Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI)

Endi Lastyono Putra, Bekti Cahyo Hidayanto, Hanim Maria Astuti
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Raya ITS, Surabaya 60111 Indonesia
e-mail: bekticahyo@its-sby.edu , hanim@its-sby.edu

***Abstrak*— PT. Telekomunikasi Indonesia Tbk. (Telkom) adalah perusahaan milik negara yang bergerak dalam bidang penyedia layanan komunikasi di Indonesia. Saat ini Telkom berpusat di kota Bandung. Banyaknya jaringan yang terhubung dengan kantor pusat Telkom tersebut, akan berdampak pada munculnya risiko keamanan informasi yang dapat mengancam Telkom dalam operasionalnya, sehingga perlu diadakan evaluasi atas keamanan informasi pada Divisi Network of Broadband kantor pusat Telkom untuk mengetahui kondisi keamanan informasi pada Divisi Network of Broadband Telkom.**

Indeks Keamanan Informasi (KAMI) merupakan suatu bentuk aplikasi yang dibuat oleh Kementerian Komunikasi dan Informatika dan digunakan untuk mencari ukuran tingkat kematangan dan kelengkapan keamanan informasi pada instasi negara yang telah disesuaikan dengan standar internasional, yaitu ISO 27001:2005. Tahap pertama dalam evaluasi indeks KAMI adalah melakukan penilaian tingkat ketergantungan TIK pada instasi tersebut, dan hasil dari tingkat ketergantungan tersebut akan digunakan sebagai batasan nilai dari penilaian lima area dalam indeks KAMI.

Hasil penilaian tingkat ketergantungan TIK adalah sebesar 44 dari total keseluruhan 48, dan termasuk dalam kategori kritis, sehingga nilai minimal penilaian kelima area yang harus didapatkan adalah sebesar 334. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 582 dari total keseluruhan 588 dan sudah termasuk dalam kategori optimal. Untuk itu akan dibuatkan suatu saran perbaikan pada bagian-bagian yang masih kurang dari hasil penilaian indeks KAMI yang telah dilakukan.

***Kata Kunci*— indeks KAMI, ISO 27001, Keamanan informasi,**

I. PENDAHULUAN

Penggunaan Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi baik kecil maupun besar. PT. Telekomunikasi Indonesia Tbk (Telkom) merupakan perusahaan Badan Usaha Milik Negara (BUMN) yang bergerak dalam bidang layanan komunikasi dan jaringan terbesar di Indonesia.

Sebagai salah satu upaya untuk meningkatkan kualitas keamanan informasi pada instasi milik pemerintah, maka Kementrian Kominfo membuat suatu alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan indeks Keamanan Informasi (KAMI). Indeks KAMI dibuat dengan acuan ISO 27001:2005 yang berisi tentang keamanan informasi[1].

Sedangkan ISO 27001 adalah suatu bentuk kerangka keja standar internasional yang berisi tentang standar-standar dalam area keamanan informasi. ISO 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi dan pengelolaan aset yang membantu organisasi memastikan bahwa keamanan informasi sudah efektif. Hal ini termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas atas informasi yang dimilikinya[2].

Dalam proses bisnis utama Telkom yang sudah sangat luas, Telkom memiliki banyak kantor cabang yang tersebar di seluruh wilayah Indonesia dan terhubung langsung dengan kantor pusat Telkom di kota Bandung. Saat ini Divisi Network of Broadband bertugas untuk menangani segala jaringan yang ada dalam Telkom Bandung. Baik itu dari segi jaringannya maupun perangkat, hingga perencanaan perangkat tersebut. Dengan banyaknya jaringan yang terhubung dengan kantor pusat Telkom tersebut, akan berdampak pada munculnya risiko keamanan data yang dapat mengancam Telkom dalam kegiatan operasionalnya, sehingga perlu diadakan evaluasi atas keamanan informasi dengan indeks KAMI pada Divisi Network of Broadband Telkom kota Bandung untuk mengetahui kondisi terkini keamanan informasi yang kemudian dilanjutkan dengan membuat rekomendasi perbaikan terhadap keamanan informasi tersebut dengan harapan rekomendasi yang telah dibuat digunakan sebagai bahan pertimbangan dalam rangka upaya meningkatkan kualitas keamanan informasi Divisi Network of Broadband Telkom Bandung agar dapat memberikan pelayanan yang lebih baik dan dapat diandalkan.

II. TINJAUAN PUSTAKA

A. Divisi Network of Broadband

Divisi Network of Broadband merupakan gabungan antara divisi akses dan divisi infrastruktur telekomunikasi yang sebelumnya memiliki tugas yang terpisah dalam PT. Telekomunikasi Indonesia Tbk. Peleburan kedua divisi ini dimulai sejak tahun 2014. Divisi Network of Broadband adalah divisi dalam PT. Telekomunikasi Indonesia Tbk yang bertanggung jawab atas segala jaringan yang ada dalam perusahaan tersebut.

Saat ini Divisi Network of Broadband menggunakan ISO 27001:2005 sebagai panduan dalam penerapan keamanan informasi. Tetapi dimulai dari tahun 2014, divisi network of broadband sedang melakukan implementasi ISO 27001:2013.

- **Visi**

  Memberikan support dan layanan jaringan yang dapat diandalkan oleh seluruh PT. Telkom Group

- **Misi**
  - Mengelola jaringan yang mengutamakan keamanan sesuai dengan standar internasional
  - Memberikan support jaringan yang dapat diandalkan untuk PT. Telkom Group

B. Keamanan Informasi

Pengertian dari keamanan informasi adalah upaya untuk mengamankan aset informasi dari segala ancaman

yang mungkin terjadi untuk mengurangi resiko negatif yang diterima. Semakin banyak informasi yang disimpan di sebuah organisasi maka semakin banyak juga juga resiko yang akan terjadi seperti kerusakan, kehilangan atau juga informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak bertanggung jawab. Terdapat lima layanan jaminan keamanan, diantaranya adalah sebagai berikut[3] :

1. *Confidentiality*, yaitu memastikan bahwa infomasi hanya dapat diakses oleh pihak yang memiliki wewenang.
2. *Authenticity*, yaitu menjamin informasi tersebut asli
3. *Integrity*, yaitu memastikan informasi tersebut tepat, lengkap, dan sesuai dengan bentuk semula.
4. *Availability*, yaitu memastikan informasi dapat diakses oleh orang yang memiliki wewenang tanpa ada keterlambatan waktu jika data sedang dibutuhkan.
5. *Non-repudiation*, yaitu menjamin pihak pengguna tidak dapat menyangkal keaslian tanda tangan digital (*digital signature*) pada suatu dokumen atau tempat dalam jaringan tersebut.

a. Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) adalah suatu bentuk susunan proses yang dibuat berdasarkan pendekatan resiko bisnis untuk merencanakan (Plan), mengimplementasikan dan mengoperasikan (Do), memonitoring dan meninjau (Check), serta memelihara dan meningkatkan atau mengembangkan (Act) terhadap keamanan informasi perusahaan. Keamanan informasi ditujukan menjaga aspek kerahasian (*Confidential*), keutuhan (*Integrity*), dan ketersediaan (*Availibity*) dari informasi. Dalam menerapkan keamanan informasi aspek SMKI dan teknologi keamanan informasi tidak dapat dipisahkan. Artinya sebaiknya suatu organisasi tidak hanya menerapkan teknologi keamanan informasi saja tanpa menerapkan SMKI[1].

Tabel 1 Definisi Proses SMKI

PLAN (Menetapkan SMKI)	Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dan sasaran.
DO (Menerapkan dan menjalankan SMKI	Menerapkan dan mengoperasikan kebijakan SMKI, kontrol, proses dan prosedur-prosedur .
CHECK (Memantau dan melakukan tinjau ulang SMKI)	Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya.
ACT (Memelihara dan meningkatkan SMKI)	Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

Organisasi harus menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara dan meningkatkan SMKI dan terdokumentasi dalam konteks bisnis organisasi secara keseluruhan beserta risiko yang dihadapinya[1].

b. Indeks KAMI

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan instansi. 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 SNI ISO/IEC 27001:2009.

c. Manajemen Risiko TI

Manajemen risiko adalah proses mengelola dan mengatur risiko yang akan terjadi untuk mengurangi dampak negatif yang ditimbulkan dari risiko tersebut bagi setiap individu atau organisasi. Sedangkan manajemen risiko TI adalah proses pengelolaan risiko yang berhubungan dengan TI. Berikut ini adalah proses dari manajemen risiko:

a. *Risk Identification*, yaitu mengenal dan memahami seluruh risiko yang ada dan juga yang mungkin muncul dari aktivitas.
b. *Risk Measurement*, yaitu mengukur dampak dan kecenderungan terjadinya risiko.
c. *Risk Controlling*, yaitu evaluasi terhadap dampak risiko.
d. *Risk Financing*, yaitu menentukan kapan dan kepada siapa kerugian akibat risiko ditanggungkan.

d. Pengelolaan Aset

Pengelolaan aset merupakan serangkaian kegiatan yang berhubungan dengan:

- Identifikasi kebutuhan aset
- Identifikasi pembiayaan aset
- Memperoleh aset
- Menyediakan logistik dan perawatan sistem untuk aset
- Membuang atau memperbarui aset

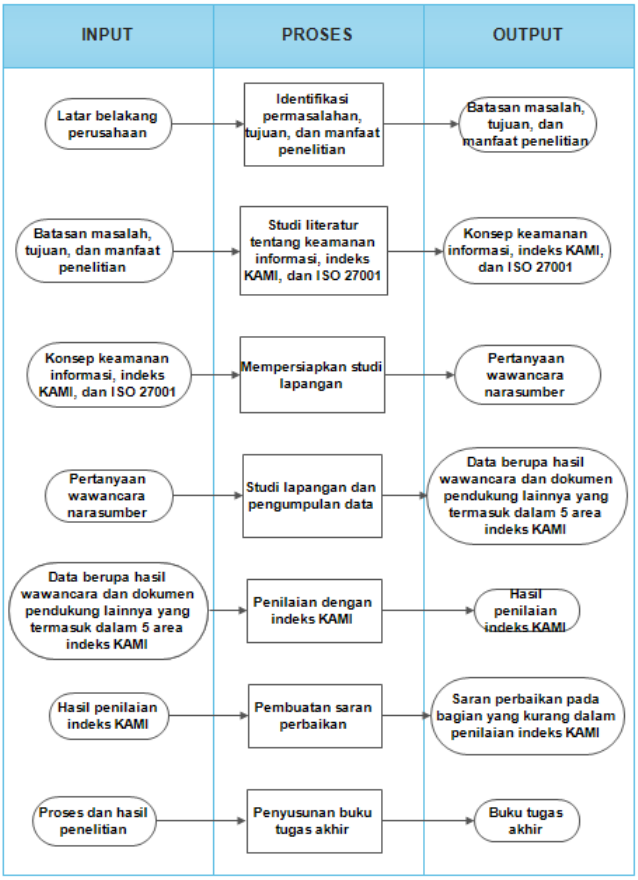
Pengelolaan aset adalah kegiatan yang sistematis dan terkoordinasi dan dipraktekan secara mendalam dimana organisasi secara optimal dan berkelanjutan mengelola aset dan sistem aset, kinerja aset, risiko dan pengeluaran selama siklus hidup aset tersebut berjalan untuk mencapai rencana strategis organisasinya. Pengelolaan aset bertujuan untuk menyediakan informasi dan kapasitas terhadap aset tersebut, sehingga dapat membantu manajer untuk mengambil keputusan dalam suatu organisasi[4].

III. METODE PENELITIAN

Pengerjaan tugas akhir ini dilakukan dengan urutan kegiatan sebagai berikut:

1. Identifikasi permasalahan, tujuan, dan manfaat penelitian
2. Studi literatur
3. Persiapan studi lapangan
4. Studi lapangan dan pengumpulan data
5. Penilaian dengan indeks KAMI
6. Pembuatan saran perbaikan
7. Penyusunan buku tugas akhir

Dibawah ini adalah diagram alur dari urutan pengerjaan tugas akhir ini:



Gambar 1 Metodologi Penelitian

IV. PEMBAHASAN

4.1 Persiapan Pengumpulan Data

Studi lapangan dilakukan di kantor Plasa Telkom Jalan Lembong no. 11 Bandung dengan melakukan wawancara kepada:

1. Bpk Suratmin - Manager IP Security Network & Services
2. Bpk Helmut – Engineer 1 Network Security Backbone
3. Bpk. Agus – Engineer 1 Network Security Broadband

4.2 Pembahasan Hasil Evaluasi Indeks KAMI

4.2.1 Tahap Persiapan

Tahap ini merupakan tahap pertama yang harus dilakukan sebelum melakukan penilaian pada bagian lainnya. Hal ini bertujuan untuk menetapkan suatu batasan nilai yang didasarkan atas tingkatan peran dan kepentingan teknologi informasi pada organisasi tersebut.

Tingkat kesiapan keamanan informasi dibagi menjadi empat tingkatan. Jika hasil tingkat kepentingan TIK mendapat nilai rendah, maka semakin rendah pula batasan yang harus dicapai organisasi tersebut dalam penilaian lima bagian indeks KAMI, dan sebaliknya. Keempat tingkatan tersebut dapat dilihat pada tabel dibawah ini.

Tabel 2 Pemetaan Tingkatan Peran TIK Dengan Nilai Akhir

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

Dalam penilaian tingkat peran TIK, terdapat lima pilihan jawaban yang terdiri dari:

Tabel 3 Tingkatan Nilai Jawaban

Jawaban	**Nilai**
Minim	0
Rendah	1
Sedang	2
Tinggi	3
Kritis	4

Berikut ini adalah hasil dari penilaian tingkat kepentingan TIK pada divisi *Network of Broadband* Telkom:

Tabel 4 Penilaian Peran dan Tingkat Kepentingan TIK

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi		
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.		
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**
#	**Karakteristik Instansi**	
No	**Pertanyaan**	**Status**

1.1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Kritis
Alasan: Anggaran yang diberikan dari pemerintah untuk bidang TIK lebih dari 20 miliar rupiah.		
1.2	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Kritis
Alasan: Seluruh staff dalam divisi menggunakan TIK untuk melaksanakan tugasnya, dan jumlah staff melebihi 600.		
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Kritis
Alasan: Digunakan sebagai bahan pertimbangan untuk pengambilan keputusan mengenai keamanan informasi.		
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**44**

Tabel di atas adalah sebagian dari hasil penilaian tingkat kepentingan TIK. Dari hasil penilaian tingkat peran dan kepentingan teknologi informasi pada divisi *network of broadband* PT. Telekomunikasi Indonesia Tbk, telah didapatkan nilai sebesar 44, sehingga masuk ke dalam kategori kritis untuk peran TIK sesuai dengan tabel sebelumnya. Untuk itu hasil dari penilaian indeks KAMI untuk tahap selanjutnya, harus mendapatkan nilai minimal di atas 333 agar dapat mencapai status layak.

4.2.2 Tahap Penilaian

Dalam penilaian lima area tersebut, akan terdapat beberapa warna yang berbeda dalam tabel penilaian. Warna tersebut menunjukan tingkatan tertentu. Berikut ini adalah keterangan tingkatan warna yang terdapat dalam penilaian lima area tersebut.

Tabel 5 Definisi Warna Dalam Indeks KAMI

Tingkat Keamanan		Tingkat Kematangan Keamanan II
		Tingkat Kematangan Keamanan III
		Tingkat Kematangan Keamanan IV
		Tingkat Kematangan Keamanan V
Kategori Pengamanan		Kategori Kematangan Pengamanan I
		Kategori Kematangan Pengamanan II
		Kategori Kematangan Pengamanan III
Status		Tidak Dilakukan
Pengamanan		Dalam Perencanaan
		Dalam Penerapan/ Diterapkan Sebagian
		Diterapkan Secara Menyeluruh

Setiap kategori pertanyaan memiliki nilai skor yang berbeda. Berikut ini adalah tabel pemetaan skor tersebut:

Tabel 6 Pemetaan Skor Dengan Jawaban

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

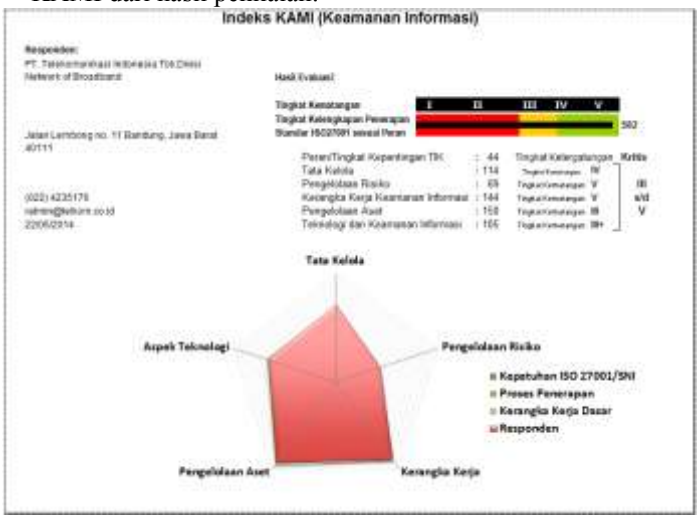
Berikut ini adalah salah satu contoh tabel dari penilaian dengan menggunakan Indeks Keamanan Informasi (KAMI) yang telah dilakukan pada divisi.

Tabel 7 Penilaian Dengan Indeks KAMI

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh					**Status**
#	**Fungsi/Instansi Keamanan Informasi**				
No			**Pertanyaan**	**Status**	**Skor**
2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Diterapkan Secara Menyeluruh	3
Alasan: Pimpinan termasuk dalam penanggung jawab keamanan informasi dalam kebijakan dari pusat, sesuai dengan dokumen kebijakan dalam Lampiran D.3 poin 1.					
2.20	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah didefinisikan di dalam kebijakan pusat yang diatur oleh direktorat IT *Strategy & Governance* (ITSG).					
Total Nilai Evaluasi Tata Kelola				**114**	

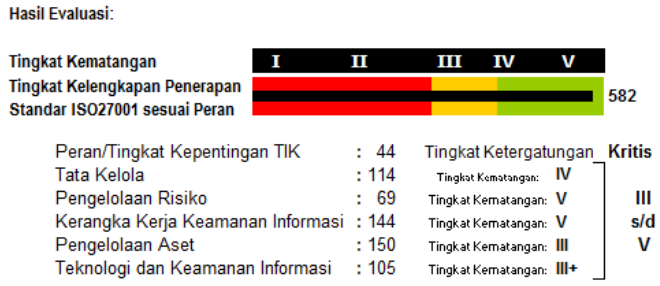
4.2.3 Analisa Hasil Penilaian Indeks KAMI

Berikut ini adalah tampilan dari *dashboard* indeks KAMI dari hasil penilaian:



Gambar 2Dashboard Hasil Indeks KAMI

Dari *dashboard* diatas, dapat dilihat bahwa tingkat kematangan keamanan informasi divisi *Network of Broadband* PT. Telekomunikasi Indonesia sudah baik, yaitu tingkat V dengan nilai sebesar 582. Dapat dilihat pada *radar chart dashboard* tersebut, bahwa hampir seluruh area yang dinilai dalam indeks KAMI telah terpenuhi dan sesuai dengan ISO 27001.



Gambar 3 Hasil Penilaian Indeks KAMI

Dari gambar diatas dapat terlihat jika nilai indeks KAMI yang telah dicapai cukup bagus, yaitu mencapai tingkat V. Dapat dikatakan bagus karena nilai yang dicapai sesuai dengan peran dan tingkat kepentingan teknologi informasi yang digunakan pada divisi *network of broadband* PT. Telekomunikasi Indonesia, yaitu mencapai tingkat kritis.

4.3 Saran Perbaikan

Setelah melakukan penilaian dengan indeks KAMI dan mengetahui hasil dari setiap area yang terdapat dalam indeks KAMI, maka tahap selanjutnya adalah membuat saran perbaikan pada setiap bagian yang masih kurang baik. Berikut ini adalah salah satu contoh tabel pemetaan dari pertanyaan evaluasi, hasil evaluasi, dan saran perbaikan yang direkomendasikan:

Tabel 8 Saran Perbaikan 1

Nomor	Pertanyaan	Jawaban	Nilai
5.11	Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko? Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Dalam Penerapan / Diterapkan Sebagian	2
	Saran Perbaikan: Peraturan yang mengatur akun dan kata sandi sudah ada, namun dalam pelaksanaan peraturan tersebut dalam kegiatan sehari-hari masih kurang. Karena penggunaan akun dan kata sandi tersebut tergantung dari setiap individu yang bekerja dalam divisi, sehingga untuk membantu menegakkan peraturan yang telah dibuat tersebut, perlu dibuat suatu kebijakan yang secara khusus mengatur tentang penggunaan akun dan kata sandi tersebut. Dokumen tersebut akan terdapat dalam Lampiran buku tugas akhir ini.		

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian tugas akhir dengan studi kasus Evaluasi Keamanan Informasi Pada Divisi Network Of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI) antara lain:

- Hasil dari penilaian tingkat kepentingan dan peran TIK adalah sebesar 44 dari total keseluruhan 48. Hal ini menunjukan bahwa divisi Network of Broadband Telkom sudah sangat kritis dalam hal penggunaan TIK.
- Hasil keseluruhan dari penilaian kelima area dalam indeks KAMI adalah sebesar 582 dari total keseluruhan 588 dan berada pada level V. Level V berarti sudah termasuk dalam kategori optimal, yang memiliki arti antara lain:
  - Pengamanan menyeluruh diterapkan secara berkelanjutan dan efektif melalui program pengelolaan risiko yang terstruktur
  - Pengamanan informasi dan manajemen risiko sudah terintegrasi dengan tugas pokok instansi
  - Kinerja pengamanan dievaluasi secara berkelanjutan dengan analisa parameter efektifitas kontrol, kajian akar permasalahan dan penerapan langkah untuk optimasi peningkatan kinerja
  - Target pencapaian program pengamanan informasi selalu dipantau, dievaluasi dan diperbaiki
  - Karyawan secara proaktif terlibat dalam peningkatan efektifitas pengamanan
- Hasil penilaian kelima area menunjukan nilai sebesar 582, dengan hasil nilai tingkat kepentingan TIK sebesar 44 maka divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk sudah dapat dikatakan matang dan sesuai dengan standart ISO 27001.

5.2 Saran

Saran yang dapat diambil dari hasil pengerjaan tugas akhir dengan studi kasus Evaluasi Keamanan Informasi Pada

Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. dengan Menggunakan Indeks Keamanan Informasi (KAMI) ini adalah sebagai berikut:

- Divisi Network of Broadband Telkom sudah sangat baik dalam kesadaran keamanan informasi, hanya tinggal menerapkan segala kebijakan dan peraturan yang telah dibuat secara berkelanjutan
- Divisi Network of Broadband harus mempertahankan tingkat kematangan yang telah dicapai dari hasil evaluasi indeks KAMI, lebih baik lagi jika ditingkatkan sesuai dengan standar internasional yang berlaku saat ini
- Perlu dibuatnya suatu instrument penilaian yang baru, karena indeks KAMI saat ini masih menyesuaikan dengan standar ISO 27001 tahun 2005. Sedangkan saat ini sudah terdapat ISO 27001 tahun 2013

DAFTAR PUSTAKA

[1] Kominfo. (2013, Oktober 28). *Keamanan Informasi*. Retrieved Februari 25, 2014, Kementrian Komunikasi dan Informatika Republik Indonesia [online]: http://www.aptika.kominfo.go.id/utama/produk/3

[2] Perera, D. (2008, Juli 26). *Daminda Perera's Home Page.* Retrieved Februari 28, 2014 Daimnda Perera's Home Page [online] : http://www.daminda.com/

[3] Sekolah Tinggi Sandi Negara. (2012, Oktober 24). *Hal Dasar Tentang Keamanan Informasi (Bagian 2)*. Retrieved February 26, 2014, Sekolah Tinggi Sandi Negara [online] : http://stsn-nci.ac.id/hal-dasar-tentang-keamanan-informasi-bag-2/

[4] Hastings, N. A. *Physical Asset Management.* London: Springer (2010)