BAB 1
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

1.1.1 Profil Singkat Perusahaan

PT Industri Telekomunikasi Indonesia (PT INTI) merupakan Badan Usaha Milik Negara yang bergerak dalam bidang industri telekomunikasi dan sistem informasi. Pada awalnya PT INTI merupakan Proyek Industri Telekomunikasi. Namun pada tanggal 30 Desember 1974, diubah bentuknya menjadi PT. Industri Telekomunikasi Indonesia (Persero), Sejarah PT INTI dapat dilihat di lampiran I (Sumber: Laporan keuangan PT INTI tahun 2014).

1.1.2 Visi dan Misi

Berdasarkan laporan keuangan PT INTI tahun 2014, Visi PT INTI adalah menjadi pilihan pertama bagi pelanggan dalam mentransformasikan "mimpi" menjadi "kenyataan".

Misi PT INTI adalah:

1. Fokus bisnis tertuju pada kegiatan jasa *Engineering* yang sesuai dengan spesifikasi dan permintaan konsumen
2. Memaksimalkan *value* (nilai) Perusahaan serta mengupayakan *growth* (pertumbuhan) yang berkesinambungan
3. Berperan sebagai *prime mover* (penggerak utama) bangkitnya industri dalam negeri

1.1.3 Struktur Organisasi

Berdasarkan Surat Keputusan Direksi Nomor KN.013/2014 tentang Struktur Organisasi Perusahaan Dua Tingkat di Bawah Direksi, dan KN.014/2014 tentang Struktur Organisasi Perusahaan Tingkat Urusan, dapat dilihat dalam Lampiran I.

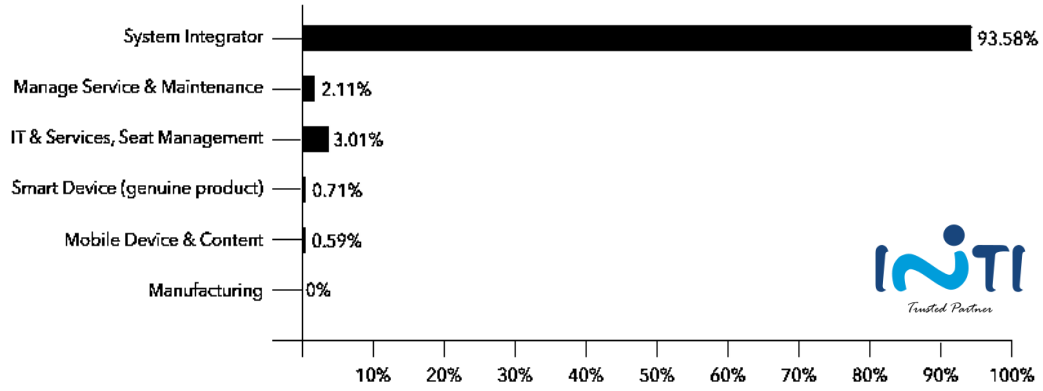
1.1.4 Bidang Usaha

PT INTI telah berkiprah dalam bisnis telekomunikasi lebih dari 40 tahun dan PT INTI telah melakukan perubahan orientasi bisnis dari yang semula berbasis *pure manufacture* menjadi sebuah industri yang berbasis solusi kesisteman, khususnya

sistem infokom, dan integrasi teknologi. Solusi *Smart Clinic* yaitu sistem informasi bagi penyedia layanan kesehatan, dan dalam bidang industri telekomunikasi PT INTI masih berkiprah dengan *Fiber Termination Management* (FTM), *Optical Splitter*, *Fiber Optic Accesoris*, dll. (Sumber: Laporan keuangan PT INTI 2014).

1.1.5 Produk

Produk dan layanan PT INTI menurut laporan keuangan 2014 PT INTI dikembangkan dari empat pilar utama yaitu ICT-E (*Information System*, *Content*, *Telecommunication System*, dan *Electronic*). PT INTI memfokuskan diri sebagai *System Integrator* di bidang ICT. Dari *core competency* tersebut, kemudian diturunkan ke dalam lini bisnis PT INTI sebagai berikut:



Gambar 1.1 - Grafik Portofolio Bisnis Perusahaan

Sumber: Laporan Keuangan Perusahaan Tahun 2014

1.2 Latar Belakang Penelitian

Jantung dari setiap organisasi bisnis yang ada di dunia sekarang ini adalah sistem teknologi informasi yang dimiliki organisasi tersebut (Patricia, 2015:2). Bagi organisasi bisnis, bersaing dan tumbuh secara kompleks membutuhkan strategi bisnis yang kuat dengan memanfaatkan teknologi informasi secara maksimal sebagai keuntungan bersaing (Harkins, 2013:11).

Thomas R. Peltier (2014:94) menyebutkan "*Technology is a wonderful thing*", dan Thomas pun menuturkan bahwa dengan kemajuan dan semakin canggihnya teknologi informasi sekarang ini, teknologi informasi masih membutuhkan campur

tangan manusia untuk menjalakan dan mengoperasikannya. Menurut Thomas semakin maju dan canggihnya teknologi informasi, akan menciptakan orang jahat dengan kemampuan mengoperasikan teknologi informasi yang canggih pula, dan orang jahat tersebut akan terus berimprovisasi dengan kemajuan yang ada. Dengan keberadaan orang jahat yang menguasai teknologi tersebut, maka akan menjadi ancaman bagi keamanan teknologi informasi yang ada. Ancaman yang dimaksud adalah dampak yang ditimbulkan atas terjadinya kejadian yang mengancam 3 aspek keamanan informasi yaitu *Confidentiality*, *Integrity*, dan *Availability* (CIA).

Oleh karena itu dapat disimpulkan bahwa teknologi informasi adalah inti dari setiap kegiatan bisnis, dengan menyadari bahwa teknologi informasi sangat penting, maka keamanan untuk teknologi informasi pun seharusnya menjadi bagian yang perlu ada, diperhatikan, dan terus dikembangkan seiring dengan perkembangan teknologi informasi.

Pada awal tahun 2015 pun terjadi kasus pencurian data krusial pada Kantor Manajemen Pegawai Amerika Serikat, dengan jumlah data yang tercuri sebanyak 21,5 juta data, data penting (sidik jari, biodata, dll.) pegawai dan mantan pegawai federal Amerika (Tribun:2015). Dengan teknologi informasi yang tinggi pada pemerintahan Amerika Serikat pun dapat di tembus dan banyak data yang tercuri.

Merujuk kepada beberapa peraturan di Indonesia seperti PER-01/MBU/2011, PER-02/MBU/2013, KIPP edisi 2.0 tahun 2011, Pemerintah Republik Indonesia sudah menyadari akan kebutuhan dan pentingnya sistem teknologi informasi pada perusahaan atau setiap penyedia layanan publik, dan pemerintah sudah menyadari bahwa keamanan teknologi informasi harus menjadi perhatian serius bagi setiap perusahaan, atau setiap penyedia layanan publik.

Dalam PER-02/MBU/2013 pemerintah sudah memberikan rincian, aturan, dan pedoman, dan terdapat peraturan pada pasal 3 mengenai *Master Plan IT* yang menyebutkan bahwa “setiap BUMN menyusun *master plan* teknologi informasi (sesuai dengan referensi) paling lambat 2 tahun setelah Peraturan ini ditetapkan”, yang berarti di tahun 2015 ini adalah tenggat waktu untuk setiap perusahaan BUMN menyusun *master plan IT* berdasarkan PER-02/MBU/2013. Dan *master plan IT* di

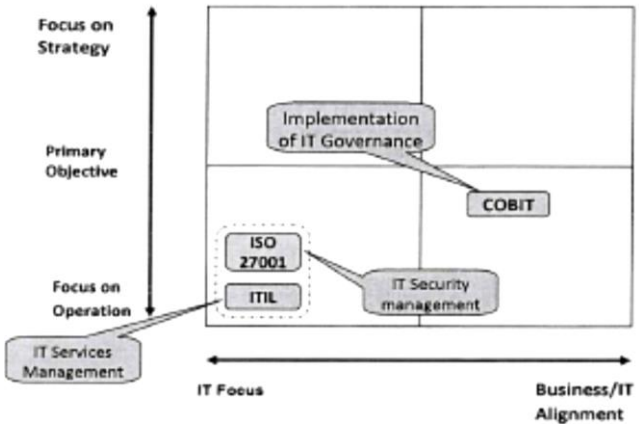
sini adalah keseluruhan dokumentasi dari perencanaan TI, kebijakan TI, prosedur, hingga *guideline* yang mengatur TI dalam perusahaan.

Tidak hanya Kementerian BUMN yang mengeluarkan peraturan mengenai *IT Governance*, Kementerian Komunikasi dan Informatika (KEMKOMINFO) pada tahun 2011 dengan tim dari Direktorat Keamanan Informasi juga mengeluarkan Buku Panduan Penerapan Tata Kelola Keamanan Informasi edisi 2.0, dan dengan buku panduan ini, KEMKOMINFO berupaya untuk meningkatkan penerapan tata kelola manajemen teknologi informasi di setiap instansi dan penyedia layanan publik yang ada di Indonesia sejak tahun 2008, hingga tahun 2011.

Tim Direktorat Keamanan Informasi (KEMKOMINFO, 2011: 7) menyebutkan "mayoritas instansi peserta belum memiliki atau sedang menyusun kerangka kerja keamanan informasi yang memenuhi standar", atau dapat dikatakan perusahaan-perusahaan di Indonesia masih minim perhatiannya terhadap tata kelola manajemen keamanan informasi.

Salah satunya adalah PT INTI, PT INTI sebagai perusahaan BUMN menyadari dukungan *IT Governance* sangat diperlukan, dan dalam implementasi perusahaan khususnya Bagian Sistem Manajemen Informasi sedang memberikan perhatian lebih kepada tata kelola manajemen teknologi informasi yang sesuai dengan referensi PER-02/MBU/2013.

Terdapat 3 referensi *framework* tata kelola IT yang ada dalam PER-02/MBU/2013, yaitu COBIT (*Control Objectives for Information and related Technology)*, ISO 27001, dan ITIL (*The IT Infrastructure Library).*



Gambar 1.2 - Referensi Tata Kelola IT *Governance Best Practice*

Sumber: Peraturan Pemerintah nomor PER-02/MBU/2013

Pada tahun 2015 ini, beberapa mahasiswa tingkat akhir dari Universitas Telkom sedang ditugaskan untuk menyusun rancangan tata kelola manajemen teknologi informasi di PT INTI menggunakan *framework* COBIT, dan tugas akhir dari mahasiswa-mahasiswa tersebut telah berhasil diselesaikan dan disahkan oleh Universitas Telkom pada tanggal 23 Juni 2015. *Framework* COBIT itu sendiri adalah merupakan *best practice* yang disarankan oleh PER-02/MBU/2013, yang dikembangkan untuk membantu perusahaan dalam melakukan penilaian tata kelola atau proses TI yang dimiliki.

Perancangan tata kelola manajemen teknologi informasi di PT INTI menggunakan *framework* COBIT telah selesai dilakukan, namun masih terdapat *framework* tata kelola manajemen teknologi informasi yang belum di analisis dan dibuat perancangannya, yaitu dengan ISO 27001 atau dengan ITIL. Dalam buku panduan tata kelola manajemen keamanan informasi dari KEMKEMKOMINFO (KEMKOMINFO, 2011: 9) menyebutkan bahwa *framework* yang harus diikuti untuk tata kelola manajemen keamanan informasi adalah *framework* ISO/IEC 27000 *family*, oleh karena itu penelitian ini memilih ISO/IEC 27001:2013 sebagai salah satu *family* dari ISO/IEC 27000 untuk dijadikan acuan.

Berdasarkan hasil observasi di Divisi Sistem dan Teknologi Informasi (SISTEKFO), dan wawancara dengan Kepala Bagian Sistem Manajemen

Informasi, terdapat beberapa gangguan dan ketidaksesuaian yang terjadi pada perusahaan seperti:

1. Tidak adanya dokumentasi dari kebijakan keamanan informasi,
2. Serangan *malware* dan virus yang membuat kegiatan operasional perusahaan terhambat,
3. Serangan *hacker* sering terjadi terhadap sistem informasi perusahaan,,
4. Hilangnya akses terhadap *username* dan *password* pegawai,
5. Tidak adanya *monitoring* akan aktivitas *logging*,
6. Kurangnya kesadaran keamanan informasi dalam perusahaan.

Gambar 1.3 – Terjadinya *Hacking* dalam sistem informasi perusahaan

Sumber: Data yang diolah

Di PT INTI sendiri, sudah memiliki sertifikasi ISO 9001 dan ISO 14001, namun kedua sertifikasi ini sudah tidak berlaku lagi sejak tahun 2014 silam, dan tidak diperpanjang oleh manajemen. Walaupun sudah sertifikasi ISO, namun dalam manajemen TI perusahaan masih terdapat dokumen yang tidak terdokumentasi, seperti kebijakan keamanan informasi. Dalam ISO/IEC 27001:2013 *annex 5*, kebijakan keamanan informasi merupakan poin pertama yang penting, dengan penulisan dokumentasi kebijakan keamanan yang baik dapat menginterpretasikan

keefektifan dari arsitektur keamanan informasi dalam perusahaan dan dokumentasi proses ini tidak ada dalam perusahaan.

Dari sisi kesadaran akan pentingnya keamanan informasi, dalam perusahaan masih kurang, padahal dalam ISO/IEC 27001:2013 disebutkan bahwa setiap orang yang berada dalam organisasi harus sadar akan pentingnya keamanan informasi, sehingga dalam proses operasional perusahaan sehari-hari masih memiliki risiko yang besar akan keamanan informasi perusahaan. Oleh karena itu, *annex 7* keamanan sumber daya manusia dipilih agar dapat meminimalisir risiko akan keamanan informasi perusahaan.

Aspek keamanan informasi yaitu *Confidentiality*, *Integrity*, dan *Availability* (CIA) dapat dicerminkan melalui *annex 9* Akses Kontrol. Apakah informasi dapat diakses oleh orang yang tepat, apakah informasi lengkap, dan dapat diakses kapan pun, dapat mencerminkan apakah aspek keamanan informasi dalam perusahaan sudah diimplementasikan secara efektif atau belum. Oleh karena itu *annex 9* ini dipilih.

Produk yang dihasilkan PT INTI sekarang 93,58% adalah *sistem integrator* dan banyak dihasilkan oleh Divisi SISTEKFO, maka perlu dipastikan keamanan yang baik untuk kegiatan operasional pada divisi SISTEKFO. Sesuai dengan *annex 12* dan *control objective*nya yang ada dalam ISO 27001 maka *annex 12* dipilih untuk dapat menjamin kegiatan operasional yang baik, dan aman.

Mengacu kepada jurnal *Vulnerability Assessment* untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi, Priandoyo (2006:14), mengatakan bahwa perlu untuk dilakukannya *assessment* untuk mengetahui tingkat kematangan perusahaan sehingga dapat dilakukan tindakan pencegahan yang tepat, dengan harapan perusahaan dapat berbenah dan dapat mengimplementasikan keamanan informasi dengan lebih baik.

Oleh karena itu untuk melanjutkan memperbaiki, mengembangkan, dan memberikan rekomendasi tata kelola manajemen teknologi informasi di PT INTI, maka perlu adanya audit sistem manajemen keamanan teknologi informasi, dan pengembangan sistem manajemen keamanan teknologi informasi di PT INTI

menggunakan *framework* ISO/IEC 27001:2013 dibantu dengan ISO/IEC 27002. Dan pelaksanaan penelitian ini akan dilakukan dengan laporan berjudul "**ANALISIS AUDIT KEAMANAN INFORMASI PADA KEBIJAKAN KEAMANAN, KEAMANAN SUMBER DAYA MANUSIA, AKSES KONTROL, DAN KEAMANAN OPERASIONAL PADA DIVISI SISTEM DAN TEKNOLOGI INFORMASI (SISTEKFO) PT INDUSTRI TELEKOMUNIKASI INDONESIA (PERSERO) MENGGUNAKAN ISO/IEC 27001:2013**".

1.3 Perumusan Masalah

Berdasarkan latar belakang, maka dapat dikemukakan identifikasi beberapa permasalahan penelitian, yang diantaranya sebagai berikut:

a. Seharusnya dalam tingkat kematangan sistem manajemen keamanan informasi di perusahaan tahun 2015 ini, sudah dalam tingkat kematangan yang sudah bagus atau matang, karena pemerintah sudah memberikan pedoman dan tenggat waktu untuk perusahaan. Namun nyatanya PT INTI belum atau dapat dikatakan sedang membangun sistem manajemen keamanan informasi yang sesuai dengan peraturan pemerintah.
b. Kurangnya kesadaran atau pengetahuan akan pentingnya keamanan informasi dalam perusahaan, baik dari implementasi dalam kegiatan operasionalnya sehari-hari, dan dari segi sumber daya manusia perusahaan, menjadikan perusahaan membutuhkan adanya perbaikan dan rekomendasi akan kematangan sistem manajemen keamanan informasi yang diinginkan oleh pemerintah.

1.4 Pertanyaan Penelitian

Sesuai dengan hasil perumusan masalah yang didapat, maka pertanyaan penelitian adalah sebagai berikut :

a. Bagaimanakah tingkat kematangan sistem manajemen keamanan informasi pada Divisi Sistem dan Teknologi Informasi PT INTI Bandung *conform* dengan standar ISO/IEC 27001:2013 dan ISO/IEC 27002 pada *annex* kebijakan keamanan informasi, keamanan sumber daya manusia, akses kontrol, dan keamanan operasional?
b. Bagaimana rekomendasi untuk mencapai tingkat kematangan sistem manajemen keamanan informasi pada Divisi Sistem dan Teknologi Informasi PT INTI Bandung yang *conform* dengan standar ISO/IEC 27001:2013 dan ISO/IEC 27002 pada *annex* kebijakan keamanan informasi, keamanan sumber daya manusia, akses kontrol, dan keamanan operasional?

1.5 Tujuan Penelitian

Penelitian ini memiliki beberapa tujuan yang menjawab rumusan masalah di atas, yaitu sebagai berikut :

a. Mengukur tingkat kematangan sistem manajemen keamanan informasi pada Divisi Sistem dan Teknologi Informasi PT INTI Bandung *conform* dengan standar ISO/IEC 27001:2013 dan ISO/IEC 27002 pada *annex* kebijakan keamanan informasi, keamanan sumber daya manusia, akses kontrol, dan keamanan operasional.
b. Memberikan rekomendasi untuk perbaikan tingkat kematangan sistem manajemen keamanan informasi pada Divisi Sistem dan Teknologi Informasi PT INTI Bandung *conform* dengan standar ISO/IEC 27001:2013 dan ISO/IEC 27002 pada *annex* yang memiliki tingkat kematangan yang rendah.

1.6 Manfaat Penelitian

Penelitian ini diharapkan akan memiliki manfaat untuk berbagai pihak, baik dari aspek teoretis maupun aspek praktis sebagai berikut:

a. Aspek Teoretis

Hasil dari penelitian ini diharapkan dapat menjadikan pelajaran dalam melaksanakan penelitian berikutnya dengan menggunakan *framework* ISO/IEC 27001:2013, dan dapat memperkaya dan melengkapi khazanah keilmuan khususnya yang terkait dengan ISO/IEC 27001:2013 dan ISO/IEC 27002.

b. Aspek Praktis

Hasil dari penelitian ini diharapkan dapat dijadikan dasar perusahaan untuk melakukan perancangan, pengembangan dan memperbaiki tata kelola keamanan manajemen teknologi informasi sesuai dengan standar ISO/IEC 27001:2013 dan ISO/IEC 27002.

1.7 Ruang Lingkup Penelitian

Ruang lingkup penelitian ini mengacu kepada *annex* dalam ISO/IEC 27001:2013 dan ISO/IEC 27002, *annex* tersebut adalah kebijakan informasi, keamanan sumber daya manusia, akses kontrol, dan keamanan operasional. Dan penelitian dilakukan pada lingkup Divisi Sistem dan Teknologi Informasi PT INTI, dan merupakan divisi penghasil produk terbesar (93,58% bisnis *system integrator* berdasarkan portofolio bisnis) di PT INTI. Dengan bisnis yang sudah beralih ke mayoritas penghasil integrasi sistem informasi, maka keamanan informasi di dalam perusahaan harus dijaga dengan baik.

Dengan *annex 5* Kebijakan Keamanan Informasi, yang merupakan salah satu bagian dari *master plan IT*, dan penting dalam ISO/IEC 27001:2013 karena dengan meilhat kebijakan keamanan informasi dapat menginterpretasikankeefektifan dari arsitektur keamanan informasi dalam perusahaan, maka kebijakan keamanan informasi diambil sebagai lingkup pembahasan.

Annex 7 Keamanan Sumber daya manusia yang merupakan kunci dari poin pentingnya kesadaran akan keamanan informasi, setiap pegawai dalam perusahaan seharusnya dibekali dengan ilmu dan perjanjian untuk menjaga keamanan informasi perusahaan. maka Keamanan Sumber daya manusia diambil sebagai lingkup pembahasan.

Annex 9 Akses Kontrol, yang merupakan kunci untuk membatasi akses dalam informasi maupun ke dalam fasilitas pengolahan informasi dan merupakan poin penting dalam menjaga bocornya informasi dan poin penting ini pun menjadi lingkup pembahasan dalam penelitian ini.

Annex 12 Keamanan Operasional, dalam *annex* ini bertujuan untuk memastikan dalam perusahaan apakah keamanan dalam kegiatan operasional pengolahan informasi perusahaan terjaga dan proses yang berjalan sesuai dengan standar keamanan prosedur yang ada dalam ISO/IEC 27001, dan oleh karena itu *annex* ini menjadi lingkup pembahasan dalam penelitian ini, dan melihat PT INTI merupakan bisnis dengan penghasil mayoritas produk *system intregator*, maka *annex-annex* ini penting dan harus dibahas dalam penelitian.

Lokasi dan objek penelitian ini dilakukan di PT. Industri Telekomunikasi Indonesia (Persero), Divisi Sistem dan Teknologi Informasi, Bagian Sistem Informasi Manajemen yang beralamat di Jl. Moch. Toha No. 77, Bandung 40253. Waktu dan periode penelitian dimulai dari 2 September 2015 s.d. 6 November 2015

1.8 Sistematika Penulisan Tugas Akhir

Pada subbab ini akan dijelaskan bagaimana sistematika dari setiap bab yang ada dalam penelitian sebagai berikut:

a. BAB I Pendahuluan

Pada bab ini menjelaskan mengenai profil singkat perusahaan, visi dan misi, bidang usaha, dan aspek manajemen yang dimiliki, latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup penelitian, lokasi dan objek penelitian, waktu dan periode penelitian, dan sistematika penelitian

b. Bab II Tinjauan Pustaka dan Lingkup Penelitian

Bab ini berisi teori dan penelitian terdahulu yang relevan dengan permasalahan dan penelitian, perbandingan dengan penelitian terdahulu, dan kerangka pemikiran.