BAB I

PENDAHULUAN

1.1 Latar Belakang

Rumah Sakit Umum Daerah (RSUD) Bangil Kabupaten Pasuruan smerupakan rumah sakit yang berdiri dan diresmikan pada tahun 1981. Tahun 1985 RSUD Bangil menjadi tipe D dan di tahun 1993 berdasarkan SK Menkes No. 20/Menkes/SK/II/1993 menjadi tipe C. Keberadaan RSUD Bangil lebih bersifat sosial ekonomi dan lebih menekankan pelayanan sosial kepada masyarakat tidak mampu dan sekaligus sebagai pusat tujuan Puskesmas dan unit-unit kesehatan yaitu di Wilayah Kabupaten Pasuruan. Tujuan RSUD Bangil adalah terwujudnya layanan kesehatan yang prima, merata, terjangkau masyarakat yang didukung dengan SDM yang professional dengan unit kerja yang mandiri.

RSUD Bangil memiliki banyak aset diantaranya aset informasi, aset perangkat lunak dan aset fisik. Mengacu pada ISO/IEC 27002:2005 berbagai fasilitas dan aset perusahaan yang perlu dilindungi mencakup banyak karakteristik yang sangat perlu dipahami oleh praktisi keamanan informasi yaitu pada dasarnya fasilitas dan aset perusahaan yang ingin dijaga adalah berkaitan dengan lima komponen dasar sistem informasi yaitu perangkat keras, perangkat lunak, pengguna, data, dan prosedur. Salah satu institusi pemerintahan yang membutuhkan perlindungan aset adalah rumah sakit sebagai sebuah institusi pelayanan kesehatan. Salah satu aset rumah sakit RSUD Bangil adalah Avesina Health System yang merupakan aset piranti lunak yang dimiliki oleh Instalasi Sistem Informasi Manajemen Rumah Sakit (SIM-RS) sejak 2011. Instalasi SIM-

RS atau Pengelola Data Elektronik (PDE) memiliki tugas dalam proses pemeliharaan data dan jaringan seperti, menjaga keamanan data SIM-RS, memberikan hak akses (otoritas), *maintenance software* yaitu *backup* data dan *backup system*, bertanggung jawab memastikan seluruh jaringan dan *hardware* di RSUD Bangil tidak bermasalah.

Pihak manajemen RSUD Bangil memiliki permasalahan terhadap lambatnya penerimaan kebutuhan informasi kepada pihak manajemen, kurangnya keutuhan data yang diterima, dan kurangnya kesesuaian atau validasi hasil data. Permasalahan tersebut disebabkan kurangnya pengelolaan aset yang tepat dari Instalasi SIM-RS. Pengelolaan Instalasi SIM-RS yang kurang tepat diantaranya permintaan informasi yang kurang terlayani dengan cepat oleh Instalasi SIM-RS sehingga pencapaian tujuan organisasi tidak maksimal, beberapa data-data Instalasi SIM-RS yang disimpan tiba-tiba hilang atau rusak sehingga data yang akan disampaikan tidak lengkap atau tidak utuh, dan data Instalasi SIM-RS yang disampaikan tidak sesuai dengan kenyataan yang ada atau tidak valid sehingga membuat pihak Instalasi SIM-RS kerja dua kali untuk mendapatkan kesesuaian laporan data yang ada. Untuk memperbaiki pengelolaan aset yang ada di Instalasi SIM-RS maka pihak manajemen RSUD Bangil membutuhkan audit.

Adapun risiko yang bisa ditimbulkan jika pengelolaan aset tidak dilindungi yaitu dari aset informasi ketika data dan dokumen penting mampu diakses dan dilihat langsung oleh orang yang tidak berhak memperoleh informasi yang berharga sehingga mampu memperoleh keuntungan dari pencurian informasi yang dapat menimbulkan kerugian bagi perusahaan. Dari segi aset layanan, risiko dapat berasal dari penyadapan yang dilakukan oleh saluran komunikasi secara

tidak sah sehingga mampu memperoleh informasi yang berharga kepada pihak yang bukan wewenangnya. Perlindungan terhadap perangkat keras juga dibutuhkan agar terhindar dari risiko kerusakan fisik yang disebabkan oleh penjahat komputer yang dapat masuk kedalam jaringan komputer yang berada jauh dari lokasi. Perlindungan aset perangkat lunak dilakukan untuk memperkecil risiko modifikasi perangkat lunak yang bisa menyebabkan pengguna yang ada di *ouput system* menerima informasi yang salah dan membuat keputusan yang salah sehingga dapat merugikan perusahaan. Aset-aset pada Instalasi SIM-RS diidentifikasi risikonya sehingga diharapkan mampu mengurangi risiko yang ada dengan sejumlah kendali keamanan informasi yang ada.

Untuk memperbaiki permasalahan keamanan informasi yang ada di bagian Instalasi SIM-RS maka pihak manajemen RSUD Bangil membutuhkan audit keamanan Sistem Informasi. Pedoman audit yang digunakan mengacu pada *Information Systems Audit and Control Association* (ISACA) dengan standar *best practice International Standard Organization* ISO 27002 (2005) yang diterbitkan oleh *International Electhronical Commission*. Standar ini merupakan standard keamanan informasi yang merupakan *best practice* atau panduan umum yang menjelaskan adanya contoh penerapan keamanan informasi dengan menggunakan bentuk kontrol sehingga dapat mencapai sasaran yang diterapkan. ISO 27002 menyediakan rekomendasi *best practice* terhadap manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab untuk proses inisiasi, implementasi, dan pemeliharaan *Information Security Management Systems* (ISMS) pada suatu organisasi.

Mengacu pada hasil *review*, survei dan wawancara yang telah dilakukan, maka klausul yang ditetapkan sebanyak 5 klausul yaitu manajemen aset (klausul 7), keamanan Sumber Daya Manusia (klausul 8), keamanan fisik dan lingkungan (klausul 9), kontrol akses (klausul 11), akuisisi sistem informasi pembangunan dan pemeliharaan (klausul 12). Kelima klausul yang ditetapkan ini telah memperoleh persetujuan dan kesepakatan bersama oleh Ketua Instalasi SIM-RS yang akan tertuang dalam dokumen *engagement letter.*

Dengan adanya audit keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil berdasarkan ISO 27002 melalui penyusun Tugas Akhir maka diharapkan dapat menghasilkan temuan audit yang berupa daftar temuan, hasil pengukuran untuk mengetahui tingkat kedewasaan berdasarkan SNI ISO/IEC 27001:2009 dan rekomendasi perbaikan. Diharapkan hasil audit dapat dijadikan acuan untuk meningkatkan keamanan informasi pada Instalasi SIM-RS RSUD Bangil serta sebagai acuan dalam upaya memperoleh ISMS *cetification* dengan standar ISO 27002: 2005.

1.2 Perumusan Masalah

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

1. Bagaimana melakukan audit keamanan sistem informasi pada Instalasi SIM-RS yang sesuai dengan tahapan ISACA yang akan dilaksanakan oleh auditor.
2. Bagaimanan cara mendapatkan temuan audit dengan cara melakukan pemeriksaan audit dan mengukur tingkat kedewasaan berdasarkan SNI ISO/IEC 27001:2009 sehingga dapat diterapkan sesuai dengan hasil pemeriksaan audit yang ada.

3. Bagaimana memberikan hasil yang berupa laporan rekomendasi atas temuan audit yang dilakukan di RSUD Bangil berdasarkan standar ISACA dengan menggunakan *best practise* ISO 27002:2005.

1.3 Batasan Masalah

Berdasarkan perumusan masalah di atas, maka batasan-batasan permasalahan sebagai berikut:

1. Audit dilakukan pada Instalasi SIM-RS RSUD Bangil kabupaten Pasuruan.
2. Perencanaan sampai dengan tahap pelaporan audit keamanan Sistem Informasi mulai dari bulan September 2012 sampai dengan Juni 2013.
3. Periode data yang digunakan untuk audit keamanan Sistem Informasi adalah Oktober 2011 sampai dengan Oktober 2012.
4. Klausul yang digunakan telah disesuaikan dengan kesepakatan Koordinator SIM-RS dan Ketua Instalasi SIM-RS yang akan terlampir pada dokumen *Engagement Letter*.

1.4 Tujuan

Berdasarkan masalah yang ada, maka tujuan yang ingin dicapai adalah sebagai berikut:

1. Melakukan dan menghasilkan rancangan audit keamanan Sistem Informasi sesuai dengan *Audit Working Plan* (AWP) yang dibuat mulai dari tahapan perencanaan, persiapan, pelaksanaan dan pelaporan pada Instalasi SIM-RS RSUD Bangil berdasarkan ISACA dengan *best practise* ISO 27002:2005.
2. Dengan melakukan pemeriksaan audit sehingga didapatkan temuan-temuan audit yang didapatkan dengan cara *review*, wawancara, dan observasi

sehingga dapat mengetahui temuan audit dan dapat mengukur *maturity level* yang berdasarkan SNI ISO/IEC 27001:2009.

3. Menyusun hasil audit keamanan Sistem Informasi pada Instalasi SIM-RS RSUD Bangil berdasarkan standar ISO 27002 dari mengevaluasi bukti-bukti yang ada, mendokumentasikan temuan-temuan audit serta menyusun laporan hasil audit yang berupa permintaan tanggapan atas daftar temuan Audit TI, rekomendasi yang dibutuhkan pada RSUD Bangil.

1.5 Sistematika Penulisan

Di dalam penulisan Tugas Akhir ini secara sistematika diatur dan disusun dalam 5 (lima) bab sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini membahas 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 membahas mengenai teori Keamanan Informasi, Aspek Keamanan Informasi, Alasan dibutuhkan Keamanan Informasi, Audit Keamanan Informasi, Langkah-langkah Audit TI, Standar Sistem Manajemen Keamanan Informasi, ISO/IEC 27002: 2005, dan *Maturiy level.*

BAB III : METODE PENELITIAN

Pada bab ini berisi penjelasan mengenai langkah-langkah yang dilakukan dalam audit keamanan Sistem Informasi yang meliputi tahap perencanaan audit, tahap persiapan audit, tahap pelaksanaan audit dan tahap pelaporan audit.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini membahas mengenai proses melakukan audit sehingga dihasilkan *maturity level* dengan SNI ISO/IEC 27001: 2009 beserta temuan dan rekomendasi dari kegiatan audit keamanan Sistem Informasi RSUD Bangil.

BAB V : PENUTUP

Pada bab ini membahas mengenai kesimpulan terakhir yang didapatkan yang terkait mengenai pencapai tujuan dan permasalahan yang ada sebelumnya serta saran yang ada sehingga memungkinkan mampu menjadikan lebih baik lagi kedepan.