AUDIT KEAMANAN SISTEM INFORMASI PADA INSTALASI SISTEM INFORMASI MANAGEMENT (SIM-RS) BERDASARKAN STANDAR ISO 27002

(Studi Kasus: Rumah Sakit Umum Haji Surabaya)

Annisa Destiara Yaner[1)], Haryanto Tanuwijaya[2)], Erwin Sutomo[3)]
Program Studi/Jurusan Sistem Informasi
STMIK STIKOM Surabaya
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1) nisak.yaner@gmail.com, 2)haryanto@stikom.edu, 3)sutomo@stikom.edu

Abstract: RSU Haji Surabaya is a government-owned hospital in East Java province. Asset management performed by one of the installation of the Installation Management Information Systems (MIS-RS) and software (Software) is used Healthy Plus application which has been operating for the last 1 year. In managing the assets of RSU Haji there are several obstacles, namely: there are many outsiders who were not authorized to be in and out of the processing room information on data center space, loss of data, manipulation of data from unauthorized access, viruses, data theft, unauthorized access to the application.

So that these constraints will not recur or become, the RSU Haji Surabaya need to conduct an audit to determine current conditions compared with conditions should be. The standard used is ISO 27002:2005 with the scope of clause 8 (eight), 9 (nine), 11 (eleven), and 12 (twelve).

From the implementation of information systems audit, the resulting value of 1.75 Maturity Level are included in the initial category, which means much of the existing information system security on the SIM-RS Installation not in accordance with the ISO 27002 standard procedures. The study also produce recommendations for process improvement and information systems can be used to enhance the security of information on RSU Haji Surabaya.

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

Perkembangan teknologi dan sistem informasi pada institusi pemerintahan semakin pesat, risiko keamanan yang melekat pada informasi juga semakin besar. Lemahnya kendali keamanan atas aset informasi memudahkan pihak-pihak yang tidak bertanggung jawab untuk mencurinya atau sekedar mengganggu jalannya aktivitas yang terkait dengan aset tersebut. Salah satu institusi pemerintahan yang membutuhkan perlindungan aset adalah Rumah Sakit sebagai sebuah institusi pelayanan kesehatan. Rumah Sakit sangat memerlukan perlindungan keamanan aset, karena aset merupakan bagian yang penting bagi kelangsungan proses operasional pada Rumah Sakit.

RSU Haji Surabaya telah menerapkan teknologi informasi dalam operasional layanan pasien. Untuk pengelolaan aset dilakukan oleh salah satu instalasi yaitu Instalasi Sistem Informasi Management (SIM-RS) yang memiliki tugas dalam proses pemeliharaan data seperti, memasukkan, mengolah dan menghasilkan informasi. Perangkat lunak (*Software*) yang digunakan untuk mengelola aset adalah *Aplikasi Healthy Plus* yang telah beroperasi selama 1 tahun terakhir. Dalam mengelola aset RSU Haji terdapat beberapa kendala yaitu: masih banyaknya pihak luar yang tidak berwenang dapat keluar masuk pada ruang pengolahan informasi di ruang pusat data, kehilangan data, manipulasi data dari pihak yang tidak berwenang, virus, pencurian data, penyalahgunaan akses pada aplikasi.

Supaya kendala tersebut tidak terulang kembali atau semakin meningkat, maka RSU Haji Surabaya perlu melakukan audit untuk mengetahui kondisi saat ini dibandingkan dengan kondisi seharusnya. Standar yang digunakan yaitu ISO 27002:2005 Standar ini merupakan pedoman dan prinsip untuk memulai, melaksanakan, memelihara dan meningkatkan manajemen keamanan informasi dalam suatu organisasi dan untuk memberikan panduan pengembangan standar keamanan organisasi. Klausul yang digunakan untuk audit keamanan informasi pada Instalasi SIM-RS disesuaikan dengan kendala-kendala yang ditemukan berdasaran survei dan wawancara, yaitu: Keamanan Sumber Daya Manusia (Klausul 8), Keamanan Fisik dan Lingkungan (Klausul 9), Kontrol Akses (Klausul 11), serta Akuisisi Sistem Informasi Pembangunan dan Pemeliharaan (Klausul 12), yang telah sesuai dengan kesepakatan dengan kepala Instalasi SIM-RS.

Dengan adanya audit sistem keamanan informasi pada Instalasi SIM-RS pada RSU Haji Surabaya dapat meningkatkan keamanan informasi, prosedur keamanan informasi yang ada dan menurunkan risiko keamanan informasi.

LANDASAN TEORI

Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimalisasi risiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang, contoh Keamanan Informasi sebagai berikut (Sarno dan Iffano, 2009: 27)

Audit Sistem Informasi

Audit secara umum adalah proses terpadu dalam pengumpulan dan penilaian terhadap informasi sebagai satu kesatuan organisasi oleh seorang ahli . Pengertian audit sistem informasi adalah proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien (Weber, 1999).

Rumah Sakit

Rumah sakit merupakan suatu institusi yang fungsi utamanya memberikan pelayanan kesehatan kepada masyarakat. Tugas rumah sakit adalah melaksanakan upaya kesehatan secara berdaya guna dan berhasil guna dengan mengutamakan upaya penyembuhan dan pemulihan yang dilaksanakan secara serasi dan terpadu dengan peningkatan dan pencegahan serta melaksanakan rujukan.Untuk dapat menyelenggarakan upaya-upaya tersebut dan mengelola rumah sakit agar tetap dapat memenuhi kebutuhan pasien dan masyarakat yang dinamis, maka setiap komponen yang ada di rumah sakit harus terintegrasi dalam satu sistem (Soejitno, 2002).

ISO 27002: 2005

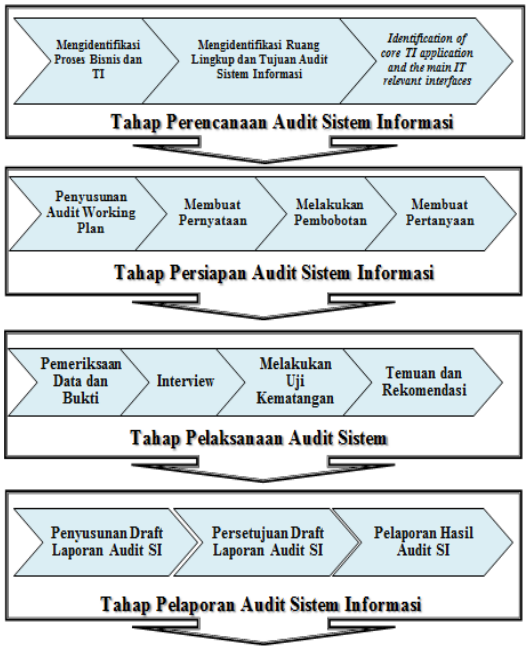
ISO 27002: 2005 berisi panduan yang menjelaskan contoh

penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 (sebelas) area pengamanan sebagaimana ditetapkan didalam ISO/IEC 27002.

Audit Keamanan

Menurut Margaret (2005), audit keamanan bertujuan mengevaluasi sistematis dari keamanan sistem informasi perusahaan dengan mengukur seberapa baik sesuai dengan beberapa kriteria yang ditetapkan. Audit menyeluruh untuk menilai keamanan konfigurasi fisik sistem dan lingkungan, perangkat lunak, proses penanganan informasi, dan praktik pengguna.

METODOLOGI PENELITIAN



Gambar 1. Tahapan – tahapan audit
(Sumber: Hermawan, 2011)

Keempat tahapan tersebut adalah:

1. Tahap Perencanaan Audit Sistem Informasi
   a. Melakukan identifikasi proses bisnis
   b. Melakukan penentuan ruang lingkup dan tujuan audit
   c. Melakukan *identification of core TI application and the main IT relevant interfaces* Tahap Persiapan Audit Sistem Informasi
2. Tahap Persiapan Audit Sistem Informasi
   a. Melakukan proses penyusunan Jadwal Kerja Audit
   b. Membuat pernyataan
   c. Melakukan pembobotan
   d. Membuat pertanyaan
3. Tahap Pelaksanaan Audit Sistem Informasi
   a. Melakukan proses pemeriksaan data dan bukti
   b. Melakukan wawancara
   c. Melakukan uji kematangan
   d. Melakukan penentuan temuan dan rekomendasi
4. Tahap Pelaporan Audit Sistem Informasi

IMPLEMENTASI DAN HASIL

Identifikasi proses bisnis

Dalam perencanaan proses audit, auditor harus melakukan pemahaman proses bisnis dan TI perusahaan yang akan diaudit. Pemahaman dilakukan dengan cara mempelajari dokumen-dokumen yang terkait dengan perusahaan, yaitu profil perusahaan, visi dan misi RSU Haji Surabaya, struktur organisasi RSU Haji dan SIM-RS, gambaran umum Instalasi SIM-RS, dan proses bisnis dan TI SIM-RS. Auditor juga harus mengetahui apakah sebelumnya perusahaan telah dilaksanakan proses audit. Apabila pernah maka auditor juga mengetahui

tentang laporan audit periode sebelumnya.

Penentuan Ruang Lingkup dan Tujuan Audit Sistem Informasi

Penentuan ruang lingkup dilakukan dengan cara melakukan observasi, wawancara dan kuesioner pada Instalasi SIM-RS RSU Haji Surabaya. Hasil penentuan ruang lingkup didapat dari wawancara dengan pihak SIM-RS didapatkan hasil dimana masih kurangnya keamanan pada akses aplikasi. Hasil ruang lingkup yaitu audit keamanan sistem informasi dengan standar yang digunakan adalah ISO 27002 dan klausul yang digunakan untuk audit keamanan sistem informasi dapat dilihat pada Tabel 1.

Tabel 1. Pemetaan Klausul ISO 27002 yang digunakan

Klausul	Desrkipsi
8	Keamanan Sumber Daya Manusia
9	Keamanan Fisik dan Lingkungan
11	Kontrol Akses
12	Akuisisi sistem informasi Pembangunan dan Pemeliharaan

Identification of core TI application and the main IT relevant interfaces

Pada proses ini langkah yang dilakukan adalah menentukan klausul, obyektif kontrol dan kontrol yang sesuai dengan permasalahan dan kebutuhan RSU Haji Surabaya. Klausul, obyektif kontrol dan kontrol yang ditentukan harus berdasarkan kesepakatan antara auditor dengan *auditee.*

Pernyataan

Membuat pernyataan berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah ditetapkan berdasarkan standar ISO 27002. Contoh Pernyataan dapat dilihat pada Tabel 2.

Tabel 2. Tabel Pernyataan

PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK DAN LINGKUNGAN)	
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.1 pembatas keamanan fisik (*Physical security perimeter*)	
Kontrol : Pembatasan keamanan (dinding pembatas, kontrol kartu akses, atau penjaga) harus disediakan untuk melindungi wilayah atau ruang penyimpanan informasi dan perangkat pemrosesan informasi	
No.	PERNYATAAN
1	Adanya perlindungan keamanan fisik (dinding,kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi
2	Adanya penggunaan parimeter keamanan untuk melindungi ruang berisikan fasilitas pemrosesan informasi (dinding,pintu,kartu kontrol dan meja dengan resepsionis)

Pernyataan yang berdasarkan standar ISO 270002 digunakan untuk memudahkan auditor sebagai acuan membuat pertanyaan untuk wawancara audit keamanan sistem informasi.

Pembobotan

Setelah membuat pernyataan, maka langkah selanjutnya adalah melakukan pengukuran pembobotan pada setiap pernyataan dimana nilai pembobotan telah disepakati oleh pihak RSU Haji Surabaya. Salah satu contoh Pembobotan dapat dilihat pada Tabel 3.

Tabel 3.Pembobotan

PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK DAN LINGKUNGAN)	Auditor: Annisa Destiara
	Auditee: Bu Pelma Yunita
	Tanggal: 19 Juli 2012
	Tanda Tangan:
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.1 pembatas keamanan fisik (*Physical security perimeter*)	
Kontrol : Pembatasan keamanan (dinding pembatas, kontrol kartu akses, atau penjaga) harus disediakan untuk melindungi wilayah atau ruang penyimpanan informasi dan perangkat pemrosesan informasi	

No.	PERNYATAAN	Bobot
1	Adanya perlindungan keamanan fisik (dinding,kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi	1

Pertanyaan

Pertanyaan yang dibuat mengacu pada Pernyataan yang ada dimana satu pernyataan bisa memiliki lebih dari satu pertanyaan, hal tersebut dikarenakan setiap pertanyaan harus mewakili pernyataan pada saat dilakukan wawancara.

Pemeriksaan Data dan Bukti

Pemeriksaan data dilakukan dengan cara melakukan observasi dan melakukan wawancara kepada *auditee* sesuai dengan ruang lingkup serta klausul yang telah disepakati oleh kepala instalasi SIM-RS RSU Haji Surabaya. Contoh dokumen pemeriksaan dapat dilihat pada Tabel 4.

Tabel 4. Dokumen Pemeriksaan

No	Pemeriksaan	Catatan Pemeriksaan	Catatan Review
Klausul 8.1 Keamanan Sumber Daya Manusia Sebelum Menjadi Pegawai (*Prior to Employement*)			
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)			
1	Cek dokumentasi peraturan pada proses penerimaan pegawai sistem informasi Ref : ISO 270002 8.1.1		

Wawancara

Pada proses ini langkah yang dilakukan adalah melakukan wawancara berdasarkan pertanyaan yang telah dibuat. Contoh hasil wawancara dengan *auditee* dapat dilihat pada Gambar 2.

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK DAN LINGKUNGAN)	Auditor : Annisa Destiara Y
	Auditee : Bu Pelma Yunita
	Tanggal: 19 Juli 2012
	Tanda Tangan:
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.1 pembatas keamanan fisik (*Physical security perimeter*)	
1	Adanya perlindungan keamanan fisik (dinding,kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi
	P: Adakah perlindungan keamanan fisik (dinding,kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi? J: Tidak ada perlindungan fisik hanya terdapat pintu dan dinding untuk akses masuk. P: Adakah dokumentasi perlindungan keamanan fisik (dinding,kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi? J: Belum ada dokumentasi untuk perlindungan keamanan fisik terhadap ruang pemrosesan informasi.

Gambar 2. Hasil Wawancara

Dari hasil wawancara dengan dengan penanggung jawab Instalasi SIM-RS pada salah satu klausul 9 (Sembilan) Keamanan Fisik dan Lingkungan dengan obyek kontrol 9.1.1 (pembatas keamanan fisik (*Physical security perimeter*)) untuk pembatas keamanan fisik masih banyak terdapat kekurangan untuk parimeter keamanan dan pembatas fisik untuk Instalasi SIM-RS sehingga masih banyak yang harus di benahi dalam keamanan pembatas fisik.

Uji Kematangan

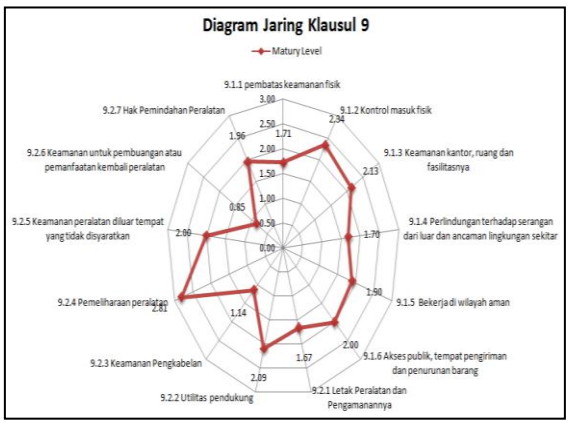
Setelah seluruh penentuan nilai telah ditetapkan, maka dapat langkah berikutnya yaitu melakukan perhitungan *marturity level*. Contoh kerangka kerja perhitungan *marturity* Perhitungan tersebut dilakukan secara bertahap. Tahapan perhitungan *maturity leve*dapat dilihat pada tabel 5, gambar 3 dan 4 .

Tabel 5. Penentuan *Maturity Level* Klausul 9 Keamanan Fisik dan Lingkungan

Klausul 9 (Keamanan Fisik dan Lingkungan)										
Klausul 9.1 Wilayah Aman (Secure Areas)										
ISO 27002 9.1.1 pembatas keamanan fisik (*Physical security perimeter*)				Tingkat Kematangan						Nilai
No	Pernyataan	Hasil Pemeriksaan	bobot	0	1	2	3	4	5	
1	Adanya perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi	Terdapat dinding untuk perlindungan keamanan fisik ruang pemrosesan informasi, tetapi penjaga pintu hanya terdapat pada pintu masuk RSU Haji untuk khusus SIM-RS tidak terdapat penjaga pintu Bukti : Foto dinding pada ruang Instalasi SIM-RS	1				3			3

Gambar 3 Hasil Maturity Level Klausul 9 Keamanan Fisik dan Lingkungan

Tabel Penentuan Maturity Level						
Klausul 11 Kontrol Akses						
No	Objektif kontrol	Kontrol keamanan	Jumlah Bobot	Nilai	Tingkat Kematangan	Rata-rata Objektif kontrol
1	Klausul 9.1 Wilayah Aman (*Secure Areas*)	9.1.1 pembatas keamanan fisik	9.80	16.80	1.71	1.96
		9.1.2 Kontrol masuk fisik	8.80	20.60	2.34	
		9.1.3 Keamanan kantor, ruang dan fasilitasnya	21.70	46.20	2.13	
		9.1.4 Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar	30.40	51.60	1.70	
		9.1.5 Bekerja di wilayah aman	11.90	22.60	1.90	
		9.1.6 Akses publik, tempat pengiriman dan penurunan barang	5.00	10.00	2.00	
2	Klausul 9.2 Keamanan Peralatan (*Equipment Security*)	9.2.1 Letak Peralatan dan Pengamanannya	6.00	10.00	1.67	1.79
		9.2.2 Utilitas pendukung	9.60	20.10	2.09	
		9.2.3 Keamanan Pengkabelan	11.10	12.70	1.14	
		9.2.4 Pemeliharaan peralatan	7.70	21.60	2.81	
		9.2.5 Keamanan peralatan diluar tempat yang tidak disyaratkan	5.00	10.00	2.00	
		9.2.6 Keamanan untuk pembuangan atau pemanfaatan kembali peralatan	5.30	4.50	0.85	
		9.2.7 Hak Pemindahan Peralatan	4.90	9.60	1.96	
Maturity Level Klausal 9 (Keamanan Fisik dan Lingkungan)						1.88



Gambar 4 Representasi Nilai *Maturity Level* Klausul 9 (Keamanan Fisik dan Lingkungan

Hasil dari proses perhitungan *maturity level* pada seluruh klausul adalah 1,75 yaitu *Initial*. Hasil tersebut munjukkan bahwa sebagian besar proses keamanan sistem informasi yang ada pada Instalasi SIM-RS belum dilakukan secara rutin dan belum sesuai dengan standar prosedur yang ada.

Temuan dan Rekomendasi

Pada proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah memeriksa data profil perusahaan, kebijakan, standar, prosedur, melakukan observasi *standard operating procedure* dan hasil wawancara dengan *auditee*. Contoh temuan dan rekomendasi dapat dilihat pada Gambar 5.

TEMUAN AUDIT TEKNOLOGI INFORMASI					Auditor : Annisa DestiaraY Auditee : Pelma Yunita
ASPEK : KLAUSUL 9 (KEAMANAN FISIK DAN LINGKUNGAN) ISO 27002 9.1.1 pembatas keamanan fisik (*Physical security perimeter*)					Tanggal : 18 Juni 2012 Tanda Tangan :
No	Pernyataan	Temuan	Ref	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
1	Adanya perlindungan keamanan fisik (dinding,kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi	Terdapat dinding untuk perlindungan keamanan fisik ruang pemrosesan informasi, tetapi penjaga pintu hanya ada di pintu masuk utama RSU Haji untuk Instalasi SIM-RS tidak ada	Pertanyaan klausul 9.1.1 no 1 ⇩ Bukti foto Lampiran 13 hal 3 no 1	Ref : ISO 270002 9.1.1 Penyebab : Pihak instalasi SIM-RS telah mengajukan untuk menambah perlindungan fisik tetapi belum mendapat jawaban persetujuan dari direksi Risiko : - Akses masuk tanpa ijin dari pihak luar yang dapat membahayakan fasilitas pemrosesan informasi - Tidak ada pembedaan antara pegawai yang memiliki akses dengan yang tidak	Tanggapan : Kami pihak SIM-RS memang tidak memiliki fasilitas maupun peralatan untuk perlindungan keamanan fisik seperti penjaga pintu dan kartu akses tetapi kami masih memiliki dinding untuk perlindungan ruang pemrosesan informasi Komitmen Penyelesaian : Kami pihak SIM-RS menyetujui rekomendasi yang diberikan untuk menambahkan buku tamu akan kami terapkan tetapi untuk penambahan alat kami masih menunggu persetujuan dari direksi

Gambar 5 Temuan dan Rekomendasi

Penjelasan sebagai berikut:

Pernyataan:

Adanya perlindungan keamanan fisik (dinding,kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi

Temuan :

Terdapat dinding untuk perlindungan keamanan fisik ruang pemrosesan informasi, tetapi penjaga pintu hanya terdapat pada pintu masuk RSU Haji untuk khusus SIM-RS tidak terdapat penjaga pintu

Rekomendasi:

- Menambahkan buku tamu untuk mencatat aktifitas yang dilakukan pengunjung pada Instalasi SIM-RS
- Mengajukan ke direksi untuk penambahan peralatan kontrol otentikasi seperti kartu gesek atau peralatan biometrik lainnya seperti *finger print*.

KESIMPULAN

1. Instalasi SIM-RS memiliki kekurangan pada keamanan fisik dan lingkungan disebabkan karena belum adanya kontrol, aturan, kebijakan, standar untuk perlindungan keamanan fisik dan lingkungan dan masih belum lengkapnya batas parimeter, peralatan otentikasi, fasilitas untuk

mendukung dalam pemeliharaan dan perlindungan keamanan fisik dan lingkungan.

2. Penyalahgunaan *password* disebabkan belum adanya dokumen maupun pernyataan tertulis untuk membuat manajemen *password*, belum terdapat pemberian sanksi bagi pengguna yang melanggar *password* dan masih banyaknya pengguna *password* yang belum memiliki kesadaran untuk menjaga keamanan *password*
3. Belum adanya pencatatan mengenai insiden kelemahan keamanan informasi yang disebabkan karena tidak terdapat kebijakan, prosedur maupun aturan untuk menanggulangi insiden kelemahan sistem informasi
4. Nilai *maturity level* yang dihasilkan oleh Instalasi SIM-RS pada RSU Haji Surabaya yaitu 1,75 yang masuk pada kategori level 1 yaitu *Initial*. Hal tersebut menandakan bahwa Instalasi SIM-RS belum menyadari kebutuhan TI dan yang dilakukan tanpa adanya standar yang sesuai dengan ISO 27002. Dapat dilihat bahwa belum adanya kebijakan dan prosedur untuk melakukan pembahasan keamanan fisik dan lingkungan, kontrol akses, dan akuisis sistem infomasi, pembangunan dan pemeliharaan, belum terdapat kontrol keamanan yang diterapkan dimana terdapat bukti bahwa masalah keamanan ada dan perlu ditangani, tidak ada kontrol untuk mengatasi masalah ini dan kurangnya pendokumentasian prosedur, kebijakan dan peraturan.

SARAN

1. RSU Haji Surabaya dapat melakukan Audit Keamanan Sistem Informasi secara berkala selama 6 bulan atau 1 tahun sekali agar keamanan sistem informasi tetap terkontrol audit dapat dilakukan oleh penanggung jawab Instalasi SIM-RS demi meningkatkan keamanan sistem informasi pada Instalasi SIM-RS.
2. Diharapkan pengembang dapat merancang tata kelola TI pada RSU Haji Surabaya dengan berdasarkan laporan audit yang telah dihasilkan.

DAFTAR PUSTAKA

DepKes RI. (1992). Keputusan Menteri Kesehatan RI No. 983/MenKes/SK/XI/1992. *Pedoman Organisasi Rumah Sakit Umum*.

Ermana, Fine. 2011. Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 20071 Pada PT. BPR JATIM : STIKOM Surabaya. Laporan Tugas Akhir STIKOM Surabaya.

Hermawan, Budi. 2011. *Dasar-Dasar Audit dan Pengendalian TI*. http://www.auditti.com/stikom. Diakses pada tanggal 1 Desember 2011.

ISACA. 2010. *Guide to the Audit of IT Application*. Switzerland : Felice Lutz.

ISO 27000 Dictionary. 2008. *The Information Portal for ISO27002*. http://www.27000.org/iso-27002.htm. Diakses tanggal 7 April 2012 pukul 08.00.