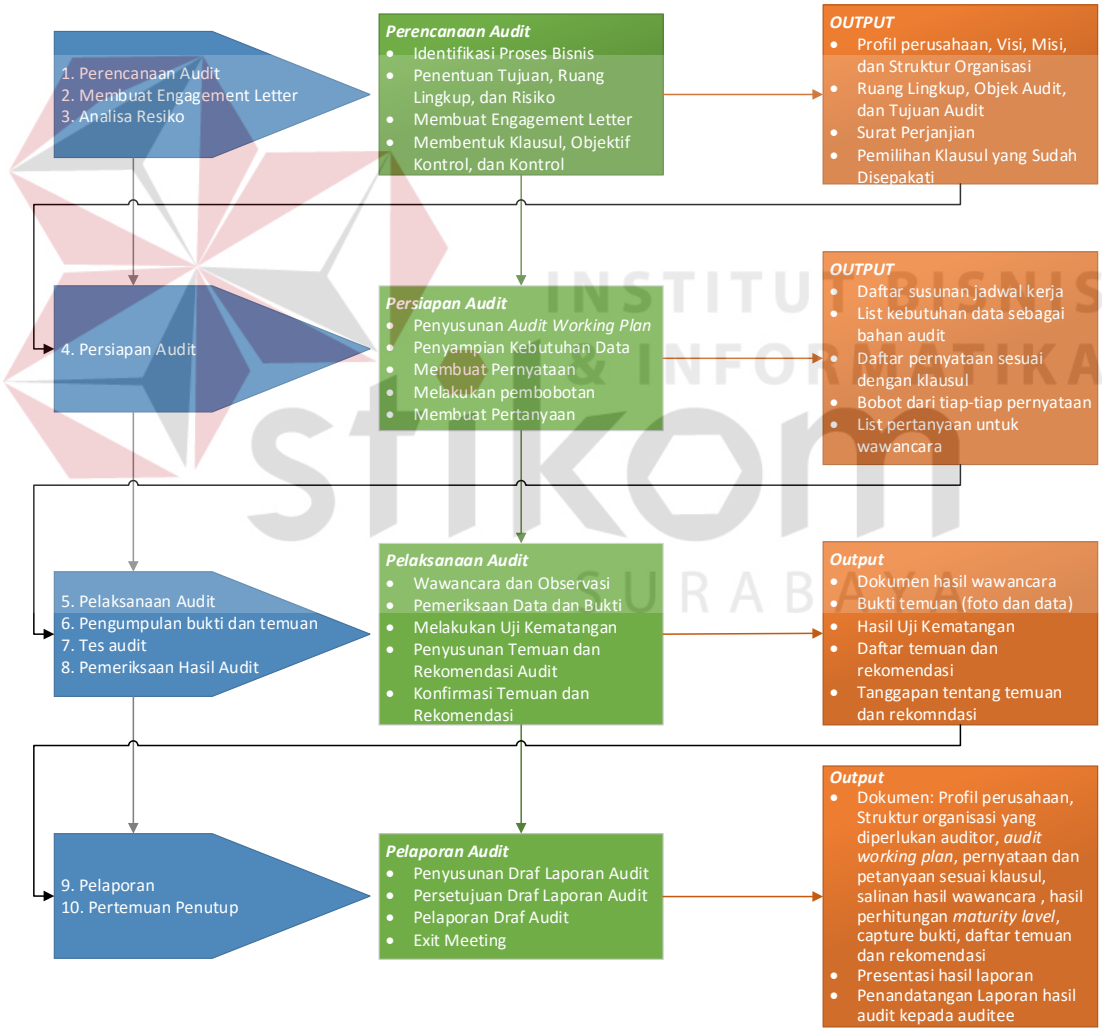
BAB III

METODE PENELITIAN

Pada bab ini akan dibahas tahapan-tahapan melakukan audit keamanan sistem informasi manajemen rumah sakit berdasar ISO 27002:2005 di RSI Jemursari yang terdapat pada Gambar 3.1.



Gambar 3.1 Langkah Audit Keamanan Sistem Informasi

(Sumber: Canon, 2011)

3.1. Tahap Perencanaan Audit

Pada tahap perencanaan audit langkah-langkah yang akan dilakukan adalah memahami proses bisnis yang ada dalam perusahaan, penentuan ruang lingkup objek audit dan tujuan audit keamanan sistem informasi, penentuan objek audit TI, dan membuat *engagement letter*. Dari semua tahapan di atas akan menghasilkan pengetahuan atau informasi tentang proses bisnis TI perusahaan, ruang lingkup perusahaan dan tujuan yang telah ditentukan, serta klausul-klausul yang telah ditentukan oleh kedua belah pihak sebagai acuan dari proses audit.

3.1.1 Identifikasi proses bisnis

Dalam tahap ini auditor harus mempelajari dan memahami proses bisnis yang ada pada perusahaan yang akan diaudit dengan cara melakukan observasi dan wawancara. Observasi dilakukan dengan cara mempelajari dokumen-dokumen perusahaan seperti profil perusahaan, visi dan misi perusahaan, struktur organisasi perusahaan, profil instalasi sistem informasi manajemen rumah sakit, alur sistem informasi manajemen rumah sakit, *job description* karyawan bagian TI RSI Jemursari. Sedangkan wawancara dilakukan untuk memastikan dari observasi yang telah dilakukan sebelumnya. Contoh proses identifikasi proses bisnis dengan melakukan wawancara manajemen dan staf dapat dilihat pada Tabel 3.1.

Output yang dihasilkan pada proses ini adalah profil perusahaan, visi, misi struktur organisasi, proses bisnis bagian teknologi dan sistem informasi serta tugas dan tanggungjawab di bagian teknologi dan sistem informasi.

Tabel 3.1 Contoh Proses Identifikasi Proses Bisnis dengan Melakukan Wawancara

Wawancara Permasalahan PadaBagian Teknologi dan Sistem Informasi RSI Jemursari	Auditor : Alfian N Rahman
	Auditee : Andik Jatmiko, ST
	Tanggal : 11 Februari 2016
Pertanyaan	Jawaban
1. Apakah ada sistem untuk membantu pengelolaan rumah sakit di RSI Jemursari?	Ada, kita memiliki sistem SIM-RS yang sudah terintegrasi ke semua bagian di RSI Jemursari.
2. Bagaimana Awal Penerapan SIM-RS di RSI Jemursari?	Penerapan dilakukan pada tahun 2009, tetapi belum di semua bagian rumah sakit. Penerapan SIM-RS sempat tidak berjalan karena ada sebagian pegawai tidak mau menerapkan SIM-RS.
dst..	dst..

3.1.2. Penentuan Ruang Lingkup, Objek, dan Tujuan Audit

Dalam penentuan ruang lingkup dilakukan dengan cara observasi dan wawancara pada bagian TI RSI Jemursari. Langkah selanjutnya ialah mengidentifikasi dari tujuan yang berhubungan dengan kebutuhan audit keamanan sistem informasi. Hasil dari tahap ini berupa ruang lingkup, objek, dan tujuan audit. Salah satu contoh proses penentuan ruang lingkup dengan melakukan wawancara dapat dilihat pada Tabel 3.2.

Tabel 3.2 Contoh Proses Penentuan Ruang Lingkup dengan Melakukan Wawancara

Wawancara Permasalahan PadaBagian Teknologi dan Sistem Informasi RSI Jemursari	Auditor : Alfian N Rahman
	Auditee : Andik Jatmiko, ST
	Tanggal : 11 Februari 2016
Pertanyaan	Jawaban
1. Apakah dalam penerapan SIM-RS mengalami kendala?	Kendala dalam penerapannya banyak, misalnya masalah *user* tidak mematuhi prosedur penggunaannya, *user* tidak pernah

Tabel 3.2 (Lanjutan)

Wawancara Permasalahan PadaBagian Teknologi dan Sistem Informasi RSI Jemursari	Auditor : Alfian N Rahman
	Auditee : Andik Jatmiko, ST
	Tanggal : 11 Februari 2016
Pertanyaan	Jawaban
	menjaga *password*nya. Selain itu kita pernah mengalami kejadian perangkat jaringan dirusak oleh hewan liar (tikus).
dst..	dst..

3.1.3. Membuat Engagement Letter

Pembuatan *engagement letter* atau surat perjanjian audit dilakukan oleh auditor kepada *auditee*. 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 dan ketentuan perjanjian audit. Pada proses ini akan menghasilkan perjanjian penetapan klausul, kontrol objektif serta kontrol yang telah disepakati oleh auditor dan *auditee*. Berikut contoh surat kesepakatan dengan *auditee* dapat dilihat pada Gambar 3.2.

Engagement Letter

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

Yang bertanda tangan dibawah ini:

Nama : Andik Jatmiko, ST

Jabatan : Kepala Bagian Teknologi dan Sistem Informasi Rumah Sakit Islam Jemursari Surabaya

Bertindak selaku **Kepala Bagian Teknologi dan Sistem Informasi Rumah Sakit Islam Jemursari Surabaya** menugaskan dan memberi wewenang melakukan audit kepada:

Nama : Alfian Noor Rahman

Nim : 124010100018

yang melaksanakan audit keamanan sistem informasi, bertindak sebagai **Auditor**.

Tujuan

Tujuan dari dilakukannya audit ini adalah untuk memeriksa dan mengevaluasi tingkat keamanan sistem informasi manajemen rumah sakit (SIM-RS) yang ada pada Rumah Sakit Islam Jemursari agar dapat mengoptimalkan dalam kinerjanya.

Gambar 3.2 Contoh Surat Kesepakatan dengan *Auditee*

3.1.4. Penentuan Klausul, Objektif Kontrol, dan Kontrol

Dalam pemilihan klausul, objektif kontrol, kontrol disesuaikan dengan permintaan dari pihak instalasi SIM-RS dan disepakati oleh kedua belah pihak (auditor dan *auditee*). Selain itu yang juga menjadi pertimbangan dalam penentuan klausul, objektif kontrol dan kontrol adalah permasalahan yang terjadi pada proses STI di RSI Jemursari. *Output* yang dihasilkan dari pemilihan klausul adalah klausul 8, klausul 9, klausul 11, klausul 12, sesuai dengan Standar ISO 27002:2005.

3.2. Tahap Persiapan Audit Sistem Informasi

Pada tahap perisapan audit langkah-langkah yang akan dilakukan adalah melakukan penyusunan audit *working plan* (AWP), penyampaian kebutuhan data, membuat pernyataan berdasarkan standar ISO 27002: 2005, melakukan pembobotan, dan membuat pertanyaan.

3.2.1. Penyusunan Audit Working Plan (AWP)

Audit Working Plan (AWP) merupakan dokumen yang dibuat oleh auditor dan digunakan untuk merencanakan dan memantau pelaksanaan audit TI secara terperinci. *Output* yang dihasilkan adalah daftar susunan AWP. Berikut contoh jadwal kerja audit dapat dilihat pada Tabel 3.3.

Tabel 3.3 Contoh Jadwal Kerja Audit

NO	Pekerjaan	Bulan											
		Maret				April				Mei			
		1	2	3	4	5	6	7	8	9	10	11	12
1	Study Literautur												
	Melakukan identifikasi proses bisnis dan TI.												
	Melakukan identifikasi terhdap klausul												
	Menentukan Standart												
	Membuat enggament letter												
2	Menyusun Proposal												
	Menyusun Working Plan												
	Membuat Pernyataan dan Pertanyaan												
	Melakukan Pembobotan												
3	Wawancara												
	Pemeriksaan												
	Penemuan Bukti												
	Uji coba Kematangan												
	Menyusun temuan dan recomendas												
4	Menyusun Draft Pelaporan												
	Presentasi Laporan												
	Meminta persetujuan laporan												
	Pendaftaran Ujian Tugas Akhir												

3.2.2. Penyampaian Kebutuhan Data

Penyampaian kebutuhan data auditor dapat disampaikan terlebih dahulu kepada *auditee* agar dapat dipersiapkan terlebih dahulu. Hal tersebut berguna untuk memastikan data-data yang dibutuhkan tersedia. *Field work* dilaksanakan auditor setelah *auditee* menginformasikan ketersediaan semua data yang diperlukan auditor sehingga *field work* dapat dilaksanakan oleh auditor secara efektif dan efisien. *Output* yang dihasilkan adalah daftar penyampain kebutuhan data perusahaan. Contoh pada tampilan Tabel 3.4.

Tabel 3.4 Daftar Penyampain Kebutuhan Data Perusahaan

Lampiran 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 instansi					
5	Dokumen kebijakan keamanan sistem informasi					
6	Dokumen prosedur aplikasi SIM-RS					

3.2.3. Membuat Pernyataan

Dalam pembuatan pernyataan didasarkan pada standar ISO 27002:2005. Pada setiap kontrol keamanan dapat ditentukan pernyataan yang menjelaskan implementasi dan pengontrolan yang dilakukan. *Output* yang dihasilkan adalah pernyataan-pernyataan dapat dilihat pada Tabel 3.5.

Tabel 3.5 Contoh Pernyataan-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.

3.2.4. Melakukan Pembobotan

Setelah membuat pernyataan, yang harus dilakukan adalah memberikan bobot untuk masing masing pernyataan. Keluaran yang dihasilkan dalam tahap ini adalah bobot dari masing-masing pernyataan setelah membuat pernyataan, selanjutnya melakukan pembobotan. Setiap pernyataan harus memiliki nilai bobot masing-masing. Bobot dari masing-masing pernyataan berbeda karena dalam penerapannya untuk kontrol keamanan yang telah ditentukan. Metode ini menggunakan bobot pada penilaian risiko metode kualitatif, karena menurut Sarno dan Iffano (2009)

risiko memiliki hubungan dengan keamanan informasi dan risiko merupakan dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi. Untuk lebih jelas dalam penentuan bobot dapat dilihat pada Tabel 3.6.

Tabel 3.6 Pembobotan Penilaian Risiko

Risiko	Bobot
Low	0,1-0,3
Medium	0,4-0,6
High	0,7-1,0

(Sarno dan Iffano, 2009)

Pembobotan ditentukan dari panduan implementasi dan tingkat seberapa penting dari tiap perusahaan. Pernyataan yang mendapatkan pembobotan dengan risiko *high* berarti pernyataan tersebut sangat penting untuk diterapkan pada perusahaan. Untuk pernyataan dengan bobot risiko *medium* berarti pernyataan tersebut tetap diterapkan meskipun risiko yang akan terjadi apabila ada ancaman keamanan tidak sebesar dengan bobot risiko *high*. Pernyataan dengan risiko *low* berarti pernyataan tersebut tidak terlalu wajib untuk diterapkan namun apabila diterapkan akan menambah keamanan pada sistem. Berikut dapat dilihat di Tabel 3.7 contoh pembobotan dari setiap pernyataan.

Tabel 3.7 Contoh Pembobotan dari Setiap Pernyataan

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

3.3.5. Membuat Pertanyaan

Pertanyaan dibuat berdasarkan pernyataan yang telah dibuat sebelumnya. Dalam satu pernyataan, bisa memiliki lebih dari satu pertanyaan, karena setiap pertanyaan harus mewakili pernyataan saat dilakukan wawancara, observasi, dan identifikasi dokumen. Contoh beberapa pertanyaan yang dihasilkan dari pernyataan dari klausul 8 tentang keamanan sumber daya manusia dengan kontrol 8.1.1 (Aturan dan Tanggungjawab Keamanan) terdapat pada Tabel 3.8.

Tabel 3.8 Contoh Pertanyaan Yang Dihasilkan dari Pernyataan Klausul 8

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?
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?
dst		

3.3. Tahap Pelaksanaan Audit

Langkah-langkah yang akan dilakukan dalam pelaksanaan audit adalah melakukan wawancara, proses pemeriksaan data dan bukti, penyusunan daftar temuan audit dan rekomendasi, konfirmasi hasil temuan audit . Pada tahap ini akan menghasilkan dokumen wawancara, temuan dan bukti, daftar temuan dan rekomendasi, dan konfirmasi temuan audit.

3.3.1. Wawancara dan Observasi

Dalam melakukan proses wawancara didasarkan pada pertanyaan yang telah dibuat oleh auditor. Wawancara dilakukan terhadap bagian-bagian yang terlibat dalam proses audit. Untuk menentukan *auditee* atau orang yang diwawancara maka diperlukan analisa untuk menentukan tabel RACI (*Responsibility, Acountability,*

Consulted, Informed). Pihak yang diwawancara adalah penanggungjawab atau *responsibility* dari tiap-tiap klausul. Hasil pada tahap ini adalah dokumen wawancara yang berisi catatan informasi wawancara dan observasi dan hasil analisis yang dilakukan selama proses audit berlangsung. Berikut contoh wawancara klausul 8 tentang keamanan sumber daya manusia dengan objek kontrol 8.1.1 (Aturan dan Tanggungjawab Keamanan) dapat dilihat pada Tabel 3.9.

Tabel 3.9 Contoh Wawancara Klausul 8

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 ?	Sudah, kita lakukan.
	2. Pendefinisian parameter sudah di sosialisasikan?	Untuk sosialisasi tentang parimater sudah kita sosialisasikan lewat kepala bagian masing masing. Sudah ada aturan tertulis tentang parimeter.
dst..		

3.3.2. Pemeriksaan Data dan Bukti

Dalam pemeriksaan data dapat dilakukan dengan cara wawancara dan observasi kepada *auditee* sesuai dengan ruang lingkup SIM-RS dan klausul yang sudah disepakati yaitu klausul 8, klausul 9, klausul 11 dan klausul 12. Hasil pada tahap ini adalah penemuan bukti dan temuan tentang permasalahan yang terjadi. Bukti dan temuan bisa berupa dokumen, foto, sampel, rekaman dan lain

sebagainya. Contoh dokumen pemeriksaan data dan bukti dapat dilihat pada Tabel 3.10.

Tabel 3.10 Contoh Dokumen 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:_____/_____		
Kontrol: 9.1.1 Pembatasan Keamanan Fisik			
NO	Pemeriksaan	Catatan Pemeriksaan	Catatan Review
1	Cek Dokumentasi standart struktur bangunan.		
dst..			

3.3.3. Melakukan Uji Kematangan

Dalam melakukan proses uji kematangan (*maturity level*) langkah yang dilakukan adalah setiap pernyataan dinilai tingkat kepatutannya sesuai dengan hasil pemeriksaan yang ada menggunakan kriteria penilaian yang ada dalam standar penilaian *maturity level*. Penilaian yang digunakan meliputi *non-eksisten* yang memiliki nilai 0 (nol) hingga ke tingkat *optimal* yang memiliki nilai 5 (lima). Jumlah kriteria nilai yang ada dibagi dengan jumlah seluruh pernyataan dalam satu kontrol keamanan untuk mendapatkan nilai *maturity level* pada kontrol keamanan tersebut.

Setelah *maturity level* setiap kontrol keamanan ISO diketahui, maka langkah selanjutnya adalah menghitung *maturity level* pada setiap objektif kontrol yang diambil dari rata-rata *maturity level* setiap kontrol keamanan yang ada. Setiap rata-

rata *maturity level* keseluruhan objektif kontrol yang ada pada klausul bersangkutan merupakan *maturity level* pada klausul tersebut. Hasil dari proses ini adalah hasil uji *maturity level*. Berikut contoh perhitungan tingkat kematangan pada klausul dapat dilihat pada Tabel 3.11.

Tabel 3.11 Contoh Perhitungan Tingkat Kematangan Pada Klausul

Klausul 9 (Keamanan Fisik dan Lingkungan)										
Objektif Kontrol : 9.1 Wilayah Aman										
Kontrol: 8.1.1 Aturan dan tanggung jawab keamanan				Penilaian						Nilai
NO	Pernyataan	Hasil Pemeriksaan	Bobot	0	1	2	3	4	5	
1	Adanya pendefinisian parimeter keamanan secara jelas terhadap ruangan pemrosesan informasi.	Pendefinisian sudah dilakukan dan sudah disosialisasikan. Bukti : - Lampiran bukti tentang pendifinisian parimeter.	1						√	5
dst..										

3.3.4 . Penyusunan Temuan dan Rekomendasi Audit

Dalam proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah memeriksa data profil perusahaan, kebijakan, standar, prosedur dan melakukan wawancara, *review* dan observasi kepada *auditee*. Seluruh kegiatan tersebut menghasilkan bukti-bukti (*evidence*) yang berarti terkait dengan sistem yang berlangsung di perusahaan. Hasil dari proses ini adalah daftar temuan dan rekomendasi dari proses audit. Berikut contoh lampiran temuan dan rekomendasi pada klausul 8 tentang keamanan sumber daya manusia dengan objek kontrol 8.1.1 (Aturan dan Tanggungjawab Keamanan) dapat dilihat pada Tabel 3.12.

Tabel 3.12 Contoh Lampiran Temuan dan Rekomendasi pada Klausul 8

Temuan dan Rekomendasi **Audit Keamanan Sistem Informasi**					**Auditor: Alfian NR** **Auditee : Andik Jatmiko, ST**
Klausul 9 (Keamanan Fisik dan Lingkungan) 8.1.1 Aturan dan tanggung jawab kemanan					**Tanggal : _____** **Tanda Tangan** _____
NO	**Pernyataan**	**Temuan**	**Bukti**	**Rekomendasi**	**Tanggapan**
1	Adanya pendefinisian parimeter keamanan secara jelas terhadap ruangan pemrosesan informasi.	Pendefinisian sudah di lakukan dan sudah di sosialisasikan.	- Lampiran bukti tentang pendifinisian parimeter		

3.3.5. Konfirmasi Temuan dan Rekomendasi

Temuan harus dikonfirmasikan terlebih dahulu kepada *auditee* sebelum dilaporkan secara formal. Konfirmasi bertujuan untuk mengklarifikasi temuan-temuan yang telah ditemukan dalam proses audit. Hasil dari konfirmasi temuan adalah dokumentasi dalam bentuk catatan dan tanggapan konfirmasi temuan.

3.4. Tahap Pelaporan Audit Sistem Informasi

Terdapat empat tahap dalam melakukan tahap pelaporan audit yaitu: 1. Penyusunan *draf* laporan audit, 2. Persetujuan *draf* laporan audit, 3. Pelaporan audit dan 4. Pertemuan penutup atau pelaporan hasil audit keamanan sistem informasi.

3.4.1. Penyusunan *Draf* Laporan Audit

Dalam melakukan penyusunan *draf* laporan audit berdasarkan daftar pertanyaan, temuan, dan tanggapan *auditee*. Auditor harus menyusun *draf* laporan audit yang telah dilaksanakan secara lengkap, jelas serta objektif..

3.4.2. Persetujuan *Draf* Laporan Audit

Pada *draf* laporan audit yang telah disusun harus dimintakan persetujuan terlebih dahulu oleh *auditee* sebelum diterbitkan sebagai laporan audit yang resmi atau formal. Persetujuan dimaksudkan sebagai tanda pengesahan hasil audit yang dilakukan oleh auditor. Persetujuan *draf* laporan audit dilakukan antara kedua belah pihak berupa notulen persetujuan *draf* laporan audit.

3.4.3. Pelaporan Audit

Pada tahap pelaporan hasil audit, auditor melakukan presentasi kepada pihak manajemen rumah sakit RSI Jemursari atas hasil audit yang dilakukan oleh auditor selama melakukan audit di RSI Jemursari. Setelah melakukan presentasi,

auditor meminta pihak *auditee* untuk memberikan tanggapan atas hasil audit yang dilakukan oleh auditor.

3.4.4 Pertemuan Penutupan dan Pelaporan Hasil Audit

Terakhir dilakukan pertemuan penutup audit yang bertujuan untuk melaporkan hasil audit kepada pihak manajemen, memberikan penjelasan kepada manajemen tentang kondisi khususnya kelemahan untuk objek-objek yang diaudit, memberikan rekomendasi utama yang perlu ditindaklanjuti. Hasil dari pertemuan adalah dokumentasi dalam bentuk notulen pertemuan penutup audit.