BAB 1
PENDAHULUAN

Dalam bab ini menjelaskan tentang latar belakang masalah, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodlogi tugas akhir, dan sistematika penulisan laporan tugas akhir.

1.1. Latar Belakang

Manajemen keamanan informasi terdiri atas perlindungan harian, yang disebut manajemen keamanan informasi dan persiapan operasional setelah suatu bencana yang disebut dengan manajemen keberlangsungan bisnis. Ancaman dapat pula bersifat tidak disengaja atau disengaja. Risiko dapat mencakup insiden pengungkapan, penggunaan, dan modifikasi yang tidak diotorisasi serta pencurian, penghancuran dan penolakan layanan[SAR09].

Keamanan Informasi atau *Information Security* adalah proteksi peralatan komputer, fasilitas, data, dan informasi, baik komputer maupun non-komputer dari penyalahgunaan oleh pihak-pihak yang tidak berwenang. Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yakni kerahasiaan yaitu perusahaan berusaha untuk melindungi data dan informasinya dari pengungkapan orang-orang yang tidak berwenang. Ketersediaan yang bertujuan dari infrastruktur informasi perusahaan untuk menyediakan data dan informasi bagi pihak-pihak yang memiliki wewenang untuk menggunakannya. Dan terakhir Integritas karena semua sistem informasi harus memberikan representasi akurat atas sistem fisik yang direpresentasikannya [SNI09].

Dalam dunia masa kini, banyak organisasi semakin sadar akan pentingnya menjaga seluruh sumber daya mereka, baik yang bersifat virtual maupun fisik agar aman dari ancaman baik dari dalam atau dari luar. Sistem komputer yang pertama hanya memiliki sedikit perlindungan keamanan, namun hal ini berubah pada saat perang vietnam ketika sejumlah instalasi keamanan komputer dirusak pemrotes. Pengalaman ini menginspirasi kalangan industri untuk meletakkan penjagaan keamanan yang bertujuan untuk menghilangkan atau mengurangi kemungkinan kerusakan atau penghancuran serta menyediakan organisasi dengan kemampuan untuk melanjutkan kegiatan operasional setelah terjadi gangguan [SNI09].

Berdasarkan undang-undang yang ada di LPSE yang telah ditemukan, Undang-Undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Republik Indonesia No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Dengan adanya UU di LPSE maka akan diterapan ISO 27001:2005 berkaitan dengan FMEA (*Failure mode and Effect Analysis*) yang terkait tentang keamanan informasi dan berdasarkan latar belakang yang telah dibuat diatas, peneliti tertarik untuk membantu menetapkan penyusunan SOP atas dasar UU yang tertera di LPSE dan keamanan informasi untuk menjaga atau mengamankan aset data, aset SDM, aset haerware di LPSE (Layanan

Pengadaan Secara Elektronik) KAB. BANDUNG BARAT agar aset IT yang di miliki tetap aman dan terjaga.

1.2. Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka permasalahan yang dimunculkan pada tugas akhir ini adalah:

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

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 di LPSE 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 di LPSE.
3. Menentukan kendali usulan untuk pengendalian risiko keamanan informasi dari setiap aset TI yang terlibat pada proses bisnis di LPSE.

1.4. Lingkup Tugas Akhir

Penyelesaian Tugas Akhir dibatasi sebagai berikut :

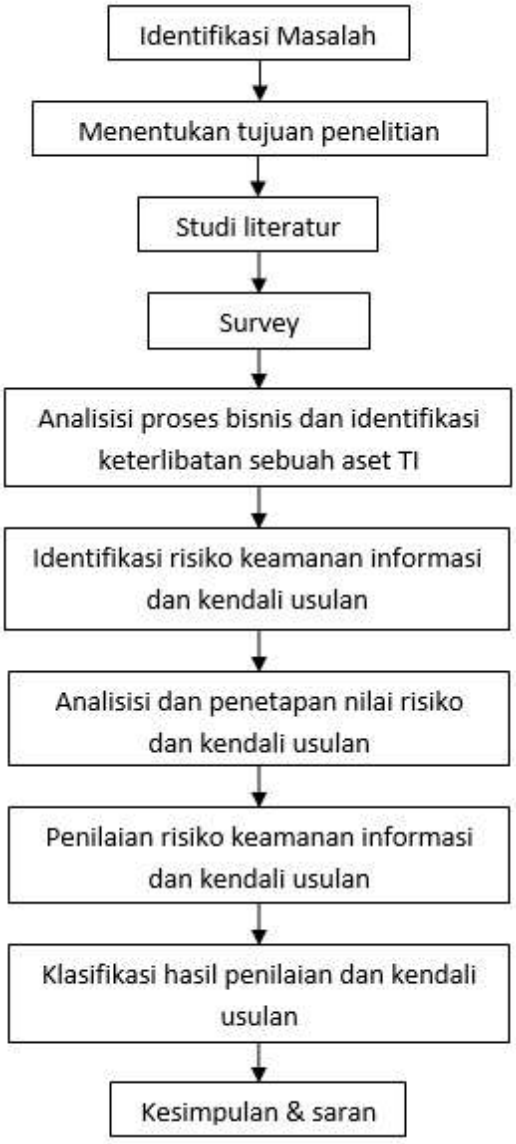
1. Penelitian menggunakan pendekatan standar ISO 27001:2005 lampiran anek A.
2. Penelitian berdasarkan ISO 27001:2005 Klausul A.7 Pengelolaan Aset, A.8 Keamanan sumber daya manusia, A.9 keamanan fisik dan lingkungan.
3. Identifikasi risiko aset TI di batasi pada Data LPSE, SDM, dan *Hardware*.
4. Metode penilaian risiko keamanan informasi pada penelitian ini menggunakan metode FMEA (*Failure Mode and Effect Analysis*).
5. Hasil dari penelitian ini berupa penyusunan Standar Operasi Prosedur (SOP) berdasarkan ISO 27001:2005.

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 LPSE dengan mengidentifikasi setiap aset TI yang terlibat yang meliputi aktivitas yang ada di LPSE.

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 langkah-langkah yang digunakan pada saat menyusun tugas akhir, yaitu sebagai berikut:



Gambar 1. 1 Metodologi Penelitian

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, artikelartikel, *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

7. 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.

8. 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

9. 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 Penulisan Laporan

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

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

BAB 1 : PENDAHULUAN

Dalam bab ini menjelaskan tentang latar belakang masalah, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodlogi tugas akhir, dan sistematika penulisan laporan 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, proses bisnis, dan metode FMEA yang dijadikan referensi dalam pengerjaan tugas akhir penilaian risiko keamanan informasi di LPSE

BAB 3 : SKEMA PENELITIAN

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

BAB 4 : PENILAIAN RESIKO KEAMANAN INFORMASI SETIAP ASET TI DAN PENYUSUNAN SOP

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

Pada bab penutup ini berisikan kesimpulan penulis yang diperoleh berdasarkan perhitungan dan pengambilan data selama penelitian berlangsung. Selain itu juga penutup berisikan tentang saran – saran dari penulis untuk mendapatkan hasil yang lebih baik dalam pengembangan yang lebih lanjut dalam penelitian ini.