

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perseroan Terbatas Aneka Jaya Baut Sejahtera (PT. AJBS) adalah sebuah perusahaan swasta nasional yang berkonsentrasi pada pengadaan perlengkapan dan peralatan pendukung industri. PT. AJBS terus berupaya untuk meningkatkan pelayanan, sejak pendiriannya pada tahun 1966. Sejalan dengan peningkatan volume usaha dan semakin luasnya wilayah usaha, PT. AJBS mengembangkan sebuah pola manajemen menuju ke arah pengelolaan usaha memperhatikan ketepatan dan kelengkapan pelayanan terhadap pelanggan.

PT. AJBS memiliki jenis dan jumlah produk yang besar, hal ini yang mengharuskan PT. AJBS untuk menerapkan teknologi informasi yang memadai. Pengelolaan inventori, transaksi, data pelanggan, dan data supplier, serta keseluruhan pelaporan dan analisa keuangan ditangani dalam sistem operasional yang terintegrasi yang bernama *Integrated Trading System (ITS)*.

Sebagai perusahaan yang berskala nasional, PT. AJBS memiliki sentral usaha di Jl. Semarang 116 D-E Surabaya. PT. AJBS sangat berperan penting dalam mengelola keamanan informasi, karena seluruh informasi perusahaan yang merupakan aset berharga bagi perusahaan berada di sana. PT. AJBS memiliki 5 (lima) *server* yang beroperasi, yaitu 2 (dua) *server* untuk data aplikasi, 1 (satu) *server* untuk *router* dan *proxy*, 1 (satu) *server* untuk *domain controller*, dan 1 (satu) *server* untuk *mail server*.

Aplikasi ITS yang digunakan pada PT. AJBS awalnya dibeli dan dikembangkan oleh pihak lain. Namun, sejak tahun 1998 telah dikembangkan sendiri sampai dengan saat ini. Seiring perkembangan bisnis yang semakin maju, maka pengembangan sistem informasi yang dilakukan juga semakin besar. Hal ini dapat dilihat dari banyaknya jumlah *server* yang dimiliki yaitu sebanyak 5 (lima) *server*. Mengingat pentingnya informasi perusahaan, maka informasi harus dilindungi atau diamankan oleh seluruh personil perusahaan. Seluruh informasi perusahaan yang ada harus memiliki *backup* dan *recovery* yang berjalan dengan baik.

Rahardjo (2005: 1) menyatakan bahwa masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Terjadinya masalah keamanan dapat menimbulkan kerugian bagi perusahaan misalnya kerugian apabila sistem informasi tidak bekerja selama kurun waktu tertentu, kerugian apabila ada kesalahan data atau informasi dan kehilangan data. Sementara itu, selama penerapan aplikasi ITS ini telah terjadi beberapa permasalahan antara lain sering ditemukan terjadinya kebocoran informasi pada karyawan yang tidak berhak atas informasi tersebut dan hal tersebut dapat mengancam kerahasiaan perusahaan. Selain itu, dikhawatirkan dapat merambat pada terjadinya penyalahgunaan informasi yang merugikan PT. AJBS dalam persaingan dengan para kompetitor. Kendala lain yang ditemukan adalah kerusakan peralatan sistem informasi yang dapat menyebabkan hilangnya data perusahaan dan sistem yang sering *hang*. Di samping itu, terjadi gangguan-gangguan yang menyebabkan kekacauan antara lain kerusakan data, *file-file* yang tidak bisa dibuka, dan lain-lain.

Selama ini PT. AJBS belum pernah melakukan analisa penyebab terjadinya permasalahan tersebut dan PT. AJBS tidak mengetahui sampai di mana tingkat keamanan sistem informasi yang miliknya. Oleh karena itu PT. AJBS membutuhkan evaluasi keamanan sistem informasi untuk menjaga keamanan sistem informasi yang dimilikinya. Evaluasi keamanan sistem informasi dapat dilakukan dengan audit keamanan sistem informasi (Asmuni dan Firdaus, 2005: 23). Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*Availability*) dari Informasi (ISO/IEC 27002, 2005: 1).

Agar audit keamanan sistem informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukan audit tersebut (Tanuwijaya dan Sarno, 2010: 80). Menurut Sarno dan Iffano (2009: 59) tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh perusahaan untuk melaksanakan audit keamanan sistem informasi. Pemilihan standar ditentukan oleh perusahaan itu sendiri. PT. AJBS memilih menggunakan standar ISO 27002. Salah satu alasan PT. AJBS memilih menggunakan ISO 27002 ini karena PT. AJBS juga telah menggunakan standarisasi ISO tentang sistem manajemen mutu yaitu ISO 9001: 2008. Standar ISO 27002 dipilih dengan pertimbangan bahwa standar ini sangat fleksibel dikembangkan tergantung pada kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai dan ukuran struktur organisasi. Selain itu, pertimbangan lainnya adalah ISO 27002 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara internasional yang disebut *Information Security Management Sistem (ISMS) certification* (Sarno dan Iffano, 2009: 59-60).

Mengingat permasalahan yang dihadapi PT. AJBS menyangkut antara lain: masalah sumber daya manusia, keamanan fisik dan lingkungan, operasional sistem informasi, kontrol akses, dan kejadian-kejadian yang menyangkut keamanan sistem informasi, maka klausul yang dipilih dalam audit keamanan sistem informasi adalah Keamanan Sumber Daya Manusia (Klausul 8), Keamanan Fisik dan Lingkungan (Klausul 9), Manajemen Komunikasi dan Operasi (Klausul 10), Kontrol Akses (Klausul 11), Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan (Klausul 12), Manajemen Kejadian Keamanan Informasi (Klausul 13), serta Manajemen Kelangsungan Bisnis (Klausul 14), yang telah sesuai dengan kesepakatan dengan pimpinan PT. AJBS.

Dengan adanya audit keamanan sistem informasi pada PT. AJBS dapat mengetahui kelemahan-kelemahan sistem yang menjadi penyebab permasalahan keamanan informasi yang selama ini terjadi. Selain itu audit ini dapat mengukur tingkat keamanan sistem informasi yang dimiliki PT. AJBS. Audit ini juga menghasilkan rekomendasi tentang perbaikan yang harus dilakukan untuk meningkatkan keamanan informasi pada perusahaan, serta menjadi pertimbangan untuk memperoleh *ISMS certification* dengan standar ISO 27002 pada masa mendatang, sehingga menambah nilai tambah akan kepercayaan pelanggan terhadap PT. AJBS.

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 PT. AJBS berdasarkan standar ISO 27002.
2. Bagaimana melaksanakan audit keamanan sistem informasi pada PT. AJBS berdasarkan standar ISO 27002.
3. Bagaimana menyusun hasil audit keamanan sistem informasi pada PT. AJBS berdasarkan standar ISO 27002.

1.3 Pembatasan Masalah

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

1. Klausul ISO 27002 yang digunakan sesuai kesepakatan dengan pimpinan PT. Aneka Jaya Baut Sejahtera yaitu:
 - a. Klausul 8: Keamanan Sumber Daya Manusia
 - b. Klausul 9: Keamanan Fisik dan Lingkungan
 - c. Klausul 10: Manajemen Komunikasi dan Operasi
 - d. Klausul 11: Kontrol Akses
 - e. Klausul 12: Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan
 - f. Klausul 13: Manajemen Kejadian Keamanan Informasi
 - g. Klausul 14: Manajemen Kelangsungan Bisnis
2. Sistem Informasi yang di audit adalah *Integrated Trading System (ITS)* PT. Aneka Jaya Baut Sejahtera (PT. AJBS).
3. Audit hanya dilakukan pada kantor PT. Aneka Jaya Baut Sejahtera (PT. AJBS) yang terletak Jl. Semarang 116 D-E Surabaya.

1.4 Tujuan

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

1. Membuat perancangan audit keamanan sistem informasi pada PT. AJBS berdasarkan standar ISO 27002 untuk menghasilkan penentuan ruang lingkup, pengumpulan data, dan langkah-langkah pelaksanaan audit.
2. Melaksanakan audit keamanan sistem informasi pada PT. AJBS berdasarkan standar ISO 27002 dengan melakukan wawancara, melakukan pemeriksaan, melakukan dokumentasi data dan bukti, menghitung dan menganalisis *maturity level*, sampai ditemukannya temuan-temuan audit untuk mengetahui sejauh mana tingkat keamanan yang dimiliki PT. AJBS.
3. Menyusun hasil audit keamanan sistem informasi pada PT. AJBS berdasarkan standar ISO 27002 ke dalam laporan hasil audit yang berupa temuan dan rekomendasi yang dapat digunakan untuk perbaikan dan peningkatan keamanan sistem yang dimiliki PT. AJBS.

1.5 Sistematika Penulisan

Laporan Tugas Akhir (TA) ini ditulis dengan sistematika penulisan sebagai berikut.

BAB I: PENDAHULUAN

Pada Bab ini membahas tentang latar belakang masalah dan penjelasan permasalahan secara umum, perumusan masalah, batasan masalah, serta tujuan dari pembuatan Tugas Akhir ini dan sistematika penulisan buku ini.

BAB II: LANDASAN TEORI

Pada Bab ini dibahas mengenai teori-teori yang berkaitan dengan audit keamanan sistem informasi, diantaranya yaitu penjelasan tentang sistem informasi, audit, audit sistem informasi, keamanan informasi, ISO/IEC 27002: 2005, model kedewasaan (*maturity model*), dan langkah-langkah kegiatan audit sistem informasi.

BAB III: METODE PENELITIAN

Pada Bab ini berisi uraian mengenai langkah-langkah yang dilakukan dalam audit keamanan sistem informasi mulai dari identifikasi proses bisnis dan TI, penentuan ruang lingkup dan tujuan audit, pelaksanaan uji kepatutan, penentuan uji kematangan, penentuan hasil audit, dan penyusunan laporan hasil audit keamanan sistem informasi.

BAB IV: HASIL DAN PEMBAHASAN

Pada Bab ini membahas tentang analisa dan evaluasi dari bukti dan temuan yang didapat saat audit keamanan sistem informasi dilakukan dan penentuan laporan akhir hasil audit keamanan sistem informasi yang berupa temuan dan rekomendasi pada PT. AJBS.

BAB V: PENUTUP

Pada Bab ini berisi kesimpulan dari Tugas Akhir, serta saran sehubungan adanya kemungkinan pengembangan pada penelitian pada masa yang akan datang.