BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini akan diuraikan tentang analisis hasil dan pembahasan dari tahap perencanaan audit sistem informasi, tahap persiapan audit sistem informasi, tahap pelaksanaan audit sistem informasi, serta tahap pelaporan audit sistem informasi.

4.1. Perencanaan Audit Sistem Informasi

4.1.1. Identifikasi Proses Bisnis dan TI

1) Profil Perusahaan

Rumah Sakit Islam Jemursari Surabaya merupakan salah satu dari 3 instansi yang dikelola oleh Yayasan Rumah Sakit Islam Surabaya (YARSIS). Dua yang lainnya adalah Rumah Sakit Islam Surabaya A. Yani dan Sekolah Tinggi Ilmu Kesehatan (STIKES) Yarsis, dengan pendirinya antara lain: KH. Zaki Goefron, KH. Abdul Majib Ridwan, KH. Thohir Syamsudin, H. Husaini Tiway dan tokoh-tokoh Islam yang lain.

Rumah Sakit Islam Jemursari Surabaya dibangun di atas lahan seluas 4.6 Ha. Konsep pembangunan rumah sakit ini adalah sebagai *garden hospital*. Oleh karena itu, Rumah Sakit Islam Jemursari Surabaya dikelilingi taman seluas 33.042 m2. Rumah Sakit ini terletak di jalan Jemursari nomor 51-57 Surabaya yang merupakan salah satu jalan protokol kota Surabaya. Rumah Sakit Islam Jemursari Surabaya resmi dibuka pada tanggal 25 Mei 2002, bertepatan dengan Maulid Nabi Muhammad SAW (12 Rabiul Awwal 1423 H). Rumah Sakit Islam Jemursari merupakan pengembangan dari Rumah Sakit Islam Surabaya jalan A. Yani. Sejak

beroperasi pada tahun 2002, Rumah Sakit Islam Jemursari Surabaya banyak mengalami perkembangan dan penambahan sarana dan prasarana, antara lain:

a. Pada akhir tahun 2005 memiliki 82 tempat tidur.

b. September 2006 bertambah menjadi 96 tempat tidur dan pembukaan ruang Kemuning (kelas III) sehingga berjumlah 108 tempat tidur.

c. September 2008 bertambah menjadi 113 tempat tidur.

d. Agustus 2009 bertambah menjadi 116 tempat tidur.

e. Awal 2011 bertambah menjadi 135 tempat tidur dengan dibukanya ruang Dahlia sebagai fasilitas rawat inap kelas II B.

f. Juli 2011 bertambah menjadi 140 tempat tidur.

g. Sekarang RSI Jemursari memiliki 202 tempat tidur.

Surat Ijin penyelenggaraan Rumah Sakit oleh Dinas Kesehatan Kota Surabaya sesuai dengan Surat Keputusan Nomor: 503.445/5342/0010/IP.RS/436.55/V tentang izin penyelenggaraan rumah sakit. RSI Jemursari merupakan rumah sakit Tipe B Non Pendidikan yang diresmikan dari Surat Keputusan Menteri Kesehatan RI Nomor: H.03.05/I/7762/2010.

2) Visi, Misi, dan Motto Perusahaan

Rumah Sakit Islam Jemursari mempunyai visi “Menjadi Rumah Sakit Islam Berstandar Internasional”. Misi dari Rumah Sakit Islam Jemursari adalah 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.

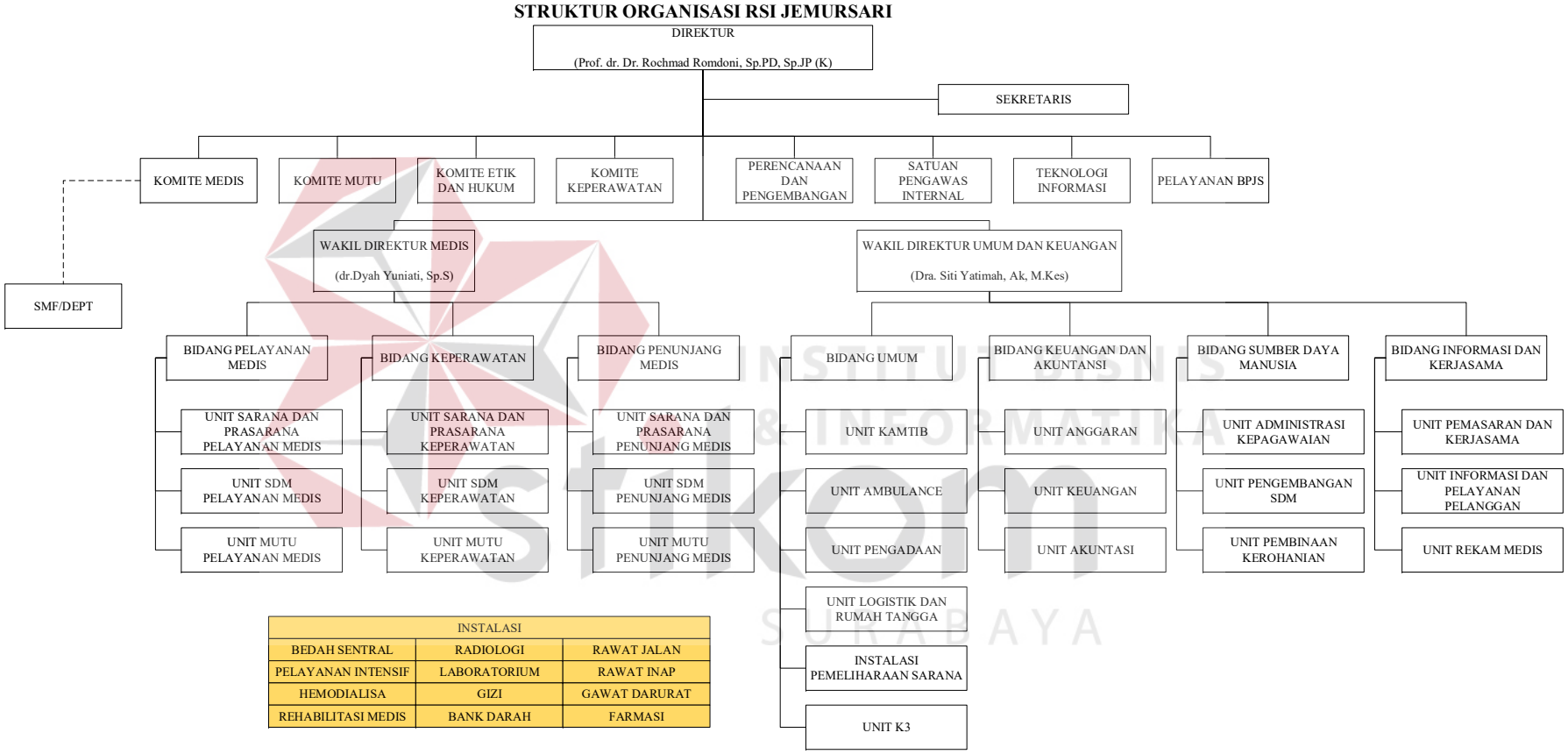
d. Menyediakan sarana prasarana rumah sakit untuk mewujudkan implementasi pelayanan islami dan berstandar internasional.

Selain itu Rumah Sakit Islam Jemursari memiliki Motto *"Kami selalu melayani dengan Ramah, Senyum, Ikhlas, dan Salam"*.

3) Struktur Organisasi

a) Struktur Organisari Rumah Sakit Jemursari

Dalam menjalankan proses bisnisnya, RSI Jemursari mempunyai bagian-bagian yang menangani bagian masing-masing. Bagian tersebut dapat dilihat pada struktur organisasi pada Gambar 4.1.



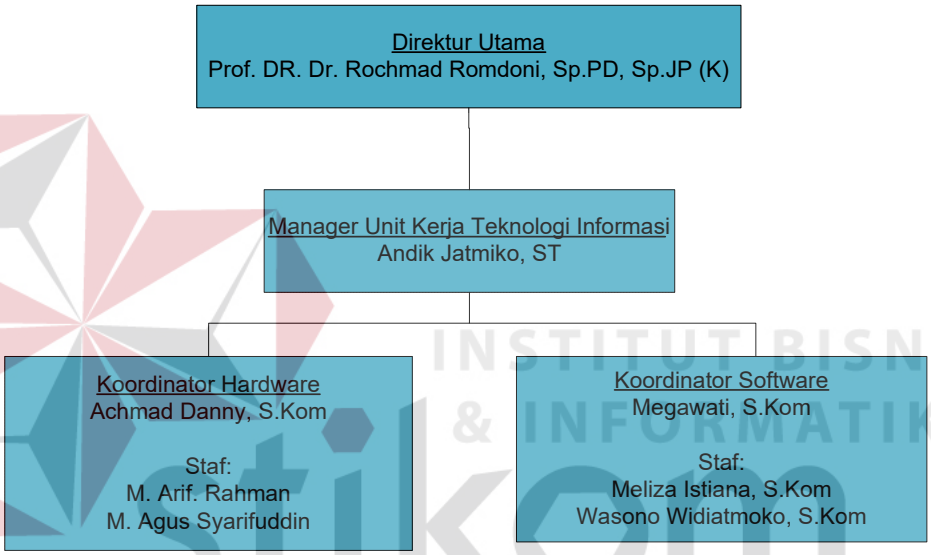
Gambar 4.1 Struktur Organisasi Rumah Sakit Islam Jemursari Sakit Islam Jemursari

Di dalam Rumah Sakit Sistem Islam Jemursari secara fungsional maka struktur organisasi terdiri dari:

1. Direktur dan Wakil Direktur (WADIR) yang masing-masing WADIR menengani bagian medis serta bagian umum dan keuangan.
2. Dibawah Direktur terdapat komite medis, komite mutu, komite etik dan hukum, komite keperawatan, bagian perencanaan dan pengembangan, bagian satuan pengawas internal, bagian teknologi dan sistem informasi, bagian pelayanan BPJS.
3. Dibawah WADIR Medis terdapat bidang pelayanan medis, bidang keperawatan, bidang penunjang medis, dan instalasi medis. Didalam naungan pelayanan medis terdapat unit sarana prasarana medis, unit SDM medis, unit mutu pelayanan medis. Di dalam naungan bidang keperawatan terdapat unit sarana prasarana keperawatan, unit SDM keperawatan, unit mutu pelayanan keperawatan. Di dalam naungan bidang penunjang medis terdapat unit sarana dan prasarana medis, unit SDM sarana dan prasaran medis, unit mutu sarana prasarana medis. Di dalam instalasi medis terdapat instalasi bedah sentral, instalasi radiologi, instalasi rawat jalan, instalasi pelayanan intensif, instalasi laboratorium, instalasi rawat inap, instalasi hemodialisa, instalasi gizi, instalasi gawat darurat, instalasi rehabilitasi medis, instalasi bank darah, dan instalasi farmasi.
4. Dibawah WADIR Umum dan Keuangan terdapat bidang informasi dan kerjasama, bidang keuangan dan akutansi, bidang sumber daya manusia, bidang umum. Di dalam naungan bidang informasi dan kerjasama terdapat unit pemasaran dan kerjasama, unit informasi dan pelayanan pelanggan, unit rekam

medis. Di bawah naungan bagian keuangan dan akuntansi terdapat unit anggaran, unit keuangan dan unit akuntasnsi. Di bawah bagian sumber daya manusia terdapat unit diklat rumah sakit, unit personalia dan unit bina rohani. Di bawah naungan bagian umum terdapat unit kamtib, unit ambulance, unit logistik dan rumah tangga, unit pemeliharaan sarana, unit pengadaan dan unit K3.

b) Struktur Organisasi Bagian Teknologi dan Sistem Informasi



Gambar 4.2 Struktur Organisasi Bagian Teknologi dan Sistem Informasi

Bagian Teknologi dan Sistem Informasi memiliki struktur organisasi yang di dalamnya terdapat dua bagian. Bagian-bagian tersebut adalah bagian *hardwere* dan bagian *softwere*. Dalam setiap bagian terdapat satu orang koordinator dan beberapa staf bagian. Setiap bagian mempunyai *job description* karyawan. Seperti dijelaskan pada Tabel 4.1:

Tebel 4.1 Laniutan Tabel 4.1 *Job Description* Karyawan

No	Nama dan Jabatan	Tanggung Jawab dan Tugas
1	**Andik Jatmiko ST** (Kepala Bagian TI dan Sistem Informasi)	a. Memberikan arahan, bimbingan dan motivasi kerja kepada semua staf. b. Mendelegasikan tugas kepada bawahan dan memantau proses pelaksanaannya. c. Monitoring dan evaluasi staf yang ada di bawahnya. d. Memelihara sarana, prasarana komputer dan jaringan. e. Mengusulkan pengadaan komputer, printer, jaringan dan lainnya. f. Mengawasi penggunaan program SIM-RS. g. Melaksanakan inventarisasi tentang kondisi seluruh perangkat yang ada. h. Melaksanakan pelatihan secara berkesinambungan terhadap operator program SIM-RS.
2	**Megawati,S.Kom** (Koordinator Sofwere)	a. Memberikan arahan, bimbingan dan motivasi kerja kepada semua staf. b. Mendelegasikan tugas kepada bawahan dan memantau proses pelaksanaannya. c. Monitoring dan evaluasi staf yang ada di bawahnya. d. Mengembangkan secara aktif kemampuan dalam pengembangan perangkat lunak. e. Mengambil bagian dalam pengembangan dan integrasi perangkat lunak. f. Backup atau memodifikasi aplikasi dan data yang terkait untuk menyediakan pemulihan kerusakan. g. Membuat laporan rutin mengenai kegiatan kepada manajer IT.

Tebel 4.1 Laniutan

No	Nama dan Jabatan	Tanggung Jawab dan Tugas
3	**Meliza Istiana, S.Kom** (Staf bagian Sofwere)	a. Mengambil bagian dalam pengembangan dan integrasi perangkat lunak. b. Mengembangkan secara aktif kemampuan dalam pengembangan perangkat lunak. c. Menerima permintaan *user* untuk masalah-masalah yang harus diselesaikan. d. *Backup* atau memodifikasi aplikasi dan data yang terkait untuk menyediakan pemulihan kerusakan. e. Membuat laporan rutin mengenai kegiatan kepada koordinator *software*.
4	**Wasono Widiatmoko,S.Kom** (Staf Bagian Sofwere)	a. Mengambil bagian dalam pengembangan dan integrasi perangkat lunak. b. Mengembangkan secara aktif kemampuan dalam pengembangan perangkat lunak. c. Menerima permintaan *user* untuk masalah-masalah yang harus diselesaikan. d. *Backup* atau memodifikasi aplikasi dan data yang terkait untuk menyediakan pemulihan kerusakan. e. Membuat laporan rutin mengenai kegiatan kepada koordinator *software*.
5	**Ahmad Danny,S.Kom** (Koordinator Hardwere)	a. Memberikan arahan, bimbingan dan motivasi kerja kepada semua staf. b. Mendelegasikan tugas kepada bawahan dan memantau proses pelaksanaannya. c. Monitoring dan evaluasi staf yang ada di bawahnya. d. Mengembangkan secara aktif kemampuan dalam pengembangan perangkat keras. e. Mengambil bagian dalam pengembangan dalam pendukung berjalannya sistem informasi rumah sakit. f. Membuat laporan rutin mengenai kegiatan kepada manajer IT.
6	**M.Arif Rahman,S.Kom**	a. Mengembangkan secara aktif kemampuan dalam pengembangan perangkat keras dan jaringan.

Tebel 4.1 Laniutan

No	Nama dan Jabatan	Tanggung Jawab dan Tugas
	(Staf Bagian Hardwere)	b. Mengambil bagian dalam pengembangan dalam pendukung berjalannya sistem informasi rumah sakit. c. Menerima permintaan *user* untuk masalah-masalah yang harus diselesaikan. d. *Maintenance* LAN dan koneksi internet. e. Membuat laporan rutin mengenai kegiatan kepada koordinator *hardware.*
7	**M. Agus Sriffudin** (Staf Bagian Hardwere)	a. Menerima, memprioritaskan dan menyelesaikan permintaan bantuan IT. b. Instalasi, perawatan dan penyediaan dukungan harian baik untuk *hardware & software windows*. c. *Maintenance* LAN dan koneksi internet. d. Membuat laporan rutin mengenai kegiatan kepada koordinator *hardware*.

4. Gambaran Umum Bagian Teknologi dan Sistem Informasi

Bagian teknologi dan sistem informasi merupakan tempat atau bagian dari RSI Jemursari yang berfungsi sebagai unit pemrosesan informasi. Selain itu bagian tersebut bertugas untuk mengurusi perangkat TI dan SI sehingga bisa digunakaan dalam pemenuhan informasi untuk kebutuhan RSI Jemursari.

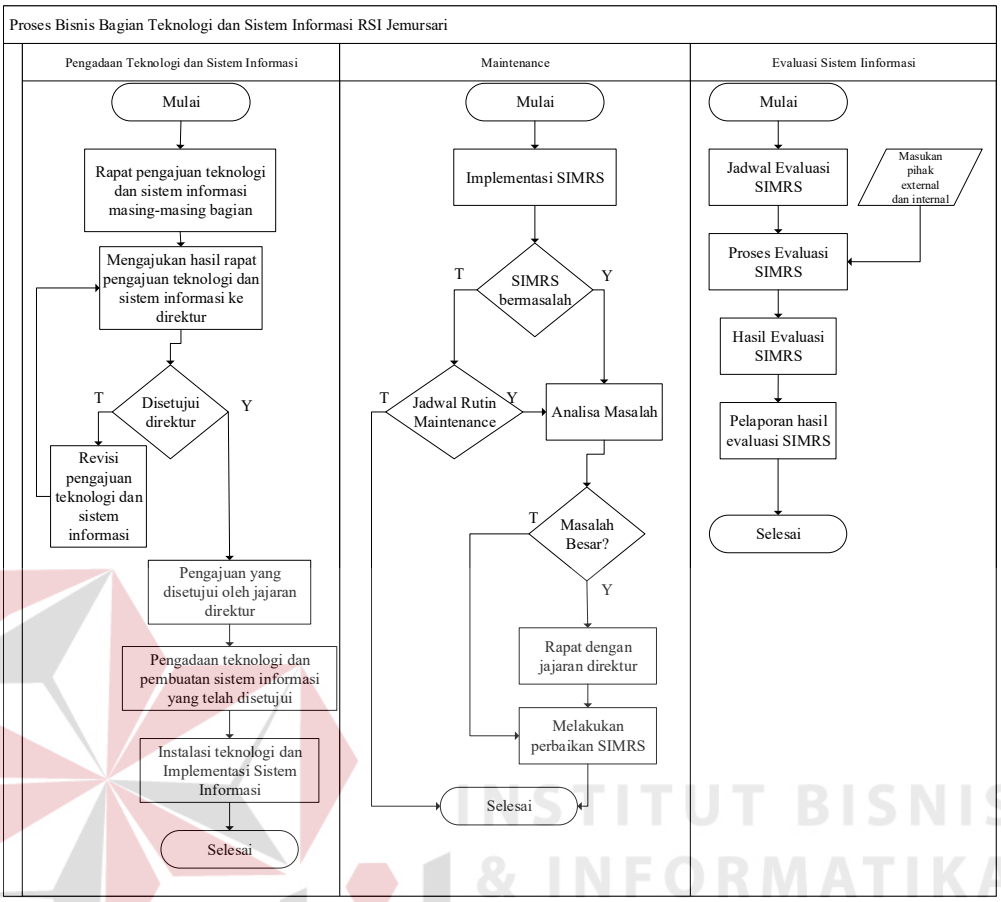
5. Gambaran Proses Bisnis dan TI pada Bagian Teknologi dan Sistem Informasi

Pada awal tahun, bagian teknologi dan sistem informasi melakukan rapat dengan semua bagian rumah sakit. Dalam rapat tersebut akan dibahas kebutuhan aplikasi atau perangkat *hardwere* yang dibutuhkan pada tiap-tiap bagian di RSI Jemursari dalam satu tahun ke depan. Selanjutnya pihak berkoordinasi dengan direktur untuk menentukan prioritas pemenuhan kebutuhan perangkat lunak dan perangkat keras. Setelah disetujui direktur, pemenuhan perangkat lunak ataupun

perangkat keras tersebut akan direalisasikan sesuai dengan jadwal yang telah dibuat.

Sedangkan untuk melakukan *maintenance* perangkat lunak dan perangkat keras, pemohon tinggal mengirim permohonan pada aplikasi SIM-RS yang telah disediakan. Selanjutnya permohonan dari *user* tersebut akan ditindak lanjuti sesuai dengan permasalahan. Apabila permasalahan tersebut membutuhkan beberapa bagian dari rumah sakit untuk koordinasi, maka kepala bagian teknologi dan sistem informasi akan mengundang untuk melakukan diskusi untuk selanjutnya dilakukan perbaikan sistem atau perangkat keras.

Proses bisnis yang terakhir adalah melakukan evalusai tentang sistem dan teknologi yang sudah berjalan. Evaluasi dilakukan setiap bulan sekali olah bagian teknologi dan sistem informasi RSI Jemursari. Hasil evaliasi akan dilaporkan kepada direktur rumah sakit. Alur proses bisnis dapat dilihat pada Gambar 4.3.



Gambar 4.3 Alur Proses Bisnis

4.1.2. Menentukan Ruang Lingkup, Objek dan Tujuan Audit

Setelah melakukan identifikasi proses bisnis di RSI jemursari dan di bagian teknologi dan sistem informasi, bisa diambil kesimpulan tentang proses bisnis yang ada. Dalam penentuan ruang lingkup dilakukan dengan cara melakukan observasi dan wawancara pada bagian teknologi dan sistem informasi RSI Jemursari. Adapun hasil penentuan ruang lingkup yang akan diaudit mengenai Sistem Informasi Manajemen Rumah Sakit (SIM-RS). Objek audit adalah bagian yang bertanggungjawab tentang SIM-RS yaitu bagian teknologi dan sistem informasi. Tujuan audit agar dapat mengukur hasil *maturity level* dengan standar ISO/IEC 27002: 2005 beserta temuan dan rekomendasi.

4.1.3. Membuat Engangement Letter

Setelah menentukan ruang lingkup, objek dan tujuan audit, langkah selanjutnya adalah membuat *engagment letter*. Dalam pembuatan *engagement letter* bertujuan untuk bukti persetujuan antara auditor dengan *auditee* tentang pelaksanaan audit yang akan dilaksanakan oleh auditor. Di dalam *engagement letter* berisi tentang *role*, tanggung jawab, lingkup audit, pelaksanaan audit dan ketentuan perjanjian audit. Pada proses ini akan menghasilkan perjanjian yang harus dipatuhi oleh auditor dan *auditee*. *Engangment Letter* dapat dilihat di Lampiran 2.

4.1.4. 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 yang terdapat pada Lampiran 1. Kesimpulan dari hasil wawancara tentang permasalahan yang terjadi di RSI Jemursari adalah:

1. Terjadinya kebocoran informasi pada karyawan yang tidak berhak atas informasi tersebut. Selain itu masih banyak karyawan 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 merugikan 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 di atas penggunaan klausul, kontrol objektif dan kontrol keamanan dapat dilihat pada halaman berikutnya pada Tabel 4.2.

Tabel 4.2 Penggunaan Klausul, Kontrol Objekttif dan Kontrol Keamanan

Klausul yang ditetapkan dalam Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Pada Rumah Sakit Islam Jemursari		
Klausul	Detail klausul	Alasan Penggunaan Klausul
Klausul 8 (Keamanan Sumber Daya Manusia)	Lampiran 3	Kontrol sesuai dengan permasalahan yang ada yaitu tentang SDM yaitu masalah kedisiplinan SDM.
Klausul 9 (keamanan fisik dan Lingkungan)	Lampiran 3	Kontrol sesuai dengan permasalahan yang ada yaitu tentang permasalahan perangkat pendukung sistem informasi belum memiliki perlindungan.
Klausul 11 (Kontrol Akses)	Lampiran 3	Kontrol digunakan untuk keamanan akses informasi dari orang yang tidak berhak.
Klausul 12 (Akuisisi Sistem Informasi,	Lampiran 3	Kontrol diperlukan karena permintaan dari pihak RSI Jemursari.

Tebel 4.2 Lanjutan

Klausul yang ditetapkan dalam Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Pada Rumah Sakit Islam Jemursari		
Klausul	Detail klausul	Alasan Penggunaan Klausul
pengembangan dan Pemeliharaan)		

4.2. Persiapan Audit

4.2.1. Penyusunan *Audit Working Plan*

Hasil dari penyusunan *audit working plan* berupa Tabel yang berisi serangkaian aktifitas yang dilakukan selama audit berlangsung. Dalam melaksanakan audit keamanan sistem informasi dilakukan secara bertahap. Untuk lebih detilnya dilihat pada Tabel 4.3.

Tabel 4.3 *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												

4.2.2. 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. Kebutuhan data bisa dilihat pada Tabel 4.4.

Tabel 4.4 Permintaan Kebutuhan Data

Permintaan Kebutuhan Data/Dokumen						
No.	Data Yang Diperlukan	Ketersediaan Data		Keterangan	Tanda Tangan	
		Ada	Tidak Ada		*Auditee*	Auditor
1	Profil RSI Jemursari	√				
2	Struktur organisasi RSI Jemursari	√				
3	*Job description* Karyawan	√				
4	Alur proses bisnis Bagian Teknologi dan Sistem Informasi	√				
5	Dokumen kebijakan keamanan sistem informasi dan jaringan	√				
6	Dokumen prosedur dan aturan aplikasi SIM-RS	√				
7	Dokumen tentang SDM	√				
8	Dokumen K3	√				
9	Dokumen Renstra bagian IT	√				

4.2.3 Membuat Pernyataan

Hasil dari proses membuat pertanyaan adalah berupa Tabel yang berisi daftar pernyataan yang diambil dari tiap-tiap klausul ISO 27002. Pernyataan yang telah dibuat dapat dilihat di Tabel 4.5 dan selanjutnya dapat dilihat pada Lampiran 4.

Tabel 4.5 Pernyataan

Klausul: 9 Keamanan Fisik dan Lingkungan	
Objektif Kontrol : 9.1 Wilayah Aman	
ISO 27002 9.1.1 Pembatasan Keamanan Fisik	
No	Pernyataan
1	Adanya pendefinisian parimeter keamanan secara jelas (dinding, kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi.
2	Adanya penggunaan parimeter keamanan untuk melindungi ruang fasilitas pemrosesan informasi .
3	Tembok terluar bangunan sudah dari kontruksi kuat.
4	Adanya pencegahan secara fisik untuk akses yang tidak sah.
5	Adanya wilayah penerimaan tamu.
6	Adanya alat pendeteksi keamanan.
7	Adanya personil keamanan.
8	Adanya jalur evakuasi.
9	Adanya tanda bahaya di jalur evakuasi.
10	Adanya mekanisme kontrol yang digunakan untuk perlindungan keamanan fisik.

4.2.4 Melakukan Pembobotan

Hasil dari proses pembobotan adalah berupa Tabel berisi pernyataan dan nilai bobot dari tiap-tiap bobot yang telah ditentukan. Nilai bobot ditentukan dari

seberapa besar risiko yang terjadi untuk perusahaan. Jika diindikasikan risiko yang berpengaruh besar untuk organisasi, maka nilai dari pembobotan tersebut adalah 1 (satu). Sedangkan diindikasikan tidak berisiko sedikitpun untuk perusahaan maka nilai dari pembobotan tersebut adalah 0 (nol). Pembobotan yang telah dibuat bisa dilihat di Tabel 4.6 dan selanjutnya dapat dilihat pada Lampiran 5.

Tabel 4.6 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	Adanya pendefinisian parimeter keamanan secara jelas (dinding, kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi.	1
2	Adanya penggunaan parimeter keamanan untuk melindungi ruang fasilitas pemrosesan informasi .	1
3	Tembok terluar bangunan sudah dari kontruksi kuat.	1
4	Adanya pencegahan secara fisik untuk akses yang tidak sah.	1
5	Adanya wilayah penerimaan tamu.	0,8
6	Adanya alat pendeteksi keamanan.	0.8
7	Adanya personil keamanan.	0.9
8	Adanya jalur evakuasi.	0.7

4.2.5 Membuat Pertanyaan

Pada proses membuat pertanyaan mengacu pada pernyataan yang telah dibuat sebelumnya. Pertanyaan disesuaikan berdasarkan pelaksanaan kontrol yang ada pada standard ISO 27002. Berikut adalah pertanyaan yang dibuat pada klausul

9 mengenai keamanan fisik dan lingkungan pada Tabel 4.7 dan untuk lebih lengkapnya dapat dilihat pada Lampiran 6.

Tabel 4.7 Pertanyaan

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 parimeter sudah di sosialisasikan?
2	Adanya penggunaan parimeter keamanan untuk melindungi ruang fasilitas pemrosesan informasi.	1. Sudahkah ada parimeter untuk melindungi ruang pemrosesan informasi tersebut? 2. Ada parimeter apa saja di RSI Jemursari?
3	Tembok terluar bangunan sudah dari kontruksi kuat.	1. Bagaimana konstruksi tembok yang ada? 2. Apakah ada perawatan rutin untuk tembok tersebut?
4	Adanya pencegahan secara fisik untuk akses yang tidak sah.	1. Apakah ada prosedur untuk mencegah orang luar (tidak punya akses) 2. Seperti apa prosedur tersebut? 3. Bagaimana cara pencegahannya?

4.3 Pelaksanaan Audit

4.3.1 Wawancara dan Observasi

Pada proses wawancara dan observasi, auditor melakukan wawancara dan observasi berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan kepada pihak yang terlibat di dalamnya yaitu *auditee*. Dalam penentuan *auditee* didapat dari analisa tabel RACI. *Auditee* adalah penanggungjawab atau *responsibility* dari proses keamanan. Tabel RACI dapat dilihat pada Tabel 4.8. Salah satu contoh hasil

wawancara terdapat pada klausul 9.1.1 mengenai pembatasan keamanan fisik yang dapat dilihat pada Tabel 4.9. Untuk lebih lengkapnya hasil wawancara tersebut terdapat pada Lampiran 7.

Tabel 4.8 Tabel RACI

Bagian / Klausul	**Manager TSI**	**Staf Sofware**	**Staf Hardwere**	**Satuan Pengawas Internal (SPI)**	**Bagian HRD**	**K3**	**Bagian Manajeman aset**
Klausul 8	R	I	I	A/C	A/R/C	I	I
Klausul 9	R	I	R	I	I	R/A/C	R/A
Klausul 10	R/A	R/C	R/C	I	I	I	I
Klausul 11	R/A/C	R/C	R/C	I	I	I	I

Tabel 4.9 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.
Adanya penggunaan parimeter keamanan untuk melindungi ruang fasilitas pemrosesan informasi.	1. Sudahkah ada parimeter untuk melindungi ruang pemrosesan informasi tersebut?	Untuk perimeternya sudah ada.
	2. Ada Parimeter apa saja di RSI Jemursari?	Di RSI Jemursari ada banyak parimeter. Di paling luar terdapat pagar beton keliling.

Tabel 4.9 (lanjutan)

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		
		Terdapat dinding, pada RSI Jemursari dinding dibagi dua, yaitu dinding partisi yang terbuat dari triplek dan dinding beton dan setiap ruangan dilengkapi kunci. Ada juga kamera CCTV yang beroprasi 24 jam. Disamping itu terdapat petugas kemanan 24 jam.
dst..		

4.3.2 Pemeriksaan Data dan Bukti

Pada Pemeriksaan data dan bukti mengacu pada hasil dari wawancara yang dilakukannya. Dalam pemeriksaan data dan bukti kita melakukan *review* tentang data atau bukti yang ditemukan dari proses wawancara. Salah satu contoh hasil pemeriksaan data dan bukti yang terdapat pada klausul 9 mengenai keamanan fisik dan lingkungan yang dapat dilihat pada Tabel 4.10. Untuk lebih lengkapnya hasil pemeriksaan data dan bukti tersebut terdapat pada Lampiran 8.

Tabel 4.10 Pemeriksaan Data dan Bukti

Pemeriksaan Bukti dan Data **Audit Keamanan Sistem Informasi** **KLAUSUL 9** **Keamanan Sumber Daya Manusia** (Objektif Kontrol : 9.1 Wilayah Aman)	Auditor : Alfian N Rahman Auditee : Andik Jatmiko, ST Reviewer : Dr Haryanto Tanuwijaya, S.Kom MMT TTD/Tanggal:_____/_____		
NO	**Pemeriksaan**	**Catatan Pemeriksaan**	**Catatan Review**
1	Cek jalur evakuasi dan tanda jalur evakuasi.	Ada jalur evakuasi di setiap gedung, dan tanda jalur evakuasi hingga diarahkan di titik kumpul evakuasi.	
2	Cek jadwal rutin perawatan.	Perawatan dilakukan secara rutin, hal ini sudah tercantum pada aturan *job desk* masing-masing staf IT.	
3	Cek kartu kunjungan.	Setian tamu yang datang diberikan kartu identitas yang diterbitkan oleh RSI Jemursari.	
4	Cek CCTV dan ruang kontrol CCTV.	Penempatan kamera CCTV terdapat di 50 titik yang tersebar di seluruh RSI Jemursari dengan kapasitas *history* penyimpanan hingga 3 bulan.	
5	Cek buku tamu.	Pencatatan buku tamu tidak dilakukan secara rutin.	
dst..			

4.3.3 Hasil Pelaksanaan Uji Kematangan

Berdasarkan hasil wawancara dengan *auditee* dan observasi di lapangan, maka diperoleh hasil uji kepatutan dari tingkat kematangan untuk masing-masing kontrol. Hasil uji kematangan diperolah dari masing-masing analisa tiap klausul yang dapat dilihat pada kerangka kerja perhitungan *maturity lavel* pada lampiran 9. Hasil perhitungan tingkat kematangan hasil audit keamanan sistem informasi adalah sebagai berikut.

a. Hasil *Maturity Level* Klausul 8 tentang Keamanan Sumber Daya Manusia

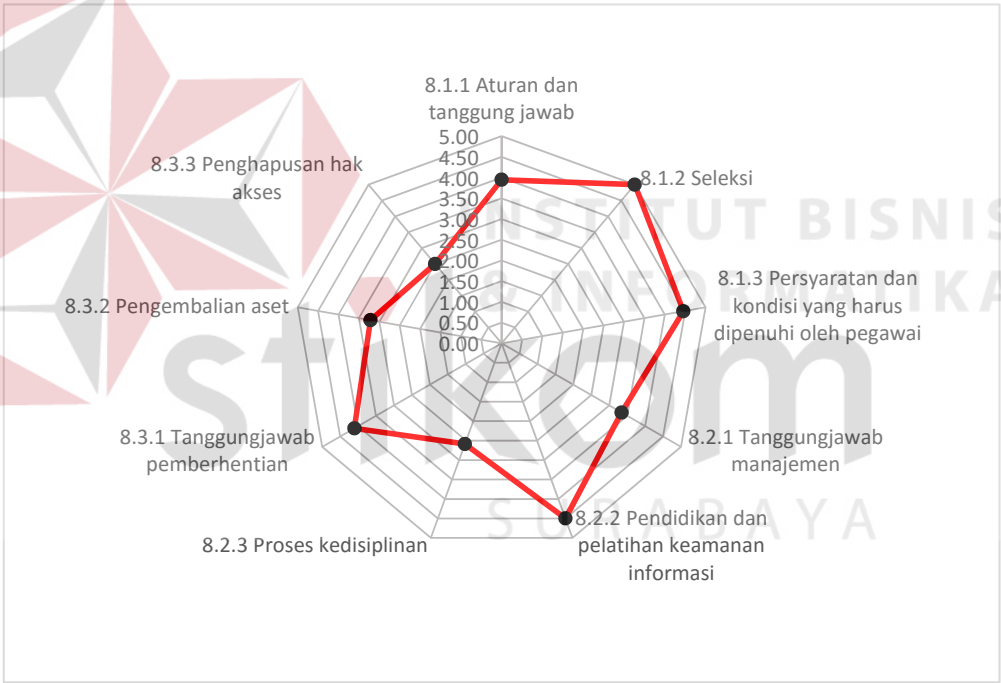
Berdasarkan hasil dari proses perhitungan *maturity lavel* pada klausul 8 tentang keamanan sumber daya manusia adalah 3,74 yaitu *defined.* Hasil tersebut menunjukan bahwa proses keamanan sumber daya manusia sudah dilengkapi aturan dan prosedur tentang sumber daya manusia. Aturan tersebut meliputi proses penerimaan karyawan baru, pelatihan karyawan, aturan kerja karyawan hingga pemberhentian karyawan. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur yang ada misalnya pelatihan hanya dilakukan pada saat ada permintaan dari pihak terkait, sebagian besar karyawan belum menyadari tentang keamanan informasi organisasi dan pendisiplinan karyawan. Hal lain adalah belum adanya aturan dan prosedur tentang pemberitahuan kepada *steakholder* ketika ada perubahan personil dan prosedur tentang penghapusan informasi aset yang diberikan kepada karyawan. Hasil perhitungan dapat dilihat pada Tabel 4.11. Hasil perhitungan *maturity lavel* klausul 8 tentang keamanan sumber daya manusia dapat dipresentasikan dalam bentuk jaring laba-laba. Presentasi dalam jaring laba-laba dapat dilihat pada Gambar 4.4.

Tabel 4.11 Hasil *Maturity Lavel* Klausul 8 Keamanan Sumber Daya Manusia

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata objektif kontrol
8 Keamanan Sumber daya manusia	8.1 Keamanan sumber daya manusia sebelum menjadi pegawai	8.1.1 Aturan dan tanggung jawab	3,95	4,47
		8.1.2 Seleksi	5,00	
		8.1.3 Persyaratan dan kondisi yang harus dipenuhi oleh pegawai	4,45	
		8.2.1 Tanggungjawab manajemen	3,34	3,48

Tabel 4.11 (lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata objektif kontrol
	8.2 Selama menjadi pegawai	8.2.2 Pendidikan dan pelatihan keamanan informasi	4,50	
		8.2.3 Proses kedisiplinan	2,59	
	8.3 Pemberhentian atau pemindahan pegawai	8.3.1 Tanggungjawab pemberhentian	4,11	3,27
		8.3.2 Pengembalian aset	3,21	
		8.3.3 Penghapusan hak akses	2,50	
Maturity Level Klausul 8				**3,74**



Gambar 4.4 Jaring Laba-Laba Nilai *Maturity Level* Klausul 8 Keamanan Sumber Daya Manusia

b. Hasil *Maturity Level* Klausul 9 tentang Keamanan Fisik dan Lingkungan

Berdasarkan hasil dari proses perhitungan *maturity lavel* pada klausul 9 tentang keamanan fisik dan lingkungan adalah 4,09 yaitu *managed.* Hasil tersebut

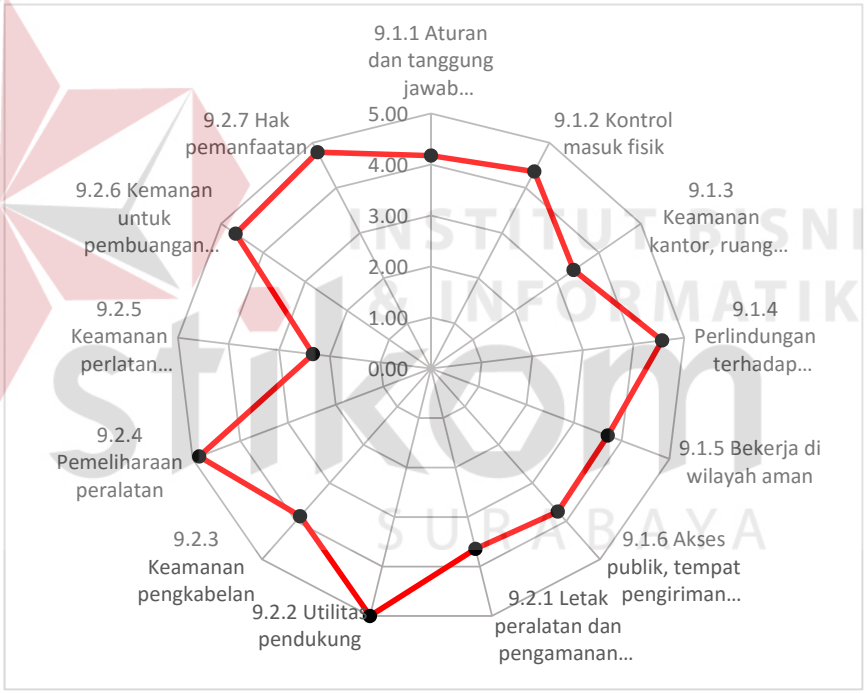
menunjukan bahwa proses keamanan fisik dan lingkungan sudah mempunyai aturan dan sebagian besar aturan tersebut sudah dilakukan dan sudah terdokumentasi. Tetapi ada beberapa proses yang masih belum dilakukan sesuai dengan aturan yang ada misalnya penempatan peralatan kerja yang cenderung kurang rapi di ruang kerja, masih ditemukan karyawan yang makan dan minum di ruang pemrosesan informasi, belum maksimalnya pengawasan dan tempat menaikkan dan menurunkan barang logistik organisasi dan perlindungan peralatan di luar ruangan. Hal lain terkait aturan masih belum ada aturan yang menjelaskan tentang parimeter, prosedur peningkatan keamanan. Hasil perhitungan dapat dilihat pada Tabel 4.12. Hasil perhitungan *maturity lavel* klausul 9 tentang keamanan fisik dan lingkungan dapat dipresentasikan dalam bentuk jaring laba-laba. Presentasi dalam jaring laba-laba dapat dilihat pada Gambar 4.5.

Tabel 4.12 Hasil *Maturity Lavel* Klausul 9 Keamanan Fisik dan Lingkungan

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata objektif kontrol
9 Keamanan Fisik dan Lingkungan	9.1 Wilayah Aman	9.1.1 Aturan dan tanggung jawab keamanan	4,18	3,99
		9.1.2 Kontrol masuk fisik	4,36	
		9.1.3 Keamanan kantor, ruang dan fasilitasnya	3,40	
		9.1.4 Perlindungan terhadap ancaman dari luar dan lingkungan sekitar	4,57	
		9.1.5 Bekerja di wilayah aman	3,71	
		9.1.6 Akses publik, tempat pengiriman dan penurunan barang	3,75	
	9.2 Keamanan Peralatan	9.2.1 Letak peralatan dan pengamanannya	3,64	4,16
		9.2.2 Utilitas pendukung	5,00	
		9.2.3 Keamanan pengkabelan	3,87	

Tabel 4.12 (lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata objektif kontrol
		9.2.4 Pemeliharaan peralatan	4,86	
		9.2.5 Keamanan perlatan diluar tempat yang tidak disyaratkan	2,33	
		9.2.6 Kemanan untuk pembuangan atau pemanfaatan kembali peralatan	4,65	
		9.2.7 Hak pemanfaatan	4,79	
Maturity Level Klausul 9				**4,09**



Gambar 4.5 Jaring Laba-Laba Nilai *Maturity Level* Klausul 9 Keamanan Fisik dan Lingkungan

c. Hasil *Maturity Level* Klausul 11 tentang Kontrol Akses

Berdasarkan hasil dari proses perhitungan *maturity lavel* pada klausul 11 tentang kontrol akses adalah 2,91 yaitu *limited/repeatable.* Hasil tersebut menunjukkan bahwa pada proses kontrol akses masih belum mempunyai aturan

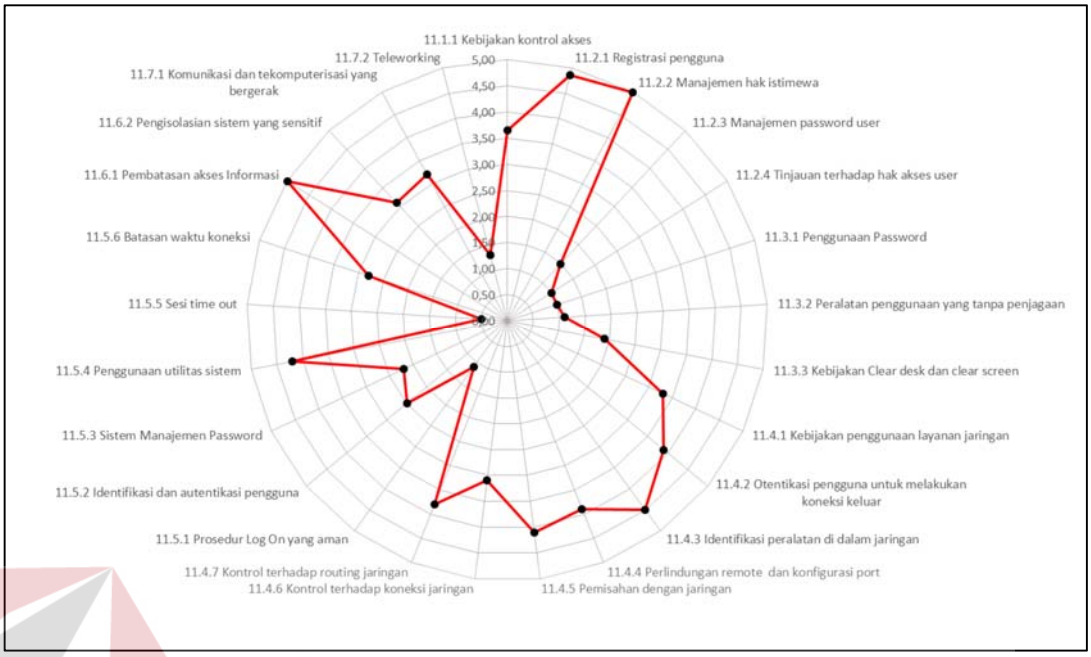
tentang manajemen *password*, keamanan kriptografi, aturan tentang *clear screen*, aturan pemindahan berkas dokumen cetak. Hal lain masalah ketidakpatuhan karyawan tentang aturan yang sudah ada misalnya penggunaan *password*, penggunaan PC yang ditinggal tanpa pengawasan, perlindungan peralatan di wilayah *user*, tidak mematuhi kebijakan *clear desk.* Hasil perhitungan dapat dilihat pada Tabel 4.13. Hasil perhitungan *maturity lavel* klausul 11 tentang kontrol akses dapat dipresentasikan dalam bentuk jaring laba-laba. Presentasi dalam jaring laba-laba dapat dilihat pada Gambar 4.6.

Tabel 4.13 Hasil *Maturity Lavel* Klausul 11 Kontrol Akses

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata objektif kontrol
11 Kebijakan Keamanan	11.1 Persyaratan bisnis untuk akses kontrol	11.1.1 Kebijakan kontrol akses	3,65	3,65
	11.2 Manajemen Akses User	11.2.1 Registrasi pengguna	4,85	3,09
		11.2.2 Manajemen hak istimewa	5,00	
		11.2.3 Manajemen *password* user	1,50	
		11.2.4 Tinjauan terhadap hak akses *user*	1,00	
	11.3 Tanggung jawab pengguna (user)	11.3.1 Penggunaan *Password*	1,00	1,33
		11.3.2 Peralatan penggunaan yang tanpa penjagaan	1,10	
		11.3.3 Kebijakan *Clear desk* dan *clear screen*	1,90	
	11.4 Kontrol akses jaringan	11.4.1 Kebijakan penggunaan layanan jaringan	3,30	3,80
		11.4.2 Otentikasi pengguna untuk melakukan koneksi keluar	3,90	
		11.4.3 Identifikasi peralatan di dalam jaringan	4,50	

Tabel 4.13 (lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata objektif kontrol
		11.4.4 Perlindungan remote diagnostic dan konfigurasi *port*	3,90	
		11.4.5 Pemisahan dengan jaringan	4,10	
		11.4.6 Kontrol terhadap koneksi jaringan	3,10	
		11.4.7 Kontrol terhadap *routing* jaringan	3,80	
	11.5 Kontrol akses sistem operasi	11.5.1 Prosedur *Log On* yang aman	1,10	2,22
		11.5.2 Identifikasi dan autentikasi pengguna	2,50	
		11.5.3 Sistem Manajemen *Password*	2,20	
		11.5.4 Penggunaan utilitas sistem	4,20	
		11.5.5 Sesi time out	0,50	
		11.5.6 Batasan waktu koneksi	2,80	
	11.6 Kontrol akses informasi dan aplikasi	11.6.1 Pembatasan akses Informasi	5,00	4,05
		11.6.2 Pengisolasian sistem yang sensitif	3,10	
	11.7 Komputasi bergerak dan bekerja dari lain tempat (teleworking)	11.7.1 Komunikasi dan tekomputerisasi yang bergerak	3,20	2,25
		11.7.2 *Teleworking*	1,30	
Maturity Level Klausul 11				**2,91**



Gambar 4.6 Jaring Laba-Laba Nilai *Maturity Level* Klausul 11 Kontrol Akses

d. Hasil *Maturity Level* Klausul 12 tentang Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan.

Berdasarkan hasil dari proses perhitungan *maturity lavel* pada klausul 11 tentang kontrol akses adalah 3,16 yaitu *defined.* Hasil tersebut menunjukkan bahwa proses akuisisi sistem informasi, pembangunan dan pemeliharaan sudah dilengkapi aturan dan prosedur tentang akuisisi sistem informasi, pembangunan dan pemeliharaan. Aturan tersebut meliputi proses implementasi sistem baru, modifikasi aplikasi dan aturan pengembangan sistem. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur yang ada misalnya dalam pengembangan sistem baru tidak ada *framework* yang digunakan dalam perencanaan pembuatan sistem baru. Hal lain adalah belum adanya peraturan tentang integritas pesan elektonik, penggunaan *kriptografi*, manajemen *password* dan peraturan tentang lesensi produk yang digunakan oleh organisasi. Hasil perhitungan dapat dilihat pada Tabel 4.14. Hasil perhitungan *maturity lavel* klausul

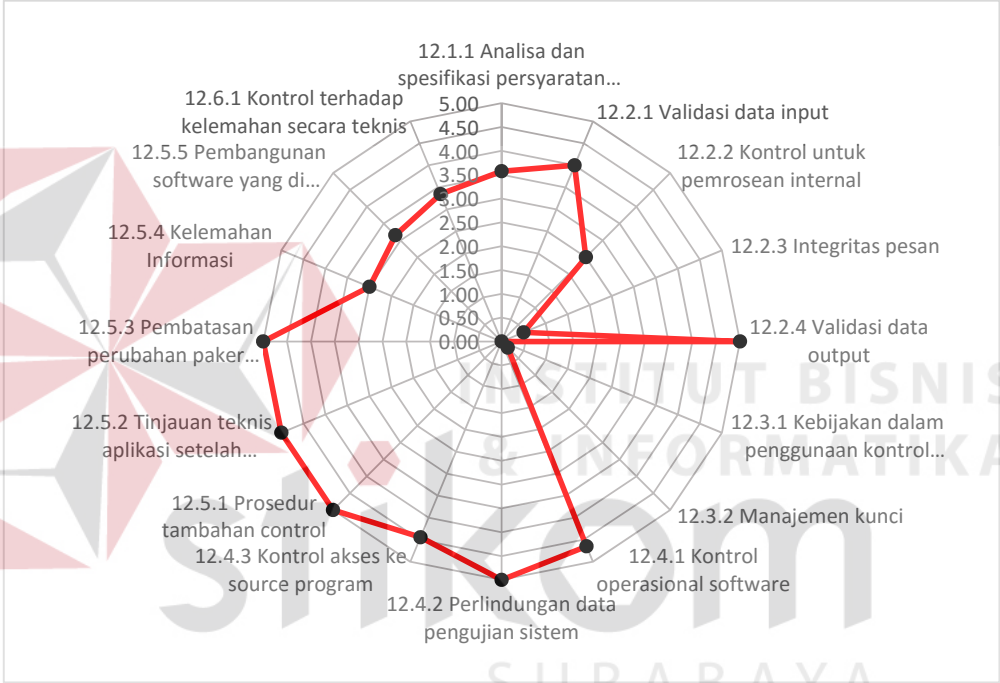
12 tentang akuisisi sistem informasi, pembangunan dan pemeliharaan dapat dipresentasikan dalam bentuk jaring laba-laba. Presentasi dalam jaring laba-laba dapat dilihat pada Gambar 4.7.

Tabel 4.14 Hasil *Maturity Lavel* Klausul 12 Akuisisi Sistem Informasi,Pembangunan dan Pemeliharaan

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata objektif kontrol
12 Akuisi Sistem Informasi, Pembangunan dan Pemeliharaan	12.1 Persyaratan keamanan untuk Sistem Informasi	12.1.1 Analisa dan spesifikasi persyaratan keamanan	3,57	3,57
	12.2 Pemrosesan yang benar dalam aplikasi	12.2.1 Validasi data *input*	4,00	3,00
		12.2.2 Kontrol untuk pemrosean internal	2,50	
		12.2.3 Integritas pesan	0,50	
		12.2.4 Validasi data *output*	5,00	
	12.3 Kontrol Kriptografi	12.3.1 Kebijakan dalam penggunaan kontrol kriptografi	0,00	0,09
		12.3.2 Manajemen kunci	0,18	
	12.4 Keamanan file sistem	12.4.1 Kontrol operasional software	4,65	4,70
		12.4.2 Perlindungan data pengujian sistem	5,00	
		12.4.3 Kontrol akses ke *source* program	4,44	
	12.5 Keamanan dalam pembangunan dan proses-proses pendukung	12.5.1 Prosedur tambahan kontrol	5,00	4,23
		12.5.2 Tinjauan teknis aplikasi setelah dilakukan perubahan sistem operasi	5,00	
		12.5.3 Pembatasan perubahan paker software	5,00	
		12.5.4 Kelemahan Informasi	3,00	
		12.5.5 Pembangunan software yang di outsource kan	3,15	

Tabel 4.14 (lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata objektif kontrol
	12.6 Manajemen teknik kelemahan	12.6.1 Kontrol terhadap kelemahan secara teknis	3,35	3,35
Maturity Level Klausul 12				**3,16**



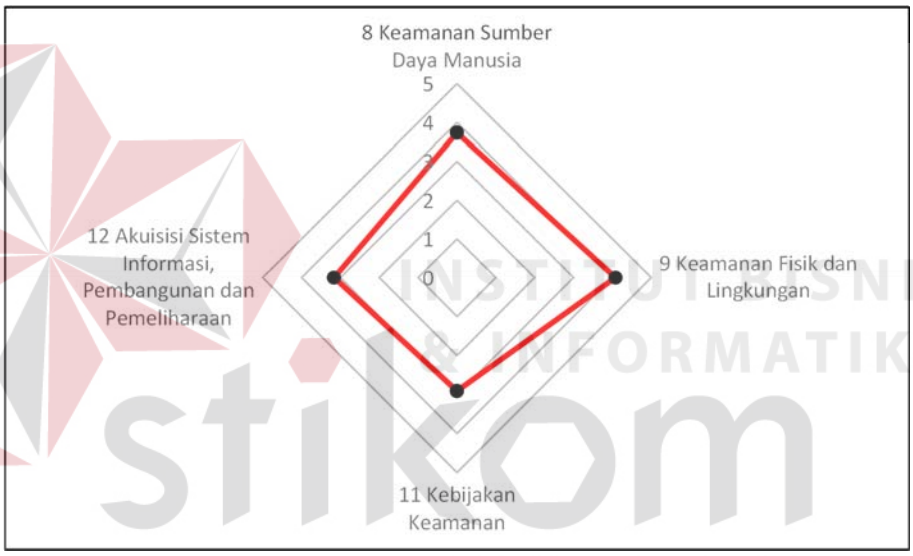
Gambar 4.7 Jaring Laba-Laba Nilai *Maturity Level* Klausul 12 Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan

e. Hasil Pembahasan Audit Keamanan Sistem Informasi pada RSI Jemursari

Hasil dari perhitungan *maturity level* pada seluruh klausul adalah 3,47 yaitu *defined.* Hal tersebut menunjukkan bahwa sebagian besar proses keamanan sistem informasi sudah mempunyai aturan dan dilakukan secara rutin. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.15 dan representasi semua klausul yang digunakan dapat disajikan dengan jaring laba-laba pada Gambar 4.8.

Tabel 4.15 Rekapitulasi Klausul

Klausul	Tingkat Kematangan
8 Keamanan Sumber Daya Manusia	3,74
9 Keamanan Fisik dan Lingkungan	4,08
11 Kebijakan Keamanan	2,91
12 Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	3,16
Rata-rata tingkat kematangan	***3,47***



Gambar 4.8 Jaring Laba-Laba Rekapitulasi 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 manajemen 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 manajemen 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 manajemen sedang melakukan pengembangan pada proses kontrol akses dan belum mempunyai sebegian besar aturan dasar tentang kontrol akses.

Berdasarkan hasil audit keamanan sistem informasi yang telah dilakukan, permasalahan yang terjadi merupakan akibat banyak *user* yang tidak mematuhi peraturan yang telah dibuat oleh organisasi, selain itu organisasi terkesan kurang tegas dalam menindak *user* yang melakukan pelanggaran. *User* belum sepenuhnya menyadari tentang keamanan informasi, hal tersebut dibuktikan masih banyak ditemui *user* yang meninggalkan *personal computer* mereka dalam keadaan *log-on* tanpa penjagaan dan tidak pernah mengganti *password* sejak *password* pertama kali diberikan dan dipertegas dengan hasil *maturity level* kontrol keamanan 11.3.1 tentang penggunaan *password* yang memiliki nilai 1,00 dan 11.3.2 tentang peralatan tanpa penjagaan yang memiliki nilai 1,10. Hal tersebut diperparah dengan manajemen jarang melakukan proses penegakan aturan karyawan yang dalam hal ini dibuktikan dalam hasil *maturity level* kontrol keamanan 8.2.3 tentang proses kedisiplinan yang bernilai 2,59.

Kerusakan peralatan yang ditempatkan di luar ruangan merupakan akibat dari tidak adanya perlindungan pada peralatan tersebut. Hal tersebut daat dilihat

dari hasil uji *maturity lavel* kontol keamanan 9.2.5 tentang perlindungan peralalatan di luar yang bernilai 2,33.

Hal lainnya yang ditemukan dalam audit adalah tidak adanya aturan tentang manajemen *password* dan standar kemanan *password* yang ada dalam organisasi. Hal tersebut dan dilihat dari hasil uji *maturity lavel* kontrol keamanan 11.2.3 tentang manajemen *password user* yang bernilai 1,50 dan hasil uji *maturity lavel* kontrol keamanan 12.3.1 tentang kebijakan penggunaan kriptografi yang bernilai 0,00.

4.3.4 Hasil 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. Berdasarkan hasil temuan tersebut selanjutnya akan diberikan rekomendasi dengan tujuan dilakukan perbaikan di kemudian hari. Perbaikan harus dilakukan dengan tujuan meningkatkan sistem kemanan yang dimiliki organisasi. Salah satu contoh temuan dan rekomendasi pada kalusul 11 tentang kontrol akses dengan kontrol 11.2.4 tinjauan terhadap hak *user* dapat dilihat pada Tabel 4.16 dan untuk lebih lengkapnya dapat dilihat pada Lampiran 10 .

Tabel 4.16 Hasil Temuan dan Rekomendasi

Temuan dan Rekomendasi **Audit Keamanan Sistem Informasi**					Auditor : Alfian N Rahman Auditee : Andik Jatmiko ST
Klausul: 11 (Kontrol Akses) **11.2.4 Tinjauan Terhadap Hak User**					Tanda Tangan Tanggal: _____
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.
2	Adanya otorisasi untuk hak khusus yang dikaji ulang dalam rentang waktu sering	Pemberian Otorisasi hak khusus jarang dilakukan karena pengkajian ulang hak akses juga jarang dilakukan	• Manajemen menyatakan pengkajian jarang dilakukan	• Lakukan otorisasi untuk pengkajian ulang hak khusus dalam rentan waktu yang berkala • Dokumentasikann prosedur untuk otorisasi untuk otorisasi pengkajian ulang hak khusus pada waktu pada waktu yang berkala (3 bulan)	• Manajeman mengakui sangat jarang dilakukan • Manajemen menyetujui rekomendasi tersebut.

4.3.5 Konfirmasi Temuan dan Rekomendasi

Konfirmasi temuan dan rekomendasi dilakukan pada saat setelah selesai melakukan penyusunan temuan dan rekomendasi. Konfirmasi ditunjukkan kepada *auditee* dengan tujuan mengklarifikasi temuan yang ada dan meminta tanggapan tentang rekomendasi yang diberikan. Tanggapan dapat dilihat pada Lampiran 10.

4.4 Hasil Pelaporan Audit

Dalam tahap pelaporan bertujuan untuk memberikan laporan audit (*audit report*) sebagai pertanggungjawaban atas penugasan proses audit keamanan sistem informasi yang dilaksanakan. Laporan audit ditunjukkan kepada pihak yang manajemen yang memiliki hak saja, karena laporan audit keamanan sistem informasi merupakan dokumen yang bersifat rahasia. Hasil pelaporan audit dapat dilihat pada Lampiran 12.

4.5 Pembahasan Audit

Audit keamanan sistem informasi pada RSI Jemursari telah selesai dilakukan. Audit keamanan dimulai pada bulan Maret dan selesai pada bulan Juni 2016. Dalam melakukan audit, auditor melakukan wawancara tahap awal dengan kepala bagian teknologi dan sistem informasi RSI Jemursari. Melakukan wawancara tahap awal dimaksudkan untuk mengetahui masalah yang ada pada RSI Jemursari. Dari hasil wawancara tahap awal, auditor malakukan diskusi berdasarkan masalah yang terjadi dengan kepala bagian teknologi dan sistem informasi RSI Jemursari. Dari hasil diskusi tersebut, auditor dan kepala bagian teknologi dan sistem informasi memutuskan untuk menggunakan standar ISO 27002 : 2005 dengan menggunakan empat klausul. Klausul yang digunakan adalah klausul 8 tentang keamanan sumberdaya manusia, klausul 9 tentang keamanan fisik dan lingkungan, klausul 11 tentang kontrol akses dan klausul 12 tentang akuisi sistem informasi, pembangunan dan pemeliharaan.

Setelah melakukan diskusi auditor melakukan persiapan audit dengan melakukan pemetaan dari kontrol yang ada pada tiap-tiap klausul. Pemataan kontrol

mencangkup pembuatan pernyataan, pembobotan hingga menyiapkan pertanyaan untuk wawancara. Tahap setelah melakukan persiapan audit, auditor melakukan pelaksanaan audit.

Pelaksanaan audit dilakukan dengan melakukan wawancara dan observasi. Wawancara dilakukan dengan kepala bagian teknologi dan sistem informasi RSI Jemursari beserta koordinator *sofwere* dan koordinator *hardwere*. Selain melakukan wawancara auditor juga melakukan observasi. Dalam melakukan observasi, auditor menemukan beberapa temuan diantaranya tidak adanya pengawasan komputer yang menyala dengan kondisi *log-on* aplikasi SIM-RS. Selain hal tersebut ditemui perangkat yang ditempatkan diluar tidak ada perlindungan keamanan.

Setelah melakukan wawancara dan observasi, auditor melakukan perhitungan nilai *maturity level* dari tiap-tiap klausul. Dari rata-rata *maturity level* dari tiap-tiap klausul, didapat nilai hasil audit keamanan sistem informasi pada RSI Jemursari adalah 3,47 dengan menggunakan perhitungan CMMI. Nilai *maturity level* 3,47 yaitu berada pada level 3 *(defined)* yang berarti manajemen 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 atau belum dilakukan sesuai sesuai dengan aturan.

Hasil pengukuran *maturity level* klausul 8 tentang keamanan sumber daya manusia yaitu 3,74 yaitu berada pada level 3 *(defined)* yang berarti manajemen sudah mempunyai dasar tentang aturan, prosedur dan kebijakan pada proses keamanan sumber daya manusia. Aturan tersebut meliputi proses penerimaan karyawan baru, pelatihan karyawan, aturan kerja karyawan hingga pemberhentian

karyawan. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur yang ada misalnya pelatihan hanya dilakukan pada saat ada permintaan dari pihak terkait, sebagian besar karyawan belum menyadari tentang keamanan informasi organisasi dan pendisiplinan karyawan. Hal lain adalah belum adanya aturan dan prosedur tentang pemberitahuan kepada *steakholder* ketika ada perubahan personil dan prosedur tentang penghapusan informasi aset yang diberikan kepada karyawan. Dari hasil temuan tersebut, auditor memberikan rekomendasi yaitu manajeman harus lebih menegakkan kedisiplinan setiap pagawai dengan mengacu pada aturan kepagawaian yang telah dibuat sebalumnya.

Hasil pengukuran *maturity level* klausul 9 tentang keamanan fisik dan lingkungan yaitu 4,09 yaitu berada pada level 4 (*managed)* yang berarti manajemen sudah mempunyai dasar tentang aturan, prosedur dan kebijakan dan hampir semuanya sudah terdokumentasi pada proses keamanan fisik dan lingkungan. Tetapi ada beberapa proses yang masih belum dilakukan sesuai dengan aturan yang ada misalnya penempatan peralatan kerja yang cenderung kurang rapi di ruang kerja, masih ditemukan karyawan yang makan dan minum di ruang pemrosesan informasi, belum maksimalnya pengawasan dan tempat menaikkan dan menurunkan barang logistik organisasi dan perlindungan peralatan di luar ruangan. Dari hasil temuan tersebut, auditor memberikan rekomandasi yaitu penegakan aturan yang telah dibuat manajeman sebelumnya dan pembuatan sarana untuk melindungi peralatan yang dimiliki organisasi.

Hasil pengukuran *maturity level* klausul 11 tentang kontrol akses yaitu 2,91 yaitu berada di level 2 (*limited/repeatable*) yang berarti manajemen sedang melakukan pengembangan pada proses kontrol akses dan belum mempunyai

sebegian besar aturan dasar tentang kontrol akses. Aturan yang belum ada adalah aturan tentang manajemen *password*, keamanan kriptografi, aturan tentang *clear screen,* aturan pemindahan berkas dokumen cetak. Hal lain masalah ketidakpatuhan karyawan tentang aturan yang sudah ada misalnya penggunaan *password,* penggunaan PC yang ditinggal tanpa pengawasan, perlindungan peralatan di wilayah *user*, tidak mematuhi kebijakan *clear desk.* Dari hasil temuan tersebut, auditor memberikan rekomandasi yaitu manajeman harus segera membuat peraturan terkait manajemen *password*, keamanan kriptografi, aturan tentang *clear screen,* aturan pemindahan berkas dokumen cetak. Rekomandasi yang yang lain adalah manajeman harus memberikan teguran hingga *punishment* kepada karyawan yang tidak patuh dalam penggunaan *password,* penggunaan PC yang ditinggal tanpa pengawasan, perlindungan peralatan di wilayah *user*, tidak mematuhi kebijakan *clear desk.*

Hasil dari pengukuran *maturity level* klausul 12 tentang akuisisi sistem informasi, pembangunan dan pemeliharaan yaitu 3,16 yaitu berada pada level 3 *(defined)* yang berarti manajemen sudah mempunyai dasar tentang aturan, prosedur dan kebijakan pada proses. Aturan tersebut meliputi proses implementasi sistem baru, modifikasi aplikasi dan aturan pengembangan sistem. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur yang ada misalnya dalam pengembangan sistem baru tidak ada *framework* yang digunakan dalam perencanaan pembuatan sistem baru. Hal lain adalah belum adanya peraturan tentang integritas pesan elektonik, penggunaan *kriptografi*, manajemen *password* dan peraturan tentang lesensi produk yang digunakan oleh organisasi. Dari hasil temuan tersebut, auditor memberikan rekomandasi yaitu manajeman harus segera

menantukan *framework* yang digunakan untuk perencanaan dalam pembuatan sistem yang baru. Rekomendasi yang lain adalah manajeman harus segera membuat pereturan tentang penggunaan pesan elektronik, menajeman *password* dan lesensi produk yang dimiliki organisasi.

Secara keseluruhan rekomendasi yang diberikan auditor mengarah pada pendisiplinan karyawan yang menggunakan aplikasi SIM-RS dan pembuatan aturan yang lebih detil dengan tujuan menjamin keamanan aplikasi SIM-RS milik RSI Jemursari.