AUDIT KEAMANAN SISTEM INFORMASI MANAJEMEN RUMAH SAKIT BERDASARKAN ISO 27002:2005 PADA RUMAH SAKIT ISLAM JEMURSARI

Alfian N Rahman [1] Haryanto Tanuwijaya [2] Erwin Sutomo [3]
Fakultas Teknik Informatika
Program Studi S1 Sistem Informasi
Institut Bisnis dan Informatika Stikom Surabaya
Jl. Kedung Baruk 98 Surabaya, 60298
Email : 1) fian.nr@gmail.com, 2) haryanto@stikom.edu, 3) sutomo@stikom.edu

Abstract

Jemursari Islamic Hospital Surabaya is a company which focuses on medical service. This hospital uses Hospital Management Information System (SIM-RS) to undergo its business processes. There are obstacles during the implementation of HMIS including: frequent of information leak, the defect of information tools, and the low awareness of information security among the employees. It causes the emerge of some risk such as information misuses, privileges misuse by the unconcerned employees, failure in data processing, even cybercrime or data theft that causes data lost.

To overcome those problems, Jemursari Islamic Hospital Surabaya performs information system security audit using ISO 27002:2005 as the best practice in information security. The steps are taken from ISACA steps. The scopes which are checked based on the problems are Human Resource Security, Physical and Environmental Security, Information System Access Control and Acquisition, Development and Maintenance.

The management information system security audit produces maturity level 3,47 which is in defined category. It shows that most of information system security processes already have rules and routinely implemented. This research also produce a recommendation to improve the processes of HMIS in Jemursari Islamic Hospital Surabaya.

Keywords: Information System Security Audit, Hospital, ISO 27002, SIM-RS

Rumah Sakit Islam Jemursari telah menerapkan Sistem Informasi Manajemen Rumah Sakit (SIM-RS) tahun 2008 yang sudah terintegrasi oleh bagian-bagian rumah sakit mulai dari layanan penerimaan pasien hingga, pelayanan rawat inap, pelayanan rawat jalan, pelayanan poli, rekam medik, apotek hingga pelayanan administrasi.

Dalam praktik penerapan SIM-RS masalah yang terjadi antara lain sering terjadinya kebocoran informasi oleh karyawan yang tidak berhak, masih banyak karyawan yang membiarkan unit komputernya menyala pada saat meninggalkan atau saat sedang jam istirahat, masih banyak karyawan yang tidak menjaga data dan *password*, kerusakan peralatan. Hal-hal tersebut dapat beresiko hak akses disalahgunakan oleh karyawan yang tidak berkepentingan, kegagalan dalam pemrosesan informasi, pencurian informasi, kerusakan peralatan yang dapat merambat pada kehilangan data.

Untuk menyelesaikan permasalahan RSI Jemursari dibutuhkan untuk melakukan audit keamanan sistem informasi untuk mengetahui permasalahan yang terjadi. Keamanan informasi yang ditujukan untuk menjaga aspek Kerahasiaan (*Confidentiality*), Keutuhan (*Integrity*) dan Ketersediaan (*Availability*) dari Informasi (ISO/IEC 27002, 2005). Menurut Tanuwijaya dan Sarno (2010) agar audit keamanan sistem informasi berjalan dengan baik, maka diperlukan suatu standar untuk melakukan audit keamanan sistem informasi. Standar audit yang digunakan mengacu pada *Information Systems Audit and Control Association* (ISACA) dengan standar best *practice International Standard Organization* ISO 27002 (2005). Standar ISO 27002 sebagai *best practice* penerapan keamanan informasi dengan menggunakan bentuk kontrol agar dapat mencapai sasaran yang diterapkan.

Ruang lingkup yang digunakan dalam audit keamanan sistem informasi ini adalah Keamanan Sumber Daya Manusia (Klausul 8), Keamanan Fisik dan Lingkungan (Klausul 9), Kontrol Akses (Klausul 11), Akuisi Sistem Informasi, Pengembangan dan Pemeliharaan (Klausul 12) yang telah dengan permasalahan dan kesepakatan dengan manajeman RSI Jemursari.

Dengan dilakukannya audit keamanan informasi pada Rumah Sakit Islam Jemursari dapat menghasilkan nilai *maturity level*, jaring laba-laba dan memberikan rekomendasi tentang keamanan SIM-RS yang dimiliki RSI jemursari. Hasil audit ini dapat menjadi rekomendasi yang dapat digunakan untuk meningkatkan keamanan sistem informasi yang ada pada Rumah Sakit Islam Jemursari.

Landasan Teori

Audit

Menurut (Canon, 2011) Audit merupakan suatu proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti dan dievaluasi secara objektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang diterapkan.

Audit Keamanan Sistem Informasi

Menurut (Ahmad, 2012) Audit Keamanan Sistem Informasi adalah proses atau kejadian yang mengacu pada kebijakan atau standar keamanan guna menentukan semua kondisi dari perlindungan yang ada dan untuk melakukan verifikasi perlindungan yang ada sudah berjalan dengan baik dan benar.

Sistem Informasi Manajeman Rumah Sakit

Berdasarkan Peraturan Menteri Kesehatan No 82 Tahun 2013 SIM-RS adalah sistem teknologi informasi komunikasi untuk melakukan proses dan mengintegrasikan seluruh alur proses pelayanan suatu Rumah Sakit dalam bentuk jaringan koordinasi, pelaporan dan prosedur administrasi untuk memperoleh informasi secara tepat dan akurat, dan merupakan bagian dari Sistem Informasi Kesehatan.

ISO 27002 : 2005

ISO 27002: 2005 merupakan suatu standar keamanan informasi sebagai best practice atau panduan umum yang dapat menejaskan contoh penerapan keamanan informasi dengan mempergunakan bentuk kontrol sehingga dapat dicapainya sasaran yang diterapkan. Standar ISO 27002: 2005 dapat dipergunakan sebagai titik awal dalam menyusun dan mengembangkan ISMS. Standar ISO 27002: 2005 mampu memberikan panduan dalam merencanakan dan mengimplementasian suatu program untuk melindungi aset-aset informasi.

Tingkat Kedewasaan (Maturity Level)

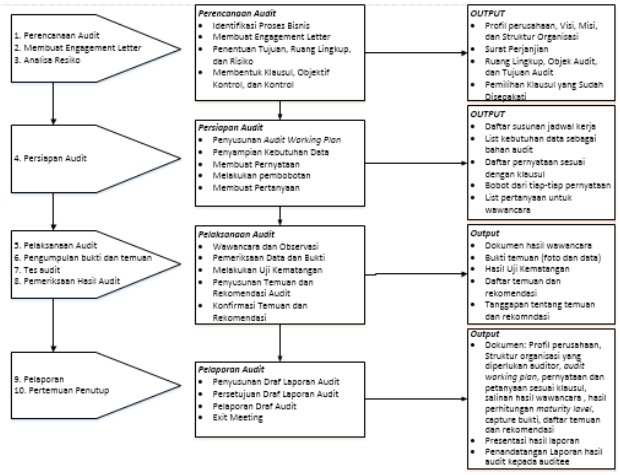
Menurut IT Governance Institute (2007: 17) *maturity level* merupakan model yang digunakan untuk pengendalian suatu proses TI yang terdiri dari pengembangan metode penilaian sehingga suatu organisasi dapat mengukur dirinya sendiri. Dalam penilaian *maturity level*, dilakukan menggunakan lima tingkatan proses CMMI. Metode CMMI digunakan sebagai acuan untuk perbandingan serta memiliki peran sebagai alat bantu untuk memahami tingkah laku, praktik, dan proses-proses dalam organisasi. Lima tingkatan kerangka kesatuan CMMI adalah sebagai berikut

a. Level 0 *(non-existent)*: Tidak ada kontrol sama sekali.
b. Level 1 *(initial)*: Pada level ini, organisasi memiliki pendekatan yang tidak konsisten, kontrol keamanan dilakukan secara informal.
c. Level 2 *(limited/repeatable)*: Pada level ini, kontrol keamanan masih dalam pengembangan dan ada dokumentasi terbatas untuk mendukung kebutuhan.

d. Level 3 *(defined)*: Pada level ini, kontrol keamanan telah terdokumentasikan secara rinci dan telah dilakukan komunikasi kepada user melalui pelatihan, tetapi tidak ada pengukuran kepatuhan.
e. Level 4 *(managed)*: Pada level ini, sudah ada pengukuran efektivitas kontrol keamanan, tetapi tidak ada bukti dari setiap ulasan kepatuhan dan kontrol memerlukan perbaikan lebih lanjut untuk mencapai tingkat kepatuhan yang diperlukan.
f. Level 5 *(optimized)*: Pada level ini, kontrol keamanan telah disempurnakan hingga sesuai dengan ISO 27002 berdasarkan pada kepemimpinan yang efektif, manajemen perubahan, perbaikan berkelanjutan, dan pengkomunikasian internal.

METODE

Dalam dahapan audit dibagi menjadi sepuluh tahapan yang terdiri dari: membuat dan mendapatkan surat persetujuan audit, perencanaan audit, analisis risiko, persiapan audit, pelaksanaan audit, pengumpulan bukti dan temuan, tes audit, pemeriksaaan hasil audit, pelaporan audit, pertemuan penutup. (Cannon, 2010)



Gambar 1 Langkah-langkah Audit Sistem Informasi (Sumber Cannon, 2011)

IMPLEMENTASI DAN HASIL

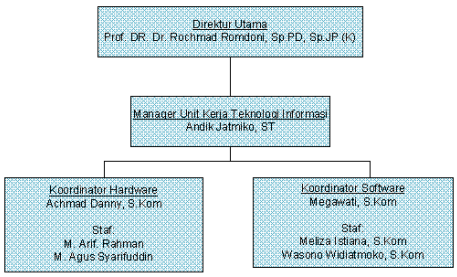
Identifikasi Proses Bisnis dan TI

Dalam menjalankan proses bisnisnya RSI Jemursari mempunyai visi "Menjadi Rumah Sakit Islam Berstandar Internasional". Untuk mencapau visi tersebut, RSI Jemursari mempunyai misi sebagai berikut:

a. Memberikan pelayanan jasa rumah sakit secara prima dan Islami menuju Standar Mutu Pelayanan Internasional dengan dilandasi prinsip kemitraan
b. Melaksanakan Manajemen Rumah Sakit berdasarkan Manajemen Syariah yang berstandar Internasional
c. Membangun SDM Rumah Sakit yang profesional sesuai standar Internasional yang Islami dengan diiringi integritas yang tinggi dalam pelayanan
d. Menyediakan sarana prasarana rumah sakit untuk mewujudkan implementasi pelayanan Islami dan berstandar Internasional.

RSI Jemursari mempunyai motto "Kami selalu melayani dengan Ramah, Senyum, Ikhlas, dan Salam".

Bagian Teknologi dan Sistem Informasi Rumah Sakit Jemursari memiliki struktur organisasi seperti di Gambar 2



Gambar 2 Struktur Organisasi Bagian Teknologi dan Sistem Informasi

Menentukan Ruang Lingkup, Objek dan Tujuan Audit

Untuk menentukan ruang lingkup dilakukan dengan cara melakukan observasi dan wawancara

pada bagian teknologi dan sistem informasi RSI Jemursari. Adapun hasil penentuan ruang lingkup yang akan di audit mengenai Sistem Informasi Manajemen Rumah Sakit (SIM-RS). Objek audit adalah bagian yang bertanggungjawab tentang SIM-RS yaitu bagian teknolodi dan sistem informasi. Tujuan audit agar dapat mengukur hasil *maturity level* dengan standar ISO/IEC 27002 : 2005 beserta temuan dan rekomendasi

Membuat *Engangement Letter*

Setelah menentukan ruang lingkup, objek dan tujuan audit, langkah selanjutnya adalah membuat *Engagment Letter*. Isi dari *Engagement Letter* adalah *role*, tanggung jawab, lingkup audit, pelaksanaan audit dan ketentuan selama dilakukan audit audit. Pada proses ini akan menghasilkan perjanjian yang harus di patuhi oleh auditor dan *auditee*.

Penentuan Klausul, Objektif Kontrol, dan Kontrol

Hasil dari tahap identifikasi ruang lingkup adalah penentuan klausul yang digunakan beserta pemetaan klausul, kontrol objektif dan kontril keamanan. Dalam menentukan klausul yang digunakan, diperolah dari hasil wawancara. Kesimpulan dari hasil wawancara tentang permasalahan yang terjadi di RSI Jemursari adalah:

1. Adanya kebocoran informasi pada pegawai yang tidak memiliki hak atas informasi tersebut. Selain itu masih banyak pegawai yang membiarkan unit komputernya menyala pada saat meninggalkan atau saat sedang jam istirahat. Masalah lain adalah masih banyak karyawan yang tidak mengubah *password* dan ada karyawan lain mengetahui *password* dari karyawan lainnya. Hal tersebut berisiko penyalahgunaan hak akses oleh karyawan yang tidak berkepentingan dan bisa merambat untuk penyalahgunaan informasi yang meruginakan pihak RSI Jemursari.
2. Ditemukan kerusakan peralatan pendukung sistem informasi misal perangkat jaringan misal kabel LAN (*Local Area Network*) dan *Router* karena dirusak oleh binatang. Selain itu ada kerusakan alat yang disebabkan oleh air dikarenakan alat-alat tersebut tidak mempunyai perlindungan perangkat kemamanan yang ada ataupun belum ditempatkan pada tempat yang memenuhi standart keamanan SIM-RS dari peraturan pemerintah. Hal tersebut bisa berakibat kegagalan dalam pemrosesan data yang bisa merambat kehilangan data sehingga mengakibatkan kerugian organisasi.

Dari kesimpulan wawancara diatas penggunaan klausul, kontrol objektif dan kontrol keamanan adalah

1. Klausul 8 tentang Keamanan Sumberdaya Manusia
2. Klausul 9 tentang Keamanan Fisik dan Lingkungan
3. Klausul 11 tentang Kontrol Akses
4. Klausul 12 tentang Akuisisi Sistem Informasi, Pengembangan dan Pemeliharaan

Penyusunan *Audit Working Plan*

Penyusunan *audit working plan* dilakukan untuk merencanakan dan mengawasi audit sistem informasi. Pelaksanaan audit keamanan sistem informasi manajeman rumah sakit pada Rumah Sakit Islam Jemursari dilakukan secara bertahap sesuai dengan jadwal.

Tabel 1 *Audit Working Plan*

NO	Pekerjaan	Bulan											
		Maret				April				Mei			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Study Literautur												
	Melakukan identifikasi proses bisnis dan TI.												
	Melakukan identifikasi terhdap klausul												
	Menentukan Standart												
	Membuat enggament letter												
2	Menyusun Working Plan												
	Membuat Pernyataan dan Pertanyaan												
	Melakukan Pembobotan												
3	Wawancara												
	Pemeriksaan												
	Penemuan Bukti												
	Uji coba Kematangan												
	Menyusun temuan dan recomendasi												
4	Menyusun Draft Pelaporan												
	Presentasi Laporan												
	Meminta persetujuan laporan												

Audit Working Plan dapat dilihat pada Tabel 1

Penyampaian Kebutuhan Data

Dalam proses penyampaian kebutuhan data, auditor memberikan list kebutuhan data-data yang digunakan selama proses audit kepada *auditee*. List kebutuhan data digunakan untuk menunjang proses audit. Contoh list kebututuhan data dapat dilihat pada Tabel 2

Tabel 2 Permintaan Kebutuhan Data

Permintaan Kebutuhan Data/Dokumen						
No.	Data Yang Diperlukan	Ketersediaan Data		ket	Tanda Tangan	
		Ada	Tidak Ada		*Auditee*	Auditor
1	Profil RSI Jemursari	√				
2	Struktur Organisasi RSI Jemursari	√				
3	Tugas Pokok dan Fungsi Karyawan	√				

Membuat Pernyataan

Pernyataan dibuat berdasarkan kontol keamanan yang terdapat pada setiap klausul yang terdapat pada ISO 27002. Contoh Pernyataan dapat dilihat pada Tabel 3.

Tabel 3 Tabel Pernyataan

Klausul: 9 Keamanan Fisik dan Lingkungan	
Objektif Kontrol : 9.1 Wilayah Aman	
ISO 27002 9.1.1 Pembatasan Keamanan Fisik	
No	Pernyataan
1	Terdapat pendefinisian parimeter keamanan secara jelas terhadap ruangan pemrosesan informasi
2	Terdapat penggunaan parimeter keamanan untuk melindungi ruang fasilitas pemrosesan informasi

Membuat Pembobotan

Pembobotan diberikan kepada tiap pernyataan. Pembobotan disesuaikan seberapa besar resiko yang terjadi untuk organisasi dan juga disesuaikan dengan fokus audit yang digunakan. Jika ada indikasi resiko berpengaruh besar pada perusahaan maka diberikan bobot satu. Apabla diindikasikan tidak beresiko sedikitpun untuk perusahaan maka nilai dari pembobotan adalah nol. Contoh Pernyataan dapat dilihat pada Tabel 4

Tabel 4 Pembobotan

Klausul: 9 Keamanan Fisik dan Lingkungan		
Objektif Kontrol : 9.1 Wilayah Aman		
ISO 27002 9.1.1 Pembatasan Keamanan Fisik		
No	Pernyataan	Bobot
1	Terdapat pendefinisian parimeter keamanan secara jelas terhadap ruangan pemrosesan informasi	1
2	Terdapatpenggunaan parimeter keamanan untuk melindungi ruang fasilitas pemrosesan informasi	1

Membuat Pertanyaan

Pada proses membuat pertanyaan mengacu pada pernyataan yang telah dibuat sebelumnya. Pertanyaan disesuaikan berdasarkan pelaksanaan kontrol yang ada pada standard ISO 27002. Contoh Pernyataan dapat dilihat pada Tabel 5

Tabel 5 Pernyataan

Klausul: 9 Keamanan Fisik dan Lingkungan		
Objektif Kontrol : 9.1 Wilayah Aman		
ISO 27002 9.1.1 Pembatasan Keamanan Fisik		
No	Pernyataan	Pertanyaan
1	Adanya pendefinisian parimeter keamanan secara jelas terhadap ruangan pemrosesan informasi	1. Apakah sudah didefinisikan tentang parimeter ? 2. Pendefinisian parameter sudah di sosialisasikan?

Wawancara dan Observasi

Proses wawancara dan observasi, auditor melakukan wawancara dan observasi berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan kepada pihak yang terlibat didalamnya yaitu auditee. Contoh wawancara dapat dilihat pada Tabel 6.

Tabel 6 Wawancara

Audit Keamanan Sistem Informasi **KLAUSUL 9** **Keamanan Sumber Daya Manusia** (Objektif Kontrol : 9.1 Wilayah Aman)		Auditor : Alfian N Rahman Auditee : Andik Jatmiko, ST Tanggal : _____ TTD:_____
Kontrol: 9.1.1 Pembatasan Keamanan Fisik		
Peryataan	Pertanyaan	Jawaban
Adanya pendefinisian parimeter keamanan secara jelas terhadap ruangan pemrosesan informasi	1. Apakah sudah didefinisikan tentang parimeter?	Belum ada pendefinisian parimeter secara jelas
	2. Pendefinisian parameter sudah di sosialisasikan?	Belum ada sosialisasi tentang parimeter

Pemeriksaan Data dan Bukti

Pemeriksaan data dan bukti mengacu pada hasil dari wawancara yang dilakukannya. Dalam pemeriksaan data dan bukti kita melakukan *review* tentang data atau bukti yang di temukan dari proses wawancara. Contoh pemeriksaan data dan bukti dapat dilihat pada Tabel 7.

Tabel 7 Pemeriksaan Bukti dan Data

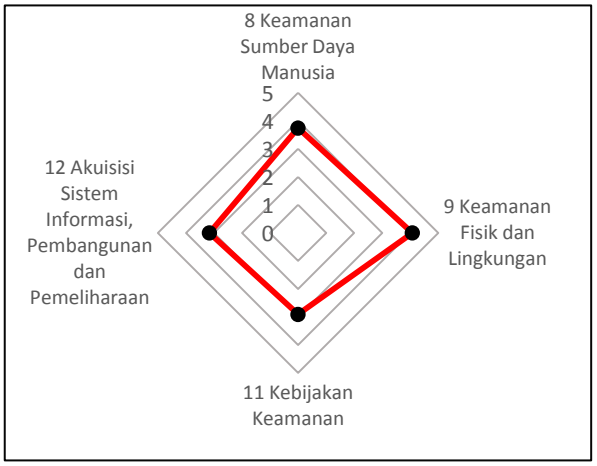
Pemeriksaan Bukti dan Data **KLAUSUL 9** **Keamanan Sumber Daya Manusia** (Objektif Kontrol : 9.1 Wilayah Aman)		Auditor : Alfian N Rahman Auditee : Andik Jatmiko, ST Reviwer : Haryanto Tanuwijaya
Pemeriksaan	**Catatan Pemeriksaan**	**Catatan Reviewer**
Cek Jalur Evakuasi dan tanda jalur evakuasi	Ada jalur evakuasi di setiap gedung, dan tanda jalur evakuasi hingga diarahkan di titik kumpul evakuasi.	

Melakukan Uji Kematangan

Setelah Seluruh penentuan nilai ditetapkan, maka tahap selanjutnya adalah melakukan penghitungan *maturity level*. Dari hasil keseluruhan perhitungan *maturity level* semua kalusul mendapatkan nilai 3,47 yaitu *defined*. Hal tersebut menunjukan bahwa sebagian besar proses keamanan sistem informasi sudah mempunyai aturan dan dilakukan secara rutin. Untuk lebih detil dapat dilihat pada Tabel 8 detil nilai tiap klausul dan Gambar 3 representasi semua klausul jaring laba-laba.

Tabel 8 Detil Nilai Klausul

Klausul	**Tingkat Kematangan**
8 Keamanan Sumber Daya Manusia	3,74
9 Keamanan Fisik dan Lingkungan	4,09
11 Kebijakan Keamanan	2,91
12 Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	3,16
Rata-rata tingkat kematangan	***3,47***



Gambar 3. Representasi Jaring Laba-Laba Semua Klausul

Hasil pengukuran *maturity level* klausul 8 tentang Keamanan Sumber Daya Manusia yaitu 3,74 dan klausul 12 tentang Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan yaitu 3,16 yaitu berada pada level 3 *(defined)* yang berarti manajeman sudah mempunyai dasar tentang aturan, prosedur dan kebijakan pada proses keamanan sumber daya manusia dan pemeliharaan serta pengembangan sistem informasi. Tetapi ada beberapa hal yang terkait dengan penerapan aturan yang belum dilakukan. Hasil pengukuran *maturity level* klausul 9 tentang Keamanan Fisik dan Lingkungan yaitu 4,09 yaitu berada pada level 4 (*managed)* yang berarti manajeman sudah mempunyai dasar tentang aturan, prosedur dan kebijakan dan hampir semuanya sudah terdokumentasi pada proses keamanan fisik dan lingkungan. Tetapi masih ditemukan beberapa aturan kecil yang belum dilakukan dan dimiliki oleh organisasi. Hasil pengukuran *maturity level* klausul 11 tentang Kontrol Akses yaitu 2,91 yaitu berada di level 2 (*limited/repeatable*) yang berarti manajeman sedang melakukan pengembangan pada proses kontrol akses dan belum mempunyai sebegian besar aturan dasar tentang kontrol akses.

Penyusunan Temuan dan Rekomendasi

Penyusunan temuan dan rekomendasi sebagai hasil dari evaluasi muncul setelah dilakukan pembandingan antara apa dan hal yang seharusnya dilakukan dengan proses yang sedang berlangsung di perusahaan. Contoh temuan dan rekomdasi dapat dilihat pada Tabel 9.

Tabel 9. Temuan dan Rekomendasi

Temuan dan Rekomendasi Audit Keamanan Sistem Informasi				Auditor : Alfian N Rahman Auditee : Andik Jatmiko ST Tanda Tangan Tanggal: _____	
Klausul: 11 (Kontrol Akses) **11.2.4 Tinjauan Terhadap Hak User**					
No	Pernyataan	Temuan	Bukti	Rekomendasi	Tanggapan
1	Adanya pengkajian ulang hak akses pengguna dalam rentang waktu secara berkala	Pengkajian jarang dilakukan oleh manajemen IT terkait hak akses yang telah diberikan kepada pengguna dalam rentang waktu secara berkala	• Manajemen menyatakan pengkajian jarang dilakukan	• Membuat Penjadwalan untuk pengkajian ulang hak akses secara berkala • Membuat prosedur yang terdapat kebijakan dan aturan untuk pengkajian ulang hak akses • Evaluasi hasil daripengkajian agar dapat menentukan keamanan informasi pada organisasi Refrensi : Lampiran Surat Edaran Bank Indonesia Nomor: 9/30/DPNP Tanggal 12 Desembar 2007	• Manajeman mengakui sangat jarang dilakukan pengkajian hak akses • Manajemen menyetujui rekomendasi tersebut.

KESIMPULAN

1. Pelaksanaan audit keamanan sistem informasi dengan standar ISO 27002:2005 telah berhasil dilakukan pada Rumah Sakit Islam Jemursari. Hasil dari perhitungan *maturity level* pada seluruh klausul adalah 3,47 yaitu *defined*. Hal tersebut menunjukan bahwa sebagian besar proses keamanan sistem informasi sudah mempunyai aturan dan dilakukan secara rutin. Tetapi masih ada beberapa kebijakan, peraturan dan prosedur yang belum ada pada organisasi seperti: peraturan tentang keamanan *password*, keamanan kriptografi dan prosedur perlindungan penempatan peralatan. Selain hal tersebut masih ditemui beberapa karyawan yang tidak melaksanakan kebijakan, peraturan dan prosedur yang ada
2. Berdasarkan temuan dan bukti-bukti yang ada dalam audit keamanan sistem informasi berdasar ISO 27002 pada RSI Jemursari terdapat beberapa aturan, prosedur dan kebijakan yang belum dipatuhi oleh user. Tetapi masih ada beberapa kebijakan, peraturan dan prosedur yang belum ada pada organisasi seperti: peraturan tentang

keamanan *password*, keamanan kriptografi dan prosedur perlindungan penempatan peralatan. Hal ini mengakibatkan RSI Jemursari rentan terhadap ancaman keamanan informasi. Untuk dapat meningkatkan keamanan, akan diberikan rekomendasi-rekomendasi yang sesuai dengan refrensi keamanan informasi.

SARAN

1. Dalam melindungi keamanan informasi organisasi, diharapkan manajeman meninjau ulang dan memperbaiki aturan, prosedur yang ada dengan menambahkan aspek keamanan informasi yang lebih detil. Hal tersebut bertujuan agar ancaman-ancaman terkain keamanan informasi dapat diminimalisir.
2. Diharapkan kepada manajeman untuk melaksanaakn audit keamanan sistem informasi kembali setelah dilakukan perbaikan. Hal tersebut bertujuan untuk mengukur keberhasilan penerapan dari hasil rekomandasi sebelumnya.

DAFTAR PUSTAKA

Ahmad, A. (2012). *Bakuan Audit Keamanan Informasi Kemenpora.* Indonesia: Kementerian Pemuda dan Olahraga.

Canon, D. (2011). *CISA (Certified Information System Auditor) Study Guide (Vol. 3rd edition).* Indriana Polis: Wiley Publising.

Ahmad, A. (2012). *Bakuan Audit Keamanan Informasi Kemenpora.* Indonesia: Kementerian Pemuda dan Olahraga.

Canon, D. (2011). *CISA (Certified Information System Auditor) Study Guide (Vol. 3rd edition).* Indriana Polis: Wiley Publising.

Information Technology Governance Institute. 2007. COBIT 4.10: *Control Objective, Management Guidelines, Maturity Models. United States of America: IT Governance Institute*

ISO/IEC 27002. (2005). *Information Technology - Security techniques - Code of practice for information security management International* . ISO.

Peraturan KEMENKES RI Nomor 84 Tahun 2013 tentang Sistem Informasi Manajeman Rumah Sakit (SIM-RS).