BAB I

PENDAHULUAN

1.1 Gambaran Umun Objek Penelitian

Telkom University (disingkat Tel-U) merupakan penggabungan dari beberapa institusi yang berada dibawah badan penyelenggara Yayasan Pendidikan Telkom (YPT) yaitu Institut Teknologi Telkom (IT Telkom), Institut Manajemen Telkom (IM Telkom), Politeknik Telkom, dan Sekolah Tinggi Seni Rupa dan Desain Indonesia Telkom (STISI Telkom). Untuk mempermudah pengelolaan informasi akademik di Universitas Telkom dibentuk Direktorat Sistem Informasi (SISFO) Universitas Telkom yang merupakan sebuah unit yang memberikan layanan infrastruktur teknologi informasi, layanan interkoneksi (intranet dan internet), layanan data dan sistem informasi (aplikasi sistem informasi akademik, non-akademik maupun pendukung) dan layanan komputasi sebagai *strategic tools* untuk berjalannya proses bisnis di Universitas Telkom.

Adapun visi dan misi dari Direktorat SISFO sebagai bagian dari Universitas Telkom, yaitu :

Visi Direktorat SISFO

“Menjadi unit pengelola teknologi informasi, komunikasi dan sistem informasi dengan memberikan ide dan layanan yang menginspirasi untuk mendukung tercapainya Universitas Telkom menjadi perguruan tinggi berkelas dunia “

Misi Direktorat SISFO

a. Menyediakan sarana dan prasarana layanan teknologi informasi dengan keberfungsian layanan yang handal bagi seluruh sivitas akademik Universitas Telkom.
b. Membangun dan mengelola layanan sistem informasi terintegrasi dengan sistem basis data, arsitektur, infrastruktur dan *framework* yang dibangun sebagai nilai tambah dan kompetensi unggulan Universitas Telkom.

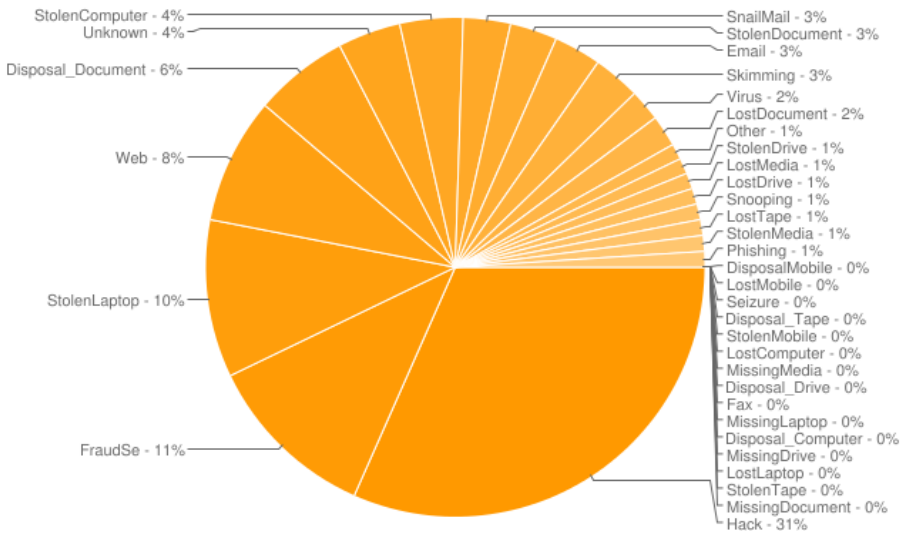
Direktorat SISFO sebagai unit yang mengelola dan menerapkan Teknologi Informasi dan Komunikasi (TIK) di Universitas Telkom dan telah merilis sistem informasi terintegrasi yaitu iGracias di URL http://igracias.telkomuniversity.ac.id. iGracias adalah sistem informasi terintegrasi Universitas Telkom kegiatan akademik dan non akademik (SDM, keuangan, dan lain-lain) sesuai dengan status fungsional maupun struktural pegawai (Is.telkomuniversity.ac.id, 2015).

1.2 Latar Belakang Penelitian

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan disetiap instansi penyelenggaraan pelayanan publik, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) (Panduan Penerapan Tata Kelola Keamanan Informasi, 2011).

Perguruan tinggi atau universitas sebagai salah satu instansi penyelenggaraan pelayanan publik juga diminta memberikan pelayanan terbaik untuk pihak yang membutuhkan informasi, seperti mahasiswa, karyawan, ataupun pihak lainnya. Oleh karena itu, perguruan tinggi membentuk suatu divisi khusus yang melayani sistem manajemen informasi dan layanan interkoneksi universitas. Namun dalam hal ini, informasi menjadi aset penting karena selain bersifat rahasia, informasi juga memiliki risiko dari akses tidak sah, modifikasi data, pencurian data, *human error*, kerusakan perangkat keras dan perangkat lunak, maupun risiko dari bencana alam (Darmawan dan Fauzi, 2013:243).

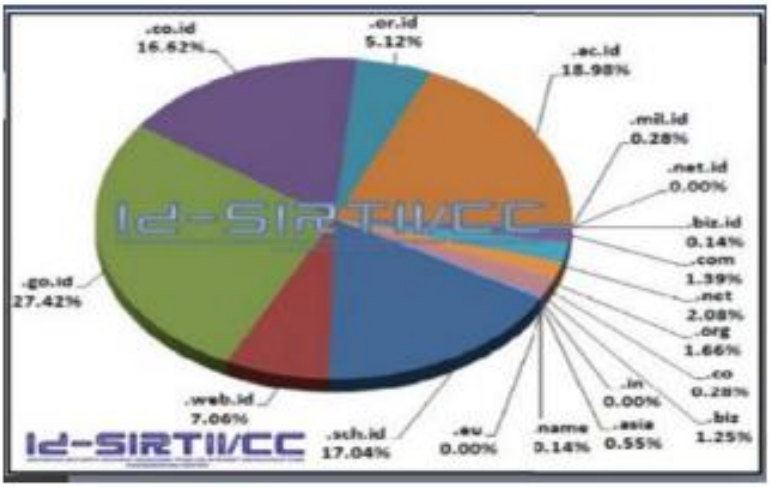
Berdasarkan data dari *Data Loss DB* sampai dengan bulan Oktober 2015 tercatat telah terjadi 1.416 insiden terkait dengan keamanan informasi pada organisasi swasta maupun pemerintah, 12% dari insiden tersebut terjadi pada sektor pendidikan. Terlihat *hack*, *fraud*, pencurian komputer dan laptop, dan insiden yang berkaitan dengan pembuangan dokumen dan serangan web mendapat persentase lebih besar dibandingkan yang lainnya (Datalossdb.org, 2015).



Gambar 1.1 Tipe dari Insiden

(*Sumber : Datalossdb.org, 2015*)

Dalam Candiwan *et al.* (2015) menjelaskan bahwa berdasarkan survei yang dilakukan oleh *Open Security Foundation* tahun 2014 menyebutkan bahwa 35% dari pelanggaran keamanan terjadi pada perguruan tinggi. Institusi pendidikan menjadi target dari *hacker* karena institusi merupakan sebuah gudang data dari data-data pribadi. Dan juga berdasarkan data dari id-SIRTII, pada gambar 1.2 menjelaskan bahwa situs akademik mengalami 18,98% serangan pada tahun 2013.



Gambar 1.2 Serangan Situs di Indonesia

(*Sumber : Id-SIRTII, dalam Candiwan, 2015*)

Berita dari *Security Intelligence* menyebutkan bahwa 95% dari semua insiden keamanan disebabkan oleh *human error*, penyebab berhasilnya insiden yang berasal dari luar organisasi adalah adanya peluang secara sadar atau tidak yang disediakan oleh orang dalam organisasi sehingga menyebabkan adanya kemungkinan untuk akses dari orang luar (Securityintelligence.com, 2014).

Survei yang dilakukan oleh *Computer Security* menemukan bahwa 49% responden menghadapi insiden keamanan yang disebabkan oleh tindakan pengguna yang sah, proporsi kejahatan komputer yang dilakukan oleh karyawan diperkirakan mencapai 81%. Ancaman yang dilakukan oleh pihak internal dinilai berpotensi lebih serius dibandingkan pihak eksternal dikarenakan pengetahuan pihak internal lebih mendalam mengenai perusahaan (McLeod, 2008:274).

Berdasarkan survei yang dilakukan oleh *Verizon* selama sepuluh tahun terakhir menyimpulkan bahwa tiga jenis insiden yang terjadi dalam bidang pendidikan yaitu *miscellaneous errors* (20%), *web app attacks* (20%), dan *physical theft/loss* (19%) (Verizon, 2014). Data dari Owasp.org menyebutkan bahwa survei yang dilakukan mengenai kerugian biaya yang disebabkan kehilangan data pada sektor pendidikan mencapai $112 juta pada tahun 2011 (Owasp.org, 2011).

Beberapa kasus *hacking* yang terjadi dibeberapa situs perguruan tinggi di Indonesia sehingga situs tersebut mengalami gangguan dalam pelayanannya. Salah satu situs fakultas di Universitas Diponegoro yang beralamat fisip.undip.ac.id juga mengalami gangguan *hacking*, gangguan juga terjadi pada situs yang beralamat siskom.undip.ac.id (Techno.okezone.com, 2009). Tahun 2012, situs Universitas Indonesia yang dengan alamat ui.ac.id mengalami gangguan dikarenakan telah di-*hack* oleh AL3X 0WN5 (Suma.ui.ac.id, 2012). Pada tahun yang sama, 20 situs berdomain unri.ac.id mengalami *hacking* oleh *hacker* yang mengatasnamakan slumd0g. Tahun 2013, situs UNM mengalami gangguan berdasarkan postingan dalam Lpmprofesi (Profesi-unm.com, 2013) menjelaskan bahwa telah terjadi *hacking* pada situs resmi UNM. Dan pada tahun yang sama, situs official FEB UNPAD mengalami gangguan karena telah di*hacking* oleh *hacker* yang mengatasnamakan *HackedBy@znuneqvxn (*fe.unpad.ac.id, *2013).* Dan kasus

terbaru, pada tahun 2015 situs Universtas Islam Jember yang beralamat *uij.ac.id* juga mengalami gangguan yang dilakukan oleh *Muslim Cyber Corp.*

Di Universitas Telkom juga pernah terjadi penyerangan terhadap beberapa subdomain situs milik Universitas Telkom, berdasarkan berita yang diposting oleh Students.telkomuniversity.ac.id pada 24 Desember 2015, diketahui beberapa subdomain dari Telkomuniversity.ac.id telah diretas oleh oknum yang mengatasnamakan *"Ghost Louay",* dan salah satu subdomain tersebut adalah website sistem informasi (Students.telkomuniversity.ac.id, 2015). Dan dari hasil observasi diawal penelitian ditemukan manajemen aset yang kurang baik, seperti sistem kabel yang masih berantakan dan CCTV belum menyala di ruang resepsionis.

Mengingat pentingnya informasi dan adanya kemungkinan risiko terjadi gangguan, perguruan tinggi perlu untuk melakukan kegiatan tata kelola keamanan informasi dilingkungannya. Salah satu standar yang dapat digunakan untuk menganalisa tingkat keamanan informasi di organisasi adalah standar ISO/IEC 27001 sesuai dengan insiden yang banyak terjadi berkaitan dengan bidang pendidikan. Pengukuran tingkat keamanan informasi diperlukan untuk menganalisa sejauh mana perguruan tinggi telah mengamankan informasi dilingkungannya. Dari analisa tingkat keamanan, sehingga dapat melakukan evaluasi dan perancangan ataupun pembaharuan sistem manajemen keamanan informasi di perguruan tinggi.

Dalam jurnal internasional *Information Security Management System Standards : A Comparative Study of Big Five*, Susanto *et al.* (2011) menjelaskan bahwa ISO/IEC 27001 menjadi *framework* yang paling banyak digunakan dengan persentase 27% dibandingkan 4 *framework* lainnya, yaitu COBIT (26%), ITIL (8%), BS7799 (18%) dan PCIDSS (21%). ISO/IEC 27001 dapat digunakan untuk semua tipe organisasi. Penggunaan standar ISO/IEC 27001 karena standar yang fleksibel dan dapat disesuaikan dengan kebutuhan dan tujuan dari organisasi. Menurut Widodo *et al.* (2013) penggunaan ISO/IEC 27001 disebabkan karena sangat fleksibel dikembangkan karena pemanfaatan standar sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan

jumlah pegawai dan ukuran struktur oganisasi. Serta untuk mengukur sejauh mana setiap kontrol dilakukan oleh perguruan tinggi dapat dilakukan pengukuran tingkat kematangan untuk setiap kontrol. Pengukuran tingkat kematangan akan dilakukan dengan menggunakan SSE-CMM (*Systems Security Engineering Capability Maturity Model*).

1.3 Perumusan Masalah

Berdasarkan latar belakang penelitian maka dapat dirumuskan masalah yang akan diteliti lebih lanjut dalam penelitian, yaitu :

a. Bagaimana tingkat keamanan informasi terkait dengan Kebijakan Keamanan Informasi, Manajemen Aset, Kontrol Akses, Keamanan Fisik dan Lingkungan, Keamanan Operasional dan Keamanan Komunikasi pada Universitas Telkom berdasarkan standar ISO/IEC 27001.
b. Bagaimana alur kegiatan dan aliran data sistem manajemen keamanan informasi.

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah maka tujuan penelitian, yaitu :

a. Menganalisis tingkat keamanan informasi terkait dengan Kebijakan Keamanan Informasi, Manajemen Aset, Kontrol Akses, Keamanan Fisik dan Lingkungan, Keamanan Operasional dan Keamanan Komunikasi pada Universitas Telkom berdasarkan standar ISO/IEC 27001.
b. Menganalisis alur kegiatan dan merancang aliran data sistem manajemen keamanan informasi.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian, yaitu :

a. Menambah wawasan untuk bidang keilmuan manajemen bisnis, khususnya untuk manajemen informasi.
b. Menjadi referensi untuk penelitian berikutnya.

c. Sebagai referensi untuk meningkatkan keamanan sistem informasi khususnya sistem informasi Universitas Telkom.
d. Sebagai bahan pertimbangan dalam mengembangan keamanan sistem informasi.

1.6 Ruang Lingkup dan Objek Penelitian

Adapun ruang lingkup dan objek penelitian ini, yaitu :

a. Analisis sistem manajemen keamanan informasi pada Universitas Telkom menggunakan standar ISO/IEC 27001.
b. Penelitian ini hanya difokuskan pada klausul A.5 Kebijakan Keamanan Informasi, A.8 Manajemen Aset, A.9 Kontrol Akses, A.11 Keamanan Fisik dan Lingkungan, A.12 Keamanan Operasional dan A.13 Keamanan Komunikasi
c. Penilaian klausul menggunakan *maturity level* dengan metode SSE-CMM.
d. Narasumber penelitian yaitu staff SISFO atau pihak-pihak yang terlibat langsung dengan Sistem Informasi Universitas Telkom.
e. Data yang digunakan dalam penelitian ini adalah data primer yang dikumpulkan dengan metode kuesioner, wawancara dan observasi dan data sekunder yang berhubungan dengan penelitian yang didapatkan dari informan penelitian.
f. Hasil tabulasi data akan dilakukan *gap analysis.*

1.6.1 Lokasi dan Objek Penelitian

Lokasi dari penelitian adalah di kampus Universitas Telkom di Jl. Telekomunikasi Terusan Buah Batu Dayeuh Kolot Bandung. Dengan objek penelitiannya adalah Direktorat SISFO.

1.6.2 Waktu dan Periode Penelitian

Waktu pelaksanaan penelitian adalah bulan September 2015-Mei 2016.

1.7 Sistematika Penulisan Tugas Akhir

BAB I PENDAHULUAN

Bab ini berisi tentang gambaran umum objek penelitian, latar belakang, perumusan masalah, tujuan, manfaat, ruang lingkup dan objek penelitian, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA DAN LINGKUP PENELITIAN

Bab ini berisi tentang tinjauan pustaka yaitu penelitian-penelitian terdahulu yang pernah membahas mengenai permasalah yang sama atau serupa dan teori-teori yang berhubungan dengan penelitian yang diperlukan dalam analisis data.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang metode penelitian yang digunakan, teknik pengumpulan data, populasi dan sampel, dan teknik analisis.

BAB IV ANALISIS DAN PEMBAHASAN

Bab ini menjelaskan tentang pembahasan yang berisi data-data yang telah dikumpulkan, diolah dan kemudian mendapatkan solusi dari permasalahan yang sedang dihadapi.

BAB V KESIMPULAN DAN SARAN

Bab ini akan berisi kesimpulan dari hasil pembahasan, memberikan masukan atau saran yang dapat diimplementasikan oleh organisasi.