

# BAB I

## PENDAHULUAN

Dalam bab ini akan dijelaskan latar belakang masalah yang terdapat dalam audit keamanan system informasi manajemen kampus UPH Surabaya yang mendasari pembuatan tugas akhir ini serta dijelaskan pula mengenai batasan masalah yang digunakan.

### 1.1 Latar Belakang

Universitas Pelita Harapan Surabaya adalah salah satu perguruan tinggi swasta Kristen yang berlokasi di Jl. A. Yani No. 288, *City of Tomorrow* (CiTo) Superblock, Surabaya. Universitas Pelita Harapan Surabaya memiliki komitmen menjadi *noble industry* dalam bidang pendidikan. Komitmen ini direfleksikan dalam manajemen yang profesional, fakultas yang berkualitas tinggi, kurikulum dan fasilitas.

Universitas Pelita Harapan menekankan pendidikan yang seimbang dan terintegrasi, mencakup bidang seni, ilmu pengetahuan dan teknologi, serta nilai-nilai spiritual yang kuat. Untuk dapat menyelenggarakan pendidikan yang berkualitas tentu saja harus didukung oleh fasilitas yang memadai. Salah satunya adalah fasilitas sistem informasi untuk mengelola data-data seperti data mahasiswa, alumni, keuangan, akademik, dan lainnya. UPH Surabaya telah menerapkan Sistem Informasi Manajemen Kampus menggunakan aplikasi bernama *Menu Maker* yang telah dibangun dan dikembangkan internal UPH Surabaya di mana semua proses bisnis saling terhubung satu sama lain yang mana aktifitasnya dimulai dari pendaftaran mahasiswa, penjadwalan perkuliahan, penyimpanan data nilai, keuangan hingga mahasiswa dinyatakan lulus dan menjadi alumni.

Untuk mengetahui kinerja penerapan *Menu Maker* ini selain dilakukan *testing* terhadap sistem *Menu Maker* seiring dengan semakin berkembangnya aplikasi IT dan kebutuhan bisnis maka diperlukan pula audit keamanan sistem informasi menggunakan standar ISO 27001. Audit ini dilakukan untuk memastikan bahwa keamanan informasi telah diterapkan sesuai dengan prosedur

yang ada. Keamanan informasi yang ditujukan untuk menjaga aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*), dan ketersediaan (*Availability*) dari Informasi (ISO 27001 dalam Sarno dan Iffano, 2009:46).

Menurut Sarno dan Iffano (2009: 46) bahwa syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan sistem manajemen keamanan informasi dijelaskan dengan terinci dalam ISO 27001 tahun 2005. Kelebihan lain dari standar ISO 27001 dibandingkan COBIT dalam hal keamanan informasi menurut Jogiyanto dan Abdillah (2011:161) adalah ISO 27001 bersifat lebih rinci dan menyediakan petunjuk struktur dan konten kebijakan keamanan informasi. Bahkan dikatakan ISO 27001 bersifat teknis sehingga ISO cenderung menjadi pilihan bagi manajer TI dan manajer keamanan informasi. Oleh karena itu, dalam Tugas Akhir ini standar ISO/IEC 27001:2005 digunakan sebagai standar pelaksanaan audit keamanan Sistem Informasi Manajemen Kampus pada UPH Surabaya.

Diharapkan melalui Tugas Akhir audit keamanan Sistem Informasi Manajemen Kampus ini maka UPH Surabaya dapat mengukur tingkat keamanan serta dapat mengukur prosedur keamanan informasi yang ada. Selain itu dengan cara mengukur atau menentukan tingkat kedewasaan Sistem Manajemen Keamanan Informasi (SMKI), sehingga akan menentukan apakah SMKI yang diterapkan sesuai dengan hasil yang diharapkan. Hasil yang didapat diharapkan dapat menjadi rekomendasi yang dapat digunakan untuk meningkatkan keamanan informasi UPH Surabaya.

## **1.2 Perumusan Masalah**

Berdasarkan penjelasan pada latar belakang, maka perumusan masalah yang di dapat adalah sebagai berikut:

1. Bagaimana membuat perencanaan audit keamanan sistem informasi pada UPH Surabaya menggunakan standar ISO/IEC 27001:2005 ?
2. Bagaimana melaksanakan audit keamanan sistem informasi pada UPH Surabaya menggunakan standar ISO/IEC 27001:2005 ?
3. Bagaimana menyusun hasil audit keamanan sistem informasi pada UPH Surabaya menggunakan standar ISO/IEC 27001:2005 ?

### 1.3 Pembatasan Masalah

Batasan-batasan masalah yang digunakan dalam pengerjaan tugas akhir ini adalah sebagai berikut:

1. Klausul ISO/IEC 27001:2005 yang digunakan adalah:
  - a. Klausul 5 : Kebijakan Keamanan
  - b. Klausul 6 : Organisasi Keamanan Informasi
  - c. Klausul 7 : Manajemen Aset
  - d. Klausul 8 : Manajemen Sumber Daya Manusia
  - e. Klausul 9: Keamanan Fisik dan Lingkungan
  - f. Klausul 10 : Manajemen Komunikasi dan Operasi
  - g. Klausul 11: Kontrol Akses
  - h. Klausul 12 : Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan
  - i. Klausul 13: Manajemen Kejadian Keamanan Informasi
2. Sistem Informasi yang di audit adalah Sistem Informasi Manajemen Kampus yang dimiliki UPH Surabaya yang terletak di Jl. A. Yani No. 288, *City of Tomorrow* (CiTo) Superblock, Surabaya.

### 1.4 Tujuan

Berdasarkan perumusan masalah di atas, maka tujuan yang hendak dicapai adalah sebagai berikut:

1. Melakukan dan menghasilkan perencanaan audit keamanan sistem informasi pada UPH Surabaya menggunakan standar ISO/IEC 27001:2005 yang terdiri dari menentukan ruang lingkup, mengumpulkan data dan menentukan langkah-langkah pelaksanaan audit.
2. Melaksanakan audit keamanan sistem informasi pada UPH Surabaya menggunakan standar ISO/IEC 27001:2005 dengan menganalisa hasil wawancara sehingga didapatkan temuan-temuan audit serta dapat mengukur *maturity level*.
3. Menyusun hasil audit keamanan sistem informasi pada UPH Surabaya menggunakan standar ISO/IEC 27001:2005 dengan melakukan evaluasi dari bukti-bukti yang ada, mendokumentasikan temuan audit dan didapat laporan hasil audit yang berupa temuan, kesimpulan dan rekomendasi.

## 1.5 Sistematika Penulisan

Di dalam penyusunan tugas akhir ini, secara sistematika diatur dan disusun dalam lima bab, yaitu:

### **BAB I : PENDAHULUAN**

Pada Bab ini dibahas tentang latar belakang masalah, rumusan masalah, serta batasan terhadap masalah yang akan dibahas, tujuan dari pembahasan masalah yang diangkat, dan sistematika penulisan laporan Tugas Akhir ini.

### **BAB II : LANDASAN TEORI**

Pada Bab ini dibahas tentang teori-teori yang berkaitan dengan audit sistem informasi, diantaranya yakni penjelasan tentang Audit, Audit Sistem Informasi, Keamanan Informasi, Sistem Informasi, Manajemen Aset, ISO/IEC 27001:2005

### **BAB III : METODE PENELITIAN**

Pada Bab ini berisi uraian tentang UPH Surabaya serta penjelasan mengenai langkah-langkah yang dilakukan dalam Audit Keamanan Sistem Informasi Manajemen Kampus yang meliputi ruang lingkup dan tujuan audit, pengumpulan bukti, pelaksanaan uji kepatutan, penentuan tingkat kematangan, penentuan hasil audit serta penyusunan laporan akhir hasil audit keamanan Sistem Informasi Manajemen Kampus.

### **BAB IV : HASIL DAN PEMBAHASAN**

Pada Bab ini dibahas tentang analisa dan evaluasi hasil temuan serta rekomendasi dari kegiatan audit keamanan Sistem Informasi Manajemen Kampus di UPH Surabaya.

### **BAB V : PENUTUP**

Pada Bab ini berisikan kesimpulan penelitian yang telah dilakukan terkait dengan tujuan dan permasalahan yang ada, serta saran sehubungan dengan adanya kemungkinan pengembangan sistem pada masa yang akan datang.