BAB 1 PENDAHULUAN

1.1. Latar Belakang

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di perusahaan mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola perusahaan yang baik. Dalam penyelenggaran tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability). [4]

Sepertinya halnya sebuah perusahaan yang menerapkan tata kelola Teknologi Informasi dan Komunikasi (TIK), perguruan tinggi di Bandung pun memerlukan Teknologi Informasi dalam rangka pengelolaan fasilitas penunjang kegiatan akademik mahasiswa. Salah satu fasilitas penunjang kegiatan akademik mahasiswa adalah layanan sistem informasi akademik (SIA). Fasilitas ini merupakan layanan yang bersifat vital karena didalamnya terdapat data mahasiswa, dosen, dan data-data penting lainnya.Data-data tersebut merupakan data yang amat penting oleh karena itu diperlukan suatu kebijakan dari pihak perguruan tinggi tersebut tentang pengamanan data tersebut agak tidak sampai bocor ke pihak luar. Audit Keamanan sistem informasi diperlukan untuk memastikan bahwa kebijakan mengenai keamanan sistem informasi akademik (SIA) di perguruan tinggi tersebut sudah sesuai dengan prosedur yang berlaku.

Salah satu perguruan tinggi yang menerapkan Sistem Informasi Akademik (SIA) adalah Sekolah Tinggi Farmasi Bandung (STFB).STFB dipilih sebagai tempat penelitian tugas akhir karena Layanan Sistem Informasi Akademik (SIA) adalah sistem yang baru dibuat 2 tahun terakhir dan belum pernah dilakukannya Audit keamanan terhadap sistem informasi tersebut dan setelah melakukan wawancara awal ke pihak STFB ternyata sistem informasi mereka sudah berhasil ditembus oleh mahasiswa yang ingin merekayasa nilai mata kuliah. Mahasiswa tersebut menembus sistem informasi dan mengubah nilai mata kuliah tertentu sehingga nilai mata kuliah mahasiswa tersebut menjadi lebih baik dari sebelumnya. Hal ini membuat pihak STFB ingin mendapatkan masukan dari berbagai pihak soal bagaimana cara untuk menjaga keamanan sistem informasi mereka

Pada tugas akhir ini akan dilakukan audit Keamanan Sistem Informasi berbasisrisiko dengan menggunakan Standar ISO 27001. Standar ISO 27001 adalah standar yang biasa digunakan untuk mengaudit keamanan sistem informasi dan digunakan untuk menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil dari audit keamanan sistem informasi STFB .Selain itu juga hasil audit akan.Menggambarkan tingkat kematangan, tingkat kelengkapan penerapan ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di STFB dengan menggunakan Capability Maturity Model for Integration (CMMI)

Standar ISO 27001 sendiri dipilih karena ISO 27001 dapat diterapkan pada semua jenis organisasi baik instansi pemerintah maupun swasta [9] sedangkan standar lainnya yaitu standar COBIT lebih banyak diterapkan pada perusahaan-perusahaan besar.ISO 27001 juga lebih fleksibel untuk dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi dan persyaratan keamanan, proses bisnis dan jumlah pegawai dan ukuran struktur organisasi [4]. ISO 27001 dipilih sebagai metode penelitian dibandingkan dengan metode COBIT karena di dalam kerangka kerja COBIT hanya memberikan bantuan kontrol dalam mengendalikan pengelolaan TI namun COBIT tidak memberikan panduan implementasi operasional sedangkanISO 27001 memberikan panduan dalam aspek teknis secara detail mengenai implementasi operasional

1.2. Rumusan Masalah

Berdasarkan pada latar belakang yang dipaparkan di atas , terdapat beberapa masalahyang dapat dirumuskan sebagai berikut :

1. Bagaimana melakukan audit keamanan sistem informasi di STFB Bandung dengan menggunakan standar SNI ISO 27001:2009 terhadap faktor keamanan informasi CIA (*Confidentiality,Integrity* dan *Availability*) ?
2. Bagaimana saran dan perbaikan yang mendukung pengelolaan sistem keamanan informasi di STFB?

Adapun batasan masalah yang ada adalah :

1. Analisis, penilaian dan identifikasi risiko dilakukan dengan menfokuskan pada penerapan SI/TI dalam hal pengelolaan Keamanan Sistem Informasi Akademik (SIA) STFB Bandung
2. Data acuan yang digunakan adalah data yang berasal dari hasil wawancara, observasi dan Questioner yang dilakukan
3. Tidak semua Kontrol keamanann yang terdapat didalam SNI ISO 27001:2009 digunakan dalam penelitian. Penentuan Kontrol keamanan disesuaikan dengan hasil analisis risiko dan hasil diskusi dengan pihak STFB
4. Hasil audit berupa temuan ataupun rekomendasi yang akan diserahkan kepada pihak manajemen STFB untuk ditindaklanjuti dikemudian hari
5. Data di lampiran B yaitu questioner identifikasi kelemahan dan ancaman aset hanya berasal dari data selama 1 bulan operational yaitu bulan January 2016.

1.3. Tujuan

1. Melakukan Audit terhadap keamanan sistem informasi STFB Bandung dengan menggunakan SNI ISO 27001:2009 berbasis risiko sebagai bahan referensi penentuan kebijakan pengelolaan keamanan informasi Sistem Informasi Akademik (SIA) STFB ke depannya

2. Menyusun hasil audit keamanan sistem informasi Akademik STFB dengan melakukan evaluasi terhadap kendala dan bukti yang ada, mendokumentasikan temuan audit dalam rangka pembuatan laporan audit.
3. Menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di STFB dengan menggunakan Capability Maturity Model for Integration (CMMI)

1.4. Manfaat Penelitian

Setelah melakukan penelitian dengan menggunakan ISO 27001 sebagai standar keamanan informasimaka hasil audit dapat digunakan oleh pihak management STFB sebagai bahan referensi untuk memastikan bahwa sistem informasi akademik STFB telah dikelola dengan efektif dan efisien. Hasil audit juga dapat digunakan oleh pihak management STFB sebagai dokumentasi pengembangan sistem informasi yang sudah ada ke depannya.

1.5. Metodologi Penyelesaian Masalah

Metodologi yang digunakan untuk penyelesaian study kasus di atas adalah sebagai berikut :

1. Studi Literatur

Pencarian literature berupa jurnal, paper dan makalah, baik secara online maupun offline.Literature yang di cari adalah yang berhubungan denganSMKI, Teknologi informasi, ISO 27001, audit berbasis risiko.

2. Penelitian

Pada tahap ini penulis melakukan penelitian dengan melakukan pemgumpulan data yang dibutuhkan berasal dari STFB Bandung melalui hasil wawancara, observasi dan questioner yang diberikan pada pegawai

3. Analisis

Melakukan analisis dari data yang telah didapat untuk kemudian dilakukan pengukuran tingkat kematangan, tingkat kelengkapan penerapan ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di STFB Bandung dengan menggunakan Capability Maturity Model for Integration (CMMI)

4. Pengambilan kesimpulan dan penulisan laporan tugas akhir

Mengambil kesimpulan dari hasil analisis dan menuliskan hasil penelitian ke dalam laporan tugas akhir

1.6. Sistematika Penulisan

Tugas akhir ini di susun dengan sistematika berikut :

1. BAB 1 Pendahuluan
   a. Latar Belakang
   b. Perumusan Masalah
   c. Batasan Masalah
   d. Tujuan
   e. Metode Penelitian
   f. Sistematika Penulisan

2. BAB 2 Landasan Teory
   Bab ini membahas teory-teory mengenai Teknologi Informasi, SMKI, ISO 27001, Risk Management, *CMMI*

3. BAB 3 Metodology dan Implementasi Penelitian
   Bab ini membahas tentang metodology yang digunakan saat penelitian

4. BAB 4 Analisis Penelitian
   Pada bab ini berisikan tentang analisa dari data yang telah didapat pada saat tahap pengumpulan data

5. BAB 5 Kesimpulan dan saran
   Berisi Kesimpulan dan saran dari Tugas Akhir.