TUGAS AKHIR – KS 091336

EVALUASI KEAMANAN INFORMASI PADA DIVISI NETWORK OF BROADBAND PT. TELEKOMUNIKASI INDONESIA TBK DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI)

Endi Lastyono Putra
NRP 5210 100 079

Dosen Pembimbing
Bekti Cahyo Hidayanto, S.Si, M.Kom
Hanim Maria Astuti, S.Kom, M.Sc

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2014

FINAL PROJECT – KS 091336

INFORMATION SECURITY EVALUATION ON PT. TELEKOMUNIKASI INDONESIA TBK NETWORK OF BROADBAND DIVISION USING INDEKS KEAMANAN INFORMASI (KAMI)

Endi Lastyono Putra
NRP 5210 100 079

Supervisor
Bekti Cahyo Hidayanto, S.Si, M.Kom
Hanim Maria Astuti, S.Kom, M.Sc

INFORMATION SYSTEM DEPARTMENT
Information Technology Faculty
Institut Teknologi Sepuluh Nopember
Surabaya 2014

EVALUASI KEAMANAN INFORMASI PADA DIVISI NETWORK OF BROADBAND PT. TELEKOMUNIKASI INDONESIA TBK DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI)

Nama Mahasiswa : Endi Lastyono Putra
NRP : 5210 100 079
Jurusan : Sistem Informasi FTIf – ITS
Dosen Pembimbing I : Bekti Cahyo Hidayanto, S.Si, M.Kom
Dosen Pembimbing II : Hanim Maria Astuti, S.Kom, M.Sc

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* : Keamanan informasi, indeks KAMI, ISO 27001**

INFORMATION SECURITY EVALUATION ON PT. TELEKOMUNIKASI INDONESIA TBK NETWORK OF BROADBAND DIVISION USING INDEKS KEAMANAN INFORMASI (KAMI)

Student Name : Endi Lastyono Putra
NRP : 5210 100 079
Department : Information System FTIf – ITS
Supervisor Lecturer I : Bekti Cahyo Hidayanto, S.Si, M.Kom
Supervisor Lecturer II : Hanim Maria Astuti, S.Kom, M.Sc

ABSTRACT

PT. Telekomunikasi Indonesia Tbk. (Telkom) is a state-owned company that engage in communication service on Indonesia. Telkom headquarters located in Bandung city East Java province Indonesia. There are so many network around the country that connected to Telkom which can create some risks that can threatened the business process of the company, especially the information security. Therefore the information security aspects need to be evaluated so that the company knows how much does the maturity of the information security.

Indeks Keamanan Informasi (KAMI) is a tool created by Ministry of Information and Communication to assess the maturity level of the information security according to ISO 27001:2005.

The first phase of the evaluation is to asses the dependant level of the IT on the organization, and the result will be used as a threshold for the overall evaluation score. The result for the dependant level is 44 from overall total score of 48, and categorized as critical, and therefore the minimum score for the overall evaluation must be above 334. The overall score from the evaluation process which has been done to the

organization is 582 from overall total score of 588. This is categorized as optimum. And therefore there will be some improvement suggestions to be made for the remaining flaw that has been detected on this evaluation.

Keyword: Information Security, Indeks KAMI, ISO 27001

EVALUASI KEAMANAN INFORMASI PADA DIVISI NETWORK OF BROADBAND PT. TELEKOMUNIKASI INDONESIA TBK DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI)

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

ENDI LASTYONO PUTRA
NRP. 5210 100 079

Surabaya, Juli 2014
Ketua Jurusan Sistem Informasi

Dr. Eng. FEBRILIYAN SAMOPA, S. Kom, M. Kom
NIP. 1973 0219 1998 02 1001

EVALUASI KEAMANAN INFORMASI PADA DIVISI NETWORK OF BROADBAND PT. TELEKOMUNIKASI INDONESIA TBK DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI)

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

ENDI LASTYONO PUTRA
NRP. 5210 100 079

Disetujui Tim Penguji : Tanggal Ujian : 2014
Periode Wisuda : ... 2014

1. **Bekti Cahyo Hidayanto, S.Si, M.Kom** **(Pembimbing I)**
2. **Hanim Maria Astuti, S.Kom, M.Sc** **(Pembimbing II)**
3. **Sholiq S. T, M.Kom, M.SA** **(Penguji I)**
4. **Anisah Herdiyanti, S.Kom, M.Sc** **(Penguji II)**

KATA PENGANTAR

Alhamdulillahhrobbil'alamiin. Puji syukur penulis ucapkan kepada Allah SWT yang telah memberikan segala kemudahan serta kekuatan bagi penulis hingga dapat menyelesaikan buku tugas akhir dengan judul:
"EVALUASI KEAMANAN INFORMASI PADA DIVISI NETWORK OF BROADBAND PT. TELEKOMUNIKASI INDONESIA TBK DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI)".

Selain itu penulis ucapkan terima kasih kepada berbagai pihak yang secara langsung maupun tidak langsung memberikan dukungan kepada penulis hingga dapat menyelesaikan tugas akhir ini. Secara khusus penulis ucapkan terima kasih sebesar-besarnya kepada:

1) Allah SWT, yang telah memberikan rahmat hidayahNya kepada hambaNya sehingga tugas akhir ini dapat terselesaikan.
2) Kedua orang tua, Alm Bapak Ir. Pamudji dan Ibu Ida Desyana yang selalu memberikan dukungan dan do'a hingga tugas akhir ini dapat terselesaikan.
3) Kepada dosen pembimbing, Bapak Bekti Cahyo Hidayanto, S.Si, M.Kom dan Ibu Hanim Maria Astuti, S.Kom, M.Sc, yang telah dengan sabar memberikan bimbingan dan motivasi kepada penulis.
4) Kepada dosen penguji, Bapak Sholiq S. T, M.Kom, M.SA dan Ibu Anisah Herdiyanti, S.Kom, M.Sc, yang telah memberikan perbaikan-perbaikan terhadap Tugas Akhir penulis.
5) Kepada Bapak Suratmin, Bapak Helmut Prayogo, Bapak Agus Gunarso, dan Bapak Akhmad Aryandi selaku pembimbing dan pendamping pada PT. Telekomunikasi Indonesia Tbk.

6) Kepada seluruh teman-teman Foxis yang telah berjuang dan bersenang-senang bersama selama empat tahun ini.
7) Kepada dosen wali, Ibu Feby Artwodini S.Kom, M.T dan seluruh Bapak dan Ibu dosen pengajar Jurusan Sistem Informasi ITS yang telah memberikan ilmu kepada penulis.

Terima kasih atas segala dukungan dan do'a yang telah diberikan, semoga Allah SWT senantiasa memberikan balasan berupa rahmat dan hidayahNya.

Tidak lupa penulis sampaikan permohonan maaf atas segala kekurangan yang terdapat dalam tugas akhir ini. Saran dan kritik yang membangun untuk perbaikan dalam tugas akhir ini akan penulis terima dengan tangan terbuka.

Semoga tugas akhir ini dapat memberikan manfaat bagi penulis, pihak PT. Telekomunikasi Indonesia dimana merupakan tempat studi kasus tugas akhir ini, serta pihak lain yang memerlukannya.

Surabaya, 2014

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

Bab pendahuluan ini berisi latar belakang pengerjaan tugas akhir, permasalahan yang ada dalam pengerjaan tugas akhir, batasan permasalahan pengerjaan tugas akhir, tujuan pengerjaan tugas akhir, dan manfaat pengerjaan tugas akhir.

1.1 Latar Belakang

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 di Indonesia. Meskipun perusahaan besar, Telkom perlu untuk tetap memperhatikan aspek keamanan informasinya karena lingkup layanan Telkom yang sangat luas, yaitu seluruh wilayah Indonesia untuk memastikan terjaganya keamanan informasi agar dapat memberikan layanan yang maksimal dan dapat diandalkan kepada pelanggan.

Dalam proses penyelenggaraan tata kelola teknologi informasi (TIK), faktor keamanan informasi merupakan bagian yang sangat penting untuk diperhatikan karena proses tata kelola TIK dapat terganggu jika informasi yang merupakan salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi. 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.

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. (Kominfo, 2013)

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 (Perera, 2008).

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 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 agar dapat memberikan pelayanan yang lebih baik dan dapat diandalkan.

1.2 Perumusan Masalah

Masalah yang akan diangkat pada tugas akhir ini adalah:

1. Berapa tingkat kematangan dan kelengkapan keamanan informasi pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk?
2. Bagaimana cara meningkatkan keamanan informasi berdasarkan tingkat kematangan dan kelengkapan keamanan informasi Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk?

1.3 Batasan Tugas Akhir

Batasan permasalahan dalam tugas akhir ini adalah:

1) Menggunakan lima (5) area cakupan penilaian dalam evaluasi indeks KAMI.
2) Penilaian indeks KAMI dilakukan berdasarkan wawancara dengan pihak PT. Telkom.
3) Hasil dari penilaian indeks KAMI digunakan untuk membuat rekomendasi perbaikan Teknologi Informasi dan Komunikasi (TIK) Divisi Network of Broadband Telkom.

1.4 Tujuan Tugas Akhir

Tujuan dari tugas akhir ini adalah:

1) Untuk mengetahui tingkat kematangan dan kelengkapan keamanan informasi pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk.

2) Membuat rekomendasi perbaikan sebagai sarana peningkatan keamanan informasi pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk.

1.5 Relevansi atau Manfaat Kegiatan Tugas Akhir

Tugas akhir ini diharapkan dapat membantu PT. Telekomunikasi Indonesia Tbk khususnya Divisi Network of Broadband untuk mengetahui tingkat kesiapan dan kelengkapan terhadap keamanan informasi dengan menggunakan indeks Keamanan Informasi (KAMI) sebagai alat ukur dalam penilaian tersebut. Hasil dari penilaian tersebut dapat memberikan Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk gambaran atas kesiapan dan kelengkapan dalam keamanan informasi.

BAB II
TINJAUAN PUSTAKA

Bab tinjauan pustaka berisi tentang teori-teori yang berkaitan dengan permasalahan yang ada pada Tugas Akhir. Hasil dari bab tinjauan pustaka digunakan sebagai dasar pengetahuan yang akan membantu dalam pengerjaan Tugas Akhir.

2.1 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. Divisi Network of Broadband ini bertugas untuk menangani segala perawatan hingga perencanaan jaringan baik untuk internal maupun eksternal. Proses bisnis utama Divisi Network of Broadband adalah menangani secara langsung jaringan yang terhubung dengan pelanggan Telkom. Mulai dari instalasi hingga perawatan yang diperlukan agar pelanggan dapat menggunakan jaringan yang disediakan dengan baik. Selain itu Divisi Network of Broadband bertugas untuk memonitor dan melakukan perawatan jaringan internal antar divisi dalam Telkom.

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. Hal ini bertujuan agar keamanan informasi yang dikelola sesuai dengan standar

internasional yang saat ini berlaku di dunia untuk dapat memberikan layanan yang lebih baik kepada pelanggan.

Seluruh aktifitas yang berhubungan dengan jaringan, adalah lingkup kerja dari Divisi Network of Broadband. Termasuk dalam hal keamanan informasi. Keamanan informasi yang masuk dalam lingkup divisi tersebut adalah keamanan secara logikal. Karena lingkup yang cukup luas, perlu diadakan suatu evaluasi atas keamanan informasi agar mengetahui kondisi keamanan informasi saat ini.

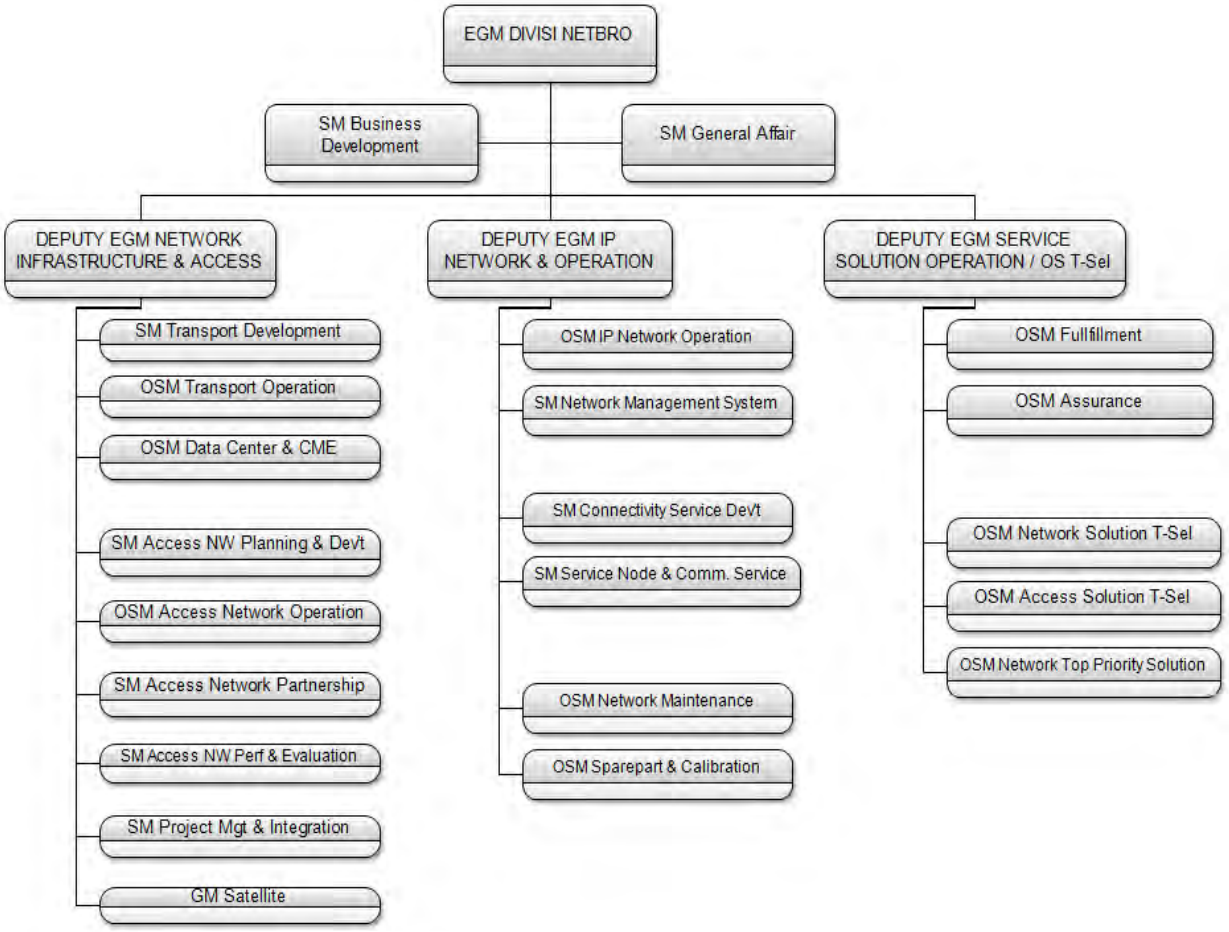
Divisi network of broadband memiliki visi dan misi sebagai berikut ini:

- **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

Berikut ini adalah bagan organisasi divisi Network of Broadband



Gambar 2.1 Struktur Organisasi Divisi Network Of Broadband

Secara umum tugas utama dari setiap bagian divisi Network of Broadband adalah sebagai berikut:

- Network Infrastructure & Access
  - Mengembangkan sistem transport atau media untuk menyalurkan jaringan kepada pelanggan (*fiber optics, wireless,* dll)
  - Mendirikan jaringan untuk pelanggan dan partner Telkom
  - Mengatur setiap proyek pengembangan jaringan
- IP Network & Operation
  - Mengkonfigurasi IP jaringan untuk jaringan luar dan jaringan internal Telkom
  - Mengelola jaringan keseluruhan secara logikal
  - Menghubungkan jaringan yang telah terpasang pada pelanggan dan partner
- Service Solution Operation / OS T-Sel
  - Memenuhi kebutuhan setiap permintaan pelanggan
  - Memastikan kualitas layanan jaringan yang diberikan kepada pelanggan
  - Mengelola jaringan Telkomsel
  - Mengelola akses Telkomsel ke dalam jaringan Telkom
  - Memberikan layanan kepada pelanggan VVIP

2.2 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 (ISO/IEC 2009, 2009):

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.

Selain itu juga ada beberapa strategi yang digunakan untuk mendukung keamanan informasi dimana strategi tersebut masing-masing mempunyai fokus dan tujuan tertentu sesuai dengan kebutuhan. Contoh dari keamanan informasi adalah sebagai berikut (Whitman & Mattord, 2013):

1. *Physical security*, yaitu keamanan informasi yang mengutamakan unsur fisik dengan arti untuk mengamankan suatu indivdu atau sebuah organisasi seperti aset fisik, dan tempat kerja dari berbeagai ancaman berupa kebakaran atau bencana alam lainnya.
2. *Personal security*, yaitu keamanan infomasi yang berhubungan dengan keamanan personil. Biasanya personal security berkolaborasi dengan physical security karena fungsinya saling berkaitan.
3. *Operasional security*, yaitu keamanan informasi yang berhubungan dengan startegi dari sebuah

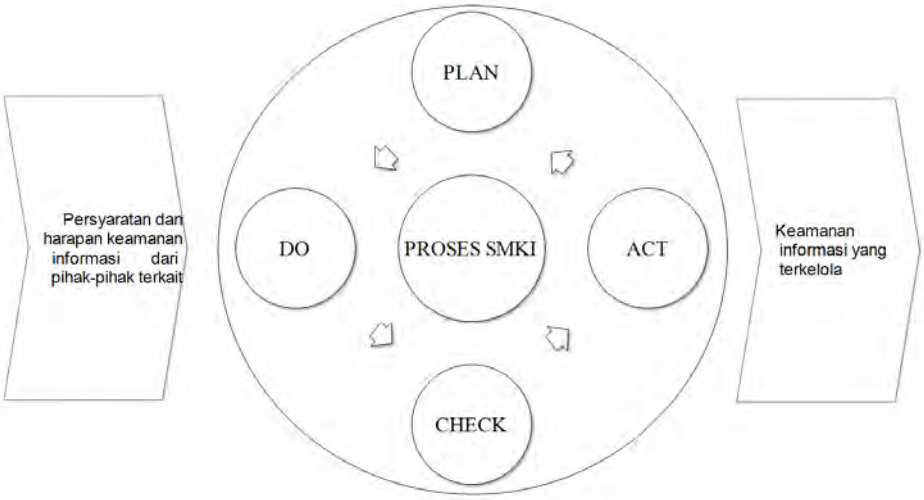
orhganisasi agar organisasi tersebut bisa berjalan dengan baik tanpa ada ancaman atau gangguan.

4. *Communication security*, yaitu keamanan informasi yang berhubungan dengan keamanan komunikasi, teknologi infomasi dan juga semua yang terkait dengan teknologi informasi.
5. *Network security*, yaitu keamanan informasi yang berhubungan dengan keamanan jaringan disebuah organisasi seperti peralatan jaringan, data organisasi, jaringan itu sendiri dan juga kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

2.3 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 SMKI, desain dan penerapan SMKI dari suatu organisasi dipengaruhi oleh kebutuhan dan sasaran organisasi. (Kominfo, 2013).

Model *PLAN-DO-CHECK-ACT (PDCA)* diterapkan terhadap struktur keseluruhan proses SMKI. Definisi keseluruhan dari model PDCA adalah seperti tabel di bawah ini.



Gambar 2.2 Proses SMKI

Tabel 2.1 Definisi PDCA 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	Mengkaji dan mengukur

melakukan tinjau ulang SMKI)	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. (Kominfo, 2013)

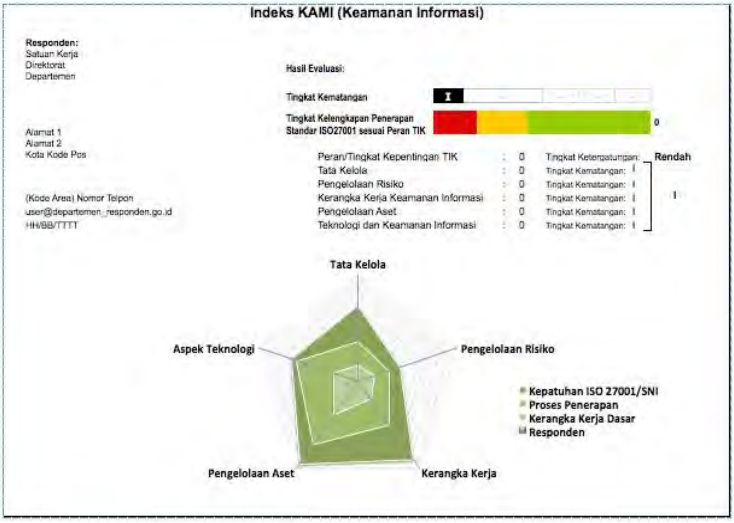
2.4 Indeks KAMI

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. Ada beberapa area target untuk penerapan kemanan informasi yang didefinisikan oleh SNI ISO 27001:2009 yaitu (Kominfo, 2013):

1. Peran dan tingkat kepentingan TIK dalam instansi, area ini merupakan area tingkatan peran dan kepentingan TIK dalam instansi.
2. Tata kelola keamanan informasi, area ini menilai kesiapan bentuk tata kelola keamanan informasi beserta fungsi, tugas, dan tanggung jawab pengelola keamanan informasi
3. Pengelolaan risiko keamanan informasi, area ini menilai kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
4. Kerangka kerja pengelolaan keamanan informasi, area ini menilai kelengkapan dan kesiapan kerangka kerja pengelolaan keamanan informasi dan strategi penerapannya.
5. Pengelolaan aset informasi, area ini menilai kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.
6. Teknologi dan keamanan informasi, area ini menilai kelengkapan, konsistensi, dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

Sebagai gambaran, hasil evaluasi indeks KAMI dapat dilihat pada Gambar.



Gambar 2.3 Tampilan Dashboard Indeks KAMI

Gambar diatas adalah tampilan dari *dashboard* dari hasil penilaian indeks KAMI. *Dashboard* tersebut berisi nilai-nilai total dari setiap area yang ada dalam indeks KAMI dan menampilkan nilai-nilai total tersebut dalam bentuk grafik *spider chart*. Selain itu juga ditampilkan tingkat kematangan keamanan informasi dengan menggunakan grafik batang yang menunjukan seberapa besar kematangan keamanan informasi tersebut

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan potret indeks kesiapan – dari aspek kelengkapan maupun kematangan – kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan

sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari programkerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (*stakeholders*).

Penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di instansi pemerintah. Pertukaran informasi dan diskusi dengan instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari *lesson-learned* yang sudah dilalui.

Alat evaluasi Indeks KAMI ini secara umum ditujukan untuk digunakan oleh instansi pemerintah di tingkat pusat. Akan tetapi satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat juga dapat menggunakan alat evaluasi ini untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya.

2.5 ISO 27001

ISO 27001 adalah suatu standar internasional yang mencakup keamanan informasi. ISO 27001 menyediakan kerangka kerja dalam penggunaan teknologi dan manajemen sistem pengelolaan yang membantu suatu

organisasi memastikan keamanan informasi sudah efektif. Hal ini termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas atas informasi yang dimilikinya (Perera, 2008). Beberapa alasan penerapan ISO 27001 adalah untuk mencegah :

1. Perusakan / terorisme
2. Kebakaran
3. Kesalahan penggunaan
4. Pencurian
5. Serangan yang diakibatkan oleh virus

ISO 27001 dapat digunakan pada setiap organisasi untuk mencegah kesalahan dalam penggunaan, kerusakan, atau hilangnya data bisnis yang dapat berdampak merugikan pada aktifitas bisnis utama perusahaan. Berikut ini adalah tiga atribut yang disebutkan dalam ISO 27001 (Calder, Information Secutiry Based on ISO 27001/ISO 27002: A Management Guide, 2009):

1. *Availability,* informasi dapat diakses dan digunakan melalui suatu sistem atau aplikasi atas permintaan pengguna yang berwenang.
2. *Confidentiality,* menjaga kerahasiaan informasi dari pihak yang tidak berwenang.
3. *Integrity,* menjaga kelengkapan dan ketepatan aset informasi.

2.5.1 Perbedaan ISO 27001:2005 dan ISO 27001:2013

Sebagai panduan referensi untuk pengerjaan tugas akhir ini, berikut ini adalah lampiran tabel perbedaan yang terdapat dalam ISO versi tahun 2005 dan tahun 2013:

Tabel 2.2 Perbandingan ISO 27001:13 dan 27001:2005

ISO 27001:2013	ISO 27001:2005
A.5 Information Security Policy	A.5 Security policy
A.5.1 Management Directions for Information Security	A.5.1 Information security policy
A.6 Organisation of Information Security	A.6 Organization of information security
A.6.1 Internal Organisation	A.6.1 Internal organization
A.7 Human Resource Security	A.6.2 External parties
A.7.1 Prior to Employment	A.7 Asset management
A.7.2 During Employment	A.7.1 Responsibility for assets
A.7.3 Termination and Change of Employment	A.7.2 Information classification
A.8 Asset Management	A.8 Human resources security
A.8.1 Responsibility for Assets	A.8.1 Prior to employment
A.8.2 Information Classification	A.8.2 During employment
A.8.3 Media Handling	A.8.3 Termination or change of employment
A.9 Logical Security / Access Control	A.9 Physical and environmental security
A.9.1 Business Requirement of Access Control	A.9.1 Secure areas

A.9.2 User Access Management	A.9.2 Equipment security
A.9.3 User Responsibilities	A.10 Communications and operations management
A.9.4 System and Application Access Control	A.10.1 Operational procedures and responsibilities
A.10 Cryptography	A.10.2 Third party service delivery management
A.10.1 Cryptographic Controls	A.10.3 System planning and acceptance
A.11 Physical and Environmental Security	A.10.4 Protection against malicious and mobile code
A.11.1 Secure areas	A.10.5 Back-up
A.11.2 Equipment	A.10.6 Network security management
A.12 Operations Securiy	A.10.7 Media handling
A.12.1 Operational Procedures and Responsibilities	A.10.8 Exchange of information
A.12.2 Protection From Malware	A.10.9 Electronic commerce services
A.12.3 Back-up	A.10.10 Monitoring
A.12.4 Logging and Monitoring to Record Events and Generate Evidence	A.11 Access control

A.12.5 Controls of Operational Software	A.11.1 Business requirement for access control
A.12.6 Technical Vulnerability Management	A.11.2 User access management
A.12.7 Information Systems Audit Considerations	A.11.3 User responsibilities
A.13 Communication Security	A.11.4 Network access control
A.13.1 Network Security Management	A.11.5 Operating system access control
A.13.2 Information Transfer	A.11.6 Application and information access control
A.14 System acquisition, development and maintenance	A.11.7 Mobile computing and teleworking
A.14.1 Security requirements of information systems	A.12 Information systems acquisition, development and maintenance
A.14.2 Security in development and support process	A.12.1 Security requirements of information systems
A.14.3 Test Data	A.12.2 Correct processing in applications
A.15 Supplier Relationship	A.12.3 Cryptographic controls
A.15.1 Security in Supplier Relationsip	A.12.4 Security of system files
A.15.2 Supplier Service Delivery Management	A.12.5 Security in development and support processes

A.16 Information Security Incident Management	A.12.6 Technical Vulnerability Management
A.16.1 Management of Information Security Incidents and Improvements	A.13 Information security incident management
A.17 Business Continuity	A.13.1 Reporting information security events and weaknesses
A.17.1 Information Security Aspects of Business Continuity Management	A.13.2 Management of information security incidents and improvements
A.17.2 Redundancies	A.14 Business continuity management
A.18 Compliance	A.14.1 Information security aspects of business continuity management
A.18.1 Information Security Reviews	A.15 Compliance
A.18.2 Compliance With Legal and Contractual Requirements	A.15.1 Compliance with legal requirements
	A.15.2 Compliance with security policies and standards, and technical compliance
	A.15.3 Information systems audit considerations

2.5.2 Pemetaan Indeks KAMI dengan ISO 27001:2005

Pemetaan indeks KAMI dengan ISO 27001:2005 dilihat dari *control objectives and control* ISO 27001, mulai dari *security policy* sampai dengan *compliance* yang dihubungkan dengan enam bagian pada indeks KAMI, yaitu:

1. Peran dan tingkat kepentingan TIK dalam instasi
2. Tata kelola keamanan informasi
3. Pengelolaan risiko keamanan informasi
4. Kerangka kerja pengelolaan keamanan informasi
5. Pengelolaan aset informasi
6. Teknologi dan keamanan informasi

Berikut ini adalah tabel pemetaan indeks KAMI dengan ISO 27001:2005:

Tabel 2.3 Pemetaan ISO 27001:2005 dengan Indeks KAMI

	INDEKS KAMI					
	1	2	3	4	5	6
ISO 27001:2005						
A.5 Security policy		✓	✓	✓	✓	✓
A.6 Organization of information security	✓	✓		✓	✓	
A.7 Asset management		✓	✓	✓	✓	✓
A.8 Human resources security		✓		✓	✓	
A.9 Physical and environmental security		✓	✓	✓	✓	
A.10 Communications and operations management		✓	✓	✓	✓	✓
A.11 Access control		✓		✓	✓	✓
A.12 Information systems acquisition, development and maintenance	✓	✓		✓	✓	✓
A.13 Information security incident management		✓		✓	✓	✓

A.14 Business continuity management	✓	✓	✓	✓		
A.15 Compliance	✓	✓	✓	✓	✓	✓

2.6 Tata Kelola TI

Tata kelola merupakan serangkaian kegiatan yang meliputi sejumlah peraturan, kebijakan, program dan keputusan yang didesain untuk menyelesaikan masalah umum melalui serangkaian tindakan yang telah disusun. (Enderlein, Walti, & Zurn, 2010)

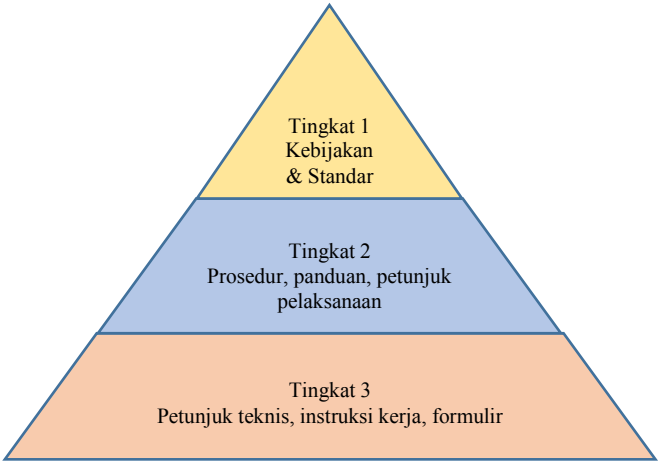
Terdapat beberapa jenis dalam bidang tata kelola, diantaranya adalah tata kelola perusahaan yang didalamnya terdapat tata kelola teknologi informasi. Tata kelola perusahaan mencakup aspek-aspek umum, dimana tata kelola perusahaan adalah rangkaian dari proses, kebijakan, peraturan serta pengendalian dari suatu organisasi atau perusahaan. Pihak-pihak utama dalam tata kelola perusahaan diantaranya adalah pemegang saham, manajemen dan dewan direksi. Adapun tata kelola teknologi informasi termasuk didalam tata kelola perusahaan dimana tata kelola teknologi informasi adalah tata kelola yang berfokus kepada teknologi informasi yang ada di suatu perusahaan termasuk manajemen kinerja dan risikonya yang ada didalamnya.

Tata kelola teknologi informasi adalah keputusan-keputusan yang diambil, yang memastikan adanya alokasi penggunaan teknologi informasi dalam strategi-strategi organisasi yang bersangkutan. Tata kelola teknologi informasi merefleksikan adanya penerapan prinsip organisasi dengan memfokuskan pada kegiatan manajemen dan penggunaan teknologi informasi untuk pencapaian organisasi (Weill, 2004)

Lima alasan utama untuk melakukan tata kelola teknologi informasi adalah (Calder, IT Governance: Guidlines for Directors, 2005):

1. Bersaing dengan kompetitor dalam dunia informasi dan ekonomi dengan cara menggunakan aset intelektual, informasi, dan teknologi informasi.
2. Berkembang pesatnya kebutuhan dan peraturan dari OECD (*Organisation for Economic Co-operation and Development*).
3. Semakin banyaknya hukum yang berkaitan dengan informasi dan privasi.
4. Semakin banyaknya ancaman dalam dunia aset intelektual, informasi, dan teknologi informasi.
5. Memastikan teknologi informasi dapat selaras dengan tujuan strategis organisasi.

Dokumen tata kelola memiliki beberapa jenis yang dapat digunakan sesuai dengan tujuan tata kelola. Dokumentasi yang ditetapkan oleh Kementerian Komunikasi dan Informatika pada umumnya terdiri dari tiga tingkatan.



Gambar 2.4 Tingkatan Dokumen Tata Kelola

1. Dokumen tingkat 1
Dokumen tingkat 1 adalah dokumen dengan hirarki tertinggi dalam tingkatan dokumentasi. Dokumen tingkat 1 bersifat strategis yang berisi kebijakan, tujuan, standar, dan rencana yang berhubungan dengan penerapan, pengembangan, dan peningkatan keamanan informasi.

2. Dokumen tingkat 2
Dokumen tingkat 2 adalah dokumen yang berisi prosedur dan panduan, dan dikembangkan berdasarkan dokumen tingkat 1 yang telah dibuat. Dokumen ini berisi cara penerapan kebijakan yang telah dibuat sebelumnya beserta penanggung jawab dari kebijakan tersebut. Dokumen tingkat 2 bersifat operasional.

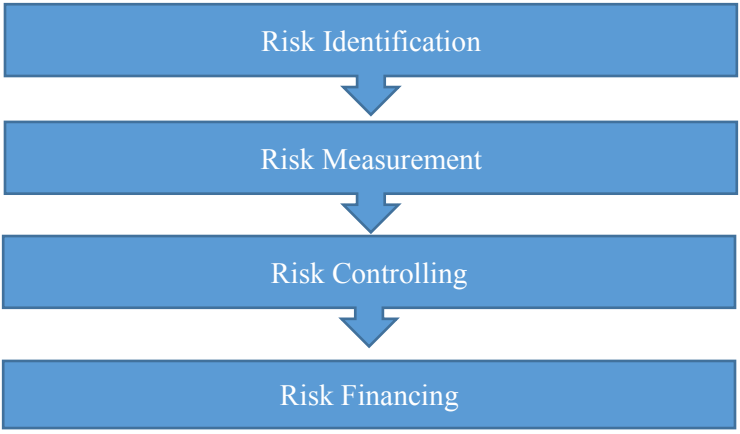
3. Dokumen tingkat 3
Dokumen tingkat 3 berisi petunjuk teknis, panduan kerja serta formulir yang digunakan untuk mendukung pelaksanaan kebijakan yang telah dibuat dalam tingkatan teknis.

2.7 Manajemen Risiko TI

Salah satu area dalam indeks KAMI membahas masalah manajemen risiko. Manajemen risiko untuk bidang teknologi informasi perlu dilakukan untuk membantu kelancaran operasional perusahaan dalam hal teknologi informasinya. Manajemen risiko tersebut meliputi proses identifikasi, penilaian, hingga bagaimana cara mengatasi risiko tersebut jika terjadi.

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 (Hopkin, 2012). Berikut ini adalah proses dari manajemen risiko:



Gambar 2.5 Urutan Proses 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.

2.8 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. (Hastings, 2010)

Dalam area perencanaan dan finansial, aktifitas dalam pengelolaan aset meliputi :

- Pengembangan dan implementasi aset
- Perencanaan dan implementasi kontinuitas aset
- Pengembangan dan pengelolaan fasilitas pendukung

Dalam area operasional, aktitifas dalam pengelolaan aset meliputi :

- Perencanaan dan pengelolaan pengadaan
- Pengelolaan dan pemeliharaan aset secara keseluruhan dalam organisasi.
- Pengembangan dan pengelolaan untuk pemeliharaan aset melalui *outsourcing*
- Kepatuhan terhadap peraturan regulasi

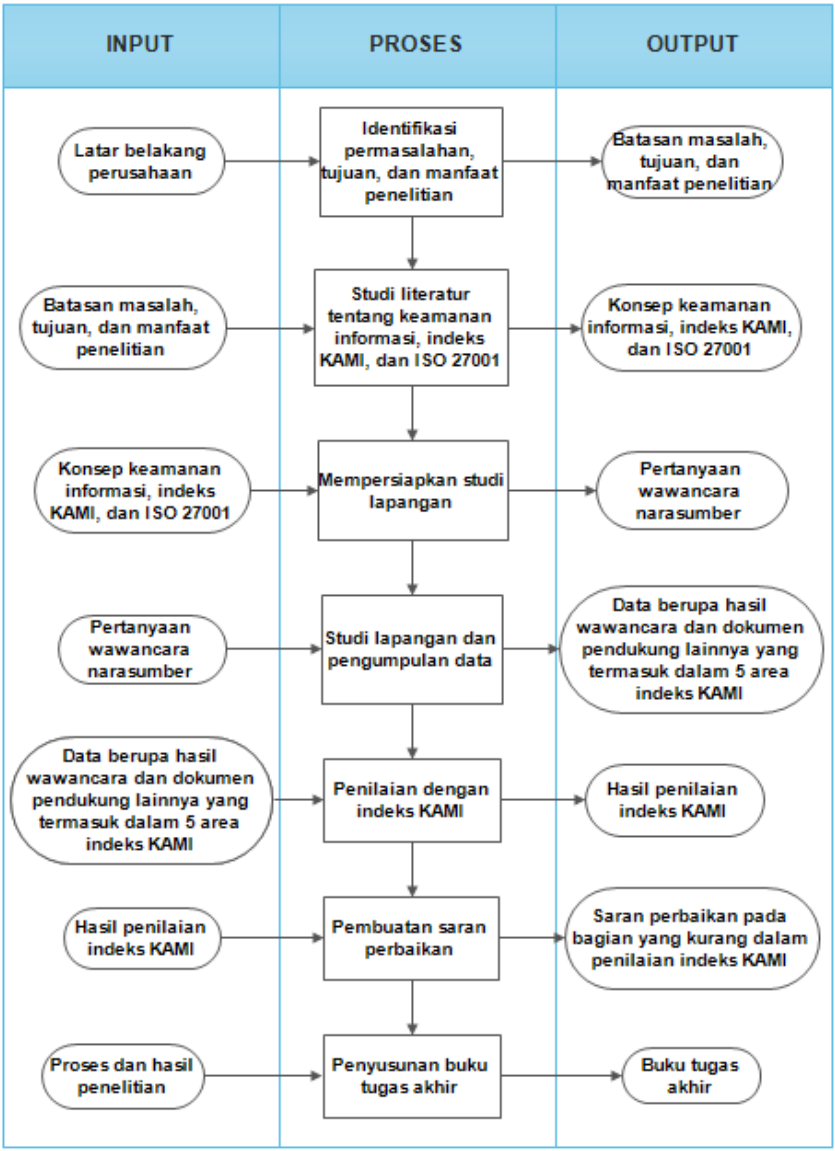
BAB III
METODE PENELITIAN

Bab ini membahas tentang metodologi pengerjaan tugas akhir. Metodologi atau tahapan pengerjaan sangat diperlukan sebagai kerangka atau panduan proses pengerjaan tugas akhir supaya rangkaian pengerjaan tugas akhir dapat terarah, teratur dan sistematis.

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 3.1 Metodologi Penelitian

3.1 Identifikasi Permasalahan, Tujuan, Dan Manfaat

Tahapan ini adalah tahap awal, setelah mengetahui latar belakang perusahaan studi kasus, dapat ditentukan dan dicari permasalahan, tujuan, dan manfaat yang terdapat dalam penelitian tugas akhir ini.

3.2 Studi Literatur

Studi literatur merupakan tahapan dimana terdapat proses pembelajaran yang terkait dengan semua metode dan teori yang diingingkan sesuai dengan permasalahan yang dihadapi dalam studi kasus. Pembelajaran dilakukan dengan mencari suatu sumber referensi dan acuan yang relevan terhadap studi kasus yang dikembangkan dalam tugas akhir tersebut. Literatur yang digunakan diambil dari sejumlah paper, jurnal, e-book, tesis, serta sumber yang ada di internet.

3.3 Persiapan Studi Lapangan

Pada tahap ini, akan dipersiapkan beberapa pertanyaan yang akan digunakan untuk mewawancarai narasumber pada divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Pertanyaan yang dibuat berkaitan dengan kelima area dalam indeks KAMI

3.4 Studi Lapangan Dan Pengumpulan Data

Melakukan pengamatan dan pengumpulan data secara langsung berdasarkan teori dan dengan menggunakan metode yang telah dipelajari sebelumnya pada objek studi kasus yang merupakan Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Pengumpulan data

merupakan proses mengumpulkan data proses bisnis, keamanan, jurnal, wawancara dan data-data lain yang berkaitan dengan studi kasus yang ada pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk.

3.5 Penilaian Dengan Indeks KAMI

Melakukan penilaian terhadap kesiapan dan kelengkapan keamanan informasi pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk berdasarkan data-data yang telah dikumpulkan sebelumnya.

3.6 Pembuatan Saran Perbaikan

Pada tahapan ini, seluruh hasil dari proses evaluasi indeks KAMI yang telah dilakukan akan dianalisa dan digunakan sebagai dasar untuk membuat saran perbaikan pada bagian-bagian yang dinilai masih kurang.

3.7 Penyusunan Buku Tugas Akhir

Tahap ini adalah proses penyusunan hasil dan proses selama pengerjaan tugas akhir, dan disusun menjadi buku sebagai dokumentasi dari pengerjaan tugas akhir.

BAB IV
ANALISIS & PEMBAHASAN

Bab ini adalah bab yang berisi pembahasan dan analisa hasil dari penelitian yang telah dilakukan pada PT. Telekomunikasi Indonesia Tbk. divisi Network of Broadband. Bab ini akan dibagi menjadi dua bagian, yaitu pada bagian pertama akan dilakukan pembahasan dan analisa tentang hasil evaluasi dengan indeks KAMI. Kemudian pada bagian kedua akan dibahas tentang saran perbaikan yang diberikan terhadap hasil dari evaluasi indeks KAMI.

4.1. Persiapan Pengumpulan Data

Studi lapangan pertama dilakukan di kantor Plasa Telkom Jalan Lembong no. 11 Bandung, Jawa Barat pada tanggal 26 Maret 2014 dengan pokok bahasan antara lain:

- Perkenalan dengan pihak Telkom:
  1. Nama : Bpk. Suratmin
     Jabatan : Manager IP Security Network & Services
  2. Nama : Bpk. Helmut Prayogo
     Jabatan : Engineer 1 Network Security Backbone
  3. Nama : Bpk. Agus Gunarso, ST
     Jabatan : Engineer 1 Network Security Broadband
  4. Nama : Bpk. Akhmad Aryandi
     Jabatan : Engineer 2 Network Security Metro
- Visi dan misi divisi Network of Broadband
- Struktur organisasi divisi Network of Broadband

- Proses bisnis organisasi divisi Network of Broadband

Studi lapangan kedua dilakukan pada tanggal 28 April 2014 dengan pokok bahasan antara lain:

- Visi dan misi divisi Network of Broadband
- Detail proses bisnis divisi Network of Broadband
- Detail struktur organisasi divisi Network of Broadband
- Pembahasan gambaran secara umum indeks KAMI

Pada tanggal 14 Mei 2014, kominfo mengadakan bimbingan teknis yang membahas indeks KAMI yang dilaksanakan di Alana Hotel Surabaya. Penulis mengikuti bimtek tersebut untuk mempersiapkan aplikasi indeks KAMI yang akan digunakan untuk evaluasi pada divisi Network of Broadband Telkom.

Sebelum melakukan studi lapangan berikutnya yang akan membahas penilaian dengan indeks KAMI, penulis menyiapkan pertanyaan-pertanyaan yang akan digunakan dalam wawancara untuk menilai keamanan informasi dengan indeks KAMI. Pertanyaan-pertanyaan tersebut telah dipetakan dengan indeks KAMI. Pertanyaan-pertanyaan yang telah dibuat dilampirkan dalam Lampiran B buku tugas akhir ini.

Wawancara dilakukan dengan beberapa narasumber secara bersamaan, yaitu:

1. Bapak Suratmin - Manajer IP Security Network & Services
2. Bapak Agus - Engineer 1 Network Security Broadband
3. Bapak Helmut - Engineer 1 Network Security Backbone

Pada tanggal 22 Mei 2014, wawancara dan pengisian indeks KAMI dimulai dengan narasumber yang telah disebutkan sebelumnya. Pengisian indeks KAMI meliputi kelima area dalam indeks KAMI.

4.2. Pembahasan Hasil Evaluasi Indeks KAMI

Berikut ini adalah pembahasan dari hasil penilaian yang telah dilakukan dengan menggunakan indeks KAMI. Sesuai dengan literatur yang telah dijelaskan sebelumnya, indeks KAMI terdiri dari lima kategori penilaian. Sebelum melakukan penilaian terhadap lima kategori tersebut, perlu melakukan penilaian terhadap tingkat kesiapan keamanan informasi terlebih dahulu. Hal ini bertujuan untuk menetapkan batasan nilai akhir yang didapatkan sesuai dengan tingkat kepentingan atau peran TIK dalam organisasi tersebut.

4.2.1. Tahap Penilaian Kesiapan Keamanan Informasi

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. Keempat tingkatan tersebut dapat dilihat pada tabel dibawah ini.

Tabel 4.1 Tingkatan Kematangan Indeks KAMI

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

Penilaian yang dilakukan dalam empat tingkatan tersebut dilakukan berdasarkan penilaian peran dan kepentingan TIK dalam organisasi itu sendiri. 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.

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

Tabel 4.2 Nilai Jawaban Tahap Persiapan Indeks KAMI

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* PT. Telekomunikasi Indonesia:

Tabel 4.3 Hasil Penialain 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.		
1.3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi Instansi anda	Kritis
Alasan: TIK digunakan untuk menjalankan operasional sehari-hari divisi		
1.4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Tinggi
Alasan: Data bersifat internal, dan setiap divisi mampu melihat data tersebut namun hanya divisi yang terkait yang dapat merubah atau menambahkannya.		
1.5	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Kritis
Alasan: Jika sistem gagal maka tidak bisa memantau jaringan keseluruhan dan aktifitas bisnis tidak dapat berjalan.		
1.6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis
Alasan: Sistem merupakan bagian dari komponen penting yang berskala nasional.		
1.7	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional	Kritis
Alasan: Jika sistem gagal maka tidak dapat melacak aktifitas jaringan yang terhubung dengan instasi lain.		
1.8	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Kritis
Alasan: Setiap pegawai sangat membutuhkan TIK untuk menjalankan operasional divisi.		
1.9	Tingkat kepatuhan terhadap UU dan perangkat	Kritis

	hukum lainnya	
Alasan: Sudah dijalankan sesuai dengan peraturan kementerian.		
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Kritis
Alasan: Dapat berpotensi hilangnya aset informasi milik negara, dan terganggunya jaringan keseluruhan internal dan eksternal.		
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Rendah
Alasan: Pihak ketiga hanya datang untuk melakukan pemeriksaan dan perwawatan seperlunya dalam beberapa kali setiap tahun.		
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**

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. Karena kategori kritis memiliki nilai sebesar 37 sampai dengan 48.

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 Lima Area Indeks KAMI

Penilaian lima area ini bertujuan untuk menilai kondisi kematangan keamanan informasi sesuai dengan standar

ISO 27001:2005. Lima area dalam indeks KAMI tersebut adalah sebagai berikut:

I. Tata kelola keamanan informasi
II. Pengelolaan risiko keamanan informasi
III. Kerangka kerja keamanan informasi
IV. Pengelolaan aset informasi
V. Teknologi dan keamanan informasi

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 4.4 Penjelasan Tingkatan Warna Dalam Penilaian 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 Pengamanan		Tidak Dilakukan
		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 4.5 Pemetaan Nilai Indeks KAMI Berdasarkan Kategori

	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

4.2.2.1. Hasil Penilaian Bagian Tata Kelola

Tabel 4.6 Hasil Penilaian Tata Kelola

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.					
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan	Diterapkan Secara Menyeluruh	3

			informasi dan menjaga kepatuhannya?		
Alasan: Ada, sudah diatur sesuai dengan dokumen kebijakan dalam Lampiran D.3 poin 1. Diatur oleh IT *Strategy & Governance* (ITSG) dan divisi IT *Service & Solution* (ITSS).					
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah diberikan wewenang sesuai dengan kebijakan pusat pada Lampiran D.3 poin 1.					
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah diberikan anggaran dasar sesuai dengan Berita Negara RI Nomor 5 tanggal 18 Januari 2005 Tambahan Berita Negara RI Nomor 569.					
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi	Diterapkan Secara Menyeluruh	3

			kewenangan?		
Alasan: Sudah diatur oleh direktorat IT *Strategy & Governance* (ITSG) dan divisi IT *Service & Solution* (ITSS).					
2.8	II	1	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Diterapkan Secara Menyeluruh	3
Alasan: Ada dan disampaikan melalui surat elektronik masing-masing staff					
2.10	II	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?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah disesuaikan dengan poin-poin yang ada dalam ISO dan disesuaikan dengan kebijakan pusat.					
2.12	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah	Diterapkan Secara Menyeluruh	6

			kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?		
Alasan: Sudah termasuk dalam lingkup yang diatur oleh direktorat IT *Strategy & Governance* (ITSG).					
2.13	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah dilakukan sebagai bahan evaluasi atas kondisi keamanan informasi, struktur tim pelaksana dilampirkan dalam dokumen kebijakan dalam Lampiran D.3 poin 1.					
2.15	IV	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 tanggung jawabnya?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah terdapat program tahunan untuk keamanan informasi, seperti pelatihan, bimbingan teknis, dan sejenisnya.					

2.16	IV	3	Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah terdapat parameter tertentu dalam pengelolaan kinerja keamanan informasi. Batasan nilai ditentukan berdasarkan standar ISO dan COBIT.					
2.18	IV	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?	Diterapkan Secara Menyeluruh	9
Alasan: Proses evaluasi sudah dilakukan secara berkala dengan menggunakan standar COBIT.					
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**	

Tabel di atas merupakan sebagian hasil penilaian berkaitan dengan tata kelola yang ada pada divisi *Network of Broadband* PT. Telekomunikasi Indonesia Tbk yang mana didapatkan total nilai untuk evaluasi tata kelola adalah 114. Untuk hasil lengkapnya terdapat dalam Lampiran A dokumen ini.

4.2.2.2. Hasil Penilaian Bagian Pengelolaan Risiko

Tabel 4.7 Hasil Penilaian Pengelolaan Risiko

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**	
#	**Kajian Risiko Keamanan Informasi**				
No			**Pertanyaan**	**Status**	**Skor**
3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah terdapat dan sudah disesuaikan dengan standar ISO dan COBIT.					
3.2	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Diterapkan Secara Menyeluruh	3

Alasan: Sudah ada dan dikelola oleh direktorat IT *Strategy & Governance* (ITSG).					
3.4	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah disesuaikan dengan standar ISO dan COBIT.					
3.5	II	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
Alasan: Sudah dikelola secara keseluruhan oleh bagian *General Support* unit.					
3.8	II	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)?	Diterapkan Secara Menyeluruh	3

Alasan: Evaluasi terhadap risiko dan kinerja keamanan informasi sudah dilakukan secara berkala dengan menggunakan standar COBIT.					
3.9	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Diterapkan Secara Menyeluruh	3
Alasan: Mitigasi risiko dilakukan setelah melakukan analisa risiko yang telah dilakukan sebelumnya dengan standar COBIT.					
3.10	III	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
Alasan: Alokasi dana untuk keamanan informasi termasuk risikonya sudah disesuaikan berdasarkan Anggaran Dasar Perusahaan yang telah diumumkan dalam Berita Negara RI Nomor 5 tanggal 18 Januari 2005.					
3.12	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?	Diterapkan Secara Menyeluruh	6

Alasan: Hasil mitigasi risiko yang telah dilakukan dipantau secara berkala untuk memastikan efektifitasnya.					
3.14	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Diterapkan Secara Menyeluruh	9
Alasan: Dipantau dan diuji secara berkala dengan menggunakan COBIT.					
3.15	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Diterapkan Secara Menyeluruh	9
Alasan: Pengelolaan risiko termasuk dalam penilaian kinerja keamanan informasi sesuai dengan standar ISO.					
Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi				**69**	

Tabel di atas merupakan sebagian dari hasil penilaian berkaitan dengan pengelolaan risiko yang ada pada divisi *Network of Broadband* PT. Telekomunikasi Indonesia Tbk yang mana didapatkan total nilai untuk evaluasi pengelolaan risiko adalah 69. Untuk hasil lengkapnya terdapat dalam Lampiran A dokumen ini.

4.2.2.3. Hasil Penilaian Bagian Kerangka Kerja

Tabel 4.8 Hasil Penilaian Kerangka Kerja

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	**Skor**
#	**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**				
No			**Pertanyaan**	**Status**	**Skor**
4.1	II	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?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada kebijakan yang secara khusus memiliki lingkup SMKI dan dikelola oleh *Regulatory Management Unit* (RMU), salah satu contohnya ada pada Lampiran D.3 poin 1 dan 2.					
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Diterapkan Secara Menyeluruh	3

Alasan: Sudah dipublikasikan kepada seluruh pihak oleh *Regulatory Management Unit* (RMU).					
4.3	II	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
Alasan: Seluruh dokumen sudah dikelola dan didistribusikan oleh *Regulatory Management Unit* (RMU) kepada seluruh pihak yang terkait.					
4.9	III	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?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah dilakukan oleh bagian *Innovation & Design Center* (IDeC).					
4.10	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem	Diterapkan Secara Menyeluruh	6

			baru dan menanggulangi permasalahan yang muncul?		
Alasan: Seluruh pengujian terhadap sistem baru sudah dilakukan oleh bagian *Innovation & Design Center* (IDeC).					
4.12	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Diterapkan Secara Menyeluruh	6
Alasan: Kerangka kerja pengelolaan kelangsungan layanan TIK sudah dibuat oleh direktorat IT *Strategy & Governance* (ITSG).					
4.13	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah dibuat dan sudah ada bagian yang bertanggung jawab untuk menangani risiko keamanan informasi, yaitu departemen *Compliance Risk Management* (CRM)					
4.16	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Diterapkan Secara Menyeluruh	9

Alasan: Seluruh kebijakan dikelola dan dievaluasi kelayakannya oleh direktorat IT *Strategy & Governance* (ITSG).					
#			**Pengelolaan Strategi dan Program Keamanan Informasi**		
4.17	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Diterapkan Secara Menyeluruh	3
Alasan: Seluruh prosedur yang berkaitan dengan risiko sudah dibuat dan dijalankan sesuai dengan kebijakan dari *Compliance Risk Management* (CRM)					
4.19	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Diterapkan Secara Menyeluruh	3
Alasan: Keamanan informasi merupakan salah satu aspek utama dalam menjalankan bisnis operasional sehari-hari divisi.					
4.20	III	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

Alasan: Audit sudah dilakukan secara rutin dan sesuai dengan standar COBIT dan ISO 27001.					
4.21	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Audit yang dilakukan sudah mencakup seluruh aspek yang ada dalam ISO, contoh hasil audit terdapat dalam Lampiran D.3 poin 3					
4.24	IV	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	9
Alasan: Segala perbaikan disesuaikan dengan Anggaran Dasar Perusahaan sesuai dengan Berita Negara RI Nomor 5 tanggal 18 Januari 2005.					
4.25	V	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 Menyeluruh	9

			diterapkan secara efektif?		
Alasan: Pengujian sudah dilakukan secara periodik dengan menggunakan standar COBIT.					
4.26	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Diterapkan Secara Menyeluruh	9
Alasan: Program peningkatan dilakukan setiap tahun seperti pelatihan, bimbingan, dan lain-lain. Untuk program strategis direncanakan oleh direktorat IT *Strategy & Governance* (ITSG).					
Total Nilai Evaluasi Kerangka Kerja				**144**	

Tabel di atas merupakan sebagian dari hasil penilaian berkaitan dengan kerangka kerja yang ada pada divisi *Network of Broadband* PT. Telekomunikasi Indonesia Tbk yang mana didapatkan total nilai untuk evaluasi kerangka kerja adalah 144. Untuk hasil lebih lengkapnya terdapat dalam Lampiran A dokumen ini.

4.2.2.4. Hasil Penilaian Bagian Pengelolaan Aset

Tabel 4.9 Hasil Penilaian Pengelolaan Aset

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**	Skor
#	**Pengelolaan Aset Informasi**				
No			**Pertanyaan**	**Status**	**Skor**
5.1	II	1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	Diterapkan Secara Menyeluruh	3
Alasan: Inventaris dikelola oleh unit *General Support* masing-masing divisi.					
5.2	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Diterapkan Secara Menyeluruh	3
Alasan: Evaluasi terhadap keamanan suatu perangkat dilakukan oleh *Innovation & Design Center* (IDeC).					
5.3	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut	Diterapkan Secara Menyeluruh	3
Alasan:					

Pengaturan akses aset informasi diatur oleh *Regulatory Management Unit* (RMU).					
5.6	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Segala proses pembaharuan aset dan perangkat baru dilakukan dan diuji oleh oleh *Innovation & Design Center* (IDeC).					
			Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		
5.7	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Diterapkan Secara Menyeluruh	3
Alasan: Sudah terdapat dokumen terkait dan didistribusikan oleh *Regulatory Management Unit* (RMU) pada setiap staff.					
5.10	II	1	Peraturan pengamanan data pribadi	Diterapkan Secara Menyeluruh	3
Alasan: Tata tertib sudah dibuat berdasarkan SMKI.					
5.11	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap	Dalam Penerapan / Diterapkan Sebagian	2

			pelanggarannya		
Alasan: Kebijakan tentang akun sudah dibuat, namun yang secara spesifik mengatur password belum ada.					
5.12	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Diterapkan Secara Menyeluruh	3
Alasan: Pemberian hak akses aset informasi dikelola oleh *Regulatory Management Unit* (RMU).					
5.13	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Diterapkan Secara Menyeluruh	3
Alasan: *Regulatory Management Unit* (RMU) mengelola aset informasi juga bertanggung jawab dalam hal penghancuran data.					
5.15	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Diterapkan Secara Menyeluruh	3
Alasan: Proses penyelidikan dilakukan secara langsung ketika terjadi permasalahan.					
5.16	II	1	Prosedur *back-up* ujicoba pengembalian data (*restore*)	Diterapkan Secara Menyeluruh	3
Alasan: Prosedur *back-up* dan pengembalian dilakukan oleh *General Support* masing-masing divisi.					
5.18	III	2	Proses pengecekan	Dalam	4

			latar belakang SDM	Penerapan / Diterapkan Sebagian	
Alasan: Proses pengecekan latar belakang SDM sudah dilakukan, namun hanya pada beberapa aspek saja.					
5.20	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Diterapkan Secara Menyeluruh	6
Alasan: *Regulatory Management Unit* (RMU) mengelola aset informasi juga bertanggung jawab dalam hal penghancuran data. Selain itu *General Support* divisi juga bertanggung jawab atas aset fisik divisi.					
5.23	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah terdapat rekaman (*log*) yang merekam aktifitas pengguna. Contoh dari *log* ditampilkan pada Lampiran D.3 poin 5.					
#			**Pengamanan Fisik**		
5.25	II	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?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada penjagaan secara fisik pada lokasi-lokasi sensitif perusahaan dan divisi.					

5.27	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Diterapkan Secara Menyeluruh	3
Alasan: Bangunan sudah disesuaikan dengan standar ISO.					
5.28	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh	3
Alasan: Letak perangkat infrastruktur sudah disesuaikan dengan standar ISO.					
5.29	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada dan dikelola oleh *General Support* divisi.					
5.31	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Diterapkan Secara Menyeluruh	6

Alasan: Ada dan dilakukan oleh *General Support* unit					
5.34	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Diterapkan Secara Menyeluruh	9
Alasan: Proses untuk mengamankan lokasi kerja ketika terdapat pihak ketiga sudah dibuat dengan standar ISO.					
Total Nilai Evaluasi Pengelolaan Aset				**150**	

Tabel di atas merupakan sebagian dari hasil penilaian berkaitan dengan pengelolaan aset yang ada pada divisi *Network of Broadband* PT. Telekomunikasi Indonesia Tbk yang mana didapatkan total nilai untuk evaluasi pengelolaan aset adalah 150. Untuk hasil lebih lengkapnya terdapat dalam Lampiran A dokumen ini.

4.2.2.5. Hasil Penilaian Bagian Teknologi

Tabel 4.10 Hasil Penilaian Teknologi

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**				
No			**Pertanyaan**	**Status**	**Skor**
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada pengamanan secara logikal yang diterapkan dalam sistem. Dikembangkan oleh *Innovation & Design Center* (IDeC)					
6.3	II	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
Alasan: Sudah ada konfigurasi standar dan disesuaikan dengan kebutuhan bisnis.					
6.4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan	Diterapkan Secara Menyeluruh	3

			konfigurasi standar yang ada?		
Alasan: Secara rutin kesesuaian konfigurasi dipantau untuk memastikan kesesuaian dengan kebutuhan bisnis divisi.					
6.5	II	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
Alasan: Sudah dilakukan secara rutin dengan cara memberikan instruksi pada pihak eksternal untuk mencoba menerobos pengamanan akses jaringan divisi.					
6.7	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah terdapat *log* yang merekam aktifitas dalam sistem, *log* dilampirkan dalam Lampiran D.3 poin 5.					
6.9	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Diterapkan Secara Menyeluruh	3
Alasan: Seluruh aktifitas sudah direkam di dalam sistem untuk ditinjau dan diawasi.					
6.10	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset	Diterapkan Secara Menyeluruh	3

			informasi penting sesuai kebijakan pengelolaan yang ada?		
Alasan: Sistem sudah menerapkan enkripsi untuk meningkatkan keamanan akses jaringan.					
6.12	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Diterapkan Secara Menyeluruh	6
Alasan: Pengelolaan enkripsi dilakukan oleh bagian yang melakukan implementasi sistem, yaitu *Innovation & Design Center* (IDeC).					
6.13	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Dalam Penerapan / Diterapkan Sebagian	4
Alasan: Sistem sudah terdapat standar dasar pembuatan password, namun belum ada peraturan tertulis yang mengatur setiap pengguna dalam pengelolaan password akun mereka.					
6.15	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout*	Diterapkan Secara Menyeluruh	6

			setelah kegagalan *login*,dan penarikan akses?		
Alasan: Sistem sudah menerapkan keamanan seperti disebutkan sesuai dengan standar ISO 27001.					
6.17	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Diterapkan Secara Menyeluruh	3
Alasan: Pengamanan dilakukan berupa enkripsi dan pengamanan lain yang sesuai dengan ISO 27001.					
6.18	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
Alasan: Beberapa perangkat sudah dimutakhirkan, namun masih banyak perangkat lain yang belum diperbaharui sistem operasinya.					
6.19	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh	3
Alasan: Antivirus sudah dijalankan dalam setiap perangkat untuk mencegah kerusakan data.					
6.21	III	2	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	Diterapkan Secara Menyeluruh	6
Alasan: Segala upaya perbaikan pada perangkat dilakukan oleh *General Support* unit divisi.					

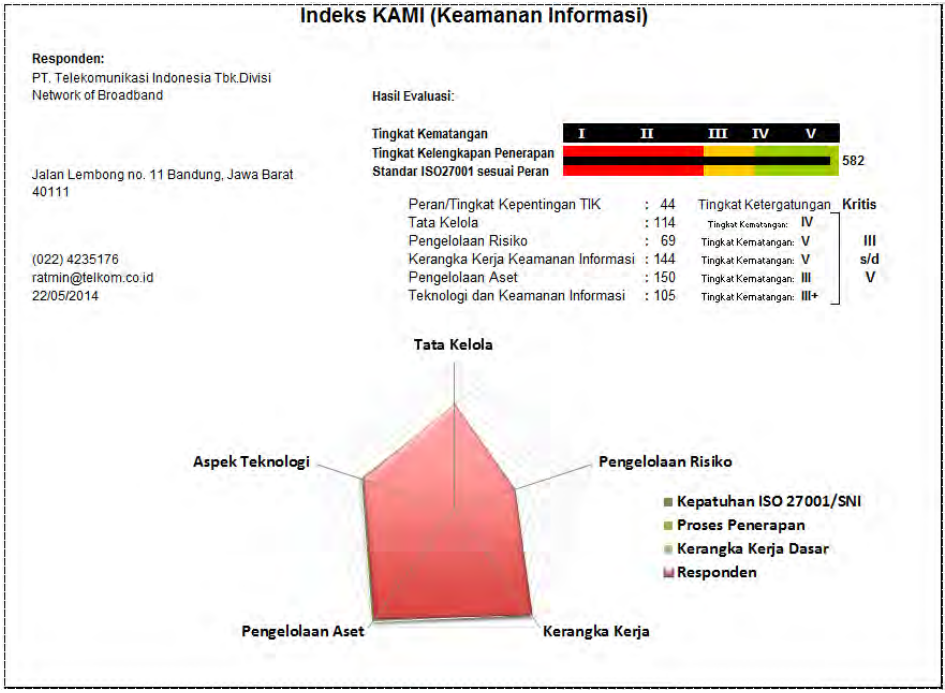
6.22	III	2	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah disesuaikan dengan server pusat.					
6.23	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?	Diterapkan Secara Menyeluruh	6
Alasan: Seluruh perangkat diuji coba sebelum diimplementasikan oleh bagian *Innovation & Design Center* (IDeC).					
6.24	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Diterapkan Secara Menyeluruh	9
Alasan: Divisi memerintahkan pihak luar untuk mencoba menerobos keamanan jaringan untuk mengetahui celah keamanan jaringan.					
Total Nilai Evaluasi Teknologi dan Keamanan Informasi				**105**	

Tabel di atas merupakan sebagian dari hasil penilaian berkaitan dengan teknologi keamanan informasi yang ada pada divisi *Network of Broadband* PT. Telekomunikasi Indonesia Tbk yang mana didapatkan total nilai untuk

evaluasi teknologi adalah 105. Untuk hasil lebih lengkapnya terdapat dalam Lampiran A dokumen ini.

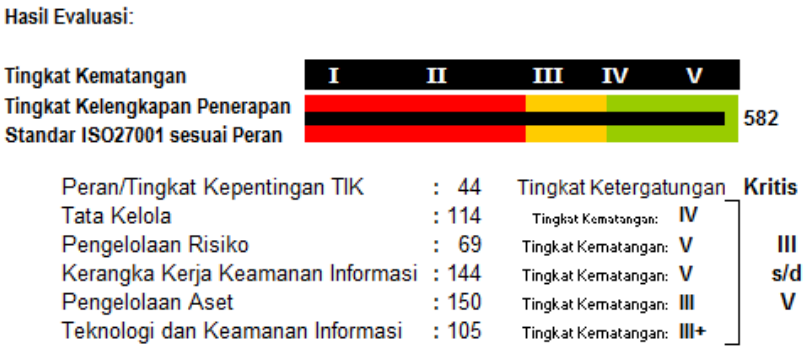
4.2.3. Analisa Hasil Penilaian Indeks KAMI

Bagian ini akan menjelaskan hasil dari penilaian indeks KAMI pada divisi *Network of Broadband* PT. Telekomunikasi Indonesia. Berikut ini adalah tampilan dari *dashboard* indeks KAMI:



Gambar 4.6 Hasil Dashboard Indeks KAMI

Dashboard diatas merupakan gambaran secara keseluruhan dari penilaian yang telah dilakukan dengan menggunakan 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 4.7 Hasil Evaluasi Indeks KAMI

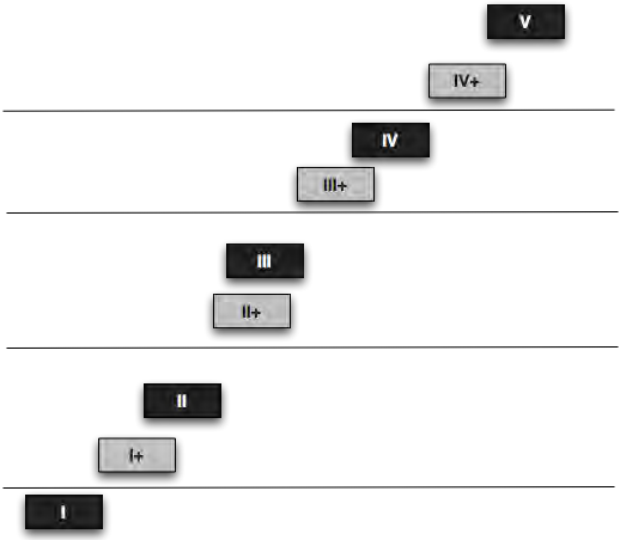
Dari gambar diatas dapat terlihat jika nilai indeks KAMI yang telah dicapai cukup bagus, yaitu mencapai tingkat V. Dapat dikatakan bagus karena nilai yang dicapai sesuai dengan peran dan tingkat kepentingan teknologi informasi yang digunakan pada divisi *network of broadband* PT. Telekomunikasi Indonesia,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

Untuk tingkat kematangan setiap area yang telah dinilai dalam indeks KAMI sudah bagus. Berikut ini adalah uraian dari tingkat kematangan kelima area yang telah dinilai.

Tabel 4.11 Tingkat Kematangan Kelima Area

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Aspek Teknologi
Tingkat II					
Status	II	II	II	II	II
Tingkat III					
Validitas	Yes	Yes	Yes	Yes	Yes
Status	III	III	III	III	III
Tingkat IV					
Validitas	Yes	Yes	Yes	No	Yes
Status	IV	IV	IV	No	III+
Tingkat V					
Validitas	No	Yes	Yes	No	No
Status	No	V	V	No	No
Status Akhir	**IV**	**V**	**V**	**III**	**III+**

Berikut ini adalah gambar urutan tingkat kematangan dari yang terendah hingga yang tertinggi.



Gambar 4.8 Tingkat Kematangan Indeks KAMI

Dalam gambar diatas, tingkat kematangan terendah adalah I, sedangkan paling tinggi adalah V. Dan batasan minimal yang harus dicapai agar dapat melakukan sertifikasi ISO adalah III. Saat ini Telkom sudah melakukan sertifikasi pada beberapa kantor di daerah tertentu, dan adalah salah satunya.

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 tabel pemetaan dari pertanyaan evaluasi, hasil evaluasi, dan saran perbaikan yang direkomendasikan:

Tabel 4.12 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 C buku tugas akhir ini.

Tabel 4.13 Saran Perbaikan 2

Nomor	Pertanyaan	Jawaban	Nilai
5.18	Proses pengecekan latar belakang SDM	Dalam Penerapan / Diterapkan Sebagian	4
Saran Perbaikan: Proses pemeriksaan latar belakang setiap sumber daya manusia yang bekerja dalam divisi sudah diberlakukan. Namun dari hasil pengamatan lapangan telah diketahui beberapa staff yang bekerja belum pernah merasakan atau menjalani proses pemeriksaan latar belakang. Dan telah diketahui pula bahwa hal ini disebabkan karena kebijakan dan prosedur mengenai pemeriksaan latar belakang baru mulai diberlakukan ketika sertifikasi ISO pada tahun 2012			

Tabel 4.14 Saran Perbaikan 3

Nomor	Pertanyaan	Jawaban	Nilai
6.13	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan	Dalam Penerapan / Diterapkan Sebagian	4

	penggunaan kembali *password* lama?		
Saran Perbaikan: Pengaturan password dalam sistem masih sebatas peringatan dan pemberitahuan. Dalam pelaksanaannya masih bergantung pada setiap individu yang menggunakan sistem. Untuk itu, sama seperti saran rekomendasi pada nomor 5.11, perlu dibuatkan suatu dokumen kebijakan tentang akun dan kata sandi.			

Tabel 4.15 Saran Perbaikan 4

Nomor	Pertanyaan	Jawaban	Nilai
6.18	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
Saran Perbaikan: Sebagian besar perangkat yang terdapat dalam divisi belum dimutakhirkan dengan versi terbaru saat ini. Dari hasil studi lapangan diketahui bahwa perangkat *desktop* yang terdapat dalam kantor divisi masih belum menggunakan sistem operasi terbaru saat ini, yaitu *Windows 8.1*. Hal ini disebabkan karena sistem operasi yang saat ini digunakan sudah memadai dan dapat mengatasi seluruh kebutuhan operasional divisi saat ini. Namun karena semakin berkembangnya arus informasi, akan menyebabkan meningkatnya kerentanan dari sistem operasi tersebut, sehingga akan lebih baik jika sistem operasi diperbarui untuk meningkatkan efektifitas keamanan informasi serta meningkatkan kinerja dari sistem tersebut.			

BAB V
KESIMPULAN DAN SARAN

Bab ini adalah bab yang berisi kesimpulan dari penelitian tugas akhir ini dan juga berisi saran dalam hal keamanan informasi untuk divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk.

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

Amsyah, Z. (2005). *Manajemen Sistem Informasi.* Jakarta: PT Gramedia Pustaka.

Calder, A. (2005). *IT Governance: Guidlines for Directors.* Ely: IT Governance Publishing.

Calder, A. (2009). *Information Secutiry Based on ISO 27001/ISO 27002: A Management Guide.* Zaltbommel: Van Haren Publishing.

Crockford, N. (1986). *An Introduction to Risk Management (2nd Edition).* Cambridge: Woodhead-Faulkner.

Dorfman, M. (2007). *Introduction to Risk Management and Insurance (9th Edition).* Prentice Hall: Englewood Cliffs.

Enderlein, H., Walti, S., & Zurn, M. (2010). *Handbook on Multi-level Governance.* Cheltenham: Edward Elgar Publishing Limited.

Floridi, L. (2005). *Philosophy and Phenomenological Research.* Oxford: Oxford University.

Gaol, C. J. (2008). *Sistem Informasi Manajemen.* PT Grasindo.

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

Hopkin, P. (2012). *Fundamentals of Risk Management.* London: Kogan Page Limited.

ISO/IEC 2009. (2009, 05 01). International Standard ISO/IEC 27000. Switzerland: ISO/IEC.

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

Maryono, Y., & Patmi, B. I. (2008). *Teknologi Informasi & Komunikasi.* Yudhistira.

Mauritus, R. o. (n.d.). *ISO 27001 Controls and Objectives*. Retrieved Februari 25, 2014, from Republic of Mauritus: http://gender.gov.mu/English/Documents/activities/gender%20infsys/AnnexIX1302.pdf

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

Sadgrove, K. (2005). *The Complete Guide to Business Risk Management.* Burlington: Gower Publishing.

Weill, P. &. (2004). *IT Governance, How Top Performers Manage IT Decision Rights for Superior Results.* Boston: Harvard Business School Press.

Whitman, M. E., & Mattord, H. J. (2013). *Management of Information Security.* Boston: Course Technology.

BIODATA PENULIS

Penulis dilahirkan di Surabaya pada tanggal 14 Mei 1992, merupakan anak ketiga dari tiga bersaudara. Penulis menempuh pendidikan formal di SD Al-Hikmah Surabaya, kemudian dilanjutkan di SMP Al-Hikmah Surabaya, dan dilanjutkan di SMA Muhammadiyah 2 Surabaya. Pada tahun 2010 penulis diterima sebagai mahasiswa di Jurusan Sistem Informasi Fakultas Teknologi Informasi Institut Teknologi Sepuluh Nopember Surabaya (ITS) dengan NRP 5210100079.

Selama menempuh masa perkuliahan, penulis aktif dalam kegiatan jurusan, maupun luar jurusan, seperti pengisi acara *Information System Expo* (ISE) tahun 2010 hingga 2013, pengisi acara Seminar Sistem Informasi Nasional Indonesia (SESINDO) 2010-2012, pengisi acara *Information Systems International Conference* (ISICO) 2011, pengisi acara *ITS Expo* 2010-2014, menjadi *vendor* dalam acara TEDx ITS 2012, dan lain sebagainya. Selain itu penulis juga mengikuti beberapa pelatihan seperti pelatihan implementasi SAP, bimbingan teknis Kominfo (2014), dan lain-lain. Saat ini penulis sedang mengelola perusahaan Dewi Music Studio, penyedia jasa studio dan sound system di Surabaya

LAMPIRAN A

LAMPIRAN A

Berikut ini adalah lampiran dari penilaian kelima area dalam indeks KAMI:

A.1. Hasil Penilaian Bagian Tata Kelola

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.					
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai	Diterapkan Secara Menyeluruh	3

			tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?		
Alasan: Ada, sudah diatur sesuai dengan dokumen kebijakan dalam lampiran D.3 poin 1. Diatur oleh IT *Strategy & Governance* (ITSG) dan divisi IT *Service & Solution* (ITSS).					
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah diberikan wewenang sesuai dengan kebijakan pusat pada lampiran D.3 poin 1.					
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah diberikan anggaran dasar sesuai dengan Berita Negara RI Nomor 5 tanggal 18 Januari 2005 Tambahan Berita Negara RI					

Nomor 569.					
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah diatur oleh direktorat IT *Strategy & Governance* (ITSG) dan divisi IT *Service & Solution* (ITSS).					
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah diatur oleh direktorat IT *Strategy & Governance* (ITSG) dan divisi IT *Service & Solution* (ITSS).					
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Diterapkan Secara Menyeluruh	3

Alasan: Sudah diatur oleh direktorat IT *Strategy & Governance* (ITSG) dan divisi IT *Service & Solution* (ITSS).					
2.8	II	1	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Diterapkan Secara Menyeluruh	3
Alasan: Ada dan disampaikan melalui surat elektronik masing-masing staff					
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah diatur oleh direktorat IT *Strategy & Governance* (ITSG) dan divisi IT *Service & Solution* (ITSS).					
2.10	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal	Diterapkan Secara Menyeluruh	6

			maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?		
Alasan: Sudah disesuaikan dengan poin-poin yang ada dalam ISO dan disesuaikan dengan kebijakan pusat.					
2.11	II	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?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah disesuaikan dengan poin-poin yang ada dalam ISO dan disesuaikan dengan kebijakan pusat.					
2.12	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah	Diterapkan Secara Menyeluruh	6

			kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?		
Alasan: Sudah termasuk dalam lingkup yang diatur oleh direktorat IT *Strategy & Governance* (ITSG).					
2.13	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah dilakukan sebagai bahan evaluasi atas kondisi keamanan informasi, struktur tim pelaksana dilampirkan dalam dokumen kebijakan dalam lampiran D.3 poin 1.					
2.14	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah dilakukan sebagai bahan evaluasi atas kondisi keamanan					

informasi.					
2.15	IV	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 tanggung jawabnya?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah terdapat program tahunan untuk keamanan informasi, seperti pelatihan, bimbingan teknis, dan sejenisnya.					
2.16	IV	3	Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah terdapat parameter tertentu dalam pengelolaan kinerja keamanan informasi. Batasan nilai ditentukan berdasarkan standar ISO dan COBIT.					
2.17	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas)	Diterapkan Secara Menyeluruh	9

			pelaksananya?		
Alasan: Program penilaian dilakukan secara berkala dengan standar COBIT.					
2.18	IV	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?	Diterapkan Secara Menyeluruh	9
Alasan: Proses evaluasi sudah dilakukan secara berkala dengan menggunakan standar COBIT.					
2.19	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah diidentifikasikan di dalam kebijakan pusat yang diatur oleh direktorat IT *Strategy & Governance* (ITSG).					
2.20	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah	Diterapkan Secara Menyeluruh	9

			penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?		
Alasan: Sudah didefinisikan di dalam kebijakan pusat yang diatur oleh direktorat IT *Strategy & Governance* (ITSG).					
Total Nilai Evaluasi Tata Kelola				**114**	

A.2. Hasil Penilaian Bagian Pengelolaan Risiko

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**	
#	**Kajian Risiko Keamanan Informasi**				
No			**Pertanyaan**	**Status**	**Skor**
3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah terdapat dan sudah disesuaikan dengan standar ISO dan					

COBIT.					
3.2	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada dan dikelola oleh direktorat IT *Strategy & Governance* (ITSG).					
3.3	II	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?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah disesuaikan dengan standar ISO dan COBIT.					
3.4	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah disesuaikan dengan standar ISO dan COBIT.					

3.5	II	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
Alasan: Sudah dikelola secara keseluruhan oleh bagian *General Support* unit.					
3.6	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah disesuaikan dengan standar ISO dan COBIT.					
3.7	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terangguny a fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah disesuaikan dengan standar ISO dan COBIT.					

3.8	II	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)?	Diterapkan Secara Menyeluruh	3
Alasan: Evaluasi terhadap risiko dan kinerja keamanan informasi sudah dilakukan secara berkala dengan menggunakan standar COBIT.					
3.9	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Diterapkan Secara Menyeluruh	3
Alasan: Mitigasi risiko dilakukan setelah melakukan analisa risiko yang telah dilakukan sebelumnya dengan standar COBIT.					
3.10	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan	Diterapkan Secara Menyeluruh	6

			tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?		
Alasan: Alokasi dana untuk keamanan informasi termasuk risikonya sudah disesuaikan berdasarkan Anggaran Dasar Perusahaan yang telah diumumkan dalam Berita Negara RI Nomor 5 tanggal 18 Januari 2005.					
3.11	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Diterapkan Secara Menyeluruh	6
Alasan: Dipantau dan diuji secara berkala dengan menggunakan COBIT.					
3.12	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?	Diterapkan Secara Menyeluruh	6
Alasan: Hasil mitigasi risiko yang telah dilakukan dipantau secara berkala untuk memastikan efektifitasnya.					
3.13	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara	Diterapkan Secara Menyeluruh	6

			berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?		
Alasan: Dipantau dan diuji secara berkala dengan menggunakan COBIT.					
3.14	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Diterapkan Secara Menyeluruh	9
Alasan: Dipantau dan diuji secara berkala dengan menggunakan COBIT.					
3.15	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Diterapkan Secara Menyeluruh	9
Alasan: Pengelolaan risiko termasuk dalam penilaian kinerja keamanan informasi sesuai dengan standar ISO.					
Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi				**69**	

A.3. Hasil Penilaian Bagian Kerangka Kerja

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	**Skor**
#	**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**				
No			**Pertanyaan**	**Status**	**Skor**
4.1	II	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?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada kebijakan yang secara khusus memiliki lingkup SMKI dan dikelola oleh *Regulatory Management Unit* (RMU), salah satu contohnya ada pada lampiran D.3 poin 1 dan 2.					
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan	Diterapkan Secara Menyeluruh	3

			dengan mudah diakses oleh pihak yang membutuhkannya?		
Alasan: Sudah dipublikasikan kepada seluruh pihak oleh *Regulatory Management Unit* (RMU).					
4.3	II	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
Alasan: Seluruh dokumen sudah dikelola dan didistribusikan oleh *Regulatory Management Unit* (RMU) kepada seluruh pihak yang terkait.					
4.4	II	1	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Diterapkan Secara Menyeluruh	3
Alasan: Seluruh dokumen sudah dikelola dan didistribusikan oleh *Regulatory Management Unit* (RMU) kepada seluruh pihak yang terkait termasuk bila terjadi perubahan.					

4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Seluruh hasil penilaian risiko membutuhkan dokumen terkait manajemen risiko untuk membuat mitigasinya.					
4.6	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah mencakup pelaporan insiden, kerahasiaan, dan hal lainnya yang disebutkan dalam ISO.					
4.7	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Diterapkan Secara Menyeluruh	6
Alasan: Segala peraturan dan pelanggaran disampaikan melalui surat elektronik masing-masing staff.					

4.8	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	Diterapkan Secara Menyeluruh	6
Alasan: Penerapan keamanan informasi beserta hal-hal lain yang berkaitan sudah disesuaikan dengan standar ISO.					
4.9	III	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?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah dilakukan oleh bagian *Innovation & Design Center* (IDeC).					
4.10	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi	Diterapkan Secara Menyeluruh	6

			permasalahan yang muncul?		
Alasan: Seluruh pengujian terhadap sistem baru sudah dilakukan oleh bagian *Innovation & Design Center* (IDeC).					
4.11	III	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?	Diterapkan Secara Menyeluruh	6
Alasan: Seluruh pengujian terhadap sistem baru sudah dilakukan oleh bagian *Innovation & Design Center* (IDeC).					
4.12	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Diterapkan Secara Menyeluruh	6

Alasan: Kerangka kerja pengelolaan kelangsungan layanan TIK sudah dibuat oleh direktorat IT *Strategy & Governance* (ITSG).					
4.13	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah dibuat dan sudah ada bagian yang bertanggung jawab untuk menangani risiko keamanan informasi, yaitu departemen *Compliance Risk Management* (CRM)					
4.14	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Diterapkan Secara Menyeluruh	9
Alasan: Pengujian dilakukan secara berkala pada divisi.					
4.15	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang	Diterapkan Secara Menyeluruh	9

			diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?		
Alasan: Hasil dari pengujian dievaluasi secara berkala oleh namanya departemen *Compliance Risk Management* (CRM).					
4.16	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Diterapkan Secara Menyeluruh	9
Alasan: Seluruh kebijakan dikelola dan dievaluasi kelayakannya oleh direktorat IT *Strategy & Governance* (ITSG).					
#	**Pengelolaan Strategi dan Program Keamanan Informasi**				
4.17	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Diterapkan Secara Menyeluruh	3
Alasan: Seluruh prosedur yang berkaitan dengan risiko sudah dibuat dan dijalankan sesuai dengan kebijakan dari *Compliance Risk Management* (CRM)					

4.18	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Diterapkan Secara Menyeluruh	3
Alasan: Seluruh prosedur yang berkaitan dengan risiko sudah dibuat dan dijalankan sesuai dengan kebijakan dari *Compliance Risk Management* (CRM)					
4.19	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Diterapkan Secara Menyeluruh	3
Alasan: Keamanan informasi merupakan salah satu aspek utama dalam menjalankan bisnis operasional sehari-hari divisi.					
4.20	III	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	Diterapkan Secara Menyeluruh	3

			(atau sesuai dengan standar yang berlaku)?		
Alasan: Audit sudah dilakukan secara rutin dan sesuai dengan standar COBIT dan ISO 27001.					
4.21	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Audit yang dilakukan sudah mencakup seluruh aspek yang ada dalam ISO, contoh hasil audit terdapat dalam lampiran D.3 poin 3					
4.22	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Diterapkan Secara Menyeluruh	6
Alasan: Hasil audit digunakan sebagai langkah pembenahan agar sesuai dengan standar ISO 27001.					
4.23	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan	Diterapkan Secara Menyeluruh	6

			informasi?		
Alasan: Hasil audit disampaikan kepada pimpinan selaku penanggung jawab penerapan SMKI.					
4.24	IV	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	9
Alasan: Segala perbaikan disesuaikan dengan Anggaran Dasar Perusahaan sesuai dengan Berita Negara RI Nomor 5 tanggal 18 Januari 2005.					
4.25	V	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	Diterapkan Secara Menyeluruh	9

			efektif?		
Alasan: Pengujian sudah dilakukan secara periodik dengan menggunakan standar COBIT.					
4.26	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Diterapkan Secara Menyeluruh	9
Alasan: Program peningkatan dilakukan setiap tahun seperti pelatihan, bimbingan, dan lain-lain. Untuk program strategis direncanakan oleh direktorat IT *Strategy & Governance* (ITSG).					
Total Nilai Evaluasi Kerangka Kerja				**144**	

A.4. Hasil Penilaian Bagian Pengelolaan Aset

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**	Skor

#	Pengelolaan Aset Informasi				
No			**Pertanyaan**	**Status**	**Skor**
5.1	II	1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	Diterapkan Secara Menyeluruh	3
Alasan: Inventaris dikelola oleh unit *General Support* masing-masing divisi.					
5.2	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Diterapkan Secara Menyeluruh	3
Alasan: Evaluasi terhadap keamanan suatu perangkat dilakukan oleh *Innovation & Design Center* (IDeC).					
5.3	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut	Diterapkan Secara Menyeluruh	3
Alasan: Pengaturan akses aset informasi diatur oleh *Regulatory Management Unit* (RMU).					
5.4	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang	Diterapkan Secara Menyeluruh	3

			diterapkan secara konsisten?		
Alasan: Segala perubahan dikelola secara teratur untuk menghindari risiko baru.					
5.5	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
Alasan: Segala perubahan dikelola secara teratur untuk menghindari risiko baru.					
5.6	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Diterapkan Secara Menyeluruh	3
Alasan: Segala proses pembaharuan aset dan perangkat baru dilakukan dan diuji oleh oleh *Innovation & Design Center* (IDeC).					
			Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		
5.7	II	1	Definisi tanggungjawab pengamanan informasi secara individual	Diterapkan Secara Menyeluruh	3

			untuk semua personil di Instansi anda		
Alasan: Sudah terdapat dokumen terkait dan didistribusikan oleh *Regulatory Management Unit* (RMU) pada setiap staff.					
5.8	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Diterapkan Secara Menyeluruh	3
Alasan: Tata tertib dasar sudah diberlakukan untuk setiap staff.					
5.9	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Diterapkan Secara Menyeluruh	3
Alasan: Tata tertib tersebut sudah dibuat berdasarkan SMKI.					
5.10	II	1	Peraturan pengamanan data pribadi	Diterapkan Secara Menyeluruh	3
Alasan: Tata tertib sudah dibuat berdasarkan SMKI.					
5.11	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Dalam Penerapan / Diterapkan Sebagian	2
Alasan: Kebijakan tentang akun sudah dibuat, namun yang secara spesifik mengatur password belum ada.					
5.12	II	1	Persyaratan dan prosedur pengelolaan/pemberia	Diterapkan Secara Menyeluruh	3

			n akses, otentikasi dan otorisasi untuk menggunakan aset informasi		
Alasan: Pemberian hak akses aset informasi dikelola oleh *Regulatory Management Unit* (RMU).					
5.13	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Diterapkan Secara Menyeluruh	3
Alasan: *Regulatory Management Unit* (RMU) mengelola aset informasi juga bertanggung jawab dalam hal penghancuran data.					
5.14	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Diterapkan Secara Menyeluruh	3
Alasan: Proses pertukaran data sudah diatur dalam kebijakan SMKI.					
5.15	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Diterapkan Secara Menyeluruh	3
Alasan: Proses penyelidikan dilakukan secara langsung ketika terjadi permasalahan.					
5.16	II	1	Prosedur *back-up* ujicoba pengembalian data (*restore*)	Diterapkan Secara Menyeluruh	3
Alasan: Prosedur *back-up* dan pengembalian dilakukan oleh *General*					

Support masing-masing divisi.					
5.17	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Diterapkan Secara Menyeluruh	6
Alasan: Pengamanan fisik sudah dilakukan dengan menyeluruh pada kantor divisi.					
5.18	III	2	Proses pengecekan latar belakang SDM	Dalam Penerapan / Diterapkan Sebagian	4
Alasan: Proses pengecekan latar belakang SDM sudah dilakukan, namun hanya pada beberapa aspek saja.					
5.19	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Diterapkan Secara Menyeluruh	6
Alasan: Proses penyelidikan dilakukan secara langsung ketika terjadi permasalahan.					
5.20	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Diterapkan Secara Menyeluruh	6
Alasan: *Regulatory Management Unit* (RMU) mengelola aset informasi juga bertanggung jawab dalam hal penghancuran data. Selain itu *General Support* divisi juga bertanggung jawab atas aset fisik divisi.					

5.21	III	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
Alasan: Prosedur tersebut sudah dibuat berdasarkan SMKI.					
5.22	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Diterapkan Secara Menyeluruh	9
Alasan: Untuk pengelolaan aset informasi beserta prosedur *backup* nya dilakukan oleh *General Support* masing-masing divisi untuk data local.					
5.23	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Diterapkan Secara Menyeluruh	9
Alasan: Sudah terdapat rekaman (*log*) yang merekam aktifitas pengguna. Contoh dari *log* ditampilkan pada lampiran D.3 poin 5.					
5.24	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah	Diterapkan Secara Menyeluruh	9

			informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?		
Alasan: Prosedur sudah dibuat berdasarkan SMKI.					
#			**Pengamanan Fisik**		
5.25	II	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?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada penjagaan secara fisik pada lokasi-lokasi sensitif perusahaan dan divisi.					
5.26	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada penjagaan secara fisik pada lokasi-lokasi sensitif perusahaan dan divisi.					

5.27	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Diterapkan Secara Menyeluruh	3
Alasan: Bangunan sudah disesuaikan dengan standar ISO.					
5.28	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh	3
Alasan: Letak perangkat infrastruktur sudah disesuaikan dengan standar ISO.					
5.29	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada dan dikelola oleh *General Support* divisi.					
5.30	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan	Diterapkan Secara Menyeluruh	6

			rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?		
Alasan: Bangunan sudah disesuaikan dengan standar ISO.					
5.31	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Diterapkan Secara Menyeluruh	6
Alasan: Ada dan dilakukan oleh *General Support* unit					
5.32	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak	Diterapkan Secara Menyeluruh	6

			ketiga?		
Alasan: Ada dan dilakukan oleh *General Support* unit					
5.33	II	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)	Diterapkan Secara Menyeluruh	6
Alasan: Sudah ada peraturan yang dibuat berdasarkan standar ISO.					
5.34	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Diterapkan Secara Menyeluruh	9
Alasan: Proses untuk mengamankan lokasi kerja ketika terdapat pihak ketiga sudah dibuat dengan standar ISO.					

Total Nilai Evaluasi Pengelolaan Aset	**150**	

A.5. Hasil Penilaian Bagian Teknologi

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**				
No			**Pertanyaan**	**Status**	**Skor**
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah ada pengamanan secara logikal yang diterapkan dalam sistem. Dikembangkan oleh *Innovation & Design Center* (IDeC)					
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3

Alasan: Jaringan sudah dipisahkan berdasarkan kebutuhan dan letak dari akses poinnya.					
6.3	II	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
Alasan: Sudah ada konfigurasi standar dan disesuaikan dengan kebutuhan bisnis.					
6.4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Diterapkan Secara Menyeluruh	3
Alasan: Secara rutin kesesuaian konfigurasi dipantau untuk memastikan kesesuaian dengan kebutuhan bisnis divisi.					
6.5	II	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

Alasan: Sudah dilakukan secara rutin dengan cara memberikan instruksi pada pihak eksternal untuk mencoba menerobos pengamanan akses jaringan divisi.					
6.6	II	1	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh	3
Alasan: Pengawasan dilakukan secara rutin untuk memastikan kapasitas yang tersedia.					
6.7	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
Alasan: Sudah terdapat *log* yang merekam aktifitas dalam sistem, *log* dilampirkan dalam lampiran D.3 poin 5.					
6.8	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
Alasan: Ada *log* merekam aktifitas illegal dalam jaringan, dan selalu dipantau.					
6.9	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan	Diterapkan Secara Menyeluruh	3

			forensik)?		
Alasan: Seluruh aktifitas sudah direkam di dalam sistem untuk ditinjau dan diawasi.					
6.10	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Diterapkan Secara Menyeluruh	3
Alasan: Sistem sudah menerapkan enkripsi untuk meningkatkan keamanan akses jaringan.					
6.11	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Diterapkan Secara Menyeluruh	6
Alasan: Standar enkripsi adalah standar internasional yang berlaku saat ini sesuai dengan ISO.					
6.12	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Diterapkan Secara Menyeluruh	6
Alasan: Pengelolaan enkripsi dilakukan oleh bagian yang melakukan implementasi sistem, yaitu *Innovation & Design Center* (IDeC).					

6.13	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Dalam Penerapan / Diterapkan Sebagian	4
Alasan: Sistem sudah terdapat standar dasar pembuatan password, namun belum ada peraturan tertulis yang mengatur setiap pengguna dalam pengelolaan password akun mereka.					
6.14	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Diterapkan Secara Menyeluruh	6
Alasan: Sudah diberikan pengamanan lebih dari satu.					
6.15	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan	Diterapkan Secara Menyeluruh	6

			login,dan penarikan akses?		
Alasan: Sistem sudah menerapkan keamanan seperti disebutkan sesuai dengan standar ISO 27001.					
6.16	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Diterapkan Secara Menyeluruh	6
Alasan: Segala aktifitas jaringan dipantau, sehingga dapat mengetahui akses illegal.					
6.17	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Diterapkan Secara Menyeluruh	3
Alasan: Pengamanan dilakukan berupa enkripsi dan pengamanan lain yang sesuai dengan ISO 27001.					
6.18	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
Alasan: Beberapa perangkat sudah dimutakhirkan, namun masih banyak perangkat lain yang belum diperbaharui sistem operasinya.					
6.19	II	1	Apakah setiap *desktop* dan *server* dilindungi	Diterapkan Secara	3

			dari penyerangan virus (*malware*)?	Menyeluruh	
Alasan: Antivirus sudah dijalankan dalam setiap perangkat untuk mencegah kerusakan data.					
6.20	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?	Diterapkan Secara Menyeluruh	6
Alasan: Untuk laporan atas perubahan perangkat sudah dilakukan oleh *General Support* unit divisi.					
6.21	III	2	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	Diterapkan Secara Menyeluruh	6
Alasan: Segala upaya perbaikan pada perangkat dilakukan oleh *General Support* unit divisi.					
6.22	III	2	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh	6

Alasan: Sudah disesuaikan dengan server pusat.					
6.23	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?	Diterapkan Secara Menyeluruh	6
Alasan: Seluruh perangkat diuji coba sebelum diimplementasikan oleh bagian *Innovation & Design Center* (IDeC).					
6.24	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Diterapkan Secara Menyeluruh	9
Alasan: Divisi memerintahkan pihak luar untuk mencoba menerobos keamanan jaringan untuk mengetahui celah keamanan jaringan.					
Total Nilai Evaluasi Teknologi dan Keamanan Informasi				**105**	

Halaman ini sengaja dikosongkan

LAMPIRAN B

LAMPIRAN B

Berikut ini adalah list pertanyaan yang digunakan untuk mengumpulkan data terkait keamanan informasi dalam indeks KAMI.

Tabel B.1 Hasil Wawancara

No	Pertanyaan	Korelasi Dengan Indeks KAMI
1	Berapakah rata-rata anggaran yang diberikan untuk bidang TIK dalam divisi ini?	1.1
Jawaban: Anggaran yang dialokasikan untuk TIK lebih dari Rp20 Miliar		
2	Apakah untuk menjalankan kegiatan operasional sehari-hari, setiap pegawai perlu menggunakan TIK? Berapa orang dari keseluruhan pegawai divisi yang menggunakan TIK?	1.2 1.3 1.6 1.8 1.11
Jawaban: Dalam menjalankan operasional sehari-hari seluruh staff menggunakan IT. Semua pegawai disini menggunakan IT, IT adalah sesuatu yang sangat penting dalam divisi ini.		
3	Apakah sistem yang terdapat dalam divisi ini hanya dapat digunakan dalam divisi ini saja?	1.4
Jawaban: Setiap divisi diberikan akses yang berbeda untuk mengakses sistem keseluruhan Telkom, sehingga divisi hanya dapat menjalankan tugas pokok saja dari sistem tersebut.		

4	Jika sistem gagal, apakah akan berdampak buruk dalam kegiatan operasional divisi?	1.5 1.7 1.10 1.12
Jawaban: Jika sistem gagal, maka kami tidak dapat melacak seluruh aktifitas jaringan Telkom		
5	Apakah proses kerja sistem pada divisi sudah memenuhi UU dan perangkat hukum lainnya?	1.9
Jawaban: Sudah diijalankan sesuai dengan peraturan kementerian		
6	Apakah pimpinan divisi bertanggung jawab secara penuh atas keamanan informasi?	2.1
Jawaban: Pimpinan termasuk dalam penanggung jawab keamanan informasi dalam kebijakan dari pusat.		
7	Apakah dalam divisi ini terdapat fungsi atau pelaksana yang memiliki kompetensi untuk bertanggung jawab secara spesifik atas keamanan informasi dan diberikan alokasi sumber daya yang sesuai untuk mengelola keamanan informasi?	2.2 2.3 2.4 2.5 2.6 2.7 2.9
Jawaban: Ada, diatur dari pusat, direktorat IT *Strategy & Governance* (ITSG) dan divisi IT *Service & Solution* (ITSS). Diberikan tanggung jawab dalam mengelola keamanan informasi.		
8	Apakah dalam divisi terdapat sosialisasi terkait keamanan informasi?	2.8
Jawaban: Ada, disampaikan melalui e-mail masing-masing staff		

9	Apakah tanggung jawab pengelola keamanan informasi sudah mencakup kordinasi dengan pihak pengguna aset informasi dari internal maupun eksternal?	2.10 2.11
Jawaban: Iya sudah disesuaikan dengan kebijakan dan ISO		
10	Apakah tanggung jawab pengelola keamanan informasi sudah mencakup *business continuity* dan *disaster recovery plan*?	2.12
Jawaban: Iya sudah masuk ke dalam lingkupnya.		
11	Apakah pengelola keamanan informasi melaporkan kondisi secara rutin dan laporan tersebut digunakan sebagai bahan pertimbangan pengambilan keputusan?	2.13 2.14
Jawaban: Iya dan digunakan untuk evaluasi kondisi keamanan informasi tersebut		
12	Apakah pimpinan divisi menerapkan program khusus untuk memenuhi kepatuhan keamanan informasi?	2.15
Jawaban: Iya ada program setiap tahun untuk meningkatkan keamanan informasi, seperti pelatihan, bimbingan teknis, dan sejenisnya.		
13	Apakah divisi sudah mendefinisikan batasan dan mekanisme pengukuran kinerja keamanan informasi dan penerapannya berikut target hasilnya?	2.16 2.17 2.18
Jawaban: Semua disesuaikan dengan ISO dan COBIT		
14	Apakah divisi sudah mendefinisikan	2.19

	perangkat hukum yang terkait dan memiliki kebijakan untuk menanggulangi insiden keamanan informasi?	2.20
Jawaban: Sudah didefinisikan dalam kebijakan SMKI		
15	Apakah divisi memiliki program dan kerangka kerja yang mencakup definisi serta klasifikasi tingkat risiko keamanan informasi beserta ambang batasnya?	3.1 3.2 3.3 3.4 3.6 3.7
Jawaban: Sudah sesuai dengan ISO dan COBIT		
16	Apakah divisi sudah mendefinisikan kepemilikan aset informasi yang ada?	3.5
Jawaban: Sudah dikelola secara keseluruhan oleh bagian *General Support* unit		
17	Apakah divisi sudah membuat analisa risiko keamanan informasi yang terstruktur beserta langkah mitigasi yang disusun sesuai tingkatan prioritasnya dan dipantau secara berkala?	3.8 3.9 3.10 3.11 3.12 3.13
Jawaban: Sudah ada dan sudah sesuai dengan ISO		
18	Apakah kerangka kerja pengelolaan risiko dikaji secara berkala?	3.14
Jawaban: Pengujian pemulihan risiko diuji secara berkala		
19	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian kinerja efektifitas pengamanan?	3.15
Jawaban:		

Iya, semua disesuaikan dengan ISO		
20	Apakah dalam divisi sudah terdapat kebijakan dan prosedur yang telah disusun dengan jelas serta dipublikasikan dan dikelola dengan baik?	4.1 4.2 4.3 4.4 4.16
Jawaban: Sudah ada kebijakan yang secara khusus memiliki lingkup SMKI dan dikelola oleh *Regulatory Management Unit* (RMU)		
21	Apakah kebijakan dan prosedur tersebut disusun dari kebutuhan mitigasi hasil kajian risiko?	4.5
Jawaban: Iya risiko merupakan salah satu kajian dalam kebijakan tersebut		
22	Apakah kebijakan tersebut sudah mencakup masalah pelaporan insiden serta konsekuensi pelanggaran yang terjadi berikut pengecualiannya?	4.6 4.7 4.8
Jawaban: Sudah mencakup semua itu, disesuaikan dengan ISO		
23	Apakah divisi sudah menerapkan kebijakan terkait implementasi sistem baru atau *patch* beserta evaluasi risiko yang muncul?	4.9 4.10 4.11
Jawaban: Sudah dilakukan oleh bagian *Innovation & Design Center* (IDeC)		
24	Apakah dalam divisi terdapat kebijakan mengenai kelangsungan layanan TIK (*business continuity planning*) dan dijadwalkan uji cobanya?	4.12
Jawaban:		

Sudah ada dan diuji secara berkala		
25	Apakah *disaster recovery plan* sudah mencakup wewenang dan tanggung jawab tim yang ditunjuk beserta jadwal pengujian untuk mengetahui kekurangan yang ada dalam perencanaan tersebut?	4.13 4.14 4.15
Jawaban: Sudah dibuat dan sudah ada bagian yang bertanggung jawab untuk menangani risiko keamanan informasi, namanya departemen *Compliance Risk Management* (CRM)		
26	Apakah divisi memiliki langkah penerapan dan penggunaan teknologi keamanan informasi sesuai dengan hasil analisa risiko dan diterapkan menjadi bagian dari program kerja divisi?	4.17 4.18 4.19
Jawaban: Seluruh prosedur sudah dibuat dan dijalankan sesuai dengan kebijakan dari *Compliance Risk Management* (CRM)		
27	Apakah divisi melakukan audit internal yang dilakukan oleh pihak luar dengan cakupan seluruh aspek keamanan informasi dan melaporkan hasil audit tersebut kepada pimpinan agar dilakukan perbaikan terhadap temuan dalam audit tersebut?	4.20 4.21 4.22 4.23
Jawaban: Audit sudah dilakukan secara rutin dan sesuai dengan standar COBIT		
28	Apakah sisi finansial ikut dipertimbangkan ketika melakukan perubahan atas kebijakan dan	4.24

	prosedur yang telah berlaku?	
Jawaban: Iya dan disesuaikan dengan anggarannya		
29	Apakah divisi melakukan pengujian terhadap kepatuhan keamanan informasi secara periodik?	4.25
Jawaban: Iya dilakukan sesuai dengan standar COBIT		
30	Apakah divisi memiliki program untuk meningkatkan keamanan informasi?	4.26
Jawaban: Iya dengan melakukan pelatihan-pelatihan, bimbingan teknis, dan sejenisnya		
31	Apakah tersedia daftar inventaris aset informasi yang telah diklasifikasi dan terdefinisi tingkatan akses aset tersebut?	5.1 5.2 5.3
Jawaban: Sudah dikelola oleh bagian *General Support* unit		
32	Apakah terdapat proses yang mengatur perubahan terhadap sistem beserta *update* isi dari inventaris jika terdapat aset baru?	5.4 5.5 5.6
Jawaban: Iya sudah disesuaikan jika terdapat perubahan		
33	Apakah divisi telah memberikan tanggung jawab pengamanan informasi secara individual untuk seluruh staff?	5.7
Jawaban: Penyuluhan untuk meningkatkan kesadaran keamanan informasi sudah disampaikan secara rutin melalui email staff		
34	Apakah dalam divisi terdapat	5.8

	peraturan tata tertib penggunaan komputer beserta isinya termasuk aset informasi (baik pihak internal maupun eksternal)?	5.9 5.10 5.11 5.12 5.13 5.14 5.21 5.24
Jawaban: Sudah dibuat sesuai dengan kebijakan SMKI		
35	Apakah dalam divisi menerapkan investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi?	5.15 5.19
Jawaban: Jika terjadi masalah dalam keamanan informasi, kami langsung mencari sumber masalah dan solusinya		
36	Apakah dalam divisi terdapat prosedur *back-up* data berikut penghancuran data yang tidak diperlukan?	5.16 5.20 5.22
Jawaban: Sudah ada dan dilakukan oleh *General Support* unit		
37	Apakah divisi memiliki peraturan keamanan fisik yang telah mendefinisikan zona dan klasifikasi aset yang ada?	5.17 5.25 5.26
Jawaban: Sudah ada, sebagai contohnya adalah anda menggunakan kartu tamu untuk masuk ke kantor ini.		
38	Apakah divisi melakukan pengecekan latar belakang SDM-nya?	5.18
Jawaban: Iya, dilakukan sesuai dengan ISO		
39	Apakah divisi merekam seluruh	5.23

	pelaksanaan keamanan informasi?	
Jawaban: Semua aktifitas sudah terekam di dalam sistem		
40	Apakah infrastruktur terlindungi dari dampak lingkungan seperti kebakaran, listrik dan suhu ruangan?	5.27 5.28 5.30
Jawaban: Bangunan sudah disesuaikan dengan standar ISO		
41	Apakah terdapat peraturan mengenai penggunaan infrastruktur diluar lingkungan kerja resmi termasuk dalam pengiriman?	5.29 5.32
Jawaban: Sudah ada, dan dilakukan oleh *General Support* unit		
42	Apakah terdapat proses inspeksi dan perawatan terhadap infrastruktur?	5.31
Jawaban: Ada dan dilakukan oleh *General Support* unit		
43	Apakah terdapat peraturan untuk mengamankan lokasi infrastruktur dari peralatan berbahaya termasuk kehadiran dari pihak luar?	5.33 5.34
Jawaban: Ada, disesuaikan dengan ISO		
44	Apakah sistem TIK yang menggunakan internet sudah dilindungi dengan lebih dari 1 pengamanan?	6.1
Jawaban: Sudah ada pengamanan secara logikal yang diterapkan dalam sistem. Dikembangkan oleh *Innovation & Design Center* (IDeC)		
45	Apakah jaringan komunikasi telah dipisahkan sesuai dengan kepentingannya?	6.2

Jawaban: Jaringan dipisahkan berdasarkan keperluan dan letaknya.		
46	Apakah tersedia konfigurasi standar yang secara rutin dievaluasi dan dimutakhirkan?	6.3 6.4
Jawaban: Ada, dan disesuaikan dengan perkembangan kebutuhan bisnis		
47	Apakah seluruh jaringan dan sistem di-*scan* untuk mengidentifikasi celah keamanan?	6.5
Jawaban: Sudah dilakukan secara rutin oleh pihak internal dan eksternal yang secara khusus diperintahkan untuk membobol sistem		
48	Apakah seluruh infrastruktur diawasi untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	6.6
Jawaban: Pengawasan dilakukan secara rutin		
49	Apakah setiap perubahan sistem direkam termasuk upaya akses illegal dan rekaman tersebut dianalisa secara berkala?	6.7 6.8 6.9
Jawaban: Seluruh aktifitas sudah direkam di dalam sistem untuk ditinjau dan diawasi		
50	Apakah sistem menerapkan enkripsi yang telah distandarkan termasuk pengelolaannya?	6.10 6.11 6.12
Iya dan sudah diterapkan dalam sistem		
51	Apakah sistem juga mengelola password termasuk pembagian	6.13 6.14

	pengguna dan ketentuan waktu pengguna?	6.15
Jawaban: Iya sesuai standar kebijakan SMKI		
52	Apakah divisi menerapkan pengamanan untuk mendeteksi penggunaan akses jaringan illegal?	6.16 6.17
Jawaban: Seluruh aktifitas termasuk akses sudah terekam otomatis ke dalam sistem		
53	Apakah sistem operasi komputer dan server selalu dimutakhirkan beserta pengamanan virusnya?	6.18 6.19
Jawaban: Iya, antivirus tersebut selalu diperbarui untuk menjaga keamanan informasi		
54	Apakah terdapat rekaman pemutakhiran sistem operasi beserta pengaman virus serta laporan penyerangan virus?	6.20 6.21
Jawaban: Iya, sudah dibuat oleh bagian *General Support* unit		
55	Apakah keseluruhan sistem sudah menggunakan mekanisme sinkronisasi waktu yang akurat dan sesuai standar yang ada?	6.22
Jawaban: Iya, sudah disesuaikan dengan server pusat		
56	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang telah divalidasi pada saat pengembangan dan uji coba?	6.23
Jawaban: Iya, setiap pengujian telah dilakukan sebelum diimplementasikan ke dalam keseluruhan divisi		

57	Apakah divisi melibatkan pihak ketiga untuk mengkaji keandalan keamanan informasi secara rutin?	6.24
Jawaban: Iya, digunakan untuk menguji celah keamanan informasi		

LAMPIRAN C

LAMPIRAN C

Berikut ini adalah lampiran dari dokumen kebijakan penggunaan akun dan kata sandi yang dibuat sebagai saran untuk meningkatkan tingkat kematangan salah satu poin dalam indeks KAMI.

Telkom Indonesia
the world in your hand

KEBIJAKAN DAN STANDAR PENGGUNAAN AKUN DAN KATA SANDI PENGGUNA DI LINGKUNGAN DIVISI NETWORK OF BROADBAND PT. TELEKOMUNIKASI INDONESIA TBK. BANDUNG

1. TUJUAN

Kebijakan dan standar ini bertujuan untuk mengatur penggunaan akun dan kata sandi pengguna sistem Teknologi Informasi dan Komunikasi (TIK) pada lingkungan Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Bandung.

2. RUANG LINGKUP

Kebijakan dan standar ini berlaku untuk seluruh pengguna akun dan kata sandi untuk mengakses sistem TIK pada lingkungan Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Bandung.

3. KEBIJAKAN

3.1. Pimpinan divisi bertanggung jawab dalam menerapkan kebijakan dan standar penggunaan akun dan kata sandi dalam lingkungan divisi.

3.2. Unit TIK divisi bertanggung jawab dalam menerapkan kebijakan dan standar penggunaan akun dan kata sandi pengguna dalam lingkungan divisi.

3.3. Pengguna bertanggung jawab terhadap akun dan kata sandi yang diberikan oleh Unit TIK dan wajib mematuhi standar penggunaan akun dan kata sandi pengguna yang telah diatur dalam lingkungan divisi.

3.4. Akun yang dimiliki pengguna akan dicabut secara otomatis oleh unit TIK apabila yang bersangkutan tidak lagi bekerja di Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Bandung.

4. STANDAR

4.1. Tanggung Jawab Pengguna:

4.1.1. Memakai kata sandi yang tidak mudah ditebak.

4.1.2. Mengubah kata sandi yang telah diberikan pada saat pertama kali digunakan sesuai dengan kriteria kata sandi.

4.1.3. Mengubah kata sandi secara berkala, paling lama dalam jangka waktu 30 (tiga puluh) hari. Jika kata sandi telah diketahui pihak lain atau jika diperintahkan oleh pimpinan dan unit TIK, maka segera lakukan perubahan.

4.1.4. Melindungi informasi dalam perangkat komputer masing-masing dengan cara menggunakan *screen saver* yang aktif setelah 5 (lima) menit tidak digunakan serta harus menggunakan kata sandi pada saat mengaktifkan kembali.

4.1.5. Mengaktifkan konfigurasi yang akan mematikan perangkat komputer setelah 30 (tiga puluh) menit tidak digunakan.

4.2. Larangan Pengguna:

4.2.1. Memberitahu atau membagikan kata sandi melalui media apapun kepada siapapun dengan cara apapun termasuk kepada orang yang mengaku berasal dari dukungan teknis, layanan pengguna, atau pejabat organisasi.

4.2.2. Membuat kata sandi sistem TIK dalam lingkup divisi Network of Broadband yang sama dengan kata sandi yang digunakan dalam akun di luar sistem TIK divisi Network of Broadband.

4.2.3. Menuliskan kata sandi dimanapun dan/atau menyimpan kata sandi pada berkas elektronik pada seluruh perangkat (termasuk *smartphone* dan sejenisnya) tanpa menggunakan metode enkripsi.

4.3. Kriteria Kata Sandi:

4.3.1. Terdiri dari minimal 6 (enam) karakter

4.3.2. Harus menggunakan kombinasi karakter:

a. Huruf besar dan huruf kecil
b. Angka dari 0 sampai 9
c. Karakter khusus, yaitu @ # $! & dan seterusnya

4.3.3. Bukan merupakan kata atau akronim dari nama diri atau kerabat, tanggal lahir, alamat, jabatan kerja, lokasi kerja, dan hal lain yang berhubungan dengan pribadi pemilik kata sandi

4.3.4. Tidak boleh sama dengan akun selain sistem TIK divisi baik seutuhnya atau sebagian.

5. SANKSI ATAS PELANGGARAN

Pelanggaran terhadap kebijakan dan standar ini dikenakan:

5.1. Peringatan yang dikirim melalui surat elektronik kepada pengguna yang melakukan pelanggaran.

5.2. Pencantuman nama pengguna yang melakukan pelanggaran dalam bagian kolom pelanggaran *website*/forum internal PT. Telekomunikasi Indonesia Tbk

5.3. Sanksi teknis berupa penonaktifan akun sampai dengan ada perintah resmi untuk mengaktifkan kembali.

6. ISTILAH YANG DIGUNAKAN

6.1. Akun adalah identifikasi pengguna yang diberikan oleh divisi, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan menggunakan sistem TIK.

6.2. Kata sandi adalah serangkaian kode yang dibuat pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan akun pengguna.

6.3. Pengguna adalah pegawai divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Bandung dan/atau pihak ketiga serta tidak terbatas pada pengelola TIK dan kelompok kerja yang diberikan hak untuk menggunakan sistem TIK pada lingkungan divisi Network of Broadband.

6.4. Pihak ketiga adalah semua unsur di luar lingkup PT. Telekomunikasi Indonesia Tbk. Bandung, missal mitra kerja (*vendor hardware*, *auditor*) dan lain sebagainya.

6.5. Sistem TIK adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/internet, dan lain sebagainya yang terdapat dalam lingkup PT. Telekomunikasi Indonesia Tbk. Bandung.

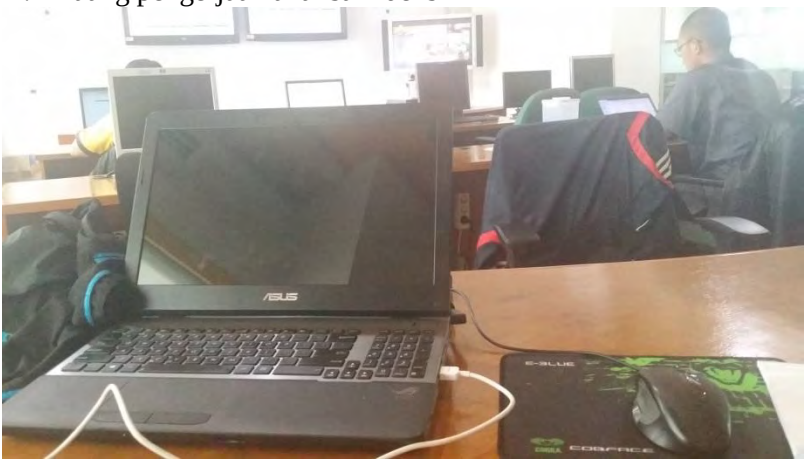
Halaman ini sengaja dikosongkan

LAMPIRAN D

LAMPIRAN D

Berikut ini adalah lampiran yang terdiri dari dokumentasi pendukung dalam melakukan evaluasi keamanan informasi dengan indeks KAMI.

D.1 Ruang pengerjaan analisa indeks KAMI



D.2 Dokumentasi bimbingan teknis indeks KAMI

D-2

D.3 Beberapa dokumen-dokumen yang berhubungan dengan keamanan informasi pada divisi Network of Broadband

1. Dokumen kebijakan sekuriti sistem informasi

TELKOM INDONESIA

KEPUTUSAN DIREKSI PERUSAHAAN PERSEROAN (PERSERO)
PT. TELEKOMUNIKASI INDONESIA, Tbk.
NOMOR : KD. 57/HK-290/ITS-30/2006

TENTANG

KEBIJAKAN SEKURITI SISTEM INFORMASI

DIREKSI PERUSAHAAN PERSEROAN (PERSERO)
PT. TELEKOMUNIKASI INDONESIA, Tbk.

Menimbang:

a. bahwa Teknologi Informasi/Sistem Informasi mempunyai peranan strategis dan menentukan dalam upaya Perusahaan melaksanakan misi dan mencapai sasaran-sasaran usaha yang telah ditetapkan;

b. bahwa informasi merupakan aset yang mempunyai nilai tinggi dan merupakan salah satu sumber daya yang penting dalam upaya pencapaian misi dan sasaran-sasaran perusahaan, serta untuk menunjang kemampuan bersaing PT Telekomunikasi Indonesia, Tbk. di bidang industri telekomunikasi;

c. bahwa sehubungan dengan hal dimaksud butir a. dan b. diatas, perlu kebijakan yang mengatur standar pengamanan untuk memberikan perlindungan terhadap aset informasi yang dimiliki oleh PT Telekomunikasi Indonesia, Tbk. yang dilaksanakan oleh setiap unit beserta seluruh jajarannya;

d. bahwa untuk melaksanakan Sekuriti Sistem Informasi yang baik dan optimal diperlukan penyempurnaan Kebijakan yang tertuang pada KD. 33/HK-270/IFO-00/2001, tanggal 16 November 2001, tentang Standarisasi Pengamanan Aset Informasi Perusahaan; dengan mempertimbangkan beberapa referensi, diantaranya : *ISO/IEC 17799:2005.*

e. bahwa untuk maksud tersebut di atas perlu adanya penetapan Kebijakan Sekuriti Sistem Informasi Perusahaan.

Mengingat:

a. Anggaran Dasar Perusahaan Perseroan (Persero) PT. Telekomunikasi Indonesia, Tbk yang telah diumumkan dalam Berita Negara RI No. 5, tanggal 17 Januari 1992, tambahan Berita Negara RI Nomor 210 sebagaimana telah beberapa kali diubah dan terakhir telah diumumkan dalam Berita Negara RI Nomor 5 tanggal 18 Januari 2005 Tambahan Berita Negara RI Nomor 569;

b. Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk., nomor: KD. 04/PS150/CTG-10/2006, tanggal 13 Januari 2006, tentang Organisasi Kantor Perusahaan;

c. Keputusan /....

Committed 2 U

c. Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk., nomor: KD. 49/PW000/KUG-10/2004, tanggal 29 Oktober 2004, tentang Kebijakan Pengendalian Intern dalam Rangka Penyajian Laporan Keuangan Perusahaan yang sesuai dengan *Sarbanes-Oxley Act Section 302 & 404*;

d. Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk., nomor: KD. 16/PW000/PRO-IIC/2006, tanggal 3 Februari 2006, tentang Manajemen Risiko Perusahaan (*TELKOM Risk Management*);

e. Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk., nomor: KD. 37/UM400/SEK-40/2005, tanggal 16 September 2005, tentang Pengamanan Dokumen Perusahaan;

f. Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. nomor: KD. 04/HK-620/CTG-20/2005, tanggal 31 Januari 2005, tentang *Good Corporate Governance.*

Memperhatikan:

a. bahwa Perusahaan bertanggung jawab penuh terhadap investasi, biaya dan manfaat teknologi dan sistem informasi yang beroperasi di lingkungan Perusahaan;

b. bahwa Perusahaan memiliki wewenang penuh terhadap penerapan Sekuriti Sistem Informasi yang ditujukan untuk melindungi aset informasi di lingkungan Perusahaan demi menjamin kelangsungan bisnis Perusahaan sesuai dengan rencana usaha Perusahaan;

c. bahwa menggarisbawahi kebutuhan *Sarbanes-Oxley Act Compliance* yang berhubungan dengan penyelenggaraan pengembangan dan operasi Teknologi Informasi Perusahaan.

MEMUTUSKAN :

Menetapkan : **KEPUTUSAN DIREKTUR UTAMA PERUSAHAAN PERSEROAN (PERSERO) PT. TELEKOMUNIKASI INDONESIA, Tbk. TENTANG KEBIJAKAN SEKURITI SISTEM INFORMASI.**

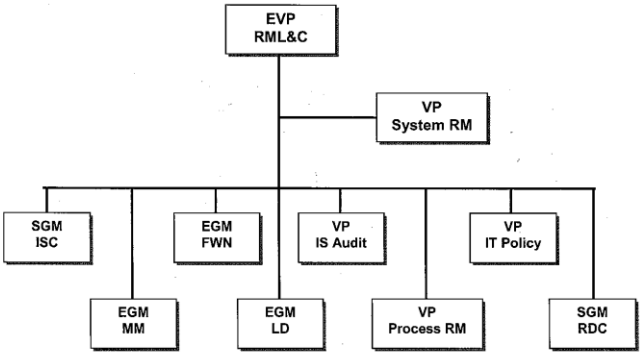
BAB I /....

TELKOM

Lampiran I
Keputusan Direksi Perusahaan Perseroan (Persero)
PT. Telekomunikasi Indonesia, Tbk.
No. KD. 57/HK-290/ITS-30/2006

PEDOMAN PELAKSANAAN TUGAS KOMITE SEKURITI SISTEM INFORMASI

1. STRUKTUR ORGANISASI DAN KEANGGOTAAN



a. Susunan keanggotaan Komite Sekuriti Sistem Informasi adalah sebagai berikut;

Ketua	: EVP Risk Management, Legal, & Compliance
Sekretaris	: VP System Risk Management
Anggota Tetap	: SGM Information System Center EGM Multimedia EGM Fixed Wireless Network EGM Long Distance VP Information System Audit VP Process Risk Management VP IT Policy SGM Research and Development Center

b. Ketua dan Sekretaris merangkap Anggota Komite Sekuriti Sistem Informasi.

c. Anggota *Ad-Hoc* terdiri dari pimpinan dari unit-unit terkait yang antara lain Kantor Perusahaan, Divisi, Pusat, Proyek, dan unit Sekuriti.

d. Keanggotaan Komite Sekuriti Sistem Informasi bersifat *ex-officio* (melekat pada jabatan).

2. TUGAS DAN TANGGUNG JAWAB

Komite Sekuriti Sistem Informasi memiliki tugas dan tanggung jawab dalam hal;

a. Menentukan standar, strategi, memahami permasalahan, dan menyiapkan pemecahan atas permasalahan yang berkaitan dengan sekuriti sistem informasi Perusahaan;

b. Memantau dan mengevaluasi secara berkala pelaksanaan standar sekuriti aset informasi di seluruh tingkat unit kerja Perusahaan;

c. Memberdayakan program peningkatan kesadaran sekuriti aset informasi;

d. Berkoordinasi dengan Forum Sekuriti Sistem Informasi tingkat Divisi / Pusat / Proyek / setingkat;

e. Melakukan pengendalian terhadap implementasi Sekuriti Informasi lintas unit kerja;

f. Memberikan laporan kepada Direksi Perusahaan.

3. MEKANISME PENYELENGGARAAN DAN PENGAMBILAN KEPUTUSAN

Penyelenggaraan tugas dan pengambilan keputusan Komite Sekuriti Sistem Informasi diatur sebagai berikut;

a. Komite Sekuriti Sistem Informasi melaksanakan rapat sekurang-kurangnya satu kali dalam setahun atau berdasarkan laporan Insiden Sekuriti Sistem Informasi dari Forum Sekuriti Sistem Informasi, maupun bilamana diperlukan pengambilan keputusan tingkat Komite yang menyangkut penerapan Sekuriti Sistem Informasi Perusahaan;

b. Pertemuan dianggap sah dan dapat mengambil keputusan bila dihadiri oleh lebih dari setengah anggota Komite yang diundang, dihadiri oleh Ketua, Sekretaris, dan minimal satu Anggota Tetap yang memiliki kepentingan terhadap materi pembahasan rapat;

c. Pengambilan keputusan dalam rapat Komite Sekuriti Sistem Informasi dinyatakan sah bila disetujui lebih dari setengah anggota yang hadir;

d. Agenda rapat harus diterima oleh seluruh anggota Komite minimal 1 (satu) hari sebelum rapat dilaksanakan;

e. Rapat Komite Sekuriti Sistem Informasi dipimpin oleh Ketua atau Sekretaris Komite yang ditunjuk oleh Ketua;

f. Anggota Komite diperkenankan mendelegasikan kewenangannya kepada pejabat bawahannya untuk mengikuti rapat Komite Sekuriti Sistem Informasi atas rekomendasi Ketua;

g. Komite Sekuriti Sistem Informasi dapat mengundang staf atau *senior leader* (anggota *Ad-Hoc*) yang dianggap perlu;

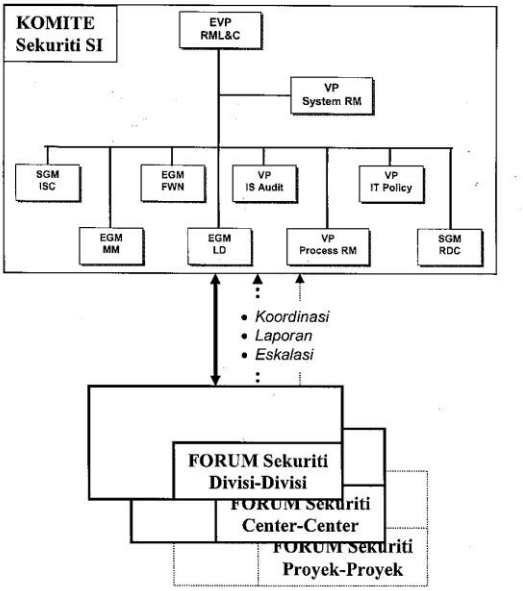
h. Koordinasi pelaksanaan rapat Komite Sekuriti Sistem Informasi dilakukan oleh Sekretaris Komite Sekuriti Sistem Informasi.

TELKOM

Lampiran II
Keputusan Direksi Perusahaan Perseroan (Persero)
PT. Telekomunikasi Indonesia, Tbk.
No. KD. 57/HK-290/ITS-30/2006

PEDOMAN PELAKSANAAN TUGAS FORUM SEKURITI SISTEM INFORMASI

1. STRUKTUR ORGANISASI DAN KEANGGOTAAN



a. Pembina Forum Sekuriti Sistem Informasi : masing-masing EGM / SGM / KaPro;

b. Ketua dan Anggota Forum Sekuriti Sistem Informasi dipilih dan ditetapkan oleh Pembina Forum Sekuriti Sistem Informasi;

c. Ketua Forum Sekuriti bertanggung jawab kepada Pembina Forum Sekuriti Sistem Informasi;

d. Organisasi, peran dan tanggungjawab, mekanisme penyelenggaraan dan pengambilan keputusan menjadi otoritas masing-masing unit PO, unit DC, Center.

TELKOM

Lampiran III
Keputusan Direksi Perusahaan Perseroan (Persero)
PT. Telekomunikasi Indonesia, Tbk.
No. KD. 57/HK-290/ITS-30/2006

PETA PERAN UNIT KERJA TERHADAP FUNGSI SEKURITI SISTEM INFORMASI

Organisasi Fungsional Sekuriti Sistem Informasi	Organisasi Struktural (Koordinator)	Organisasi Struktural Terkait
Unit Pengelola Kebijakan TI	VP IT Policy	VP System RM, ISC, RDC
Unit Pengelola TI	ISC	Unit PO, Center
Unit Audit Sistem Informasi	VP IS Audit	VP IT Policy, RDC
Unit Manajemen Risiko	-	RMLC
Unit Pengelola SAS	VP System RM	Unit SAS
Komite Sekuriti Sistem Informasi	EVP RMLC	Unit PO, Unit DC, Center, ISC, RDC, VP IS AUDIT, VP IT Policy, VP Process RM
Forum Sekuriti Sistem Informasi	Senior Leader di Unit PO, Unit DC, Center, Proyek	Manajemen di Unit terkait
Pengelola SDM	HR Center	HR Area
Pengelola Infrastruktur Teknologi Informasi	ISC	Unit PO, RDC
Pengelola Jaringan	ISC	Unit PO
Pengelola Layanan Teknologi Informasi	ISC	Unit PO
Pengelola Properti	-	GSD
Pengguna	-	Seluruh Karyawan
Pemilik data	-	Unit PO, Unit DC, Center, Direktorat, CO
Custodian	ISC	Unit PO, Unit DC, Center, Direktorat, CO
Originator	-	Seluruh Karyawan

Keterangan :
CO : Corporate Office
PO : Product Owner
DC : Delivery Channel
GSD : Graha Sarana Duta
RMLC : Risk Management, Legal & Compliance

2. Dokumen pedoman pengaturan privilege akses network element IP Network Divisi Network of Broadband

KEPUTUSAN EGM DIVISI NETWORK OF BROADBAND
PERUSAHAAN PERSEROAN (PERSERO)
PT. TELEKOMUNIKASI INDONESIA, Tbk.
NOMOR : KV. /TK400/DIT/A1000000/2013

TENTANG

PEDOMAN PENGATURAN PRIVILEGE AKSES
NETWORK ELEMENT IP NETWORK DIVISI NETWORK OF BROADBAND

EGM DIVISI NETWORK OF BROADBAND
PERUSAHAAN PERSEROAN (PERSERO) PT. TELEKOMUNIKASI INDONESIA, Tbk.

Menimbang :

a. bahwa network element IP Network yang terpasang jumlahnya terus bertambah, dengan fungsinya yang strategis untuk mendukung infrastruktur NGN;

b. bahwa unit yang terkait pengelolaan operasional network element semakin banyak sejalan dengan pengembangan infrastrukturnya;

c. bahwa untuk menjaga keamanan network, efektifitas dan ketertiban dari operasional yang melibatkan multi unit, perlu dibuat pedoman pemakaian hak akses privilege network element IP Network yang ditetapkan dalam suatu Surat Keputusan EGM Divisi Network of Broadband.

Mengingat :

1. Anggaran Dasar Perusahaan Perseroan (PERSERO) PT TELEKOMUNIKASI INDONESIA, Tbk yang telah diumumkan dalam Berita Negara RI Nomor 5 Tambahan Berita Negara RI Nomor 210 tanggal 17 Januari 1992, sebagaimana telah beberapa kali diubah dan terakhir diumumkan dalam Berita Negara RI Nomor 84 tanggal 17 Oktober 2008, Tambahan Berita Negara RI No. 2055;
2. Peraturan Direksi Nomor PD.202.16/r.00/HK.200 /COP-J4000000/2013 tanggal 24 September 2013, tentang Organisasi Divisi Network Of Broadband
3. Peraturan Direksi Nomor PD.202.06/r.00/PS150 /COP-B0400000/2012 tanggal 19 Desember 2012, tentang Organisasi Divisi Telkom Barat/ Timur

Memperhatikan	:	Nota Dinas DEGM IP nomor CTel.372/TK000/DIT-A1000000/2012 tanggal 11 Mei 2012 perihal Pengaturan Privilege/ Hak Akses IP & Data Network Dalam Masa Regrouping

M E M U T U S K A N

Menetapkan	:	Keputusan EGM Disivi Network of Broadband tentang Pedoman Pengaturan Privilege Akses Network Element IP Network Divisi Network of Broadband
KESATU	:	Mengesahkan dan memberlakukan Pedoman Pengaturan Privilege Akses Network Element IP Network Divisi Network of Broadband
KEDUA	:	Pedoman Pengaturan Privilege Akses Network Element IP Network Divisi Network of Broadband sebagai acuan unit-unit di kantor Divisi Network of Broadband dalam melakukan kegiatan dimaksud sesuai prosedur yang berlaku.
KETIGA	:	Dengan berlakunya Keputusan ini, maka keputusan terdahulu nomor KV.56/TK400/DIT-060/2008 tentang Pedoman Pengaturan Privilege akses Network Elemen Divisi Infratel dinyatakan tidak berlaku.
KEEMPAT	:	Hal-hal yang belum cukup diatur dalam keputusan ini, akan diatur dan ditetapkan kemudian.
KELIMA	:	Keputusan ini berlaku sejak tanggal ditetapkan.

Ditetapkan : JAKARTA
Pada Tanggal : 2013

A.n. DIREKSI PERUSAHAAN (PERSERO)
PT. TELEKOMUNIKASI INDONESIA, Tbk

EGM DIVISI NETWORK OF BROADBAND

DAVID BANGUN
NIK. : 651282

Tembusan Keputusan ini disampaikan kepada :

1. Sdr. VP ISG DIT NITS
2. Sdr. Kepala Unit Divisi Network Of Broadband

3. Laporan hasil audit eksternal

Nonconformity Report (list of nonconformities)

TÜVRheinland®
Precisely Right.

Client	Certification No.
PT. Telkomunikasi Indonesia Tbk	103 153 11004
Type of audit	Standard (s)
1st Follow Up Audit	ISO/IEC 27001:2005

Management System	Mr. Alip Priyono
Audit Team Leader:	Andreas Gehrmann
Auditor(s)/Expert:	Mr. Nguyen Van Sac, Mr. Abdul Qohar (Trainee),Mr. To Hoang Nam , Mr. Rachmat Kurniawan (Trainee), Mr. Riki Andi Nugraha (Trainee),Mr. Ramoncito Puyat, Mr. Vickres Legowo (Trainee)
Audit Date:	2012-11-26 to 29

2012-11-29		Andreas Gehrmann		Mr. Alip Priyono
Date		Audit Team Leader		Management System Representative

The client is required to analyze the root cause of the nonconformities. This results and the correction(s) and corrective action(s) has (have) to be described in the nonconformity report and has (have) to be forwarded to the audit team leader rapidly. Documents, which prove the elimination of the nonconformities have to be submitted.

Please note that the actions for the nonconformities have to be taken and corresponding documents have to be submitted until 2012-12-28

☐	Correction(s) and corrective action(s) are appropriate. Correction(s) has (have) been verified, including documents submitted later.
☐	A re-audit was performed.

Date, processing auditor

Rev.1.2 (2011-03)

Nonconformity Report (list of nonconformities)

TÜVRheinland®
Precisely Right.

Client	Certification No.
PT. Telkomunikasi Indonesia Tbk	103 153 11004
Type of audit	Standard (s)
1st Follow Up Audit	ISO/IEC 27001:2005

No	Ref	Nonconformity [Discussed with whom and where?]	proof	Cause analysis [by whom?]	Corrections and Corrective Action [by whom?]	Completion date
1	6.a	**Discussed with: Mr.Jumala and Mr.Benny** **Department(Area): Semarang and Head Office DIVA** **Non-conformity**: 1) The last internal audit did not cover all aspects of the management system requirements; e.g. Risk assessment, corrective actions, record control (refer to audit records in Semarang, Palembang August 7-8) 2) There is no internal audit in Access Division -Jakarta	D	Responsible Person : Root Causes:	Responsible Person : Correction : Responsible Person : Corrective Action :	 Date: Date:

Remarks under „proof": D = submit documents; NA = re-audit

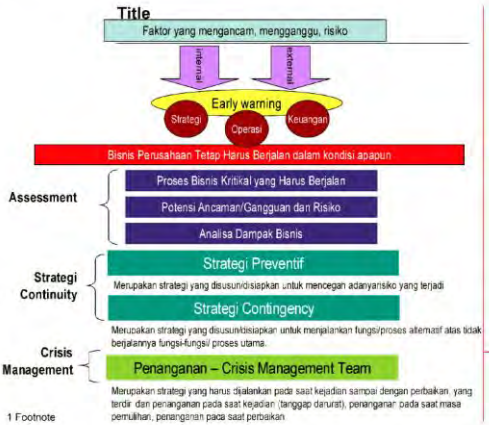
4. Materi pelatihan penanggulangan bencana

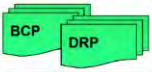
TRACKER

Bcm by KD.32/2009

Unit of measure

Telkom Indonesia





- Unit Bisnis harus memiliki dokumen BCP & DRP
- BCP: merupakan dokumen yang berisi skenario kelangsungan bisnis
- DRP: merupakan dokumen yang berisi skenario kelangsungan alat produksi
- BCP & DRP merupakan satu kesatuan yg saling mendukung
- Dokumen BCP & DRP harus rutin dilakukan simulasi & *update*

- Dibentuknya CMT mulai dari tingkat Nasional, Regional , Lokal & Area Khusus Jakarta

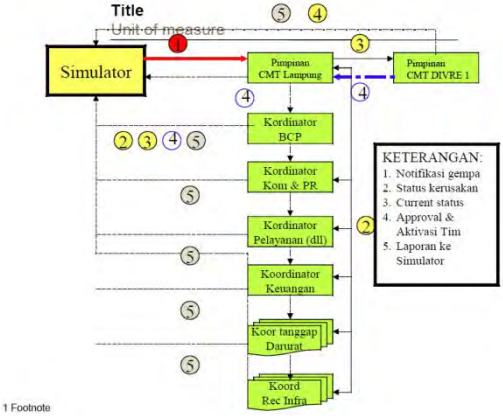
SOURCE: Source

TRACKER

Contoh: simulasi bcp (koordinasi & komunikasi)

Unit of measure

Telkom Indonesia



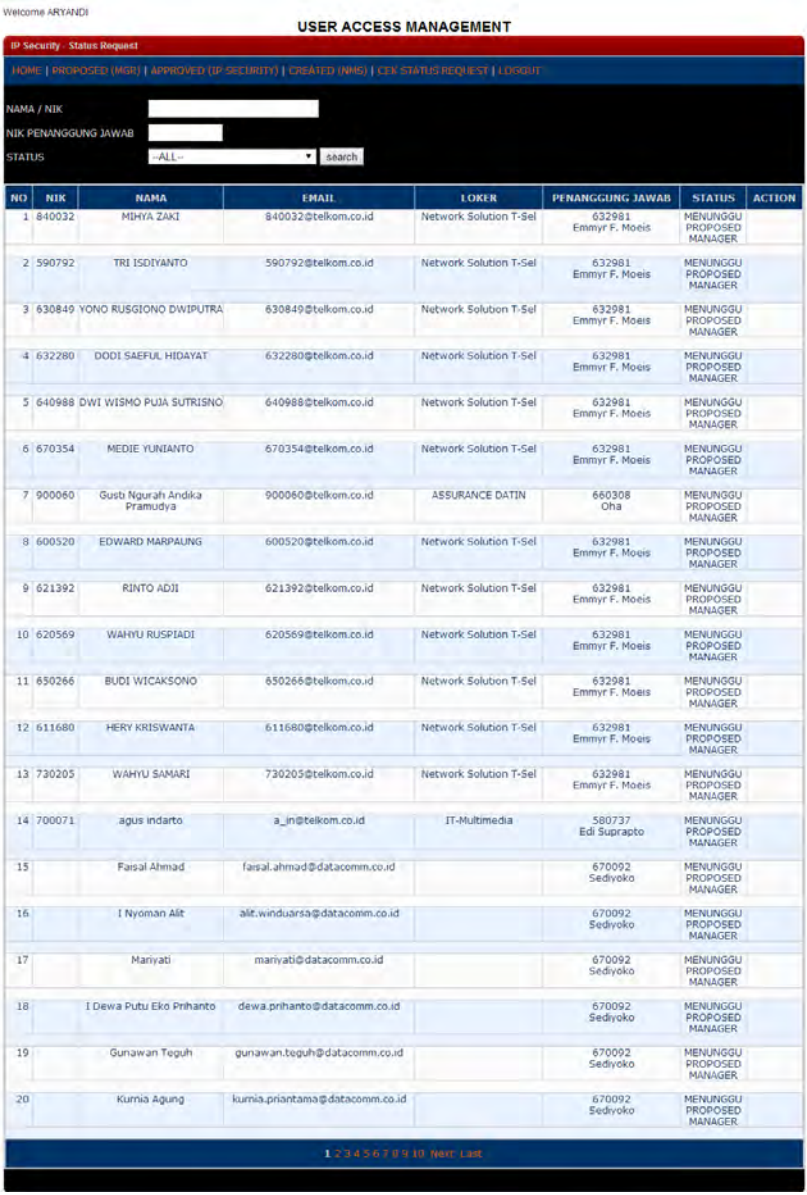
DAFTAR NO TELEPON
1. Simulator : 0751xxxxxxx
2. Pimpinan CMT :
3. Koord BCP
4. Koord Kom & PR
5. Koord Pelayanan :
6. Koord SDM
7. Koord Pelayanan
8. Koord Log & Security
9. Koord Tanggap Darurat
10. Koord Pemulihan Infra

Catatan :
1. Dalam latihan ini, SMS yang dikirim ke SIMULATOR minimal 3 person dari setiap Koord.
2. Isi berita a.l kesiapan anggota dan kondisi terakhir .

1 Footnote

SOURCE: Source

5. Contoh log aktifitas sistem informasi



Welcome ARYANDI

USER ACCESS MANAGEMENT

IP Security - Status Request

HOME | PROPOSED (MGR) | APPROVED (IP SECURITY) | CREATED (NMS) | CEK STATUS REQUEST | LOGOUT

NAMA / NIK

NIK PENANGGUNG JAWAB

STATUS --ALL-- search

NO	NIK	NAMA	EMAIL	LOKER	PENANGGUNG JAWAB	STATUS	ACTION
1	840032	MIHYA ZAKI	840032@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
2	590792	TRI ISDIYANTO	590792@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
3	630849	YONO RUSGIONO DWIPUTRA	630849@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
4	632280	DODI SAEFUL HIDAYAT	632280@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
5	640988	DWI WISMO PUJA SUTRISNO	640988@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
6	670354	MEDIE YUNIANTO	670354@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
7	900060	Gusti Ngurah Andika Pramudya	900060@telkom.co.id	ASSURANCE DATIN	660308 Oha	MENUNGGU PROPOSED MANAGER	
8	600520	EDWARD MARPAUNG	600520@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
9	621392	RINTO ADJI	621392@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
10	620569	WAHYU RUSPIADI	620569@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
11	650266	BUDI WICAKSONO	650266@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
12	611680	HERY KRISWANTA	611680@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
13	730205	WAHYU SAMARI	730205@telkom.co.id	Network Solution T-Sel	632981 Emmyr F. Moeis	MENUNGGU PROPOSED MANAGER	
14	700071	agus indarto	a_in@telkom.co.id	IT-Multimedia	580737 Edi Suprapto	MENUNGGU PROPOSED MANAGER	
15		Faisal Ahmad	faisal.ahmad@datacomm.co.id		670092 Sediyoko	MENUNGGU PROPOSED MANAGER	
16		I Nyoman Alit	alit.winduarsa@datacomm.co.id		670092 Sediyoko	MENUNGGU PROPOSED MANAGER	
17		Mariyati	mariyati@datacomm.co.id		670092 Sediyoko	MENUNGGU PROPOSED MANAGER	
18		I Dewa Putu Eko Prihanto	dewa.prihanto@datacomm.co.id		670092 Sediyoko	MENUNGGU PROPOSED MANAGER	
19		Gunawan Teguh	gunawan.teguh@datacomm.co.id		670092 Sediyoko	MENUNGGU PROPOSED MANAGER	
20		Kurnia Agung	kurnia.priantama@datacomm.co.id		670092 Sediyoko	MENUNGGU PROPOSED MANAGER	

1 2 3 4 5 6 7 8 9 10 Next Last

Welcome ARYANDI

USER ACCESS MANAGEMENT

IP Security - Status Request

HOME | PROPOSED (MGR) | APPROVED (IP SECURITY) | CREATED (NMS) | CEK STATUS REQUEST | LOGOUT

NAMA / NIK

NIK PENANGGUNG JAWAB

STATUS --ALL-- search

NO	NIK	NAMA	EMAIL	LOKER	PENANGGUNG JAWAB	STATUS	ACTION
1161		Mohammad Syahronny	gurita.darat@gmail.com	Assurance Speedy Engineer	740172 Bambang Mujiono	CREATED NMS	
1162		M Ridwan	mridwan30@gmail.com	Assurance Speedy Engineer	740172 Bambang Mujiono	CREATED NMS	
1163	880007	LUNEL CANDRA	lunelcandra@telkom.co.id	INNOVATION & DESIGN CENTER	720416 Fidar Adjie Laksono	CREATED NMS	
1164	720416	FIDAR ADJIE LAKSONO	fidar@telkom.co.id	INNOVATION & DESIGN CENTER	720416 Fidar Adjie Laksono	CREATED NMS	
1165	680061	BAMBANG CAHYONO	bcahyono@telkom.co.id	INNOVATION & DESIGN CENTER	720416 Fidar Adjie Laksono	CREATED NMS	
1166	720419	LESMIN NAINGGOLAN	esmint@telkom.co.id	INNOVATION & DESIGN CENTER	720416 Fidar Adjie Laksono	CREATED NMS	
1167	640918	WAHYUDI	yudioslo@telkom.co.id	INNOVATION & DESIGN CENTER	720416 Fidar Adjie Laksono	CREATED NMS	
1168	830070	MAHARDI PRABOWO	prabu_mahardi@telkom.co.id	INNOVATION & DESIGN CENTER	720416 Fidar Adjie Laksono	CREATED NMS	
1169	641074	Slamet Sudarto	Divisi Netbro	Speedy Problem Handling 6	740172 Bambang Mujiono	CREATED NMS	
1170	TLH	RIZKI ADI NUGRAHA	coberanoys@gmail.com	ASSURANCE CARE CENTRE	660308 Oha	CREATED NMS	
1171	840056	Hanif Fauzan	hanif.fauzan@telkom.co.id	Service Operation, SI Divisi Broadband	710381 Iskandar Satyogo Prasetyo	CREATED NMS	
1172	650694	dida trisyadi	dida@telkom.co.id	fulfillment DNB	650694 Dida trisyadi	CREATED NMS	
1173	601655	Tonny Hendi Suryanto	601655@telkom.co.id	Asman Service Delivery & Integration Area 3	590777 Fitri Yohanto	CREATED NMS	
1174	631281	KANI	kani63@telkom.co.id	INFRATEL	630657 Lawrence Boston	CREATED NMS	
1175	850050	Eryk Lesmono	eryk_l@telkom.co.id	CSD Netbro	730430 Jerry Alvijano Harjadi	CREATED NMS	
1176	-	Aditya Nugraha	aditya.nugraha@sigma.co.id	Mitra MS (Sigma)	730379 I Wayan Mulastika	CREATED NMS	
1177	-	2. Sapta Rizki Fauzi	sapta.fauzi@sigma.co.id	Mitra MS (Sigma)	730379 I Wayan Mulastika	CREATED NMS	

Next Previous 50 51 52 53 54 55 56 57 58 59