BAB I

PENDAHULUAN

1.1. Latar Belakang

Parahita Diagnostic Center (PDC) adalah perusahaan yang bergerak pada bidang jasa pelayanan kesehatan masyarakat, khususnya pada bidang laboratorium. PDC ini didirikan pada tahun 1987 dengan nama Laboratorium Klinik Pramita. Pada tanggan 1 April 2007 laboratorium ini berubah nama menjadi "Pramita Utama Diagnostic Center" dengan berkantor pusat di Jl. Dharmawangsa 66 & 70 Surabaya. Tetapi pada tanggal 1 Juni 2010 perusahaan ini beruba nama menjadi "Parahita Diagnostic Center". Seiring perkembangannya PDC kini telah memiliki 50 cabang yang tersebar di 11 kota besar di Indonesia, seperti Surabaya, Gresik, Jember, Solo, Yogyakarta, Bandung, Bekasi, Tangerang, Jakarta, dan Makassar.

PDC memiliki peran penting dalam mengelola sistem informasi bagi seluruh kantor cabang yang ada. PDC memiliki visi untuk menjadi diagnostic center terlengkap, terintegrasi, dan terpercaya dengan layanan sepenuh hati. Dalam mencapai visi tersebut perusahaan memiliki beberapa misi, salah satunya yaitu menyediakan layanan diagnostic yang didukung oleh teknologi dan terintegrasi. Oleh karena itu perusahaan ini menerapkan teknologi yang terintegrasi dan terpusat untuk menangani seluruh proses bisnisnya. Teknologi tersebut adalah Sistem Informasi Parahita (PARIS).

PARIS digunakan untuk menunjang proses bisnis PDC secara keseluruhan meliputi proses keuangan, proses marketing, proses SDM, proses pendaftaran pasien, proses pemerikasaan hingga proses keluarnya hasil laboratorium.

PARIS menyediakan berbagai informasi penting, antara lain: informasi data pasien, data hasil pemeriksaan, data dokter, data keuangan, data karyawan serta data perusahaan yang bekerjasama dengan Parahita. PARIS digunakan oleh berbagai bagian yang terkait di PDC, yaitu bagian laboratorium, bagian pelayanan, bagian penjualan, bagian keuangan, bagian sumber daya insani (SDI) & umum, bagian penanggung jawab lab dan penanggung jawab medis.

Seiring berkembangnya perusahaan yang semakin maju, maka PDC terus berupaya dalam melakukan pengembangan sistem informasi yang mereka miliki. hal ini dapat dilihat dari migrasi PARIS yang awalnya berbasis desktop menjadi berbasis web. Dengan adanya pengembangan PARIS ini tidak dapat dipungkiri PDC menemui beberapa permasalahan. Sehingga data dan informasi penting seperti data pasien, dokter, hasil pemeriksaan, data lab, hingga data karyawan perlu untuk dilindungi dari ancaman-ancaman yang disebabkan oleh permasalahan yang ada. Mengingat pentingnya informasi terkait kebutuhan data yang ada, maka informasi harus dilindungi atau diamankan oleh seluruh karyawan PDC. Seluruh informasi yang ada di PDC harus memiliki *backup* dan *recovery* yang berjalan dengan baik.

Menurut Rahardjo (2005:1) menyatakan bahwa masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Terjadi permasalahan keamanan dapat menimbulkan kerugian bagi perusahaan. Adapun permasalahan yang sering terjadi yaitu sering adanya serangan kode-kode berbahaya (*malicious code*) yang dapat menyebabkan kerusakan data, seperti data yang telah diinputkan pada PARIS tidak tersimpan seutuhnya di dalam database. Apabila hal ini dibiarkan dapat mengancam keutuhan (*Integrity*) data perusahaan dan juga dapat menyebabkan hilangnya data, dikarenakan kerusakan data yang

telah tersimpan di database dapat mengancam ketersediaan (*Availability*) data perusahaan. selain serangan *malicious code* terdapat permasalahan lain yaitu penyalahgunaan yang dilakukan oleh beberapa pihak, contoh kasus persetujuan dana pengeluaran perusahaan selama satu minggu yang seharusnya dilakukan oleh kepala bagian keuangan, tetapi dapat dilakukan oleh staff keuangan. Hal ini dapat menyebabkan kebocoran informasi kepada karyawaan yang tidak bertanggungjawab sehingga dapat disalahgunakan. Hal ini mengancam kerahasiaan (*Confidentiality*) data perusahaan.

Selain itu dalam pengembangan PARIS ini PDC masih sulit mengidentifikasi kelemahan keamanan sistem informasi sehingga dikhawatirkan data informasi yang penting jatuh ketangan yang tidak bertanggungjawab. Hal ini dapat menyebabkan terpublikasinya teknik-teknik kelemahan (*vulnerability*) yang dimilik perusahaan sehingga dapat mengancam kerahasiaan (*Confidentiality*) data perusahaan. Sementara itu dari segi perawatan PARIS, PDC masih kurang sesuai dengan standar keamanan yang ada. Contoh kasus pemeriksaan SIP dilakukan apabila ada gangguan saja bukan dilakukan secara berkala. Hal ini menyebabkan gangguan kinerja sistem informasi yang ada. Dari semua permasalahan yang ada dapat menimbulkan risiko menurunya tingkat kepercayaan customer pada perusahaan dan menyebabkan kerugian besar bagi perusahaan hingga dapat menyebabkan kebangkrutan.

Berdasarkan kendala tersebut PDC perlu melakukan audit keamanan sistem informasi untuk mengetahui terjadinya permasalahan yang sering terjadi, agar perusahaan dapat menjaga keamanan sistem informasi yang dimiliki. Audit keamanan sistem informasi ini digunakan sebagai evaluasi keamanan sistem

informasi (Asmuni dan Firdaus, 2005). Tiga aspek keamanan informasi yang harus dijaga adalah aspek kerahasiaan (*Confidentiality*), Keutuhan (*Integrity*) dan ketersediaan (*Availability*) dari informasi (ISO/IEC 27002, 2005). Menurut Tanuwijaya dan Sarno (2010) diperlukan standar untuk melakukan audit tersebut agar audit keamanan sistem informasi dapat berjalan dengan baik. Oleh karena itu dalam penelitian tugas akhir ini standar yang dipilih adalah ISO 27002.

Standar ISO 27002 dipilih dengan pertimbangan bahwa standar ini berisikan panduan praktis (*code of practice*) teknik keamanan informasi. Selain itu ISO 27002 menyediakan sertifikat implementasi Manajemen Keamanan Sistem Informasi (MKSI) yang diakui secara internasional yaitu *Information Security Management System* (ISMS) *certification* (Sarno dan Iffano, 2009). PDC juga telah berkomitmen untuk selalu memenuhi kebutuhan dan persyaratan pelanggan dengan menerapkan ISO 9001:2008 dan ISO 15189:2012 untuk akreditasi laboratorium kesehatannya.

Mengingat permasalahan yang telah dijabarkan diatas menyangkut backup recovery, serangan malicious code yang mengancam keutuhan data perusahaan, modifikasi tanpa hak yang mengancam kerahasian perusahaan, sulitnya dalam mengidentifikasi kelemahan keamanan sistem informasi serta tidak sesuainya pemeriksaan sistem sesuai dengan standar keamanan yang ada. Oleh karena itu klausul yang dipilih dalam audit keamanan sistem informasi ini adalah Manajemen komunikasi dan operasi (Klausul 10), Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan (Klausul 12), Manajemen Kejadian Keamanan Informasi (Klausul 13), Manajemen Kelangsungan Bisnis (Klausul 14), dan Kepatuhan (Klausul 15). Hal ini sesuai dengan keinginan manajemen tentang keamanan pada PDC.

Dengan dilakukannya audit keamanan informasi pada PDC diharapkan dapat mengetahui tingkat keamanan sistem informasi yang ada, sehingga dapat mengetahui permasalahan yang terjadi selama ini. Hasil audit ini berupa temuan dan diharapkan menjadi rekomendasi yang dapat digunakan untuk meningkatkan keamanan sistem informasi yang ada pada PDC serta menjadi acuan untuk mendapatkan ISMS certification dengan standar ISO 27002:2005.

1.2. Perumusan Masalah

Berdasarkan penjelasan pada latar belakang, maka perumusan masalah yang didapat sebagai berikut:

1. Bagaimana membuat perencanaan audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center.
2. Bagaimana mempersiapkan audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center.
3. Bagaimana melaksanakan audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center.
4. Bagaimana menyusun hasil audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center.

1.3. Batasan Masalah

Berdasarkan perumusan masalah tersebut batasan masalah dalam pengerjaan tugas akhir ini adalah sebagai berikut.

1. Sistem informasi yang di audit adalah Sistem Informasi Parahita (PARIS).
2. Audit hanya dilakukan pada kantor pusat Parahita Diagnostic Center yang terletak di Jl. Dharmawangsa 66 & 70 Surabaya.

3. Klausul ISO 27002:2005 yang digunakan sesuai kesepakatan dengan pimpinan Parahita Diagnostic Center yaitu.
   a. Klausul 10 : Manajemen Komunikasi dan Operasi
   b. Klausul 12 : Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan
   c. Klausul 13 : Manajemen Kejadian Keamanan Informasi
   d. Klausul 14 : Manajemen Kelangsungan Bisnis
   e. Klausul 15 : Kepatuhan
4. Tahapan audit yang digunakan adalah Canon (2011) yang merupakan hasil pengembangan dari ISACA (2010).
5. Perhitungan Maturity Level menggunakan CMMI.

1.4. Tujuan

Berdasarkan perumusan masalah yang ada, maka tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut.

1. Menghasilkan perencanaan audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center untuk menentukan ruang lingkup, mengumpulkan data, dan menentukan klausul yang digunakan.
2. Melakukan persiapan audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center untuk menghasilkan pernyataan, melakukan pembobotan dan membuat pertanyaan.
3. Melaksanakan audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center untuk

menghasilkan hasil wawancara berupa bukti dan menghitung maturity level sehingga dapat terbentuknya jaring laba-laba.

4. Menyusun hasil audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center untuk menghasilkan bukti, temuan dan rekomendasi.

1.5. Sistematika Penulisan

Dalam penyusunan Tugas Akhir ini secara sistematika diatur dan disusun dalam 5 (lima) bab, yaitu.

BAB I :PENDAHULUAN

Pada bab ini membahas tentang latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian serta sistematika penulisan buku laporan tugas akhir.

BAB II :LANDASAN TEORI

Pada bab ini membahas mengenai teori yang mendukung, antara lain mengenai sistem informasi, sistem informasi parahita, keamanan informasi, audit, audit sistem informasi, audit keamanan sistem informasi, tahapan audit, standar sistem manajemen keamanan informasi, ISO/IEC 27002:2005 serta teori tentang tingkat kedewasaan (*maturity level*).

BAB III :METODE PENELITIAN

Pada bab ini berisi tentang langkah-langkah yang dilakukan dalam audit keamanan sistem informasi yang meliputi tahap perencanaan, tahap persiapan, tahap pelaksanaan dan tahap pelaporan.

BAB IV **:HASIL DAN PEMBAHASAN**

Pada bab ini membahas tentang hasil pelaksanaan audit keamanan sistem informasi berdasarkan tahapan audit hingga hasil temuan dan rekomendari dari kegiatan audit keamanan sistem informasi di Parahita Diagnostic Center.

BAB V **:PENUTUP**

Pada bab ini embahas tentang kesimpulan dari tugas akhir, serta berisi saran sehubungan dengan adanya kemungkinan pengembangan sistem pada masa yang akan datang