat Report 2017 Trends* terdapat 10 besar yang menjadi target kejahatan terhadap situs web yang paling sering di terjadi adalah :

Rank	Domain Categories	2015 (%)	2016 (%)	Percentage Point Difference
1	Technology	23.2	20.7	-2.5
2	Business	8.1	11.3	3.2
3	Blogging	7.0	8.6	1.6
4	Hosting	0.6	7.2	6.6
5	Health	1.9	5.7	3.8
6	Shopping	2.4	4.2	1.8
7	Educational	4.0	4.1	< 0.1
8	Entertainment	2.6	4.0	1.4
9	Travel	1.5	3.6	2.1
10	Gambling	0.6	2.8	2.2

Gambar.1 Kejahatan terhadap situs web

Urutan pertama web yang paling sering mengalami kejahatan atau eksploitasi adalah situs web dibidang teknologi, dan rata – rata dari 10 besar kategori web site tersebut mengalami peningkatan sehingga hal tersebut dapat menjadi ancaman bagi institusi.

Indonesia Computer Emergency Response Team (ID-CERT) melaporkan jumlah insiden ancaman keamanan sistem informasi yang masuk pada September – Oktober 2016. Dari laporan insiden yang masuk dapat disajikan dalam bentuk gambar 2 berikut:



Gambar.2 Jumlah pengaduan semua kategori September – Oktober 2016

Dengan melihat gambar 2 tersebut, jumlah pengaduan yang paling tinggi adalah spam sebesar 5257 pengaduan, kemudian disusul dengan IPR (*Intellectual Property Rights*) sebesar 1429 pengaduan dan terdapat pengaduan – pengaduan yang lain, oleh karena itu keamanan informasi perlu diperhatikan oleh setiap institusi.

Institusi XYZ adalah institusi yang mempunyai tugas menyelenggarakan urusan dibidang pemerintahan. Institusi XYZ menggunakan sistem informasi yang dapat diakses oleh pegawai kepemerintahan maupun masyarakat umum. Pada institusi XYZ terdapat bidang PUSDATIN (Pusat Data dan Informasi) yang berfungsi untuk mengelola layanan informasi kepada masyarakat maupun operasional sehari – hari dilingkungan institusi tersebut. Informasi dikelola secara elektronik untuk mewujudkan good governance , sehingga terdapat keterbukaan informasi bagi masyarakat dan pertukaran informasi antar institusi yang saling terkoneksi. Data – data yang diproses pada bidang PUSDATIN terkoneksi dengan jaringan komputer.

Data dan jaringan merupakan hal yang sangat berisiko dalam bidang keamanan informasi, risiko yang sering terjadi diantaranya penyebaran virus komputer dan terjadi pencurian data yang dimiliki dan dapat menyebabkan kerugian. Dengan menyadari adanya risiko-risiko yang dapat menyebabkan terganggunya pelayanan publik dalam rangka mencapai target yang telah ditetapkan sehingga dibutuhkan adanya evaluasi terhadap keamanan informasi, untuk mengetahui apakah sistem dan keamanan informasi institusi sudah siap atau tidak terhadap risiko yang mungkin terjadi setiap saat.

Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika (Kemkominfo) telah menghimbau kepada seluruh instansi pemerintahan, baik itu pusat maupun daerah, sebagai badan penyelenggara layanan publik untuk meningkatkan kesadaran akan pentingnya keamanan informasi. Berbagai cara dilakukan untuk meningkatkan kesadaran bagi aparatur negara tentang keamanan informasi, mulai dari sosialiasasi maupun bimbingan teknis (bimtek).

Sosialisasi yang dilakukan berisikan materi-materi tentang definisi, pengertian, kontrol-kontrol, persyaratan dokumentasi keamanan informasi dan contoh-contoh tindakan untuk mengamankan informasi. Sementara pada setiap bimbingan teknis, dijelaskan metode atau cara melakukan penilaian mandiri (*self assessment*) terhadap status keamanan informasi pada masing-masing instansi menggunakan alat bantu berupa perangkat penilaian yang bernama indeks Keamanan Informasi (KAMI).

Alat evaluasi Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Indeks KAMI dapat digunakan mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001 serta peta area tata kelola keamanan sistem informasi di suatu instansi dan standar komprehensif yang membantu institusi dalam mencapai tujuan dan menghasilkan nilai melalui tata kelola dan manajemen teknologi informasi yang efektif. Evaluasi dilakukan terhadap beberapa area target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001, yaitu :

1) Kategori Sistem Elektronik
2) Tata Kelola Keamanan Informasi
3) Pengelolaan Risiko Keamanan Informasi
4) Kerangka Kerja Keamanan Informasi
5) Pengelolaan Aset Informasi, dan
6) Teknologi dan Keamanan Informasi

B. *Perumusan Masalah*

Berdasarkan latar belakang yang telah disampaikan, berikut ini adalah uraian permasalahan yang akan dibahas dalam penelitian ini :

1) Berapakah total skor dari penilaian kelima area Indeks KAMI pada institusi XYZ?
2) Bagaimana rekomendasi untuk meningkatkan manajemen keamanan informasi pada institusi XYZ?

C. *Tujuan Penelitian*

1) Mengetahui nilai kematangan manajemen keamanan informasi institusi XYZ.
2) Memberikan rekomendasi kepada pihak institusi XYZ untuk keamanan informasi yang harus dijalankan.

II. TINJAUAN PUSTAKA

A. *Pengertian Informasi*

Informasi adalah segala sesuatu keterangan yang bermanfaat untuk para pengambil keputusan/manajer dalam rangka mencapai tujuan organisasi yang telah ditetapkan [1].

Informasi merupakan salah satu aset bagi sebuah organisasi. Sebagaimana aset lainnya, informasi memiliki nilai tertentu bagi organisasi tersebut sehingga harus dilindungi, untuk menjamin kelangsungan organisasi, meminimalisir kerusakan

karena kebocoran sistem keamanan informasi, mempercepat kembalinya investasi dan memperluas peluang usaha.

Beragam bentuk informasi yang mungkin dimiliki oleh sebuah organisasi diantaranya informasi yang tersimpan dalam komputer (desktop dan mobile computer), informasi yang ditransmisikan melalui network, informasi yang dicetak pada kertas, dikirim melalui fax, tersimpan dalam disket, CD, DVD, flashdisk, atau media penyimpanan lain, informasi yang dilakukan dalam pembicaraan (termasuk percakapan melalui telepon), dikirim melalui email, informasi yang tersimpan dalam database, tersimpan dalam film, dipresentasikan dengan OHP atau media presentasi yang lain, dan metode-metode lain yang dapat digunakan untuk menyampaikan informasi dan ide-ide organisasi [2].

Dari pendapat – pendapat tersebut dapat disimpulkan informasi merupakan hal yang sangat penting bagi organisasi karena informasi adalah aset yang dimiliki oleh institusi dalam mencapai tujuan dari institusi.

Informasi yang dimiliki oleh institusi dapat disimpan di dalam beragam bentuk sesuai dengan kebutuhan dari organisasi tersebut, informasi yang berupa data – data organisasi disimpan untuk menjaga keamanan dari data tersebut agar terhindar dari resiko kejahatan terhadap data yang dimiliki sehingga sistem dalam organisasi dapat berjalan dengan baik tanpa mengalami gangguan pencurian data.

B. Keamanan Informasi

Masalah keamanan informasi dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Organisasi harus menyadari arti penting dari keamanan informasi tersebut, yaitu bagaimana informasi tersebut disalurkan oleh pengirim sampai kepada tahapan ke penerima informasi tersebut [3].

Ketika melakukan pengiriman informasi tersebut sangat rentan terhadap kejahatan seperti pembajakan dan penyadapan yang dapat dilakukan oleh pihak – pihak yang tidak bertanggung jawab sehingga data yang dikirimkan diambil oleh pihak lain untuk keperluan mereka sendiri dan menguntungkan pihak yang tidak bertanggung jawab tersebut.

Tujuan keamanan informasi adalah untuk memastikan kelangsungan usaha, meminimalkan kerugian usaha, dan memaksimalkan laba atas investasi [4].

Informasi yang terjaga dengan baik akan menjaga keberlangsungan organisasi, dengan penggunaan dan keamanan informasi yang dijaga dengan baik akan melancarkan sistem yang ada dalam organisasi tersebut.

Manajemen keamanan informasi yang dimiliki oleh institusi harus menyimpan informasi dengan baik agar terhindar dari kejahatan yang mungkin terjadi. Keamanan informasi memiliki tiga komponen dasar yang harus dikelola, yaitu kerahasiaan informasi sensitif dari pihak yang tidak berwenang.

Integritas informasi untuk memastikan keakuratan dan kelengkapannya; dan ketersediaan informasi dan layanan vital kepada pengguna yang berwenang kapan pun dibutuhkan. Selain tiga tujuan dasar tersebut, keamanan informasi juga mencakup isu-isu yang dapat mengancam akuntabilitas, keandalan, ketidaktergajaran, privasi, otentikasi dan kepercayaan informasi. Manajemen keamanan informasi terdiri dari empat tahap dalam bentuk dasar:

1) Mengidentifikasi ancaman yang dapat menyerang sumber informasi institusi,
2) Menentukan risiko yang mungkin disebabkan oleh ancaman tersebut,
3) Menentukan kebijakan keamanan informasi
4) Menerapkan kontrol untuk mengatasi risiko yang ada.

Sehingga dapat disimpulkan bahwa informasi dan sistem yang dimiliki oleh institusi sangan rentan terhadap ancaman – ancaman yang mungkin terjadi baik itu ancaman aktif maupun ancaman pasif. Ancaman yang ada harus mampu dihindari ataupun dihadapi oleh organisasi agar sistem dan data dapat berjalan dengan lancar dan digunakan dengan baik. Informasi dan sistem harus dikelola oleh orang yang tepat untuk mengindari tindakan kejahatan terhadap sistem dan data tersebut.

C. Sistem Manajemen Keamanan Informasi / Information Security Management System (ISMS)

Sistem Manajemen Keamanan Informasi atau "*Information Security Management System* (ISMS)" adalah hal yang sangat penting dalam pengelolaan informasi dalam organisasi. Informasi yang dimiliki institusi saling terintegrasi dengan seluruh pengeloaan yang ada dalam organisasi.

Sistem Keamanan Informasi merupakan kebutuhan pokok bagi organisasi yaitu sebagai kebutuhan jangka panjang dan jangka pendek yang digunakan menjalankan sistem dalam organisasi.

Manajemen keamanan informasi bertanggung jawab atas program khusus, aspek – aspek tertentu yang ada dalam organisasi dan memilik tanggung jawab yang unik yang dikenal dengan nama "s*ix P*s" [5] :

1) Perencanaan (*Planning*), manajemen keamanan informasi digunakan untuk membuat perencanaan jangka panjang sesuai dengan kebutuhan institusi. Perencanaan harus dilakukan dengan baik agar tujuan institusi dapat dicapai dan sesuai dengan keseluruhan strategi institusi.
2) Kebijakan (*Policy*), organisasi dalam menjalankan fungsinya dibutuhkan adanya pedoman manajemen keamanan informasi yang digunakan dalam menentukan tindakan yang sesuai dengan aturan yang ada . Ada 3 kategori kebijakan umum dalam keamanan informasi:
    - *Enterprise information security policy* (EISP)-dikembangkan dalam konteks rencana strategi teknologi informasi, untuk menetapkan kebijakan departemen keamanan informasi dan iklim keamanan informasi di seluruh organisasi. CISO (*chief information security officer*) biasanya draft program kebijakan, yang biasanya didukung dan ditandatangani oleh CIO atau CEO.
    - *Issue-specific security policies* (ISSPs)-kumpulan aturan yang mendefinisikan perilaku

yang dapat diterima dalam teknologi tertentu, seperti email atau penggunaan internet.

- *System-specific policies* (SySPs)-mengontrol konfigurasi dan/atau penggunaan sebuah peralatan atau teknologi.

Kebijakan – kebijakan yang dipaparkan diatas berguna untuk keberlangsungan pelaksanaan sistem dalam organisasi sehingga setiap elemen dapat berjalan dengan baik saling terintegrasi.

3) Program (*Programs*), mengelola entitas yang terpisah sebagai contoh SETA program (*Security education training and awareness*) yaitu memberikan informasi penting kepada karyawan untuk mempertahankan atau meningkatkan pengetahuan mereka tentang keamanan saat ini.
4) Perlindungan (*Protection*), dilaksanakan melalui serangkaian kegiatan manajemen risiko, termasuk penilaian risiko dan kontrol, serta mekanisme perlindungan, teknologi, dan alat-alat. Masing-masing mekanisme ini mewakili beberapa aspek manajemen kontrol tertentu dalam keseluruhan rencana dalam keamanan informasi.
5) Pengguna (*People*), pengguna adalah link yang paling penting dalam program keamanan informasi. Daerah ini meliputi personil keamanan dan keamanan pribadi maupun aspek program SETA yang disebutkan sebelumnya.
6) Proyek (*Projects*), manajemen proyek melibatkan mengidentifikasi dan mengendalikan sumber daya yang diterapkan pada proyek serta mengukur kemajuan dan menyesuaikan proses kemajuan yang dibuat menuju sasaran atau tujuan.

Setiap organisasi harus mampu membuat perencanaan manajemen keamanan informasi yang tepat bagi organisasinya sehingga setiap pihak dapat menjalankan fungsinya sesuai dengan tanggung jawab masing – masing dan mengetahui hal – hal apa saja yang harus dilakukan ketika terdapat ancaman atau gangguan terhadap sistem atau informasi yang dimiliki.

D.Kesadaran Keamanan Informasi (Information Security Awareness)

Setiap organisasi harus mampu membuat perencanaan manajemen keamanan informasi yang tepat bagi organisasinya sehingga setiap pihak dapat menjalankan fungsinya sesuai dengan tanggung jawab masing – masing dan mengetahui hal – hal apa saja yang harus dilakukan ketika terdapat ancaman atau gangguan terhadap sistem atau informasi yang dimiliki.

Kesadaran keamanan informasi berfungsi untuk menanamkan rasa tanggung jawab dan tujuan karyawan yang menangani dan mengelola informasi, dan mengarahkan karyawan untuk lebih peduli lingkungan pekerjaan mereka [6]. Tujuan kesadaran keamanan informasi adalah untuk meningkatkan keamanan dengan melakukan hal berikut:

1) Pemilik. Pengguna maupun custodian dari informasi paham akan tanggung jawab mereka terhadap sistem keamanan informasi dan mengajar mereka bagaimana bentuk pengamanan yang tepat sehingga membantu untuk mengubah perilaku mereka menjadi lebih sadar akan keamanan.
2) Mengembangkan kemampuan dan pengetahuan sehingga pemiliki, pengguna maupun custodian informasi dapat melakukan pekerjaan mereka dengan lebih aman.
3) Membangun pemahaman akan pengetahuan yang diperlukan untuk merancang, mengimplementasikan, atau mengoperasikan program pembinaan kesadaran keamanan informasi untuk organisasi.

Organisasi yang memiliki kesadaran terhadap keamanan informasi yang dimiliki akan memiliki tanggung jawab dan tujuan yang jelas, sehingga informasi yang mereka kelola atau miliki dapat digunakan dengan baik dan benar sesuai dengan tujuan organisasi.

E. Indeks Keamanan Informasi (KAMI)

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi [7].

Evaluasi dilakukan terhadap beberapa area target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001, yaitu :

- Kategori Sistem Elektronik
- Tata Kelola Keamanan Informasi
- Pengelolaan Risiko Keamanan Informasi
- Kerangka Kerja Keamanan Informasi
- Pengelolaan Aset Informasi, dan
- Teknologi dan Keamanan Informasi

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh instansi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan Teknologi Informasi Komputer (TIK) dalam mendukung terlaksananya tugas pokok dan fungsi yang ada.

Data yang digunakan dalam evaluasi ini nantinya akan memberikan potret indeks kesiapan – dari aspek kelengkapan maupun kematangan – kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

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 kepada pihak yang terkait (*stakeholders*).

Penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di suatu instansi yang mulai ditandai dengan penerapan tata kelola teknologi informasinya.

Pada tahapan awal dalam asesmen yang dilakukan adalah adalah menetapkan Kategori Sistem Elektronik, proses klasifikasi terhadap kategori sistem elektronik dalam instansi atau cakupan evaluasinya dengan mendeskripsikan infrastruktur sistem elektronik yang ada secara singkat. Tujuannya untuk mengelompokkan ke "ukuran " tertentu : Rendah, Tinggi dan Strategis.

TABEL I
SKOR KATEGORI SISTEM ELEKTRONIK

Skor Kategori Sistem Elektronik	
Rendah	10 - 15
Tinggi	16 - 34
Strategis	35 - 50

Setelah menentukan Kategori Sistem Elektronik, langkah selanjutnya yang dilakukan adalah melakukan asesmen terhadap kelima (5) area Indeks KAMI. Penilaian untuk kelima bagian tersebut adalah sebagai berikut:

TABEL II
SKOR TINGKAT KEMATANGAN

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

Setiap *area* yang dinilai akan diperoleh skor akhirnya. Setelah skor diperoleh yang dilakukan selanjutnya adalah menyesuaikan dengan Kategori Sistem Elektronik. Korelasi antara Kategori Sistem Elektronik dengan Status Kesiapan dapat didefenisikan melalui tabel sebagai berikut:

TABEL III
HUBUNGAN KATEGORI SISTEM ELEKTRONIK DAN STATUS KESIAPAN

KATEGORI SISTEM ELEKTRONIK				
Rendah		**Skor Akhir**		**Status Kesiapan**
10	15	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	535	Cukup
		536	645	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	272	Tidak Layak
		273	455	Perlu Perbaikan
		456	583	Cukup
		584	645	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	333	Tidak Layak
		334	535	Perlu Perbaikan
		536	609	Cukup
		610	645	Baik

III. *METODE*

Penelitian ini menggunakan metode kualitatif murni dengan maksud mendeskripsikan hasil penelitian dari objek yang diteliti, yakni Pusat Data dan Informasi. Sejalan dengan tujuan penelitian, metode ini juga mampu mengeksplorasi objek penelitian dengan serangkaian prosedur wawancara dengan pihak-pihak yang terkait.

Pada penelitian ini menggunakan teknik pengumpulan data triangulasi. Alat yang digunakan dalam penelitian ini adalah dengan menggunakan work paper, wawancara, alat perekam suara, kamera, dan dokumentasi lainnya.

Teknik analisis yang dilakukan pada penelitian ini dilakukan dengan cara analisis untuk maturity, yaitu dengan membandingkan tingkat maturity yang ada pada saat ini dengan maturity yang dituju. Pengolahan data dengan tingkat maturity dilakukan menggunakan teknik yang sederhana yaitu dengan cara menghitung interaktif dengan menggunakan Microsoft Excel. Kriteria penilaian yang digunakan untuk pengolahan data dengan menggunakan Indeks KAMI.

IV. *HASIL DAN PEMBAHASAN*

Dari hasil Kategori Sistem Elektronik berdasarkan penilaian Indeks KAMI, Kategori Sistem Elektronik di instansi XYZ mendapat skor sebesar 32 dan masuk dalam kategori Tinggi.

Maksud dari kategori Tinggi disini yaitu kepentingan penggunaan sistem elektronik di instansi XYZ merupakan bagian yang tidak dapat terpisahkan dari proses kerja yang berjalan.

A. Hasil penilaian Tata Kelola Keamanan Informasi

Pada bagian ini dilakukan evaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Dalam penilaiannya menggunakan 22 pertanyaan dimana berisi 8 (delapan) pertanyaan kategori "1", 8 (delapan) pertanyaan kategori "2" dan 6 (enam) pertanyaan dengan kategori "3", dengan status isian masing – masing pertanyaan tidak dilakukan; dalam perencanaan; dalam penerapan atau diterapkan sebagian; diterapkan secara menyeluruh [7]. Berdasarkan asesmen yang dilakukan dalam *area* Tata Kelola Keamanan Informasi dengan menggunakan Indeks KAMI, hasil yang diperoleh adalah sebagai berikut:

TABEL IV
HASIL SKOR TATA KELOLA KEAMANAN INFORMASI

Keterangan	Nilai Skor
Jumlah pertanyaan Kategori 1 sebanyak 8 pertanyaan	11
Jumlah pertanyaan Kategori 2 sebanyak 8 pertanyaan	14
Jumlah pertanyaan Kategori 3 sebanyak 6 pertanyaan	0
Batas Skor Min untuk Skor Kategori Penerapan 3	48
Total Skor Kategori Penerapan 1 & 2	25
Status Penilaian Kategori Penerapan 3	Tidak Valid
Total Nilai evaluasi Tata Kelola Informasi	25

Jumlah pertanyaan kategori 1 sebanyak 8 pertanyaan memiliki skor 11, jumlah pertanyaan kategori 2 sebanyak 8 pertanyaan memiliki skor 14, dan jumlah pertanyaan kategori 3 sebanyak 6 pertanyaan memiliki skor 0.

Minimal skor untuk kategori penerapan 3 yang dipersyaratkan bernilai 48, dirumuskan berdasarkan nilai matriks pemetaan skor "dalam penerapan/diterapkan sebagian" kategori pengamanan 1 dikalikan jumlah pertanyaan kategori 1, ditambah nilai "dalam penerapan/diterapkan sebagian" kategori pengamanan 2 dikalikan jumlah pertanyaan kategori 2.

Maka hasil penilaian status kategori penerapan 3 untuk bagian tata kelola adalah "tidak valid" karena tidak memenuhi nilai minimal yang dipersyaratkan untuk kategori 3, adapun hasil total evaluasi tata kelola adalah 25.

B. Hasil Penilaian Pengelolaan Risiko Keamanan Informasi

Pada bagian ini dilakukan evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Dalam penilaiannya menggunakan 16 pertanyaan dimana berisi 10 (sepuluh) pertanyaan kategori "1", 4 (empat) pertanyaan kategori "2" dan 2 (dua) pertanyaan dengan kategori "3", dengan status isian masing – masing pertanyaan tidak dilakukan; dalam perencanaan; dalam penerapan atau diterapkan sebagian; diterapkan secara menyeluruh[7]. Berdasarkan asesmen yang dilakukan dalam *area* Pengelolaan Risiko Keamanan Informasi dengan menggunakan Indeks KAMI, hasil yang diperoleh adalah sebagai berikut:

TABEL V
HASIL SKOR PENGELOLAAN RISIKO KEAMANAN INFORMASI

Keterangan	Nilai Skor
Jumlah pertanyaan Kategori 1 sebanyak 10 pertanyaan	0
Jumlah pertanyaan Kategori 2 sebanyak 4 pertanyaan	0
Jumlah pertanyaan Kategori 3 sebanyak 2 pertanyaan	0
Batas Skor Min untuk Skor Kategori Penerapan 3	36
Total Skor Kategori Penerapan 1 & 2	0
Status Peniliaian Kategori Penerapan 3	Tidak Valid
Total Nilai evaluasi Pengelolaan Risiko Keamanan Informasi	0

Jumlah pertanyaan kategori 1 sebanyak 10 pertanyaan memiliki skor 0, jumlah pertanyaan kategori 2 sebanyak 4 pertanyaan memiliki skor 0, dan jumlah pertanyaan kategori 3 sebanyak 2 pertanyaan memiliki skor 0.

Minimal skor untuk kategori penerapan 3 yang dipersyaratkan bernilai 36, dirumuskan berdasarkan nilai matriks pemetaan skor "dalam penerapan/diterapkan sebagian" kategori pengamanan 1 dikalikan jumlah pertanyaan kategori 1, ditambah nilai "dalam penerapan/diterapkan sebagian" kategori pengamanan 2 dikalikan jumlah pertanyaan kategori 2.

Maka hasil penilaian status kategori penerapan 3 untuk bagian Pengelolaan Risiko Keamanan Informasi adalah "tidak valid" karena tidak memenuhi nilai minimal yang dipersyaratkan untuk kategori kategori 3, adapun hasil total evaluasi area Pengelolaan Risiko Keamanan Informasi adalah 0.

C. Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

Pada bagian ini dilakukan evaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Dalam penilaiannya menggunakan 29 pertanyaan dimana berisi 12 (dua belas) pertanyaan kategori "1", 10 (sepuluh) pertanyaan kategori "2" dan 7 (tujuh) pertanyaan dengan kategori "3", dengan status isian masing – masing pertanyaan tidak dilakukan; dalam perencanaan; dalam penerapan atau diterapkan sebagian; diterapkan secara menyeluruh [7]. Berdasarkan asesmen yang dilakukan dalam *area* Kerangka Kerja Pengelolaan Keamanan Informasi dengan menggunakan Indeks KAMI, hasil yang diperoleh adalah sebagai berikut:

TABEL VI
HASIL SKOR KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI

Keterangan	Nilai Skor
Jumlah pertanyaan Kategori 1 sebanyak 12 pertanyaan	8
Jumlah pertanyaan Kategori 2 sebanyak 10 pertanyaan	16
Jumlah pertanyaan Kategori 3 sebanyak 7 pertanyaan	0
Batas Skor Min untuk Skor Kategori Penerapan 3	64
Total Skor Kategori Penerapan 1 & 2	24
Status Peniliaian Kategori Penerapan 3	Tidak Valid
Total Nilai evaluasi Kerangka Kerja Pengelolaan Keamanan Informasi	24

Jumlah pertanyaan kategori 1 sebanyak 12 pertanyaan memiliki skor 8, jumlah pertanyaan kategori 2 sebanyak 10 pertanyaan memiliki skor 16, dan jumlah pertanyaan kategori 3 sebanyak 7 pertanyaan memiliki skor 0.

Minimal skor untuk kategori penerapan 3 yang dipersyaratkan bernilai 64, dirumuskan berdasarkan nilai matriks pemetaan skor "dalam penerapan/diterapkan sebagian" kategori pengamanan 1 dikalikan jumlah pertanyaan kategori 1, ditambah nilai "dalam penerapan/diterapkan sebagian" kategori pengamanan 2 dikalikan jumlah pertanyaan kategori 2.

Maka hasil penilaian status kategori penerapan 3 untuk bagian Kerangka Kerja Pengelolaan Keamanan Informasi adalah "tidak valid" karena tidak memenuhi nilai minimal yang dipersyaratkan untuk kategori 3, adapun hasil total evaluasi Kerangka Kerja Pengelolaan Keamanan adalah 24.

D. Hasil Penilaian Pengelolaan Aset Informasi

Pada bagian ini dilakukan evaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Dalam penilaiannya menggunakan 38 pertanyaan dimana berisi 24 (dua puluh empat) pertanyaan kategori "1", 10 (sepuluh) pertanyaan kategori "2" dan 4 (empat) pertanyaan dengan kategori "3", dengan status isian masing – masing pertanyaan tidak dilakukan; dalam perencanaan; dalam penerapan atau diterapkan sebagian;

diterapkan secara menyeluruh [6]. Berdasarkan asesmen yang dilakukan dalam *area* Pengelolaan Aset Informasi dengan menggunakan Indeks KAMI, hasil yang diperoleh adalah sebagai berikut:

TABEL VII
HASIL SKOR PENGELOLAAN ASET INFORMASI

Keterangan	Nilai Skor
Jumlah pertanyaan Kategori 1 sebanyak 24 pertanyaan	27
Jumlah pertanyaan Kategori 2 sebanyak 10 pertanyaan	20
Jumlah pertanyaan Kategori 3 sebanyak 4 pertanyaan	0
Batas Skor Min untuk Skor Kategori Penerapan 3	88
Total Skor Kategori Penerapan 1 & 2	45
Status Peniliaian Kategori Penerapan 3	Tidak Valid
Total Nilai evaluasi Pengelolaan Aset Informasi	47

Jumlah pertanyaan kategori 1 sebanyak 24 pertanyaan memiliki skor 27, jumlah pertanyaan kategori 2 sebanyak 10 pertanyaan memiliki skor 20, dan jumlah pertanyaan kategori 3 sebanyak 4 pertanyaan memiliki skor 0.

Minimal skor untuk kategori penerapan 3 yang dipersyaratkan bernilai 88, dirumuskan berdasarkan nilai matriks pemetaan skor "dalam penerapan/diterapkan sebagian" kategori pengamanan 1 dikalikan jumlah pertanyaan kategori 1, ditambah nilai "dalam penerapan/diterapkan sebagian" kategori pengamanan 2 dikalikan jumlah pertanyaan kategori 2.

Maka hasil penilaian status kategori penerapan 3 untuk bagian Pengelolaan Aset Informasi adalah "tidak valid" karena tidak memenuhi nilai minimal yang dipersyaratkan untuk kategori tahap 3, adapun hasil total evaluasi Pengelolaan Aset Informasi adalah 47.

E. Hasil Penilaian Teknologi dan Keamanan Informasi

Pada bagian ini dilakukan kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Dalam penilaiannya menggunakan 26 pertanyaan dimana berisi 14 (empat belas) pertanyaan kategori "1", 10 (sepuluh) pertanyaan kategori "2" dan 2 (dua) pertanyaan dengan kategori "3", dengan status isian masing – masing pertanyaan tidak dilakukan; dalam perencanaan; dalam penerapan atau diterapkan sebagian; diterapkan secara menyeluruh [7]. Berdasarkan asesmen yang dilakukan dalam *area* Teknologi dan Keamanan Informasi dengan menggunakan Indeks KAMI, hasil yang diperoleh adalah sebagai berikut:

TABEL VIII
HASIL SKOR TEKNOLOGI DAN KEAMANAN INFORMASI

Keterangan	Nilai Skor
Jumlah pertanyaan Kategori 1 sebanyak 14 pertanyaan	21
Jumlah pertanyaan Kategori 2 sebanyak 10 pertanyaan	30
Jumlah pertanyaan Kategori 3 sebanyak 2 pertanyaan	6
Batas Skor Min untuk Skor Kategori Penerapan 3	68
Total Skor Kategori Penerapan 1 & 2	51
Status Peniliaian Kategori Penerapan 3	Tidak Valid
Total Nilai evaluasi Teknologi dan Keamanan Informasi	57

Jumlah pertanyaan kategori 1 sebanyak 14 pertanyaan memiliki skor 21, jumlah pertanyaan kategori 2 sebanyak 10 pertanyaan memiliki skor 30, dan jumlah pertanyaan kategori 3 sebanyak 2 pertanyaan memiliki skor 6.

Minimal skor untuk kategori penerapan 3 yang dipersyaratkan bernilai 68, dirumuskan berdasarkan nilai matriks pemetaan skor "dalam penerapan/diterapkan sebagian" kategori pengamanan 1 dikalikan jumlah pertanyaan kategori 1, ditambah nilai "dalam penerapan/diterapkan sebagian" kategori pengamanan 2 dikalikan jumlah pertanyaan kategori 2.

Maka hasil penilaian status kategori penerapan 3 untuk bagian Teknologi dan Keamanan Informasi adalah "tidak valid" karena tidak memenuhi nilai minimal yang dipersyaratkan untuk kategori tahap 3, adapun hasil total evaluasi Teknologi dan Keamanan Informasi adalah 57

.

F. Kajian Hasil Penilaian Indeks KAMI

Hasil dari penjumlahan skor penilaian Indeks KAMI untuk masing – masing area bagian yang telah dihasilkan kemudian ditampilkan dalam 2 (dua) instrumen, yaitu[7]:

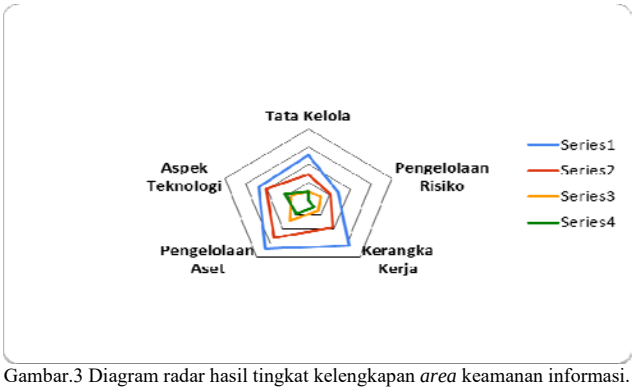
1. Tabel nilai masing – masing area, untuk melihat seberapa besar tingkat kematangan masing – masing area yang telah dicapai, Indeks KAMI mendefinisikan tingkat kematangan ke dalam 5 tingkatan yaitu: tingkat I (kondisi awal), tingkat I+ (kondisi awal dan mulai dilakukan penerapan), tingkat II (penerapan kerangka kerja dasar), tingkat II+ (penerapan kerangka kerja dasar yang mulai terdifinisi dan konsisten), tingkat III (terdifinisi dan konsisten), tingkat III+ (teriefinisi dan konsisten yang mulai terkelola dan terukur), tingkat IV (terkelola dan terukur), tingkat IV+ (terkelola dan terukur yang telah mendekati optimal), dan tingkat V (optimal) dan tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan penerapan SNI 27001 adalah tingkat III+. Tingkat kematangan berdasarkan penilaian Indeks KAMI pada institusi XYZ adalah sebagai berikut:

TABEL IX
HASIL EVALUASI BERDASARKAN *AREA* KEAMANAN INFORMASI INDEKS KAMI

Area Keamanan Informasi	Skor	Tingkat Kematangan
Kategori Sistem Elektronik	32	Tinggi
Tata Kelola	25	I+
Pengelolaan Risiko	0	I
Kerangka Kerja Keamanan Informasi	24	I
Pengelolaan Aset	47	I+
Teknologi dan Keamanan Informasi	57	I+

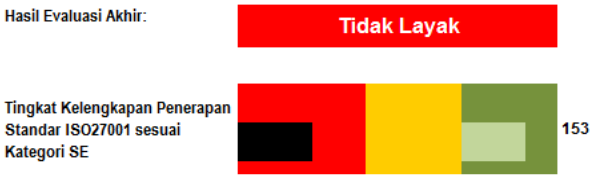
Hasil evaluasi berdasarkan area keamanan informasi Indeks KAMI maka institusi XYZ berada pada tingkatan awal dan mulai melakukan penerapan dan membutuhkan pengembangan keamanan informasi pada peningkatan kerangka kerja dan penerapan berkelanjutan kemudian institusi XYZ sudah mulai ada pemahaman mengenai perlunya pengelolaan keamanan informasi, penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan, kemudian kelemahan tekis dan non-teknis tidak teridentifikasi dengan baik, pihak yang terlibat tidak semuanya menyadari tanggung jawab mereka.

2. Radar Chart dengan 5 (lima) sumbu sesuai dengan area pengamanan, menunjukkan sejauh mana kelengkapan pengamanan sudah mendekati atau mencapai tingkat kelengkapan yang diharapkan. Dalam diagram radar,series 1 dengan warna biru menunjukkan kepatuhan terhadap ISO 27001/SNI, series 2 dengan warna merah menunjukkan proses penerapan, kemudian series 3 dengan warna kuning menunjukkan kerangka kerja dasar dan warna hijau menunjukkan hasil dari Indeks KAMI yang diperoleh oleh institusi XYZ yang menunjukkan kondisi penerapan keamanan informasi pada institusi XYZ. Perbandingan antara kondisi kesiapan sebagai hasil dari proses evaluasi dengan acuan tingkat kelengkapan yang ada yang ada pada institusi XYZ dapat dilihat pada gambar 3:



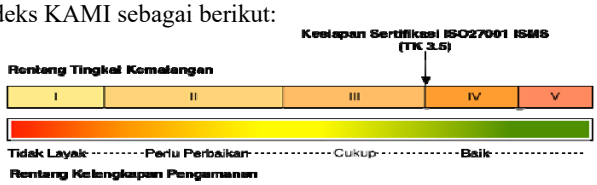
Gambar.3 Diagram radar hasil tingkat kelengkapan *area* keamanan informasi.

Dari diagram radar pada gambar 1 dapat di jelaskan sebagai berikut hampir seluruh area yang dinilai dalam Indeks KAMI belum terpenuhi dan belum sesuai dengan ISO 27001. Pada Diagram radar chart dapat dilihat bahwa hasil yang diperoleh hanya sebatas kategori kerangka kerja dan sebagian besar masih dalam tahap perencanaan dan tahap penerapan. Selanjutnya dapat diukur tingkat kelengkapan kerangka kerja dan penerapan yang sesuai dengan standar ISO 27000/SNI berdasarkan hasil penilaian Indeks KAMI pada institusi XYZ adalah seperti gambar 4:



Gambar. 4 Hasil tingkat kelengkapan pada institusi XYZ.

Pencapaian yang masih ada di area berwarna merah masih dalam status kesiapan "Tidak Layak", kemudian pencapaian di area kuning masih "Memerlukan Perbaikan", sedangkan pencapaian warna hijau menunjukkan bahwa status kesiapan sudah "Baik/Cukup", sesuai dengan acuan pada Penilaian Indeks KAMI sebagai berikut:



Gambar. 5 Hubungan Tingkat Kematangan dan Kelengkapan

Berdasarkan tabel dan diagram acuan diatas diketahui hubungan antara Kategori Sistem Elektronik dengan kesiapan penerapan pada institusi XYZ mendapatkan hasil "Tidak Layak" hal tersebut berdasarkan cakupan Kategori Sistem Elektronik pada institusi XYZ memiliki kategori tinggi tetapi belum didukung oleh bentuk penerapan yang dibutuhkan karena semakin tinggi tingkat ketergantungan terhadap Sistem Elektronik atau semakin penting peranan Sistem Elektronik terhadap tugas, maka semakin banyak bentuk pengamanan yang diperlukan dan harus diterapkan sampai tahap tertinggi.

G. Rekomendasi Sistem Manajemen Keamanan Informasi

Berdasarkan hasil kajian Indeks KAMI yang telah diperoleh, maka dapat dijabarkan beberapa hal yang berkaitan dengan kekuatan dan kelemahan dalam rangka kesiapan institusi XYZ untuk menerapkan sistem manajemen keamanan informasi yang mengacu pada tata kelola keamanan informasi bagi penyelenggara layanan publik yang dikeluarkan oleh Kementrian Komunikasi dan Informatika yang selanjutnya dapat digunakan untuk rekomendasi yang sesuai dengan kondisi sistem informasi atau teknologi informasi di institusi XYZ, antara lain:

- Kekuatan atau Kematangan Sistem Manajemen Keamanan Informasi Institusi XYZ

1) Aspek Ketersediaan Kerangka Kerja

Institusi XYZ telah menyusun beberapa dokumen yang berkaitan dengan pengelolaan TIK yang melingkupi:

a. Sudah ada draft Kebijakan Keamanan Informasi TIK.
b. Sudah ada draft SOP terkait Keamanan Informasi.
c. Sudah ada bagian yang mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya.

2) Aspek Penerapan

Institusi XYZ telah melakukan penerapan tata kelola keamanan informasi dalam mendukung layanan teknologi keamanan informasi, yaitu:

a. Sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.
b. Sudah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.
c. Infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir.
d. Konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban).
e. Sudah ada proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan.
f. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan.
g. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian unit kerja, kebutuhan aplikasi, jalur akses khusus, dan lain-lain.
h. Setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log.
i. Menerapkan enkripsi SSL untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
j. Akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis.
k. Menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar institusi XYZ.
l. Setiap desktop dan server dilindungi dari penyerangan virus (malware).
m. Sudah menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada

- Kelemahan atau Kekurangan Sistem Manajemen Keamanan Informasi Institusi XYZ

1) Aspek Kerangka Kerja

Berikut adalah beberapa kebijakan atau prosedur yang belum ada dalam rangka penerapan sistem manajemen keamanan informasi di institusi XZY, antara lain:

a. Draft Kebijakan Keamanan Informasi TIK belum di sahkan sejak Tahun 2012 karena permasalahan perubahan struktur kelembagaan dan harus lewat Sekretariat Jenderal.
b. SOP terkait Keamanan Informasi belum disahkan sebagai dasar kerangka kerja keamanan pengelolaan informasi.
c. Belum mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
d. Belum mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
e. Belum menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada.
f. Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity plan*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya baru dalam tahap perencanaan.
g. Belum memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada.
h. Belum tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya.

2) Aspek Penerapan

Berikut adalah beberapa aspek penerapan yang menjadi kelemahan dalam rangka penerapan sistem manajemen keamanan informasi di instansi XYZ, antara lain:

a. Belum tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
b. Log belum dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensic.
c. Belum menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi.
d. Aplikasi yang akan di operasionalkan, spesifikasi dan fungsi keamanan belum diverifikasi/validasi kembali setelah melalui proses pengembangan dan uji-coba.

- Rekomendasi Penerapan Sistem Manajemen Keamanan Informasi Pada Institusi XYZ

a. Draft Kebijakan Keamanan Informasi TIK yang belum di sahkan sejak Tahun 2012 disahkan lebih dahulu oleh Kepala Pusat Data.
b. SOP terkait Keamanan Informasi disahkan oleh Kepala Pusat Data sebagai dasar kerangka kerja keamanan pengelolaan informasi di Pusat Data.

c. Mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
d. Mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
e. Menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada.
f. Penyelesaian Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity plan*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya yang sudah tahap perencanaan.
g. Memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada.
h. Menerbitkan peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya.
i. Menyediakan konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
j. Melakukan analisa log secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensic.
k. Menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi.
l. Melakukan verifikasi/validasi spesifikasi dan fungsi keamanan aplikasi yang akan di operasionalkan, setelah melalui proses pengembangan dan uji-coba.

V. KESIMPULAN DAN SARAN

Kesimpulan yang dapat diperoleh dari penelitian ini adalah terkait penilaian manajemen keamanan informasi pada institusi XYZ dengan menggunakan Indeks Keamanan Informasi (KAMI) adalah sebagai berikut:

- Hasil dari penilaian tingkat penggunaan Sistem Elektronik adalah sebesar 32 dari jumlah total keseluruhan sebesar 50. Hal ini menunjukkan bahwa institusi XYZ sudah masuk dalam kategori tinggi dalam penggunaan sistem elektronik yang berarti penggunaan sistem elektronik merupakan bagian yang tidak dapat terpisahkan dari proses kerja yang berjalan pada institusi XYZ.
- Hasil skor keseluruhan berdasarkan penilaian kelima area dalam Indeks KAMI institusi XYZ memperoleh skor sebesar 153 dari total keseluruhan 645 dan berada pada level kematangan I+ dimana kondisi ini merupakan kondisi awal penerapan keamanan informasi. Dalam hal ini Institusi XYZ belum layak dalam penerapan sistem manajemen keamanan informasi untuk melindungi aset yang dimiliki, sehingga masih rentan terhadap tindak kejahatan komputer yang dapat mengakibatkan terganggunya pelayanan sistem informasi di institusi XYZ.

Adapun saran yang dapat penulis sampaikan terkait dengan sistem manajemen keamanan informasi untuk institusi XYZ dalam melindungi aset yang dimiliki adalah sebagai berikut:

- Institusi XYZ harus meningkatkan sistem manajemen keamanan informasi karena tingkat Kategori Sistem Elektronik yang tinggi dan nilai aset yang dimiliki untuk mencegah atau menanggulangi tindak kejahatan komputer yang dapat mengakibatkan terganggunya pelayanan sistem informasi pada institusi XYZ.
- Pengelolaan keamanan informasi yang telah ada harus dilakukan perbaikan dan peningkatan kontrol keamanan dengan pembuatan kebijakan dan prosedur keamanan informasi yang sesuai dengan kondisi TI/SI institusi dengan memperhatikan kesiapan, sumber daya yang dimiliki untuk mendapatkan penerapan sistem manajemen keamanan informasi yang efektif dan efisien

UCAPAN TERIMA KASIH

Ucapan terima kasih saya sampaikan kepada Tuhan Yang Maha Esa, orangtua, keluarga dan teman-teman yang membantu proses pembuatan penelitian ini. Dosen pembimbing yang mengevaluasi dan pihak lain yang tidak bisa disebutkan satu persatu serta Tim JIEET yang berkenan menerima jurnal saya. Semoga jurnal ini bermanfaat bagi peneliti lain maupun pihak yang membutuhkan.

REFERENSI

[1] Gaol, L, Jimmy. 2008. Sistem Informasi Manajemen Pemahaman dan Aplikasi. Jakarta : Penerbit PT Grasindo
[2] Soenardi, Iqbal. Ichsan, M. (2013). Analisis Kematangan Sistem Manajemen Keamanan Informasi Badan Pendidikan dan Pelatihan Keuangan Diukur Menggunakan Indeks KAMI. Jakarta: Badan Pendidikan dan Pelatihan Keuangan.
[3] Andri ,Kristanto. 2003.Perancangan Sistem Informasi. Gava Media, Yogyakarta
[4] Candiwan. Sari, Puspita Kencana. Nurshabrina. (2015). Assessment of Information Security Management on Indonesian Higher Education Institution. ICOCOE'2015 1570110525.
[5] Whitman, M., dan Mattord H. (2004). *Management Of Information Security* : Canada : Thomson Learning.
[6] P Eko Sakti. Kusyanti, Ari. Setyawan, R Arief. (2014). Audit dan Investigasi Sistem Keamanan Jaringan Komputer di Lingkungan Kampus. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), Vol. 2, No.4, 14-17.
[7] Tim Direktorat Keamanan Informasi. (2011). *Panduan Penerapan Tata Kelola Kemanan Informasi Bagi Penyelenggara Pelayanan Publik*. Jakarta: Kementrian Komunikasi dan Informatika RI.