Faktor Exacta 8(2): 169-180, 2015
ISSN: 1979-276X

KAJIAN KEAMANAN TEKNOLOGI DAN SISTEM INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KAMI: STUDI KASUS PADA PERUSAHAAN XYZ

SUTAN MOHAMMAD ARIF
sutans.axer@gmail.com
Program Studi Teknik Informatika, Fakultas Teknik, Matematika & IPA
Universitas Indraprasta PGRI Jakarta

Abstract. An agency certainly needs a good security in terms of technology or information systems security, things like this because the information technology system is essential to keep the data from things that are not desirable and also created the information quickly and accurately without the slightest failure. Given this research XYZ Company will be able to know that how the level of security readiness in terms of Governance, Framework, Asset, Risk, and even information technology and communications. For data analysis, this study used a qualitative descriptive analysis techniques and methods used to find the level of readiness and maturity of information security framework using the Indeks KAMI, the tools issued by the "Departemen Komunikasi dan Informasi" in 2008. This research is expected to result in a maturation or readiness that can support a better performance.

Kata Kunci :, Security System, Technology Information and Comunication, Indeks KAMI, ISO/IEC 27001:2005

PENDAHULUAN

Di zaman yang serba teknologi seperti ini, suatu instansi manapun baik itu pemerintah atau swasta pastinya dalam pengolahan suatu data, menerima informasi dan lain sebagainya membutuhkan suatu keamanan yang benar-benar harus bisa menjaganya, baik dari segi keamanan untuk datanya tersebut sekaligus untuk penggunaannya. Keamanan suatu data pada sistem sangatlah diperlukan sekali bagi para pembisnis pastinya, mau tidak mau suatu instansi manapun harus dapat beradaptasi dengan cepat, kebutuhan akan informasi teknologi dan koneksi data. Sistem yang dapat diakses dengan availability yang tinggi saat ini dibutuhkan, openness dan terdistribusi pasti sudah menjadi kewajiban atau keharusan untuk sistem yang terintegrasi, karena dengan adanya server yang dikoneksikan terus menerus ke suatu jaringan mau tidak mau akan membuka lubang-lubang sistem keamanan, dan sebenarnya tidak ada sistem yang sempurna, akan tetapi kita hanya bisa meningkatkan dari status tidak aman menjadi relatif lebih aman, karena banyak sekali cara atau metode untuk lubang-lubang keamanan yang dapat ditembus.

Perusahaan XYZ adalah suatu intansi dibidang percetakan yang sedang berkembang sekarang ini. Dalam pengolahan suatu data untuk diproses kedalam sistem yang ada pada setiap bagian tersebut yang telah terkoneksi pada suatu jaringan. Data dan jaringan adalah hal yang paling riskan dalam dunia keamanan sistem informasi dan teknologi, karena itulah yang biasanya mereka serang seperti penyebaran virus komputer dari segi jaringannya dan pencurian data atau jatuhnya informasi ke pihak lain (misalnya pihak lawan bisnis, hacker) dari segi database sistem.

Dengan kesadaran yang sangat tinggi adannya suatu virus komputer yang tersebar karena adanya jaringan yang menjadi terhambatnya atau terlambatnya pengolahan suatu data ke dalam server. Hal seperti inilah yang menjadi pembahasan atau perumusan masalah buat saya untuk meneliti apa sudah benar-benar siap atau tidakah sistem tersebut

ataupun jaringan tersebut. Ada beberapa yang berkata, bahwa sistem dan keamanan tersebut sudah benar-benar siap, akan tetapi kenyataan yang saya sendiri rasakan keterlambatan dalam memasukan suatu data dikarenakan virus yang telah menyebar lewat jaringan tersebut. Dengan keadaan banyaknya pemesanan dan banyakanya pelanggan, memungkinkan penyimpanan data-data pelanggan dan pemesanan tersebut akan terjadi keterlambatan walaupun sudah terkomputerisasi.

Kajian Kemanan Teknologi dan Sistem Informasi dengan metode Indeks KAMI ini, saya mencoba mencari jawaban:

1. Apakah sudah matang atau siap keamanan informasi tersebut baik dari teknologi maupun dari sistemnya?
2. Dari segi manakah yang harus diperhatikan lebih oleh Perusahaan XYZ untuk keamanan teknologi dan sistem informasinya?

Dengan Indeks KAMI ini, suatu tools yang dikeluarkan oleh DEPKOMINFO (Departemen Komunikasi dan Informasi), saya mengharapakan sistem dan teknologi yang sedang berjalan pada perusahaan XYZ menjadi lebih baik daripada sebelumnya, lebih siap, lebih cepat, dan lebih terintgrasi pastinya dalam pengolahan datanya ataupun teknologinya.

TINJAUAN PUSTAKA

Sejalan perkembangan teknologi informasi yang sangat berperan dalam khidupan bangsa Indonesia meningkat drastis termasuk pemanfaatan teknoloi informasi di suatu perusahaan mengengah ataupun atas. Seperti halnya pada perusahaan XYZ bahwa keamanan suatu sistem teknologi informasi itu sangatlah penting untuk menjaga data dari hal yang tidak diinginkan. Dalam konsep suatu keamanan sistem teknologi dan informasi mencakupi beberapa hal yang harus diperhatikan, seperti peranan Teknologi Informasi dan Komunikasi, Pengelolaan Keamanan Informasi, Asset Teknologi, Resiko Keamanan Informasi dan lain-lain.

Peranan Sistem Informasi

Menurut Indrajit (2000), Teknologi informasi adalah suatu teknologi yang berhubungan dengan pengolahan data menjadi informasi dan proses penyaluran data atau informasi tersebut dalam batas-batas ruang dan waktu. Menurut Alter (1999), Teknolgi Informasi sebagai perangkat lunak ataupun keras yang digunakan sistem informasi. Sistem informasi adalah sekumpulan hardware, software, brainware, prosedure dan atau aturan yang diorganisasikan secara integral untuk mengolah data menjai informasi yang bermanfaat guna memecahkan masalah dan pengambilan keputusan. Teknologi informasi ini sangat berperan dalam berbagai bidang baik itu bidang pendidikan, pemerintahan, perbankan ataupun perdagangan. Dalam suatu teknogi informasi baik peranan untuk bidang apapun tidak akan lepas dengan apa yang namanya suatu sistem dan informasi.

Konsep Dasar Sistem

Secara sederhana suatu sistem dapat diartikan sebagai suatu kesatuan yang terdiri dari dua atau lebih komponen atau subsistem yang berinteraksi untuk mencapai tujuan. Teori sistem secara umum pertama kali diuraikan oleh Kenneth Boulding, terutama menekankan pentingnya perhatian terhadap setiap bagian yang membentuk sebuah sistem.

Menurut Jerry Fitz Gerald dan kawan-kawan dalam jogiyanto, HM (2005), Sistem adalah suatu jaringan kerja dari prosedur-prosedur yang berupa urutan kegiatan yang saling berhubungan, berkumpul bersama-sama untuk mencapai tujuan tertentu.

Menurut Jogiyanto, HM (2005), Sistem adalah kumpulan elemen-elemen yang berintegrasi untuk mencapai suatu tujuan tertentu.
Suatu sistem dapat terdiri dari sistem-sistem bagian (*subsytem*), masing-masing subsistem dapat terdiri dari subsistem-subsistem yang lebih kecil lagi atau terdiri dari komponen-komponen. Penggunaan sistem biasanya membtuhkan beberapa mekanisme pemisah untuk mengurangi kerumitan koordinasi dan komunikasi. Pengendalian dalam sistem adalah berdasarkan umpan balik yang dapat terbuka maupun tertutup, sedangkan penyaringan dapat digunakan untuk persyaratan pengolahan dengan mengurangi masukan.

Konsep Dasar Informasi

Didalam organisasi sangatlah penting dalam mengelola sumberdaya-sumberdaya utama seperti pegawai, dan bahan mentah, tapi saat ini informasi juga merupakan sumberrdaya yang tidak kalah pentingnya harus dikelola. Para pembuat keputusan memahami bahwa informasi tudak hanya sekedar produk sampingan bisnis yang sedang berjalan, namun juga sebagai bahan pengisi bisnis dan menjadi faktor kritis dalam menentukan kesuksesan atau kegagalan suatu usaha.

Informasi ibarat darah yang mengalir di dalam tubuh suatu organisasi, sehingga informasi merupakan salah satu bentuk sumber daya utama dalam perusahaan atau instansi yang digunakan oleh manager untuk mengendalikan perusahaan untuk mencapai tujuan. Definisi Informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan yang nyata, atau dengan definisi lain bahwa data adalah representasi dunia nyata yang mewakili suatu objek seperti manusia (pegawai, mahasiswa), peristiwa, konsep, keadaan, dan lain-lain. Untuk mendapatkan data tersebut dapat diperoleh dengan cara, pengamatan langsungm wawancara, perkiraan korensponden, dan lain sebagainya.

Dengan adanya siklus informasi, data yang masih merupakan bahan mentah yang harus diolah untuk menghasilkan informasi melalui suatu model. Model yang digunakan untuk mengolah data tersebut disebut pengolahan data atau dikenal dengan siklus pengolahan data atau siklus informasi.
Kebutuhan informasi didasarkan pada :

- Kegiatan bisnis yang semakin komplek.
- Kemampuan komputer yang semakin meningkat.

Output komputer berupa informasi dapat digunakan oleh manager, non-manager ataupun perorangan dalam suatu perusahaan atau instansi.

- **Akurat**, berarti informasi harus bebas dari kesalahan-kesalahan dan tidak menyesatkan bagi orang yang menerima onformasi tersebut. Akurat juga berati informasi harus jelas mencerminkan maksudnya. Dalam prakteknya, mungkin dalam penyampaian suatu informasi banyak terjadi gangguan (noise) yang dapat merubah atau merusak isi dari informasi tersebut. Komponen akurat meliputi :
  - ***Completeness***, berati informasi yang dihasilkan atau dibutuhkan harus memiliki keelengkapan yang baik, karena bila informasi yang dihasilkan sebagian akan mempengaruhi dalam pengambilan keputusan.
  - ***Correctness***, berarti informasi yang dihasilkan atau dibutukan harus memiliki kebenaran.
  - ***Security***, berati informasi yang dihasilkan atau dibutuhkan harus memiliki keamanan.
- **Tepat waktu**, informasi yang diterima harus tepat pada waktunya, sebab informasi yang usang atau terlambat tidak mempunyai nilai yang baik, sehingga bila digunakan

sebagai dasar dalam pengambilan keputusan akan dapat berakibat fatal. Saat ini mahalnya nilai informasi disebabkan harus cepatnya informasi tersebut didapat, sehingga diperlukan teknologi-teknologi mutakhir untuk mendapatkan, mengolah dan mengirimkannya.

- **Relevan**, informasi harus mempunyai manfaat bagi penerima. Relevansi informasi untuk tiap-tiap orang satu dengan yang lainnya berbeda Misalnya informasi mengenai penyebab kerusakan mesin produksi kepada perusahaan adalah kurang relevan dan akan lebih relevan bila ditujukan kepada ahli teknik perusahaan.
- **Ekonomis**, informasi yang dihasilkan mempunyai manfaat yang lebih besar dibandingkan dengan biaya mendapatkannya dan sebagian besar informasi tidak dapat tepat ditaksir keuntungannya dengan satuan nilai uang tetapi dapat ditaksir nilai efktifitasnya

Tata Kelola Keamanan Sistem Informasi

Menurut Prof. Richardus Eko Indrajit dalam "Menyusun Kebijakan Keamanan Informasi" diakatakan bahwa : keberadaan "Kebijakan Keamanan" atau "Security Policies" merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi tersebut.

Tata kelola teknologi informasi pada proses pengelolaan data adalah manajemen pengelolaan data yang merupakan aset penting bagi perusahaan ataupun organisasi. Tata kelola keamanan teknologi informasi pada proses pengelolaan data yang kurang baik akan menimbulkan beberapa permasalahan yang merupakan kelemahan (*vulnerabilities*) sehingga akan menimbulkan ancaman (*threats*) seperti kejadian kehilangan, perusakan, pencurian dan penyadapan data penting perusahaan atau organisasi.

Pengelolaan Risiko Keamanan Informasi

Resiko adalah sesuatu yang akan terjadi yang dipengaruhi oleh faktor kemungkinan yang berupa suatu ancaman terhadap beberapa kelemahan atau lubang keamanan yang mengakibatkan dampak kerugian bagi organisasi atau perusahaan tersebut. Resiko ini merupakan sesuatu yang tidak dapat dicegah, akan tetapi setiap perusahaan atau organisasi tersebut harus bisa meminimalkan terjadinya resiko.

Resiko ini merupakan suatu ancaman bagi setiap perusahaan terutama aset perusahan. Dalam kaitannya dengan inforamasi dan data, ancaman dapat menjadi beberapa bagian, diantaranya:

- Hilangnya kerahasiaan informasi
- Hilangnya integritas informasi
- Hilangnya ketersediaan informasi
- Hilangnya otentikasi informasi

Pengelolaan Aset Informasi

Dalam kaitannya dengan Sistem Informasi, Rose et al (1995) menyatakan terdapat tiga aspek yang terdapat di dalam aset IS, yaitu *Human*, *Relationship*, dan *Technology*. Aset merupakan aktiva berwujud yang memiliki umur yang lebih panjang dari satu tahun. Aset ini juga bisa didefinisikan sebagai suatu serangkaian aktivitas yang dikaitkan dengan mengidentifikasi aset apa saja yang diperlukan, bagaimana cara mendapatkannya, cara mendukungnya dan memeliharanya, serta cara membuang dan memperbaharuinya, sehingga aset tersebut secara efektif dan dan efisien dapat mewujudkan sasaran. Dari semua yang didefinisikan pastinya memerlukan suatu manajemen yang sering dinamakan Manajemen Aset.

Indeks KAMI

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di Instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005.

Evaluasi ini biasanya dianjurkan yang secara langsujawab untuk mengelola keamanan informasi diseluruh cakupan bagian. Proses evaluasi ini dilakukan melalui sejumlah pertanyaan di masing-masing bagian antara lain :

a. Peran TIK di dalam instansi,
b. Tata kelola keamanan informasi,
c. Pengelolaan resiko keamanan informasi,
d. Kerangka kerja keamanan informasi,
e. Pengelolaan aset informasi,
f. Teknologi dan keamanan informasi yang didukung pula dengan pengelolaan jaringan, hardware atau software yang digunakan.

Data yang digunakan dalam evaluasi ini nantinya akan memberi snapshot indeks kesiapan (kelayakan) dan kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding menyusun langkah-langkah perbaikan dan penetapan prioritasnya. Penggunaan dan publikasi hasil evaluasi indeks KAMI merupakan bentuk tanggung jawab dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi. Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan atau kematangan kepada pihak yang terkait (*stakeholders*).

Untuk Peran TIK di instansi memiliki penilaian yang berbeda dari beberapa bagian lainnya dikarenakan Peranan TIK di instansi ini diharapkan untuk mendapatkan nilai dari ketergantungan instansi itu sendiri akan perananan teknologi dan sistem informasinya. Skor penilaian untuk Peran TIK di instansi adalah sebagai berikut :

Tabel 1. Skor Peranan TIK di instansi

SkorPeranTIK	
Minim	0
Rendah	1
Sedang	2
Tinggi	3
Sangat Tinggi	4

Akan tetapi untuk bagian-bagian lainnya seperti Tata kelola keamanan informasi, Pengelolaan resiko keamanan informasi, Kerangka kerja keamanan informasi, Pengelolaan aset informasi, serta Teknologi dan keamanan informasi, memiliki penilain yang berbeda dari tiap pertanyaan yang diajukannya. Berikut adalah penilaian untuk bagian-bagian yang disebutkan di atas :

Tabel 2. Skor Penilaian Penerapan

	Penetapan Skor		
Status Penerapan 1	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan / Diterapkan Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9

Jika sudah mendapatkan hasil dari penilaian atas penerapan dari tiap-tiap bagian yang ada, maka pimpinan instansi dapat melihat kebutuhan pembenahan yang diperlukan dan korelasi antara berbagai area penerapan keamanan informasi. Adapun korelasi antara peran atau tingkat kepentingan TIK dalam instansi didefinisikan melalui tabel berikut:

Tabel 3. Korelasi Peran atau Tingkat Kepentingan 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

Standar ISO/IEC 270001 : 2005

ISO 27001: 2005 digunakan sebagai icon sertifikasi ISO 27000. ISO 27001: 2005 merupakan dokumen standar sistem manajemen keamanan informasi yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka mengimplementasikan konsep-konsep keamanan informasi di perusahaan. Secara umum ada 11 aspek atau yang biasa disebut sebagai *control*, yang harus ada dalam setiap perusahaan dalam usahanya mengimplementasikan konsep keamanan informasi.

Control dalam hal ini adalah hal-hal, bisa berupa proses, prosedur, kebijakan maupun *tool* yang digunakan sebagai alat pencegahan terjadinya sesuatu yang tidak dikehendaki oleh adanya konsep keamanan informasi, seperti akses terlarang terhadap data atau informasi rahasia perusahaan. Adapun ke-11 control tersebut adalah sebagai berikut:

- *Security policy.*
- *Organization of information security.*
- *Asset management.*

- *Human resources security.*
- *Physical and environmental security.*
- *Communications and operations management.*
- *Access control.*
- *Information system acquisition, development, and maintenance.*
- *Information security incident management.*
- *Business continuity management.*
- *Compliance*.

ISO/IEC 27001 adalah standar information security yang diterbitkan pada Oktober 2005 oleh International Organization for Standarization dan International Electrotechnical Commission. Standar ini menggantikan BS-77992:2002.

ISO/IEC 27001: 2005 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO/IEC 27001: 2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa dan memelihara seta mendokumentasikan Information Security Management System dalam konteks resiko bisnis organisasi keseluruhan

ISO/IEC 27001 mendefenisikan keperluan-keperluan untuk sistem keamanan informasi. Keamanan yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari resiko kerugian/bencana dan kegagalan serius pada pengamanan sistem informasi, implementasi ini akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang tidak lama.

METODE

Penelitian yang dilakukan merupakan jenis penelitian deskriptif kualitatif yaitu penelitian yang disampaikan dalam bentuk deskripsi. Dalam melakukan penelitian ini dilakukan pendekatan kulitatif, yaitu teori keamanan sistem informasi yang telah ada akan dibandingkan dengan kondisi teknologi sistem informasi serta kerangka kerja keamanan sistem informasi di Perusahaan XYZ untuk mengetahui seberapa aman kondisi tersebut.

Pengumpulan data dilakukan dengan cara :

1. Melakukan pengamatan secara langsung ke lapangan itu sendiri untuk mendapatkan suatu gambaran langsung tentang model atau sistem informasi yang dipergunakan.
2. Teknik pengumpulan data teknologi informasi dengan cara bertanya langsung kepada pihak atau bagian yang bertugas langsung dalam pengelolaan keamanan teknologi dan informasi, untuk mengetahui sejauh mana persiapan dalam menghadapi risiko yang datang serta penggunaan alat-alat yang mendukung keamanan sistem informasi.
3. Pengisian kuisioner untuk memperoleh data yang sesuai dengan tujuan penelitian, dalam kuisioner ini akan diberikan kepada 7 orang yang berkompeten dalam bidangnya yaitu keamanan Teknologi dan Sistem Informasi di perusahaan XYZ

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 matury dilakukan dengan teknik yang sederhana, maka rangkaian prosedur pengolahan tidak dikemas dalam bentuk program, tetapi dilakukan dengan cara menghitung interaktif dengan menggunakan Microsoft Excel.

Kriteria penilaian yang digunakan untuk pengolahan data dengan menggunakan Indeks KAMI.

HASIL DAN PEMBAHASAN

Hasil Identifikasi Tata Kelola Keamanan Informasi

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

Untuk batas Skor Kematangan 3, di dapat 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 : 21

Skor tingkat 2 : 22

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (21 + 22) =43

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 **Valid**, dan sebaliknya jika tidak memenuhi syarat maka hasilnya tidak valid.

Hasil Identifikasi Pengelolaan Risiko Keamanan Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 0, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini belum dan atau tidak secara keseluruhan minimal dalam penerapan / diterapkan sebagian. Untuk batas Skor Kematangan 3, di dapat 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 tingkat 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 ($\geq$), dibandingkan dengan batas skor min kematangan 3 yaitu 34, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah valid, dan sebaliknya jika tidak memenuhi syarat maka hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 = batas skor min kematangan 3, yaitu **34 = 34** dan Status Penilaian Tingkat Kematangan 3 bernilai **Valid.**

Hasil Identifikasi Kerangka Kerja Pengelolaan Keamanan Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 3 untuk tiap-tiap pertanyaan, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini sudah sesuai secara keseluruhan minimal dalam penerapan / diterapkan sebagian. Untuk batas Skor Kematangan 3, di dapat dengan rumus :

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

(2*11) + (4*8) = 54

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 : 27
Skor tingkat 2 : 32
Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (27 + 32) = 59

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 tidak memenuhi syarat maka hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 > batas skor min kematangan 3, yaitu **59 < 54** dan Status Penilaian Tingkat Kematangan 3 bernilai **Valid.**

Identifikasi Pengelolaan Asset Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 3 untuk tiap-tiap pertanyaan, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini sudah sesuai secara keseluruhan minimal dalam penerapan / diterapkan sebagian. Untuk batas Skor Kematangan 3, di dapat 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 tingkat 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 76, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah valid, dan sebaliknya jika tidak memenuhi syarat maka hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 > batas skor min kematangan 3, yaitu **78 > 76** dan Status Penilaian Tingkat Kematangan 3 bernilai **Valid.**

Identifikasi Teknologi dan Keamanan Informasi

Untuk skoring pertanyaan tingkat 3 bernilai 3 untuk tiap-tiap pertanyaan, dikarenakan status pengamanan pada tingkat 1 dan tingkat 2 ini sudah sesuai secara keseluruhan minimal dalam penerapan / diterapkan sebagian. Untuk batas Skor Kematangan 3, di dapat dengan rumus :

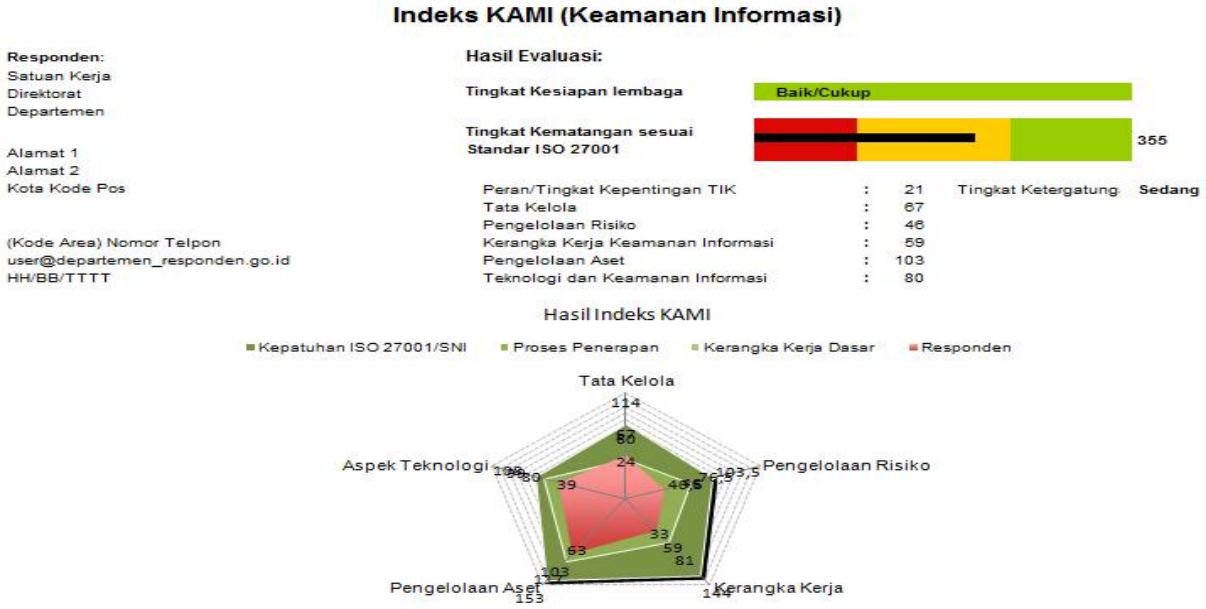
(2 * jumlah pertanyaan tingkat 1) + (4*jumlah pertanyaan tingkat 2)

(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 : 33
Skor tingkat 2 : 38

Maka hasil yang didapat untuk tingkat kematangan 1 dan 2 yaitu (33 + 38) =71. 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 66, maka hasil yang diperoleh untuk status penilaian tingkat kematangan 3 adalah **Valid**, dan sebaliknya jika tidak

memenuhi syarat maka hasilnya tidak valid. Hasil dari skor tingkat kematangan 1 dan 2 > batas skor min kematangan 3, yaitu **71 > 66** dan Status Penilaian Tingkat Kematangan 3 bernilai **Valid**



Gambar 1. Dashboard Hasil Indeks KAMI

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Aspek Teknologi	Total Skor		
Tk Kematangan								
1	8	9	11	21	13	186	62	124
2	6	4	8	9	10	222	37	148
3	6	2	7	4	1	180	20	120
Total Pertanyaan	20	15	26	34	24	588		
Agregat Skor	1	1,5	1	1	1			
1	24	40,5	33	63	39			
2	60	76,5	81	117	99			
3	114	103,5	144	153	108			
Responden	67	46	59	103	80	355		
Tk Ketergatungan TIK	Rendah	Tinggi	Klasifikasi	0	12	0	124	Tidak Layak
	0	12	Rendah			125	272	Perlu Perbaikan
	13	24	Sedang			273	588	Baik/Cukup
	25	36	Tinggi	13	24	0	174	Tidak Layak
	37	48	Kritis			175	312	Perlu Perbaikan
						313	588	Baik/Cukup
				25	36	0	272	Tidak Layak
						273	392	Perlu Perbaikan
						393	588	Baik/Cukup
				37	48	0	333	Tidak Layak
						334	453	Perlu Perbaikan
						454	588	Baik/Cukup
			Valid					
Hasil Evaluasi	Sedang		Baik/Cukup					

Gambar 2. Dashboard Nilai Hasil Indeks KAMI

Berdasarkan hasil evaluasi gambar diatas bahwa perusahaan XYZ ini memiliki tingkat ketergantungan yang sedang terhadap penggunaan TIK, dengan skor nilai akhir tingkat ketergantungan tersebut yaitu 21 (dua puluh satu) dari batas nilai 13 – 24.

Untuk tingkat kematangan sesuai standar ISO 27001 bahwa perusahaan XYZ ini sudah memasuki 1/3-nya kedalam proses penerapan yaitu tingkat yang ke 3 (tiga) dengan nilai hasil akhir adalah 355, hal ini dikarenakan beberapa aspek yang diketahui seperti aspek teknologi, tata kelola, kerangka kerja serta pengelolaan aset sudah dalam proses penerapan dan dimaksimalkan. Dengan skor akhir 355 yang masuk kedalam tingkat ketergantungan yang sedang maka status kesiapan dari perusahaan XYZ ini bisa dijadikan acuan bagi setiap pimpinan kepala bagian atau pun atasan langsung untuk melakukan pembenahan atau perubahan manajerial untuk menjadi lebih baik lagi walaupun perusahaan XYZ ini sudah tergolong Baik/Cukup.

PENUTUP

Berdasarkan hasil penelitian yang penulis lakukan pada perusahaan XYZ ini maka dapat disimpulkan:

a. Berdasarkan hasil evaluasi yang dilakukan dengan menggunakan Indeks KAMI, maka dapat diperoleh hasil kematangan dan kesiapan dari kerangka kerja keamanan informasi yang ada sebelumnya dapat dikatakan Baik/Cukup dengan tingkat ketergantungan TIK yang sedang sesuai dengan Standar ISO 27001.
b. Manajemen resiko merupakan salah satu bagian terpenting dalam pengelolaan keamanan sistem informasi. Dengan manajemen risiko ini, manajemen suatu organisasi khususnya perusahaan XYZ bisa mengetahui secara jelas asset yang harus benar-benar dilindungi.
c. Pada pengelolaan Risiko Keamanan Informasi masih tergolong kerangka kerja dasar yang perlu perhatian khusus agar tidak terjadi hal yang tidak diinginkan.

Evaluasi kebijakan keamanan sistem informasi perlu dilakukan secara periodik, untu mengetahui perkembangan keamanan sistem informasi yang telah dilakukan, karena kebijakan keamanan ini merupakan suatu aset yang harus dipahami dan perlu perhatian agar tidak terjadi kehilangan suatu data informasi.

DAFTAR PUSTAKA

Albone., Aan. 2009. **Pembuatan Rencana Keamanan Informasi Berdasarkan Analisis dan Mitigasi Risiko Teknologi Informasi**. Bandung : Universitas Pasundan.

Ariefianto., Eko. 2006.**Perencanaan Tata Kelola Keamanan Informasi Berdasarkan ISMS ISO 27001**, Fasilkom UI.

Bambang Trianto., Henricus. 2008. **Kebijakan Keamanan Dengan Standar BS 7799/ ISO 17799 Pada Sistem Manajemen Keamanan Informasi Organisasi**. Jakarta : Universitas Bina Nusantara

Damanik., Lyndia Yoslin, Kridanto Surendro. **Perencanaan Tata Kelola Teknologi Informasi Berbasis COBIT Studi Kasus**. Bandung : PT. X

Depkominfo. 2006. **Pedoman Praktis Manajemen Keamanan Informasi Pimpinan Organisasi**. Jakarta.

------. 2006. **Standar Pengelolaan Infrastruktur Teknologi Informasi dan Komunikasi**. Jakarta.

------. 2008. **Indeks KAMI**. Jakarta

Hartanto., Dwi., Indra, Aries., Tjahyanto. 2009. **Analisa Kesenjangan Tata Kelola Teknologi Informasi Untuk Proses Pengelolaan Data Menggunakan COBIT : Studi Kasus Badan Pemerika Keuangan Republik Indonesia**. Jakarta : Universitas Sepuluh November

Indrajit., Eko., Richardus, Menyusun Kebijakan Keamanan Informasi.

ISO/IEC 17799:2005 (E). 2005. **" Information Technology-Security Techniques-Code of Practice for Information Security Management "**. Geneva : International Standard Organization

Maualana., Muhammad Mahreza, Suhono Harso Supangkat. **Pemodelan Framework Manajemen Resiko Teknologi Informasi Untuk Perusahaan Di Negara Berkembang**. Bandung : Sekolah Teknik Elektro dan Informatika (STEI)

Pratiwi., Arie Andara. 2006. **Kualitas Aset Sistem informasi dan Dampaknya Terhadap Manfaat Individu Pengguna**. Bandung : Institut Teknologi Bandung (ITB).

Purwanto., Iwan. 2008. **Strategi Sistem Informasi dan Tata Kelola Teknologi Informasi : Studi Kasus Pada Rumah Sakit XYZ**. Bandar Lampung : STMIK Teknokrat Lampung..

Syafrizal., Melwin. **Information Security Management System (ISMS) Menggunakan Standar ISO/IEC 27001**:2005.