Analisis Penerapan Keamanan Sistem Informasi Pada Pt. AXA Mandiri Financial Service Menggunakan Indeks Kami

Yuli Haryanto[1)] Reza Avrizal[2)]

[1), 2)] Dosen Informatika Universitas Indraprasta PGRI
Jl Nangka No. 58 Tanjung Barat, Jakarta Selatan
Email : haryanto_yuli@yahoo.co.id[1)], reza.avrizal@unindra.ac.id [2)]

Abstract - PT. AXA Mandiri Financial Services is one company that applies information systems that are supported by computerized technology. Companies engaged in banking and insurance are supported by a variety of computerized facilities Handling information systems in these companies has indeed begun to develop technology and devices that are quite advanced at this time. However, information system security must be protected by information system security that is feasible to be applied to companies both on a small scale and large scale. This research uses OUR INDEX method to analyze the application of information system security to the company.

Keywords - Information Security, OUR Index, AXA Information.

Abstrak - PT. AXA Mandiri Financial Service merupakan salah satu perusahaan yang menerapkan keamanan sistem informasi yang didukung oleh teknologi komputerisasi. Perusahaan yang bergerak di bidang perbankan dan asuransi ini didukung oleh berbagai fasilitas komputerisasi dalam melakukan pelayanan kepada nasabahnya. Penanganan sistem informasi pada perusahaan ini memang sudah mengikuti perkembangan teknologi dan perangkat yang cukup pesat saat ini. Namun keamanan sistem informasi memiliki kerangka pedoman untuk menjamin bahwa keamanan sistem informasi layak diimplementasikan pada perusahaan baik pada skala kecil maupun skala besar. Penelitian ini berupaya menggunakan metode INDEKS KAMI untuk melakukan analisis terhadap penerapan keamanan sistem informasi pada perusahaan tersebut.

Kata kunci - Keamanan Informasi, Indeks KAMI, Informasi AXA.

I. PENDAHULUAN

Keamanan sistem informasi menjadi bagian yang sangat penting dalam upaya peningkatan kualitas pelayanan konsumen pada sebuah perusahaan. Keamanan sistem informasi saat ini dapat diterapkan dengan bantuan media komputer sehingga sistem informasi dapat lebih andal dalam mendukung kinerja perusahaan. PT. AXA Mandiri Financial Service merupakan salah satu perusahaan yang menerapkan keamanan sistem informasi yang didukung oleh teknologi komputerisasi. Perusahaan yang bergerak di bidang perbankan dan asuransi ini didukung oleh berbagai fasilitas komputerisasi dalam melakukan pelayanan kepada nasabahnya. Fasilitas komputerisasi tersebut antara lain dalam hal pelayanan pada bagian *customer service*, pengolahan data nasabah, kepegawaian, bahkan sistem monitoring nasabah.

Penanganan sistem informasi pada perusahaan ini memang sudah mengikuti perkembangan teknologi dan perangkat yang cukup pesat saat ini. Namun keamanan sistem informasi memiliki kerangka pedoman untuk menjamin bahwa keamanan sistem informasi layak diimplementasikan pada perusahaan baik pada skala kecil maupun skala besar. Untuk itu perlu adanya analisis keamanan sistem informasi yang diterapkan pada PT. AXA Mandiri Financial Service sehingga dapat diketahui kualitas keamanan sistem informasi yang sudah diterapkan. Penelitian ini berupaya menggunakan metode INDEKS KAMI untuk melakukan analisis terhadap penerapan keamanan sistem informasi pada perusahaan tersebut. Adapun rumusan masalah adalah:

a. Bagaimana penerapan keamanan sistem informasi yang ada pada PT. AXA Mandiri Financial Service?
b. Bagaimana kerangka kerja keamanan sistem informasi dan kebijakannya berdasarkan tingkat kebutuhan pengguna ?
c. Bagaimana tingkat keamanan sistem informasi berdasarkan hasil analisis menggunakan metode Indeks KAMI ?

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah melakukan analisis terhadap penerapan keamanan sistem informasi sehingga dari hasil analisis tersebut diupayakan adanya pencegahan terhadap pelanggaran keamanan maupun penyalahgunaan sumber daya informasi berdasarkan Indeks KAMI. Melakukan identifikasi, analisis, dan evaluasi tentang sejauh mana tingkat keamanan sistem informasi yang ada selama ini dan pengembangan keamanan sistem informasi tersebut. Memberikan rekomendasi pengembangan keamanan sistem informasi yang layak dan dapat menunjang profesionalisme perusahaan sesuai standarisasi yang ada pada model Indeks KAMI.

II. LANDASAN TEORI DAN METODE

Berdasarkan dari hasil penelitian, maka diketahui bahwa pengembangan keamanan sistem informasi yang ada pada PT. AXA Mandiri Financial Service ini memiliki tingkat kesiapan dalam mengelola suatu sistem informasi masih dikatakan sudah sangat baik.

Hasil Identifikasi Peran Sistem Informasi di Instansi

Berdasarkan Indeks KAMI, hasil yang didapat dari beberapa responden sebagaimana pada tabel berikut:

Tabel 1. Hasil Kuesioner Peran Sistem Informasi

No.	Jawaban Responden					Skor Kuesioner					Rata-Rata	Status Pengaman Keseluruhan
	Sucipto	Didi	Anita	Sylvianti	Danus	Sucipto	Didi	Anita	Sylvianti	Danus		
1.1	R	S	M	R	M	1	2	0	1	0	1	Minim
1.2	M	R	S	S	S	0	1	2	2	2	1	Rendah
1.3	S	S	T	T	T	2	2	3	3	3	3	Tinggi
1.4	M	T	S	R	R	0	3	2	1	1	1	Rendah
1.5	S	R	M	S	R	2	1	0	2	1	1	Rendah
1.6	S	K	S	S	R	2	4	2	2	1	2	Sedang
1.7	T	T	T	R	T	3	3	3	1	3	3	Tinggi
1.8	S	M	S	S	S	2	0	2	2	2	2	Sedang
1.9	R	T	R	R	S	1	3	1	1	2	2	Sedang
1.10	S	S	S	T	T	2	2	2	3	3	2	Sedang
1.11	M	M	R	S	M	0	0	1	2	0	1	Minim
1.12	R	S	S	R	S	1	2	2	1	2	3	Tinggi

Dari tabel di atas dapat diketahui bahwa peran sistem informasi di perusahaan ini sangat penting dalam mengelola suatu sistem informasi keuangan. Dengan tingkat ketergantungan yang tinggi maka perusahaan sangat membutuhkan suatu kesiapan dalam segi keamanan baik itu teknologinya maupun sistemnya, berikut ini acuan dari Indeks KAMI untuk mendapatkan hasil dari ketergantungan sistem informasi di perusahaan:

Tabel 2. Hasil Acuan Indeks KAMI

Bagian I: Peran dan Tingkat Kepentingan Sistem Informasi			
Bagian ini memberi tingkatan peran dan kepentingan SI dalam perusahaan Anda			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	
#	**Karakteristik Instansi**		
1,1	Total anggaran tahunan yang dialokasikan untuk SI	Sedang	2
1,2	Jumlah staff/pengguna dalam Instansi yang menggunakan	Sedang	2
1,3	Tingkat ketergantungan terhadap layanan SI untuk	Kritis	4
1,4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Sedang	2
1,5	Dampak dari kegagalan sistem SI utama yang digunakan Instansi anda	Rendah	1
1,6	Tingkat ketergantungan ketersediaan sistem SI untuk	Tinggi	3
1,7	Dampak dari kegagalan sistem SI Instansi anda terhadap	Tinggi	3
1,8	Tingkat sensitifitas pengguna sistem SI di Instansi anda	Sedang	2
1,9	Tingkat kepatuhan terhadap UU dan perangakat hukum	Tinggi	3
1.10	Potensi kerugian atau dampak negatif dari insiden	Tinggi	3
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam	Minim	0
1.12	Tingkat klasifikasi/kekritisan sistem SI di Instansi anda,	Sedang	2
	Skor Peran dan Tingkat Kepentingan SI di Instansi	**27**	

Dari tabel di atas dapat diketahui bahwa persamaan dari hasil rata-rata dengan hasil yang dipergunakan pada tools Indeks KAMI, bahwa beberapa dari pertanyaan yang ada menyinggung tentang tingkat ketergantungan suatu SI didalam mengelola informasi atau pun teknologi dalam menjaga suatu keamanan sistem informasi. Berikut adalah hal yang ketergantungan atau pun peran terhadap sistem informasi:

1. Pengolahan data keuangan
2. Pengaturan jadwal anggaran
3. Pengeluaran Anggaran

Hasil Identifikasi Tata Kelola Keamanan Informasi

Tata kelola teknologi Informasi pada proses audit data adalah manajemen audit data yang merupakan aset penting bagi perusahaan. Secara umum Tata Kelola Teknologi Informasi adalah upaya menjamin pengolahan teknologi informasi agar mendukung bahkan selaras dengan strategi bisnis suatu perusahaan atau organisasi yang dilakukan oleh atasan, manajemen eksekutif dan manajemen teknologi informasi. Oleh karena itu suatu tata kelola yang baik tergantung bagaimana atasan ataupun pimpinan bertanggung jawab dalam menjamin suatu keamanan baik itu sistem ataupun teknologinya.

Berikut adalah hasil penelitian yang didapat dari responden untuk Tata Kelola Keamanan Informasi:

Tabel 3. Hasil Tata Kelola Keamanan Informasi

A	B	C	D	E
Bagian II: Tata Kelola Keamanan Informasi				
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informa				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			**Status**	Skor
#		**Fungsi/Instansi Keamanan Informasi**		
2,1	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi, termasuk penetapan kebijakan terkait?	Dalam Penerapan / Diterapkan Sebagian	2
2,2	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
2,3	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
2,4	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
2,5	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Dalam Penerapan / Diterapkan Sebagian	2
2,6	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
2,7	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	2
2,8	1	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Penerapan / Diterapkan Sebagian	2
2,9	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Perencanaan	2
2.10	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
2.11	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4
2.12	2	Apakah tanggungjawab untuk merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Penerapan / Diterapkan Sebagian	4
2.13	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Dalam Penerapan / Diterapkan Sebagian	4
2.14	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Dalam Perencanaan	2
2.15	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Dalam Perencanaan	0
2.16	3	Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	Tidak Dilakukan	0
2.17	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Perencanaan	0
2.18	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?	Dalam Perencanaan	0
2.19	3	Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Dalam Perencanaan	0
2.20	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Perencanaan	0
		Total Nilai Evaluasi Tata Kelola	**37**	
		Jumlah pertanyaan tingkat 1	8	
		Jumlah pertanyaan tingkat 2	6	
		Jumlah pertanyaan tingkat 3	6	
		Batas Skor Min untuk Skor Kematangan 3	40	
		Total Skor Tingkat Kematangan 1 & 2	37	
		Status Penilaian Tingkat Kematangan 3	Tidak Valid	

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan/diterapkan sebagian. Untuk skor kematangan 3, didapat dengan rumus: (2* jumlah pertanyaan tingkat 1) + (4*jumlah pertanyaan tingkat 2).
(2*8) + (4*6) = 40

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana :
Skor tingkat 1 : 16
Skor tingakt 2 : 16

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (16+16)=32. Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar dibandingkan dengan batas skor min kematangan 3, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 yaitu vailid dan sebaliknya jika tidak memenuhi syarat maka hasilnya tidak valid.

Dari hasil di atas kita bisa lihat bahwa sebagian yang sudah menerapkan tata kelola untuk keamanan sistem walaupun belum dikembangkan secara menyeluruh dalam segala hal. Oleh karena itu para pimpinan dari setiap bagian di perusahaan ini masih belum memahami betapa pentingnya suatu keamanan baik itu teknologi ataupun sistem untuk dijaga dan dimanfaatkan sedemikian rupa dan tidak semua kepala bagian memahami dunia teknologi dan sistem informasi.

Rekomendasi Tata Kelola Keamanan Informasi

Agar terciptanya Tata Kelola Keamanan Informasi, maka diharapkan:

1. Adanya pelatihan khusus terhadap setiap pimpinan agar memahami betapa pentingnya suatu keamanan sistem informasi dan teknologi.
2. Pengkajian keamanan informasi secara berskala oleh pihak yang memahami dalam dunia keamanan infomasi dan teknologi.
3. Pimpinan setiap bagian wajib mengalokasikan tanggung jawab terhadap aset yang ada di perusahaan.
4. Setiap kepala bagian memastikan keutuhan data bebas dari perubahan dan modifikasi pihak-pihak tidak berwenang dan adanya kerja sama dengan pihak keamanan terkait.

Hasil Identifikasi Pengolahan Resiko Keamanan Informasi

Resiko merupakan suatu ancaman terbesar dari setiap perusahaan ataupun instansi manapun, seperti halnya perusahaan yang tak pernah luput dari serangan. Serangan yang lebih sering terjadi setelah diteliti adalah seperti terjadinya kesalahan IP Addres yang telah dipakai oleh karyawan, jaringan kabel yang tidak beraturan, tidak ada yang setiap hari memonitoring setiap waktu dan masih bekerja sama dengan pihak vendor. Hal seperti ini terjadi karena adanya lubang keamanan yang dapat ditembus dikarenakan hal seperti ini hasil dari penelitian yang didapat menggunakan tools Indeks KAMI:

Tabel 4. Hasil Pengolahan Resiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi				
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			Status	Skor
#		Kajian Risiko Keamanan Informasi		
3,1	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
3,2	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
3,3	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	Dalam Perencanaan	1
3,4	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Perencanaan	1
3,5	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Diterapkan Secara Menyeluruh	3
3,6	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Perencanaan	1
3,7	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuia dengan definisi yang ada?	Diterapkan Secara Menyeluruh	3
3,8	1	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Dalam Penerapan / Diterapkan Sebagian	2
3,9	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
3.10	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Diterapkan Secara Menyeluruh	6
3.11	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Dalam Penerapan / Diterapkan Sebagian	4
3.12	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan	Dalam Penerapan / Diterapkan Sebagian	4
3.13	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru??	Tidak Dilakukan	0
3.14	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan	0
3.15	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan	0
		Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	27	
		Jumlah pertanyaan tingkat 1	9	
		Jumlah pertanyaan tingkat 2	4	
		Jumlah pertanyaan tingkat 3	2	
		Batas Skor Min untuk Skor Kematangan 3	34	
		Total Skor Tingkat Kematangan 1 & 2	27	
		Status Penilaian Tingkat Kematangan 3	Tidak Valid	

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan diberbagi bidang hanya sebagian. Untuk skorkematangan 3, didapat dengan rumus : (2* jumlah pertanyaan tingkat 1) + (4*jumlah pertanyaan tingkat 2)

(2*9) + (4*4) = 34

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana:

Skor tingkat 1:20

Skor tingakt 2:14

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (20+14)=34. Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar atau sama dengan (≥), dibandingkan dengan batas skor min kematangan 3 yaitu 34, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 yaitu vailid. Hasil dari skor tingkat kematangan 1 dan 2= batas skor min kematangan 3, yaitu 34 = 34 dan status penilaian tingkat kematangan 3 bernilai valid.

Rekomendasi Pengelolaan Resiko Keamanan Informasi

Setelah diteliti oleh penulis, maka merekomendasikan beberapa hal yang dapat membantu agar kekurangan suatu resiko yang terjadi, diantaranya :

1. Memperhatikan kebutuhan audit yang melibatkan pengecekan sistem operasional untuk meminimalkan resiko dari gangguan proses bisnis.
2. Membatasi pengguna sistem aplikasi untuk bagian yang tidak berkompeten di bagiannya.
3. Mengupdate berskala untuk anti virus, kesalahan IP Addres komputer dan diinstrumenkan oleh setiap kepala bagian yang lebih memahami di bidang teknologi dan sistem informasi.
4. Prosedur untuk mengontrol instalasi software pada sistem operasi dan instalasi jaringan pada komputer.

5. Adanya sangsi untuk pihak yang melanggar proses audit data.

Hasil Identifikasi Kerangka Kerja Pengelolaan Keamanan Informasi

Dalam upaya meningkatkan kinerja Sistem di perusahaan, maka perlu melakukan evaluasi terhadap aktifitas kerja terutama sistem kerja yang baik pada peningkatan pelayanan untuk masyarakat. Suatu kerangka kerja yang baik pasti akan menghasilkan nilai yang baik pula. Hasil dari penelitian dengan Indeks KAMI maka dapat disimpulkan sebagai berikut:

Tabel 5. Hasil Kerangka Kerja Pengolahan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi				
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapann				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			**Status**	Sko
#		**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**		
4,1	1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Tidak Dilakukan	0
4,2	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Tidak Dilakukan	0
4,3	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Diterapkan Secara Menyeluruh	3
4,4	1	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Diterapkan Secara Menyeluruh	3
4,5	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	)alam Penerapan / Diterapkan Sebagia	2
4,6	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	Tidak Dilakukan	0
4,7	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	)alam Penerapan / Diterapkan Sebagia	4
4,8	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	Tidak Dilakukan	0
4,9	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Tidak Dilakukan	0
4.10	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Perencanaan	2
4,11	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	)alam Penerapan / Diterapkan Sebagia	4
4,12	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Tidak Dilakukan	0
4,13	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Tidak Dilakukan	0
4,14	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Tidak Dilakukan	0
4,15	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Tidak Dilakukan	0
4,16	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak Dilakukan	0
#		**Pengelolaan Strategi dan Program Keamanan Informasi**		
4,17	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	)alam Penerapan / Diterapkan Sebagia	2
4,18	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	)alam Penerapan / Diterapkan Sebagia	2
4,19	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Diterapkan Secara Menyeluruh	3
4.20	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Diterapkan Secara Menyeluruh	3
4,21	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	)alam Penerapan / Diterapkan Sebagia	2
4.22	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	)alam Penerapan / Diterapkan Sebagia	4
###	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	)alam Penerapan / Diterapkan Sebagia	4

###	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?	Dalam Perencanaan	0
###	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Diterapkan Secara Menyeluruh	0
###	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Dalam Perencanaan	
		Total Nilai Evaluasi Kerangka Kerja	**38**	

Jumlah pertanyaan tingkat 1	11
Jumlah pertanyaan tingkat 2	8
Jumlah pertanyaan tingkat 3	7
Batas Skor Min untuk Skor Kematangan 3	54
Total Skor Tingkat Kematangan 1 & 2	38
Status Peniliaian Tingkat Kematangan 3	Tidak Valid

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan/diterapkan sebagian. Untuk skor kematangan 3, didapat dengan rumus : (2* jumlah pertanyaan tingkat 1) + (4*jumlah pertanyaantingkat 2)

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana :

Skor tingkat 1 : 21

Skor tingakt 2 : 20

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (21+20)=41.

Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar atau sama dengan (≥), dibandingkan dengan batas skor min kematangan 3 yaitu 54, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah valid, dan sebaliknya jika memenuhi syarat hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 < batas skor min kematangan 3, yaitu 41 < 54 dan status penilain tingkat kematangan 3 bernilai tidak valid.

Dari hasil evaluasi yang telah diteliti di atas dengan menggunakan Indeks KAMI maka dapat disimpulkan bahwa kerangka kerja yang ada masih belum layak. Hal ini dikarenakan masih banyak proses yang belum diterapkan sama sekali sehingga proses pelayanan terhadap karyawan masih sering terjadi keterlambatan.

Rekomendasi Kerangka Kerja Keamanan Informasi

Beberapa hal yang dapat diajukan untuk Kerangka Kerja Keamanan Informasi diantaranya :

1. Kerangka kerja keamanan informasi sebaiknya harus dibuat dan mendapat perhatian khusus dari para pemimpin bagian.
2. Kerangka kerja keamanan informasi sebaiknya dikomunikasikan ke setiap karyawan oleh para pimpinan bagian masing-masing di perusahaan.
3. Diterapkan kerangka kerja yang terpadu baik segi efektivitas maupun dari segi kualitas secara keseluruhan.
4. Adanya landasan hukum pelaksanaan keamanan informasi di dalam perusahaan.

Identifikasi Pengelolaan Asset Informasi

Asset merupakan suatu nilai yang sangat berharga bagi kelangsungan hidup suatu instansi terkait, sehingga harus dijaga dan dikelola dengan baik dan benar.Dengan adanya asset ini, pastinya pengguna TIK sangat dibutuhkan dan menjadi hal utama dalam pengelolaannya.

Bebarapa asset yang diidentifikasi, di antaranya :

1. Konfigurasi jaringan
2. Perangkat jaringan komputer
3. Fasilitas internet yang digunakan

Infrastruktur Teknologi dan Informasi:

1. Spesifikasi Server
2. Spesifikasi Hardware (PC)
3. Sistem Operasi
4. Software kantor yang digunakan
5. Sistem Aplikasi

Dari hasil evaluasi yang didapat dengan menggunakan Indeks KAMI adalah sebagai berikut :

Tabel 6. Hasil Evaluasi Pengelolaan Asset Informasi

Bagian V: Pengelolaan Aset Informasi				
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			**Status**	Sko
#		**Pengelolaan Aset Informasi**		
3,1	1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	Dalam Penerapan / Diterapkan Sebagian	2
3,2	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Dalam Penerapan / Diterapkan Sebagian	2
3,3	1	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses ters	Dalam Penerapan / Diterapkan Sebagian	2
3,4	1	Apakah tersedia proses pengelolaan perubahan yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian	2
3,5	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian	2
3,6	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Dalam Penerapan / Diterapkan Sebagian	2
		Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		
3,7	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Diterapkan Secara Menyeluruh	3
3,8	1	Tata tertib penggunaan komputer, email, internet dan intranet	Diterapkan Secara Menyeluruh	3
3,9	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Diterapkan Secara Menyeluruh	3
3.10	1	Peraturan pengamanan data pribadi	Diterapkan Secara Menyeluruh	3
3.11	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Diterapkan Secara Menyeluruh	3
3.12	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Diterapkan Secara Menyeluruh	3
3.13	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dalam Penerapan / Diterapkan Sebagian	2
3.14	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak Dilakukan	0
3.15	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan / Diterapkan Sebagian	2
3.16	1	Prosedur *back-up* ujicoba pengembalian data (*restore*)	Dalam Penerapan / Diterapkan Sebagian	2
3.17	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Penerapan / Diterapkan Sebagian	4
3.18	2	Proses pengecekan latar belakang SDM	Diterapkan Secara Menyeluruh	6
3.19	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Diterapkan Secara Menyeluruh	6
3.20	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Diterapkan Secara Menyeluruh	6
3.21	2	Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.	Diterapkan Secara Menyeluruh	6
3.22	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Tidak Dilakukan	0
3.23	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak Dilakukan	0
3.24	3	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	0
#		**Pengamanan Fisik**		
3,3	1	Apakah 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?	Dalam Penerapan / Diterapkan Sebagian	2
3,3	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Tidak Dilakukan	0
3.27	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Dalam Perencanaan	1
3.28	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Dalam Penerapan / Diterapkan Sebagian	2
3.29	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Diterapkan Secara Menyeluruh	3

3.30	2	Apakah 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) yang sesuai?	Tidak Dilakukan	0
3.31	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Penerapan / Diterapkan Sebagian	4
3.32	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Tidak Dilakukan	0
3.33	2	Apakah 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? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Tidak Dilakukan	0
3.34	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Tidak Dilakukan	0
		Total Nilai Evaluasi Pengelolaan Aset	**76**	
		Jumlah pertanyaan tingkat 1	21	
		Jumlah pertanyaan tingkat 2	9	
		Jumlah pertanyaan tingkat 3	4	
		Batas Skor Min untuk Skor Kematangan 3	78	
		Total Skor Tingkat Kematangan 1 & 2	76	
		Status Penilaian Tingkat Kematangan 3	Tidak Valid	

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan/diterapkan sebagian. Untuk skor kematangan 3, didapat dengan rumus:

(2* jumlah pertanyaan tingkat 1) + (4*jumlah pertanyaan tingkat 2) .

(2*21) + (4*9) = 76

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana:

Skor tingkat 1: 46

Skor tingakt 2: 32

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (46+32)=78.

Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar atau sama dengan (≥), dibandingkan dengan batas skor min kematangan 3 yaitu 54, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah valid, dan sebaliknya jika memenuhi syarat hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 < batas skor min kematangan 3, yaitu 78 < 76 dan status penilain tingkat kematangan 3 bernilai valid.

Dari tabel di atas maka dapat dievaluasi bahwa Pengolahaan Asset Informasi dan Teknologi ini sudah valid karena setiap bagian di perusahaan sebagian besar memiliki data asset yang lengkap dan akurat dan dipertanggung jawabkan dalam pengamanan data.

Rekomendasi Asset Pengelolaan Informasi

Walaupun Asset Informasi di perusahaan ini sudah dikatakan valid akan tetapi harus ada peningkatan untuk menjadi lebih baik lagi, beberapa rekomendasi yang diusulkan diantaranya:

1. Memastikan asset yang ada terhubung dengan sarana pengolahan informasi mempunyai pemilik atau tanggung jawab.
2. Pembatasan akses yang dikaji ulang secara berkala.
3. Kesadaran dari setiap penanggung jawab asset untuk meng-update informasi keamanan dan teknologi informasi.

Hasil Identifikasi Teknologi dan Keamanan Informasi

Tabel 7. Hasil Teknologi dan Keamanan Sistem Informasi

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	Skor
#		Pengamanan Teknologi		
6,1	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Dalam Perencanaan	1
6,2	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
6,3	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	Diterapkan Secara Menyeluruh	3
6,4	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dalam Penerapan / Diterapkan Sebagia	2
6,5	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Diterapkan Secara Menyeluruh	3
6,6	1	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh	3
6,7	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6,8	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Tidak Dilakukan	0
6,9	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Penerapan / Diterapkan Sebagia	2
6.10	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Tidak Dilakukan	0
6.11	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan	0
6.12	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Tidak Dilakukan	0
6.13	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 Penerapan / Diterapkan Sebagia	4
6.14	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Dalam Penerapan / Diterapkan Sebagia	4
6.15	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk	Diterapkan Secara Menyeluruh	6
6.16	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Dalam Penerapan / Diterapkan Sebagia	4
6.17	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Tidak Dilakukan	0
6.18	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagia	2
6.19	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh	3
6.20	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?	Dalam Penerapan / Diterapkan Sebagia	4
6.21	2	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Penerapan / Diterapkan Sebagia	4
6.22	2	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagia	4
6.23	2	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?	Dalam Penerapan / Diterapkan Sebagia	4
6.24	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan	0
		Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**59**	
		Jumlah pertanyaan tingkat 1	13	
		Jumlah pertanyaan tingkat 2	10	
		Jumlah pertanyaan tingkat 3	1	
		Batas Skor Min untuk Skor Kematangan 3	66	
		Total Skor Tingkat Kematangan 1 & 2	59	
		Status Peniliaian Tingkat Kematangan 3	Tidak Valid	

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum atau tidak secara keseluruhan minimal dalam penerapan/diterapkan sebagian. Untuk skor kematangan 3, didapat dengan rumus :

(2* jumlah pertanyaan tingkat 1) + (4*jumlah pertanyaan tingkat 2)

(2*13) + (4*10) = 66

Untuk total kematangan pada tingkat 1 dan tingkat 2, didapat dengan menjumlahkan skor keseluruhan dari skor tingkat 1 dan skor tingkat 2, dimana :

Skor tingkat 1 : 28

Skor tingakt 2 : 34

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (28+34)=62.

Pada status penilaian tingkat kematangan 3, digunakan untuk menentukan validitas, jika total skor yang didapat pada tingkat kematangan 1 dan 2 lebih besar atau sama dengan (≥), dibandingkan dengan batas skor min kematangan 3 yaitu 54, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah valid, dan sebaliknya jika memenuhi syarat hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 < batas skor min kematangan 3, yaitu 62 = 66 dan status penilain tingkat kematangan 3 bernilai tidak valid.

Dari hasil di atas maka dapat disimpulkan bahwa keamanan teknologi dan informasi rata-rata diterapkan secara menyeluruh, walaupun hasil yang diperoleh masih tidak valid dikarenakan skor akhir dari evaluasi tersebut masih di

bawah batas skor minimal sehingga dapat disimpulkan kembali bahwa teknologi dan keamanan informasi masih butuh penerapan untuk yang lebih baik.
Beberapa hal yang sering terjadi pengaruh dari teknologi dan keamanan informasi diantaranya :

1. Terjadinya kemungkinan informasi di jaringan tidak terlindungi dan bisa terjadi hacker yang bisa membobol sistem di perusahaan.
2. Adanya virus jaringan yang terjadi dan ada juga pembobolan lewat jaringan.
3. Sering terjadi kegagalan dalam pengolahan data pada beberapa bagian dikarenakan sambungan jaringan wifi yang putus dan sangat berantakan.
4. Keterlambatan backup data sehingga koneksi pada server sering terjadi kesalahan pada IP Adders dan tidak ada yang memegangnya.

Rekomendasi teknologi dan Keamanan Informasi
Beberapa hal yang dapat direkomendasikan adalah sebagai berikut:

1. Memastikan jaringan komputer diatur dan dikontrol secara baik dan dapat memadai untuk memelihara keamanan pada sistem dan aplikasi yang menggunakan jaringan komputer.
2. Penggunaan Teknologi yang lebih baru untuk mendapatkan hasil yang baik dan maksimal.
3. Adanya proteksi jaringan untuk menjaga keamanan dari pihak yang tidak diinginkan.

III. PEKERJAAN DAN DISKUSI HASIL

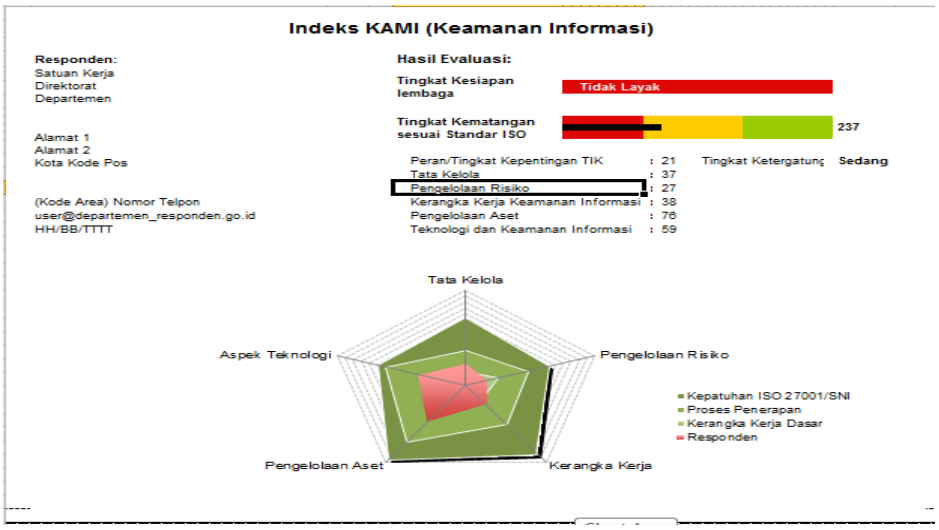
Untuk mengukur suatu tingkat kematangan kerangka kerja keamanan informasi yang memenuhi aspek keamanan berdasarkan ISO 27001:2005 ini menggunakan tools Indeks KAMI. Dimana terdapat Aspek penting yang perlu diketahui oleh setiap pimpinan bagian di perusahaan, diantaranya :

1. Tata Kelola Keamanan Informasi
2. Pengelolaan Risiko Keamanan Informasi
3. Kerangka Kerja Pengelolaan Keamanan Informasi
4. Pengelolaan Asset Informasi, dan
5. Teknologi Keamanan dan Informasi

Beberapa hal di atas akan dinilai kematangannya berdasarkan 3 kerangka penilaian, diantaranya :

1. Keputusan ISO 2700/SNI
2. Proses Penerapan
3. Kerangka Kerja Dasar

Data yang didapat oleh penulis melalui kuesioner dan dihitung rata-rata untuk mendapatkan hasil akhir yang dimasukan ke dalam bagian-bagian Indeks KAMI seperti gambar 2.6 sampai dengan gambar 3.7, maka dapat dihasil Dashbordnya sebagai berikut:



Gambar 1. Dashboard Hasil Evaluasi Berdasarkan Indek KAMI

Berdasarkan hasil evaluasi gambar di atas bahwa perusahaan memiliki tingkat ketergantungan yang sangat tinggi terhadap pengguna TIK, dengan skor nilai akhir tingkat ketergantungan tersebut yaitu 28 dari batas nilai 26-34. Untuk tingkat kematangan sesuai standar ISO 27001 bahwa perusahaan sudah memasuki 1/3nya ke dalam proses penerapan yaitu tingkat yang ke 2 dengan nilai hasil akhirnya adalah 249, dikarenakan bebarapa aspek yang diketahui seperti aspek teknologi, tata kelola, kerangka kerja serta pengolahan asset sudah dalam proses penerapan walaupun belum begitu maksimal. Sedangkan untuk satu aspek yang masih belum menuju proses penerapan yaitu pengolahan risiko, dimana aspek ini masih berada dalam kerangka kerja dasar.

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

Sumber: Depkominfo 2008

Gambar 2. TIK dan Indeks Skor Akhir

Dengan skor akhir 249 yang masuk kedalam tingkat ketergantungan yang tinggi maka status kesiapan perusahaan bisa dijadikan acuan setiap pemimpin kepala bagian atau pun atasan langsung. Untuk melakukan pembenahan atau perubahan manejerial demi menjaga keamana sistem informasi dan teknologi yang sedang berjalan dari pihak atau ancaman yang tidak diinginkan.

IV. KESIMPULAN

Penerapan keamanan sistem informasi yang ada pada PT. AXA Mandiri Financial Service dalam Pengolahaan Asset Informasi dan Teknologi ini sudah valid karena setiap bagian di perusahaan sebagian besar memiliki data asset yang lengkap dan akurat dan dipertanggung jawabkan dalam pengamanan data. Kerangka kerja keamanan sistem informasi dan kebijakannya berdasarkan tingkat kebutuhan pengguna rata-rata diterapkan secara menyeluruh, walaupun hasil yang diperoleh masih tidak valid dikarenakan skor akhir dari evaluasi tersebut masih di bawah batas skor minimal sehingga dapat disimpulkan kembali bahwa teknologi dan keamanan informasi masih butuh penerapan untuk yang lebih baik.Tingkat keamanan sistem informasi berdasarkan hasil analisis menggunakan metode Indeks KAMI bahwa perusahaan memiliki tingkat ketergantungan yang sangat tinggi terhadap pengguna sistem informasi, dengan skor nilai akhir tingkat ketergantungan tersebut yaitu 28 dari batas nilai 26-34. Untuk tingkat kematangan sesuai standar ISO 27001 bahwa perusahaan sudah memasuki 1/3nya ke dalam proses penerapan yaitu tingkat yang ke 2 dengan nilai hasil akhirnya adalah 249, dikarenakan bebarapa aspek yang diketahui seperti aspek teknologi, tata kelola, kerangka kerja serta pengolahan asset sudah dalam proses penerapan walaupun belum begitu maksimal. Sedangkan untuk satu aspek yang masih belum menuju proses penerapan yaitu pengolahan risiko, dimana aspek ini masih berada dalam kerangka kerja dasar.

REFERENSI

[1] Ariefianto, Eko. 2006. Perencanaan Tata Kelola Keamanan Informasi Berdasarkan ISMS ISO 27001. Fasilkom UI.
[2] Afrianto, Irawan. 2015. Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009. Fakultas Teknik dan Ilmu Komputer. Universitas Multimedia Nusantara.
[3] Arikunto, Suharsimi. 2010. Prosedur Penelitian : Suatu Pendekatan Praktik. Jakarta. Penerbit : PT Rineka Cipta.
[4] Ferbrian, Jack. 2004. Pengetahuan Komputer dan Teknologi Informasi. Bandung. Penerbit : Informatika.
[5] Lastyono Putra, Endi. 2014. Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. dengan Menggunakan Indeks Keamanan Informasi (KAMI). Jurusan Sistem Informasi. Fakultas Teknologi Informasi. Institut Teknologi Sepuluh Nopember (ITS).
[6] McLeod, Jr, Raymond. 2004. Sistem Informasi Manajemen, Jilid 8. PT. Buana Ilmu Populer.
[7] Nazir, Moh. 2005. Metode Penelitian. Bogor. Penerbit : Ghalia Indonesia.
[8] Syafrizal, Melwin. 2005. Information Security Management System (ISMS) Menggunakan Standar Iso/Iec 27001.