BAB 1
PENDAHULUAN

Pada bab ini menjelaskan tentang pandangan awal persoalan yang terjadi dalam penulisan laporan tugas akhir, berisi latar belakang, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi tugas akhir dan sistematika tugas akhir.

1.1 Latar Belakang

Pemanfaatan teknologi informasi untuk mendukung kegiatan operasional terutama salah satunya pada proses bisnis sebuah organisasi baik dalam skala kecil maupun besar, banyak mengalami perkembangan dan perubahan terutama pada bidang teknologi informasi. Dengan perkembangan tersebut yang semakin hari semakin meningkat. Perguruan tinggi sebagai sebuah instansi atau organisasi yang bergerak di bidang pendidikan, dengan teknologi informasi tersebut memungkinkan untuk instansi tersebut meningkatkan layanan-layanannya. Sebuah aset TI tentu memiliki risiko keamanan, yaitu salah satunya risiko keamanan informasi dari infrastruktur TI yang dibangun dan telah menjadi aset instansi atau organisasi. Maka dari itu perlu dilakukannya penilaian risiko keamanan informasi dengan cara mengidentifikasi dan mengukur dampak kegagalan infrastruktur TI terhadap tingkat kegagalan TI. Karena perkembangan teknologi informasi yang cepat membuat akan aset TI dan infrastrukturnya semakin rentan keamanan informasinya, khususnya pada salah satu *core* instansi atau organisasi pada bidang pendidikan yaitu pada proses bisnis akademik.

Universitas Pasundan merupakan instansi atau organisasi yang bergerak dibidang pendidikan turut serta berupaya dalam meningkatkan kualitas pendidikan. Fakultas teknik adalah salah satu dari beberapa fakultas yang ada di Universitas Pasundan yang telah mengimplementasikan layanan-layanan berbasis TI dengan aset-aset penunjang teknologi informasi tersebut. Maka dari itu penilaian risiko keamanan informasi terhadap aset TI yang teregister merupakan komponen yang penting bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi. Keamanan informasi tidak bisa hanya disandarkan pada *tools* atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi. Informasi adalah aset sebuah organisasi, seperti aset bisnis penting lainnya yang merupakan *core* utama dari sebuah organisasi, dan mempunyai konsekuensi jika tidak dilindungi secara tepat. Hal ini sangat penting dalam meningkatnya lingkungan bisnis yang terinterkoneksi. Peningkatan bisnis yang terinterkoneksi, meningkatkan pula ancaman dan *vulnerabilities* sistem informasi dan jaringan. Untuk itu butuh pengelolaan keamanan informasi yang sistemik dan komprehensif.

Organisasi perlu mengidentifikasi, mengukur, mengevaluasi, dan mengatur seluruh kegiatannya agar berfungsi dengan efektif. Tujuan dari penelitian ini yaitu mengidentikasi dan mengukur risiko keamanan informasi pada proses bisnis akademik di fakultas teknik universitas

pasundan, agar dapat mengantisipasi, mencegah, dan membantu memperkirakan risiko apa saja yang kemungkinan muncul. Berdasarkan latar belakang tersebut, penulis mencoba meneliti dengan penilaian risiko keamanan informasi dengan menggunakan pendekatan standar ISO 27001:2005. Karena ISO 27001:2005 merupakan standar Internasional yang mengadopsi pendekatan proses untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan perbaikan sistem managemen keamanan informasi suatu organisasi.

Proses identifikasi risiko yang akan dilakukan berbasis pada aset teknologi informasi yang telah disusun sesuai dengan standar ISO 27001:2005. Sedangkan, untuk proses penilaian risiko akan digunakan metode kuantitatif FMEA *(Failure Modes and Effects Analysis*) yang mempertimbangkan probabilitas, akibat, dan keterkaitan dengan kontrol risiko yang ada agar lebih obyektif serta akurat dalam menentukan level risiko. Dengan demikian, penentuan level risiko tersebut akan mempermudah perusahaan dalam mendefinisikan aksi-aksi penangan risiko dengan tepat.

1.2 Identifikasi Masalah

Berdasarkan dari latar belakang yang telah dipaparkan sebelumnya, maka yang menjadi permasalahan adalah sebagai berikut :

1. Bagaimana risiko pada setiap aset TI yang terlibat dari proses bisnis akademik terkait keamanan informasinya ?
2. Bagaimana mengetahui nilai risiko keamanan dari setiap aset TI sesuai dengan tingkatan risikonya terkait keamanan informasinya pada proses bisnis akademik ?
3. Bagaimana pengendalian terhadap risiko keamanan informasi yang ada dari setiap aset TI yang terlibat pada proses bisnis akademik ?

1.3 Tujuan Tugas Akhir

Berdasarkan identifikasi masalah yang telah dipaparkan sebelumnya, maka yang menjadi tujuan dalam tugas akhir ini yaitu :

1. Mengidentifikasi setiap aset TI yang terlibat pada proses bisnis akademik dengan risiko keamanan informasi yang ada.
2. Menilai risiko keamanan infomasi dari setiap aset TI yang terlibat serta berpotensial dan berpengaruh terhadap keamanan informasi pada proses bisnis akademik.
3. Menentukan kendali usulan untuk pengendalian risiko keamanan informasi dari setiap aset TI yang terlibat pada proses bisnis akademik.

.

1.4 Lingkup Tugas Akhir

Dari hasil analisa, persoalan yang dihadapi sangat kompleks, maka penulis membatasi persoalan sebagai berikut :

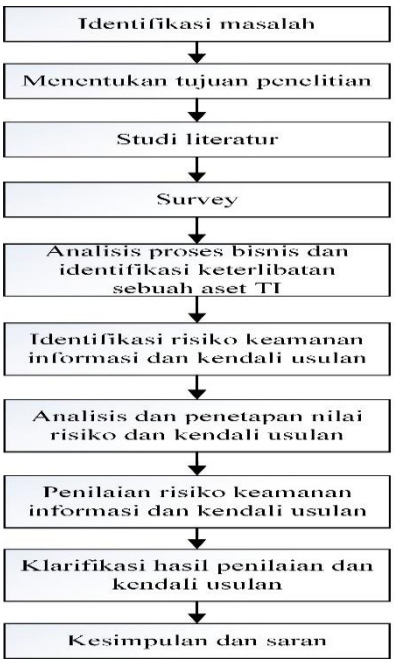
1. Proses bisnis akademik yang diteliti yaitu pada prosedur perwalian dan perkuliahan.

2. Identifikasi risiko setiap aset TI, yaitu pada data dan *database*, SDM, *software*, *hardware*, dan *network*.
3. Objek penelitian pada SDM antara lain PUSDATIN, SBAP, Staf DHMD, dosen, mahasiswa aktif dan aset TI yang *teregister* dan terlibat.
4. Penelitian menggunakan pendekatan standar ISO 27001:2005
5. Metode penilaian risiko keamanan informasi pada penelitian ini menggunakan metode FMEA (*Failure Mode and Effect Analysis*).
6. Menentukan nilai risiko dan ancaman berdasarkan aspek keamanan *confidentiality*, *integrity*, *availability*. Serta dampak kegagalan infrastruktur TI berdasarkan tingkat kegagalan TI untuk mengetahui risiko keamanan informasi pada proses bisnis akademik di Fakultas Teknik Universitas Pasundan.

1.5 Metodologi Tugas Akhir

Metodologi merupakan kerangka dasar dari tahapan penyelesaian tugas akhir. Metodologi penulisan pada tugas akhir ini mencakup semua kegiatan yang dilaksanakan untuk memecahkan masalah atau melakukan proses analisa terhadap permasalahan tugas akhir. Dalam tugas akhir ini, analisa yang dilakukan adalah tentang penilaian risiko keamanan informasi pada proses bisnis akademik FT UNPAS dengan mengidentifikasi setiap aset TI yang terlibat yang meliputi aktivitas akademik pada perwalian dan perkuliahan.

Berikut ini merupakan metodologi penelitian tugas akhir yang digunakan dalam penilaian risiko keamanan informasi pada proses bisnis akademik yang meliputi beberapa metode penelitian, metode penelitian ini dapat dilihat pada gambar 1.1 dibawah ini.



Gambar 1.1. Metodologi Tugas Akhir

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah metode deskriptif, yaitu metode yang menggambarkan suatu keadaan atau permasalahan yang sedang terjadi berdasarkan fakta dan data-data yang diperoleh dan dikumpulkan pada waktu melaksanakan penelitian. Adapun teknik pengumpulan data dilakukan dengan cara sebagai berikut :

1. Identifikasi masalah

   Menentukan dan menetapkan masalah apa yang akan di identifikasi terlebih dahulu untuk penelitian
2. Menentukan tujuan penelitian

   Merumuskan, menentukan, dan menetapkan tujuan pada penelitian yang dilakukan, berdasarkan identifikasi masalah.
3. Studi literatur (*Library Research*)

   Yaitu mempelajari tentang identifikasi setiap aset dan penilaian risiko keamanan informasi, proses bisnis, dan panduan SNI ISO 27001 : 2005, serta materi-materi yang berkaitan dengan manajemen keamanan informasi dan layanan proses bisnis dengan pemanfaatan teknologi informasi. Dengan membaca dan mempelajari *literature, journal, whitepaper*, buku, artikel-artikel, *ebook* atau melakukan *browsing* dari media internet yang berhubungan dengan masalah yang diteliti.
4. *Survey*

   Yaitu melakukan survey untuk melihat fakta di lapangan untuk mengumpulkan dan mendapatkan data untuk bahan penelitian.
5. Analisis proses bisnis dan identifikasi keterlibatan setiap aset TI

   Yaitu menganalisis proses bisnis akademik pada perwalian dan perkuliahan, dan mengidentifikasi keterlibatan setiap aset TI, yang dimana penelitian ini akan berfokus kepada aset SDM, dan aset TI. Aset SDM yang dimaksudkan adalah pengguna dan pengelola TI terkait, dan aset TI yang dimaksudkan adalah data dan *database, hardware, software*, dan *network.*
6. Identifikasi risiko keamanan informasi dan kendali usulan

   Yaitu mengidentifikasi risiko keamanan dengan metode-metode, observasi, wawancara, dan kuisioner. Untuk menentukan variable risiko aset TI berdasarkan ancaman, kelemahan atau ganguan apa saja pada setiap aset TI, dan kendali usulan berdasarkan klausul atau anek ISO 27001:2005

1.5.2 Metode Analisis dan Penilaian Risiko Keamanan Informasi

Pada metode analisis dan penilaian risiko keamanan informasi ini menjelaskan mengenai metodologi penulisan laporan tugas akhir yang dilakukan penulis. Adapun penjelasan alur penulisan yang dilakukan adalah sebagai berikut :

1. Analisis dan penetapan nilai risiko dan kendali usulan

   Yaitu melakukan analisis penetapan nilai risiko setiap aset TI berdasarkan kerentanan data dari semua identifikasi yang telah dilakukan pada tahap sebelumnya. Metode yang dilakukan yaitu identifikasi risiko berdasarkan *confidentiality*, *integrity*, *availability*. Dan dengan metode kuantitatif FMEA (*Failure mode and effect analysis*) pada setiap aset TI. Dan analisis kendali usulan berdasarkan klausul atau anek ISO 27001:2005.

2. Penilaian risiko keamanan informasi dan kendali usulan

   Yaitu melakukan penilaian risiko keamanan informasi dengan metode FMEA yang nantinya akan dilakukan penilaian risiko setiap aset TI yang terlibat berdasarkan dari hasil pengumpulan data, analisis dan penetapan nilai risiko setiap aset yang telah dilakukan pada tahap sebelumnya. Dan mengklarifikasi hasil penilaian risiko dan kendali usulan

3. Kesimpulan

   Kesimpulan berupa pendapat terakhir yang mengandung informasi yang penulis sampaikan berdasarkan tahapan/uraian alur penulisan laporan tugas akhir penilaian risiko keamanan informasi dengan pendekatan ISO 27001:2005 ini.

1.6 Sistematika Tugas Akhir

Penulisan laporan tugas akhir dibagi atas 5 (lima) bab, masing-masing bab dibagi atas subbab dengan maksud agar laporan tugas akhir dapat lebih terperinci dan akan mempermudah di dalam pemahaman masing-masing bab.

Adapun sistematika penulisan pada masing-masing bab dalam laporan tugas akhir ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini menjelaskan tentang pandangan awal persoalan yang terjadi dalam penulisan laporan tugas akhir, berisi latar belakang, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi tugas akhir dan sistematika tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini memaparkan tentang dasar-dasar teori yang digunakan dalam penelitian seperti identifikasi risiko, risiko TI, aset TI, ISO/IEC 27001:2005, SNI ISO/IEC 27001:2009, proses bisnis, dan metode FMEA yang dijadikan referensi dalam pengerjaan tugas akhir penilaian risiko keamanan informasi pada proses bisnis akademik.

BAB 3 ANALISIS DAN PERANCANGAN VARIABEL RISIKO SETIAP ASET TI

Bab ini menjelaskan mengenai analisis dan perancangan variable risiko setiap aset TI yang terlibat pada proses bisnis akademik dengan ruang lingkup tugas akhir yang diamati berdasarkan penelitian dengan fakta aktivitas akademik yang ada dilapangan.

BAB 4 PENILAIAN RISIKO KEAMANAN INFORMASI SETIAP ASET TI DAN USULAN KENDALI

Bab ini menjelaskan tentang tahap implementasi penilaian dari hasil analisis risiko setiap aset TI dan usulan kendali berdasarkan klausul atau anek ISO 27001:2005 yang dihasilkan dari bab sebelumnya. Implementasi yang dilakukan menggunakan metode FMEA sebagai salah satu metode penilaian risiko keamanan informasi yang sesuai dengan pendekatan ISO 27001:2005.

BAB 5 KESIMPULAN DAN SARAN

Bab ini mengemukakan kesimpulan yang diambil dari hasil penelitian dari penilaian risiko keamanan informasi, serta saran-saran untuk pengembangan selanjutnya, agar dapat dilakukan perbaikan-perbaikan di masa yang akan datang.