JSIKA Vol 3, No 2 (2013)/ ISSN 2338-137X

Jurnal Sistem Informasi

Situs Jurnal : http://jurnal.stikom.edu/index.php/jsika

AUDIT KEAMANAN SISTEM INFORMASI PADA INSTALASI SISTEM INFORMASI MANAJEMEN RSUD BANGIL BERDASARKAN ISO 27002

Danastri Rasmona Windirya [1] **Haryanto Tanuwijaya** [2] **Erwin Sutomo**[3]
Program Studi/Jurusan Sistem Informasi
STMIK STIKOM Surabaya
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1) danastrirasmona.w@gmail.com, 2) haryanto@stikom.edu, 3) sutomo@stikom.edu

Abstract: RSUD Bangil is a government hospital Bangil regency. RSUD Bangil have assets that must be managed properly in order to minimize the security risk. Obstacle now is the slow acceptance to the information needs of management, lack of integrity of the data received, and lack of suitability or validation data results. The problems caused by lack of proper asset management of SIM-RS Installation so that could pose a risk. So that the hospital can be minimized Bangkil audit requires action by providing information system security ISO 27002: 2005 as a security best practice standards.Audits performed at the SIM-RS with stages according to ISACA. Scope examined adjusted by mutual agreement of which asset management, human resources security, physical and environmental security, access control and information systems acquisition, pembangunaan and maintenance.Result of the implementation of information systems security audit found the average value of 3.22 which means the level of maturity of information security measures according to ISO / IEC 27001: 2009 was at a level 3 which is pro-active. The results of the findings obtained in order to provide recommendations in accordance with ISO 27002: 2005 to the RSUD Bangil.

Keywords: Audit, ISO 27002, Security *Information Systems*, *Maturity Level*

Menurut survei *Information Security Breaches Survey* (ISBS) tahun 2012, setiap tahun jumlah pelanggaran terhadap keamanan informasi semakin meningkat disertai perkembangan teknologi yang semakin maju sehingga dibutuhkan pengontrolan keamanan informasi. Adapun jenis ancamannya, yaitu: virus, kegagalan sistem, penyalahgunaan informasi oleh pengguna, tidak adanya otorisasi akses dan pencurian akses informasi.

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 permasalahan keamanan informasi yang ada di bagian Instalasi SIM-RS maka pihak manajemen RSUD Bangil membutuhkan audit keamanan sistem informasi. Audit tersebut

menggunakan ISO 27002:2005. Dalam penelitian ini audit yang dilakukan meliputi manajemen aset, keamanan Sumber Daya Manusia, keamanan fisik dan lingkungan, kontrol akses dan akuisisi sistem informasi pembangunan dan pemeliharaan.

METODE PENELITIAN

Pada penelitian ini, langkah audit keamanan sistem informasi dapat dilihat pada Gambar 1.

Gambar 1. Langkah Audit Keamanan SI (Sumber: ISACA, 2010)

1. Perencanaan Audit
   Perencanaan audit dilakukan untuk memahami kondisi lingkungan yang akan diaudit. Perencanaan audit dilakukan dengan empat tahapan sebagai berikut.
   a. Pemahaman proses bisnis dan Teknologi Informasi (TI).
   b. Menentukan ruang lingkup, objektiv kontrol dan kontrol.
   c. Menentukan klausul, objektiv kontrol dan kontrol.
   d. Membuat *engegement letter*.

   Langkah ini menghasilkan dokumen proses bisnis TI, ruang lingkup, objek dan tujuan audit. Selain itu juga menghasilkan klausul, objektiv kontrol dan kontrol dengan standar ISO 27002: 2005 serta *engement letter*.

2. Persiapan Audit
   Sebelum pelaksanaan audit, diperlukan kegiatan persiapan audit yang dilakukan dalam empat tahapan sebagai berikut.
   a. Proses penyusunan Audit *Working Plan (AWP).*
   b. Penyampaian kebutuhan data.
   c. Membuat pernyataan.
   d. Membuat pertanyaan.

   Langkah ini menghasilkan tabel *audit working plan*, surat kebutuhan data, daftar pernyataan dan daftar pertanyaan.

3. Pelaksanaan Audit
   Pada pelaksanaan audit, dilakukan pemeriksaan objek audit untuk menghasilkan bukti temuan sesuai dengan kebutuhan audit. Langkah pelaksanaan audit terdiri empat tahapan sebagai berikut.
   a. Melakukan pemeriksaan data dan bukti.
   b. Melakukan wawancara.
   c. Melakukan uji kematangan.
   d. Penyusunan daftar temuan audit dan rekomendasi.

   Langkah pelaksanaan audit menghasilkan data dan bukti berupa dokumen, foto maupun rekaman apakah data atau bukti yang dibutuhkan telah tersedia. Selain itu juga menghasilkan jawaban dari wawancara, nilai *maturity level*, susunan daftar temuan dan rekomendasi.

4. Pelaporan Audit
   Penyusunan hasil audit dilakukan dalam tiga tahapan sebagai berikut.
   a. Melakukan permintaan tanggapan atas daftar temuan audit.
   b. Penyusunan dan persetujuan draft laporan audit.
   c. Pertemuan penutup atau pelaporan hasil audit.

   Langkah ini menghasilkan permintaan tanggapan atas daftar temuan audit, hasil penyusunan dan persetujuan *draft* laporan audit dan hasil pertemuan penutup berupa *exit meeting.*

HASIL DAN PEMBAHASAN

Perencanaan Audit

Pemahaman proses bisnis TI diperoleh dengan mempelajari profil, visi dan misi, struktur organisasi, *job decription* pegawai dan proses bisnis. Selanjutnya

Instalasi SIM-RS sebagai objek audit, menentukan klausul sesauai dengan standar ISO 27002: 2005. Klausul yang digunakan sebanyak lima klausul, setiap klausul memiliki objektiv kontrol dan kontrol. Klausul yang digunakan dapat dilihat pada Tabel 1. Kemudian keseluruhan data tersebut dituangkan dalam *engagement letter*.

Tabel 1. Klausul yang Digunakan

Klausul	Keterangan
Klausul 7	Manajemen Aset
Klausul 8	Keamanan Sumber Daya Manusia
Klausul 9	Keamanan Fisik dan Lingkungan
Klausul 11	Kontrol Akses
Klausul 12	Akuisisi Sistem Informasi, Pegembanganan dan Pemeliharaan.

Persiapan Audit

Persiapan audit diawali dengan pembuatan AWP berupa jadwal kerja yang dimulai dari perencanaan sampai dengan pelaporan audit. Contoh *Audit Working Plan* dapat dilihat pada Tabel 2.

Tabel 2. Contoh Hasil *Audit Working Plan*

Tahapan	Awal Kegiatan	Akhir Kegiatan
Perencanaan Audit		
Pemahaman Proses bisnis	03/09/2012	17/09/2012
Menentukan ruang lingkup objek audit dan tujuan audit	18/09/2012	19/09/2012
Menentukan klasusul, objektiv dan kontrol	11/09/2012	13/09/2012
Membuat *engagement letter*	14/09/2012	17/09/2012
Persiapan Audit		
Penyusunana AWP	18/09/2012	22/09/2012
Penyampaian kebutuhan data	24/09/2012	27/09/2012
Membuat pernyataan	24/09/2012	05/11/2012
Membuat pertanyaan	06/11/2012	26/11/2012

Proses berikutnya dilanjutkan dengan membuat pernyataan dan pertanyaan yang digunakan auditor pada saat audit seperti ditunjukkan pada Tabel 3.

Tabel 3. Contoh Pernyataan dan Pertanyaan

No	Pernyataan	Pertanyaan
1	Terdapat penandatangan perjanjian kerahasiaan akses pada pegawai.	1. Apakah telah dilakukan penandatangan perjanjian kerahasiaan sebelum pegawai diberikan akses ?
		2. Siapa yang bertanggung jawab atas perjanjian kerahasiaanpengelolaan akses tersebut?

Pelaksanaan Audit

Pelaksanaan audit diawali pertemuan pendahuluan audit untuk mendapatkan pemahaman yang sama antara auditor dengan auditi sebelum pelaksanaan dimulai. Pendahuluan audit telah didokumentasikan kedalam notulen pertemuan pendahuluan audit.

Setelah dilakukan pertemuan pendahulan audit maka auditor melakukan pemeriksaan data dan bukti mengenai hal yang terkait dengan keamanan informasi. Hasil wawancara dan observasi digunakan untuk menilai tingkat kedewasaan menggunakan SNI ISO/IEC 27001: 2009. Penilaian mengacu pada kriteria yang terdapat pada Tabel 4, sedangkan hasil dari penilaian dilihat pada Tabel 5. Penilaian didapatkan nilai rata-rata tingkat kedewasaan seperti ditunjukkan pada Tabel 6. Berdasarkan hasil tersebut dibuatlah jaring laba-laba yang dapat dilihat pada Gambar 2.

Tabel 4. Penilaian Tingkat Kedewasaan dengan SNI ISO/IEC 27001: 2009.

Tingkat	Keterangan
0 Tidak Diketahui (Pasif)	- Status kesiapan keamanan informasi tidak diketahui. - Pihak yang terlibat tidak mengikuti atau tidak melaporkan pemeringkatan Indeks KAMI.
1 Kondisi Awal (Reaktif)	- Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi - Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada

Tingkat	Keterangan
	keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan. - Kelemahan teknis dan non teknis tidak terdefinisi dengan baik. - Pihak yang terlibat menyadari tanggung jawab mereka.
2 Penerapan Kerangka Dasar (Aktif)	- Pengamanan diterapkan walaupun sebagian besar masih diarea teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif. - Proses pengamanan informasi berjalan tanpa dokumentasi atau rekaman resmi. - Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana. - Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.
3 Terdefinisi dan Konsisten (Pro Aktif)	- Bentuk pengamanan yang berlaku sudah diterapkan secara konsisten dan terdokumentasi secara resmi. - Efektivitas pengamanan dievaluaasi secara berkala, walaupun belum melalui proses yang terstruktur. - Kerangka kerja pengamanan sudah mematuhi ambang batas minimum standar atau persyaratan hukum terkait. - Secara umum semua pihak yang terlibat menyadari tanggung jawab mereka dalam pengamanan informasi.
4 Terkelola dan Terukur	- Pengamanan diterapkan secara efektif sesuai dengan strategi menejemen risiko. - Evaluasi (pengukuran) pencapaian sasaran pengamanan dilakukan secara rutin, formal dan terdokumentasi. - Penerapan pengamanan teknis secara konsisten dievaluasi efektivitasnya. - Kelemahan manajemen pengamanan informasi terdefinisi dengan baik dan secara konsisten ditindak lanjuti pembenahannya. - Karyawan merupakan bagian yang tidak terpisahkan dari pelaksana pengamanan informasi.
5 Optimal	- Pengamanan menyeluruh diterapkan secara berkelanutan dan efektif melalui program pengelolaan risiko yang terstruktur. - Pengamanan informasi dan manajemen risiko sudah terintegrasi dengan tugas pokok instansi. - Kinerja pengamanan dievaluasi secara kontinyu, dengan analis parameter efektivitas kontrol, kajian akar permasalahan dan penerapan langkah untuk optimasi peningkatan kinerja. - Target pencapaian program pengamanan informasi selalu dipantau, dievaluasi dan diperbaiki. - Karyawan secara proaktif terlibat dalam peningkatan efektivitas pengamanan informasi.
6 Di Luar Jangkauan	- Kontrol yang berada diluar jangkauan

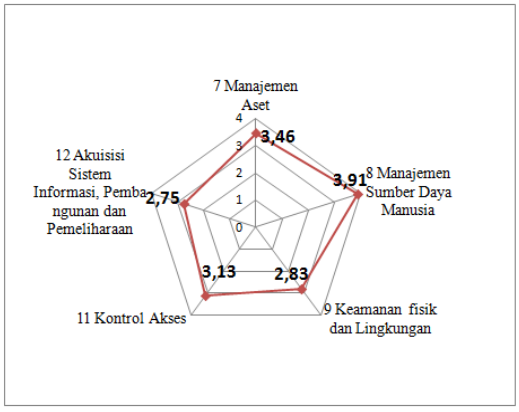
Tabel 5. Contoh Hasil Penilaian Tingkat Kedewasaan

Klausul: 7 Manajemen Aset			
Objektif Kontrol: 7.1 Tanggung Jawab Aset			
Kontrol: 7.1.1 Inventarisasi Aset			
Pernyataan: Terdapat inventarisasai aset organisasi			
No	Pertanyaan	Nilai (0-6)	Keterangan
1	Apakah organisasi sudah melakukan iventarisasi terhadap aset ?	5	
2	Berapa kali organisasi melakukan inventarisasi aset	5	
3	Adakah dokumentasi mengenai pemilik aset?	5	
4	Apakah pencatatan inventarisasi aset sudah menjelaskan pemulihan terhadap bencana?	2	
5	Apakah pencatatan inventarisasi aset sudah	3	

Klausul: 7 Manajemen Aset			
Objektif Kontrol: 7.1 Tanggung Jawab Aset			
Kontrol: 7.1.1 Inventarisasi Aset			
Pernyataan: Terdapat inventarisasai aset organisasi			
No	Pertanyaan	Nilai (0-6)	Keterangan
	menjelaskan lokasi aset?		
	Rata-Rata	4	

Tabel 6. Hasil Tingkat Kedewasaan

Klausul	Deskripsi Klausul	Hasil
7	Manajemen Aset	3,46
8	Manajemen Sumber Daya Manusia	3,91
9	Keamanan fisik dan Lingkungan	2,83
11	Kontrol Akses	3,13
12	Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	2,75
Nilai Rata-Rata Tingkat Kedewasaan		3,22



Gambar 2. Kesimpulan Jarinng Laba-Laba

Jaring laba-laba pada Gambar 2 menunjukkan bahwa hasil tertinggi terdapat pada keamanan Sumber Daya Manusia (klausul 8) sebesar 3,91. Bahwa ukuran keamanan informasi menurut SNI ISO/IEC 27001: 2009 berada pada level 3 yaitu pro aktif, artinya keamanan informasi telah dilakukan secara terdefinisi dan konsisten. Hal tersebut dapat dilihat dari adanya penandatanganan perjanjian kerja kepada pegawainya secara konsisten sebelum diberikan akses ke pengolahan informasi.

Sedangkan hasil terendah didapatkan pada Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan (klausul 12) yaitu sebesar 2,75. Bahwa ukuran keamanan informasi menurut SNI ISO/IEC 27001: 2009 berada pada level 2 yaitu aktif artinya proses keamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan proses pengamanan masih berjalan tanpa dokumentasi atau rekaman resmi. Hal tersebut dapat dilihat dari tidak adanya prosedur yang diterapkan dalam memastikan kebocoran informasi yang terjadi didalamnya.

Secara keseluruhan, tingkat kontrol keamanan yang diukur mendapat nilai sebesar 3,22 yaitu *pro aktif*, artinya sebagian besar proses keamanan sudah diterapkan secara konsisten dan terdokumentasi secara resmi, efektivitas pengamanan dievaluasi secara berkala walaupun belum melalui proses yang terstruktur, kerangka kerja pengamanan sudah mematuhi ambang batas minimum dan pihak yang terlibat telah menyadari tanggung jawab meraka dalam pengamanan informasi.

Berdasarkan hasil temuan telah diberikan rekomendasi sesuai dengan ISO 27002: 2005 agar mampu meminimalisasi terjadinya risiko yang mucul dan memperbaiki kelemahan yang terjadi.

SIMPULAN

Berdasarkan hasil audit keamanan sistem informasi yang telah dilakukan maka dapat disimpulKan sebagai berikut.

1. Audit keamanan sistem informasi manajemen pada Instalasi SIM-RS RSUD Bangil telah berhasil dilakukan sesuai dengan tahapan standar *best practice* ISO 27002: 2005 pada kontrol keamanan manajemen aset, keamanan Sumber Daya Manusia, keamanan fisik dan lingkungan, kontrol akses dan akusisi sistem informasi, pembangunan dan pemeliharaan.
2. Hasil pemeriksaan kontrol keamanan audit diperoleh tingkat kedewasaam 3,22 yaitu *pro aktif* , artinya sebagian besar proses keamanan sudah diterapkan secara konsisten dan terdokumentasi secara resmi, efektivitas pengamanan dievaluasi

secara berkala walaupun belum melalui proses yang terstruktur, kerangka kerja pengamanan sudah mematuhi ambang batas minimum dan pihak yang terlibat telah menyadari tanggung jawab meraka dalam pengamanan informasi.

3. Instalasi SIM-RS di RSUD Bangil harus segera menerapkan kebijakan dan prosedur untuk mengatasi insiden kelemahan sistem informasi.

RUJUKAN

ISACA. 2010. *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*. USA.

ISBS. 2012. *Information Security Breaches Survey: Technical Report*. United Kingdom: Pwc

ISO/IEC 17799 (27002). 2005. *Information Technology Security Techniques – Information Security Management*. Switzerland