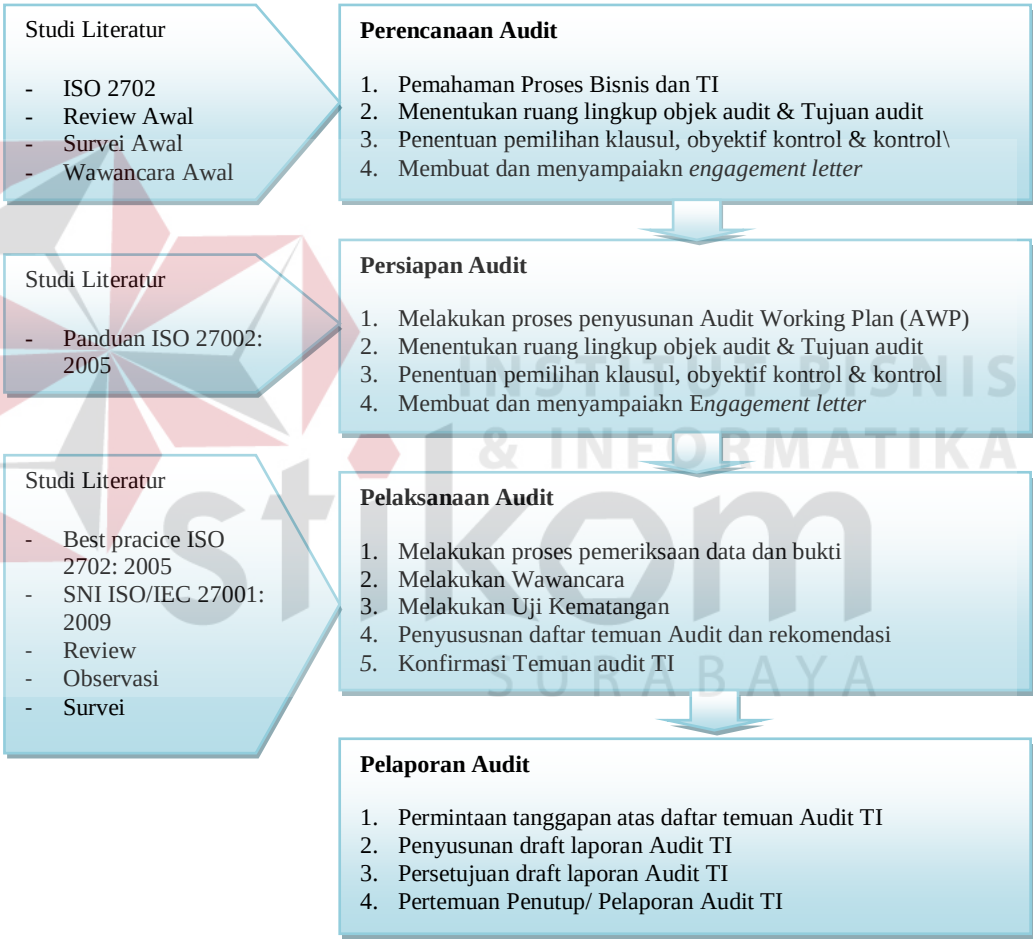
BAB III

METODE PENELITIAN

Pada Bab ini akan dilakukan pembahasan dimulai dengan profil perusahaan, gambaran struktur organisasi dan dilanjutkan dengan tahapan-tahapan audit yang terdapat pada Gambar 3.1.



Gambar 3.1 Langkah Audit Keamanan Sistem Informasi Instalasi SIM-RS

3.1 Tahap Perencanaan Audit

Pada tahap perencanaan langkah-langkah yang dilakukan yakni pemahaman proses bisnis dan TI, menentukan ruang lingkup objek audit dan tujuan audit keamanan sistem informasi, penentuan objek audit TI. Dari tahapan tersebut akan menghasilkan pengetahuan tentang proses bisnis TI perusahaan, ruang ingkup dan tujuan yang telah ditentukan serta klausul yang telah ditentukan sebelumnya dari kedua belah pihak.

3.1.1 Pemahaman Proses Bisnis dan TI

Tahap yang dilakukan saat perencanaan audit adalah mempelajari proses bisnis dan TI perusahaan yang diaudit (*auditee*) dengan mempelajari dokumen-dokumen perusahaan yang dibutuhkan. Dokumen tersebut berupa profil perusahaan, visi dan misi perusahaan, struktur organisasi perusahaan, profil Instalasi SIM-RS RSUD Bangil, Proses bisnis Instlasi SIM-RS RSUD Bangil, *Job description* pegawai IT SIM-RS RSUD Bangil. Langkah selanjutnya adalah mencari informasi apakah sebelumnya perusahaan telah melaksanakan proses audit. Apabila pernah dilakukan audit, maka auditor perlu mengetahui dan memeriksa laporan audit sebelumnya.

Untuk menggali pengetahuan tentang audit, langkah yang dilakukan adalah dengan cara mengetahui dan memeriksa dokumen-dokumen organisasi yang terkait dengan proses audit. Output yang dihasilkan dari pemahaman proses binsis adalah profile perusahaan, visi misi dan motto RSUD Bangil, profil Instalasi SIM-RS RSUD Bangil, Struktur Organisasi Fungsional Instalasi SIM-RS RSUD Bangil, deskripsi pekerjaan Instalasi SIM-RS dan proses bisnis TI di Instalasi SIM-RS RSUD Bangil.

3.1.2 Penentuan Ruang Lingkup, Objek dan Tujuan Audit

Proses kedua pada tahapan perencanaan ini adalah mengidentifikasi ruang lingkup, objek audit dan tujuannya yang akan dibahas dalam audit kali ini. Penentuan ruang lingkup dilakukan dengan cara melakukan observasi dan wawancara pada Instalasi SIM-RS RSUD Bangil. Pada proses ini, langkah yang selanjutnya dilakukan adalah mengidentifikasi tujuan yang berhubungan akan kebutuhan audit keamanan sistem informasi. Output yang dihasilkan adalah hasil ruang lingkup, objek dan tujuan audit.

3.1.3 Menentukan Klausul, Obyektif Kontrol dan Kontrol

Tahap selanjutnya adalah menentukan klausul, obyektif kontrol dan kontrol. Tahap ini ditentukan setelah tahap sebelumnya dilakukan. Pemilihan klausul, objektif kontrol dan kontrol disesuaikan dengan kesepakatan bersama kedua belah pihak dimana pemilihan klausul disesuaikan dengan standar ISO 27002: 2005. Dalam menentukan klausul sebaiknya harus ada bukti tertulis oleh pihak pihak yang bersangkutan. Output yang dihasilkan adalah hasil pemilihan klasul yang akan diperiksa, obyektif kontrol dan kontrol sesuai ISO 27002: 2005.

3.1.4 Membuat dan Menyampaikan *Engagement Letter*

Pada tahap ini adalah membuat dan menyampaikan e*ngagement letter* atau surat perjanjian audit. Surat perjanjian audit adalah surat persetujuan antara auditor dengan kliennya tentang syarat-syarat pekerjaan audit yang akan dilaksanakan oleh auditor. Adapun isi dari *engagement letter* yakni berisi tanggung jawab komite manajemen dan auditor, lingkup audit dan ketentuan perjanjian audit. Output yang dihasilkan dalam membuat dan menyampaikan

Engagement Letter ada berupa dokumen *Engagement Letter* yang disepakati kedua belah pihak.

3.2 Tahap Persiapan Audit

Pada tahap ini langkah-langkah yang dilakukan yakni melakukan proses penyusunan audit *working plan, p*enyampaian kebutuhan data, membuat pernyataan dan membuat pertanyaan. Tahap persiapan akan menghasilkan tabel *working plan,* surat penyampaian kebutuhan data, pernyataan yang telah dibuat berdasarkan standar ISO 27002, daftar pertanyaan, dan daftar pertanyaan yang telah dibuat sesuai dengan pernyataan.

3.2.1 Penyusunan Audit Working Plan (AWP)

Audit Working Plan (AWP) merupakan dokumen yang dibuat oleh Ketua Tim Auditor TI dan digunakan untuk merencanakan dan memantau pelaksanaan audit TI secara terperinci. Output yang dihasilkan adalah daftar susunan AWP.

3.2.2 Penyampaian Kebutuhan Data

Penyampain kebutuhan data diperlukan auditor TI dapat disampaikan terlebih dahulu kepada auditte agar dapat dipersiapkan terlebih dahulu. *Field work* dilaksanakan auditor TI setelah *auditte* menginformasikan ketersediaan semua data yang diperlukan auditor TI sehingga *field work* dapat dilaksanakan oleh auditor TI secara efektif dan efisien. Output yang dihasilkan adalah daftar penyampain kebutuhan data perusahaan pada tampilan Tabel 3.1.

Tabel 3.1 Contoh Lampiran Kebutuhan Data Audit

No	Data Penunjang	Status Data		Tanda Tangan		Ket
		Ada	Tidak			
Berdasarkan acuan Data ISO 27002 Klausul 7 Manajemen Aset						
1	Dokumen mengenai inventarisasi aset organisasi	√				
2	Dokumen mengenai pencatatan hasil pemeliharaan aset	√				
3	Dokumen mengenai perlindungan terhadap aset	√				
4	Dokumen mengenai pertanggung jawaban atas kepemilikan aset	√				
5	Dokumen mengenai aturan penggunaan aset	√				
6	Dokumen pencatatan dalam melakukan pengontrolan klasifikasi informasi		√			

3.2.3 Membuat Pernyataan

Pada tahap selanjutnya adalah membuat pernyataan yang telah dibuat berdasarkan standar ISO 27002: 2005. Pada setiap kontrol keamanan dapat ditentukan pernyataan yang menjelaskan implementasi dan pengontrolan yang dilakukan. Output yang dihasilkan adalah melakukann pembuatan pernyataan pada Tabel 3.2.

Tabel 3.2 Contoh Pernyataan Audit

Klausul: 7 Pengelolaan Aset	
Objektif Kontrol: 7.1 Tanggung Jawab Aset	
Kontrol: 7.1 Inventarisasi Aset	
No	Pernyataan
1	Terdapat Inventarisasi aset organisasi organisasi
2	Terdapat pemeliharaan terhadap aset organisasi
3	Terdapat perlindungan aset organisasi

3.2.4 Membuat Pertanyaan

Pertanyaan dibuat setelah menentukan pernyataan yang dibuat sebelumnya. Satu pernyataan bisa memiliki lebih dari satu pertanyaan karena setiap pertanyaan harus mewakili pernyataan pada saat dilakukan wawancara, observasi, survei dan identifikasi dokumen. Output yang dihasilkan dalam membuat pertanyaan adalah daftar pertanyaan dari pernyataan yang ada pada Tabel 3.3.

Tabel 3.3 Contoh Pertanyaan Audit

Klausul: 7 Pengelolaan Aset		
Objektif Kontrol: 7.1 Tanggung Jawab Aset		
Kontrol: 7.1 Inventarisasi Aset		
No	Pernyataan	Pertanyaan
1	Terdapat Inventarisasi aset organisasi.	1. Apakah organisasi sudah melakukan iventarisasi terhadap aset ? 2. Berapa kali organisasi melakukan inventarisasi aset ? 3. Adakah dokumetasi mengenai inventarisasi aset ? 4. Apakah pencatatan inventarisasi aset sudah menjelaskan status kondisi riil aset? 5. Apakah pencatatan inventariasai aset sudah mengandung nilai bisnis untuk organisasi?
2	Terdapat pemeliharaan terhadap aset organisasi	1. Apakah terdapat pemeliharaan aset? 2. Apa saja aset yang dilakukan pemeliharaan? 3. Berapa kali asset dilakukan pemantauan pemeliharaan? 4. Siapa saja yang m melakukan pemeliharaan tersebut? 5. Apa buktinya bahwa sudah terdapat pemeliharaan aset?
3	Terdapat perlindungan aset organisasi	1. Apakah terdapat perlindungan terhdap aset? 2. Apakah terdapat tingkatan perlindungan aset? 3. Apakah terdapat pencatatan perlindungan aset yang dilakukan secara berkala?

3.3 Tahap Pelaksanaan Audit

Langkah-langkah yang dilakukan dalam pelaksanaan audit yaitu melakukan pertemuan pendahuluan Audit TI, proses pemeriksaan data dan bukti, melakukan wawancara, melakukan uji kematangan, penyusunan daftar temuan audit TI dan rekomendasi, dan konfirmasi temuan audit TI. Tahap ini akan menghasilkan hasil pertemuan pendahuluan audit TI, hasil temuan atau bukti,

hasil uji kematangan, hasil daftar temuan dan konfirmasi serta hasil konfirmasi temuan audit.

3.3.1 Pertemuan Pendahuluan Audit

Pertemuan pendahuluan audit digunakan untuk mendapatkan pemahaman yang sama antara *auditte* dengan auditor. Pertemuan pendahuluan audit dilakukan untuk mendapatkan kesepakatan bersama dan mendapatkan pemahaman yang sama sebelum proses pelaksanaan audit dimulai.

3.3.2 Proses Pemeriksaan Data dan Bukti

Pemeriksaan data dan bukti dilakukan dengan cara melakukan observasi dan wawancara kepada *auditte* sesuai dengan ruang lingkup serta klausul yang telah disepakati oleh Ketua Instalasi SIM-RS untuk mendapatkan bukti atau temuan yang berupa foto ataupun data. Pemeriksaan data dan bukti dituangkan dalam bentuk Program Kerja Audit. Berikut adalah contoh program kerja audit pada Tabel 3.4.

Tabel 3.4 Contoh Pemeriksaan Data dan Bukti dalam Program Kerja Audit (PKA)

Program Kerja Audit Teknologi Informasi				Pemeriksa: Danastri Tanggal: 5 Januari 2013 Penyelia: Auditti: Aqib / Bag IT
Aspek: Klausul 7 Manajemen Aset				TTD:
No	**Pemeriksaan**	**Ref. KKA**	**Catatan Pemeriksaan**	**Catatan Review**
7.1 Tanggung Jawab Aset				
7.1.1 Inventarisasi Aset				
1	Identifikasi inventarisasi aset organisasi Dengan cara: 1. Identifikasi dokument pencatatan inventarisasi aset 2. Wawancara 3. Survei	A.3.a	Telah dilakukan pemeriksaan adanya pencatatan inventarisasi aset sesuai dengan kondisi riil aset, namun inventarisasi tersebut belum ada pencatatan mengenai cara pemulihan terhadap bencana dan pencatatan letak lokasi aset.	

3.3.3 Melakukan Wawancara

Wawancara dilaksanakan setelah membuat pertanyaan yang sudah dibuat sebelumnya. Wawancara dilakukan terhadap pihak yang berkepentingan sesuai dengan pertanyaan yang ada. Hasil Wawancara dilakukan pada Kertas Kerja Audit (KKA).

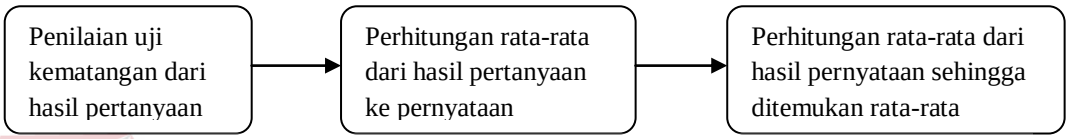
Output yang dihasilkan adalah hasil wawancara yang tertuang pada Kertas Kerja Audit (KKA) yang berisi catatan informasi yang diperoleh dan analisis yang dilakukan selama proses audit. KKA bisa mencakup perencanaan dokumen dan program audit, catatan wawancara, dan lain-lain. Berikut adalah salah satu hasil wawancara pada KKA pada Tabel 3.5.

Tabel 3.5 Contoh Kertas Kerja Audit

Klausul 7 : Manajemen Aset		
Objektif Kontrol : 7.1 Tanggung Jawab Aset		Nama dan Jabatan : Aqib S.Kom- Admin Instalasi SIM-RS
Kontrol : 7.1.1 Inventarisasi Aset		Tanggal :
Ref KKA : A.3.a inventarisasi aset organisasi		TTD :
No.	Pertanyaan	Jawaban
1	Apakah organisasi sudah melakukan iventarisasi terhadap aset ?	Sudah dilakukan pencatatan inventarisasi aset yang dilakukan oleh bagian gudang. Pencatatan inventarisasi aset dilakukan oleh bagian kepala gudang.
2	Berapa kali organisasi melakukan inventarisasi aset ?	1 tahun sekali
3	Adakah dokumentasi mengenai pemilik aset?	Kepemilikan atas aset ada dimana tercatat pada pencatatan inventarisasi aset.
4	Apakah pencatatan inventarisasi aset sudah menjelaskan status kondisi riil aset, pemulihan terhadap bencana dan lokasi aset ?	Pencatatan inventarisasi telah sesuai dengan kondisi riil aset. Namun pemulihan terhadap bencana dan Lokasi aset pada pencatatan inventarisasi aset tidak ada.
5	Apakah pencatatan inventarisasi aset sudah mengandung nilai bisnis untuk organisasi?	Pencatatan inventarisasi aset telah sesuai dengan kebutuhan bisnis rumah sakit dalam mendukung aktivitas proses bisnis di rumah sakit tersebut.

3.3.4 Melakukan Uji Kematangan

Langkah selanjutnya dilakukan uji kematangan untuk mengetahui tingkat kedewasaan atau *maturity level* yang berdasarkan SNI ISO/IEC 27001 :2009. Ouput yang dihasilkan adalah tingkat kedewasaan sesuai dengan SNI ISO/IEC 27001:2009. Adapun gambaran langkah dalam melakukan uji kematangan sebagai berikut.



Gambar 3.2 Langkah Melakukan Uji Kematangan

Berikut adalah contoh hasil penilaian tingkat kedewasaan pada pertanyaan dimana penilaian menggunakan SNI ISO/IEC 27001: 2009 yang terdapat pada Tabel 3.6.

Tabel 3.6 Contoh Penilaian Uji Kematangan Pada Pertanyaan

Klausul : 7 Pengelolaan Aset									
Objektif Kontrol : 7.1 Tanggung Jawab Aset									
Kontrol : 7.1.1 Inventarisasi Aset									
Pernyataan: Terdapat inventarisasi aset organisasi									
No	Pertanyaan	0	1	2	3	4	5	Nilai	Keterangan
1	Apakah sudah dilakukan pendokumentasian inventarisasi aset organisasi?						√	5	Sudah dilakukan pendokumentasian iventarisasi aset organisasi. Pendokumentasian dilakukan oleh pihak Gudang.
2	Apakah pencatatan inventarisasi aset telah dilakukan secara berkala?						√	5	Pencatatan inventarisasi aset telah dilakukan secara berkala setiap setahun sekali.
3	Apakah pencatatan inventarisasi aset sudah menjelaskan status kondisi riil aset?						√	5	Pencatatan inventarisasi aset sudah menjelaskan kondisi real aset. Kondisi rill aset sesuai dengan kenyataan yang ada.

Tabel 3.6 Contoh Penilaian Uji Kematangan Pada Pertanyaan (Lanjutan)

Klausul : 7 Pengelolaan Aset									
Objektif Kontrol : 7.1 Tanggung Jawab Aset									
Kontrol : 7.1.1 Inventarisasi Aset									
Pernyataan: Terdapat inventarisasi aset organisasi									
No	Pertanyaan	0	1	2	3	4	5	Nilai	Keterangan
4	Apakah pencatatan inventarisasi aset sudah menjelaskan pemulihan terhadap bencana?			√				2	Pencatatan inventarisasi aset belum menjelaskan cara pemulihan terhadap bencana.
5	Apakah pencatatan inventarisasi aset sudah menjelaskan lokasi aset?				√			3	Pencatatan inventarisasi aset sebagian belum menjelaskan lokasi aset. Aset yang belum dijelaskan lokasinya berupa aset layanan komunikasi dan aset peralatan komputer (seperti pc, printer, scanner).
		Rata-Rata						4	

Setelah dilakukan perhitungan pada seluruh pertanyaan di setiap kontrol klausul maka dilakukan perhitungan rata-rata dari hasil pertanyaan ke dalam pernyataan. Berikut adalah salah satu contoh perhitungan dari hasil pertanyaan pada Tabel 3.7 sebagai berikut.

Tabel 3.7 Contoh Salah Satu Hasil Penilaian Uji Kematangan dari Pertanyaan

Klausul : 7 Pengelolaan Aset									
Objektif Kontrol : 7.1 Tanggung Jawab Aset									
Kontrol : 7.1.1 Inventarisasi Aset									
No	Pernyataan	0	1	2	3	4	5	6	Nilai
1	Terdapat inventarisasi aset organisasi					√			4
2	Terdapat pemeliharaan aset organisasi					√			4
3	Terdapat perlindungan aset organisasi					√			4
		Rata-Rata							4

Setelah dilakukan perhitungan pada setiap pertanyaan maka dilakukan representatif dari hasil setiap pertanyaan di tiap kontrolnya sehingga didapatkan rata-rata dari objektif kontrol seperti yang terlihat pada Tabel 3.8 sebagai berikut.

Tabel 3.8 Salah Satu Hasil Penilaian Maturity Level Pada Klausul 7

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-Rata Objektif Kontrol**
7. Manajemen Aset	7.1 Tanggung Jawab Aset	7.1.1 Inventarisasi Aset	4	4,17
		7.1.2 Kepemilikan Aset	4	
		7.1.3 Penggunaan Aset yang diterima	4,5	
	7.2 Klasifikasi Informasi	7.2.1 Pedoman Klasifikasi	2	2,75
		7.2.2 Informasi Pelabelan dan Penanganan	3	
	Maturity Level Klausul 7			3,46

3.3.5 Penyusunan Daftar Temuan Audit TI dan Rekomendasi

Pada 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 aktivitas tersebut menghasilkan bukti *(evidence)* yang berarti terkait dengan sistem yang berlangsung di perusahaan. Output yang dihasilkan adalah daftar temuan dan rekomendasi seperti pada Tabel 3.9.

3.3.6 Konfirmasi Daftar Temuan dan Rekomendasi

Temuan harus dikonfirmasikan terlebih dahulu kepada auditee sebelum dilaporkan secara formal. Output dari konfirmasi temuan adalah dokumentasi dalam bentuk risalah atau notulen konfirmasi temuan.

3.4 Tahap Pelaporan Audit

Tahap pelaporan ada beberapa langkah yang dilakukan yaitu melakukan permintaan tanggapan atas daftar temuan audit TI, penyusunan dan persetujuan draft laporan audit TI, dan pertemuan penutup atau pelaporan hasil audit TI. Output yang dihasilkan adalah hasil permintaan tanggapan atas daftar temuan audit TI, hasil penyusunan draft laporan untuk perusahaan, hasil persetujuan draft laporan audit TI, hasil pertemuan penutup berupa *exit meeting.*

3.4.1 Permintaan Tanggapan atas Temuan

Permintaan tanggapan atas temuan yang telah disampaiakan auditor, *auditee* harus memberikan tanggapan dan komitmen penyelesaian. Tanggapan secara formal atas setiap temuan audit diperlukan untuk penyusunan laporan sehingga menjadi dasar pemantauan tindak lanjut penyelesaian temuan audit. Output yang dihasilkan adalah hasil tanggapan atas daftar temuan kepada *auditee*.

3.4.2 Penyusunan Draft Laporan Audit

Penyusunan *draft* laporan audit yang berdasarkan daftar pertanyaan, temuan dan tanggapan maka auditor harus menyusunan draft laporan audit yang telah selesai dilaksanakan. Laporan audit disusun secara efektif, obyektif, lengkap, jelas dan lugas. Output yang dihasilkan adalah draft laporan audit yang berdasarkan daftar pertanyaan, temuan dan tanggapan maka auditor harus menyusunan *draft* laporan audit yang telah selesai dilaksanakan oleh auditor.

Tabel 3.9 Contoh Daftar Temuan Audit TI

<table>
<tr><td colspan="4">DAFTAR TEMUAN AUDIT TEKNOLOGI INFORMASI</td><td>Pemeriksa : Danastri Rasmona W
Penyelia : Bpk. Haryanto</td></tr>
<tr><td colspan="4">Aspek : Klausul 7 Manajemen Aset (Ref A.4.a)</td><td>Auditee : Aqib Halim
Tanggal : 21 Maret 2013</td></tr>
<tr><td>No</td><td>Pernyataan</td><td>Temuan atau Bukti</td><td>Referensi, Risiko dan Rekomendasi</td><td>Tanggapan dan Komitmen Penyelesaian</td></tr>
<tr><td>1</td><td>Terdapat pemeliharaan terhadap aset</td><td>Pemeliharaan aset hanya dilakukan pada aset perangkat keras (PC, komputer, Switch Hub, Printer) dan aset perangkat lunak (Sistem operasi, SIM-RS). Sedangkan aset informasi (file data, manual pengguna) dan aset pendukung (meja komputer, lemari arsip, rak server), aset layanana komunikasi dan UPS masih belum dilakukan pemeliharaan.</td><td>Referensi :
Lampiran klausul 7 A.4.a
Ref : ISO 270002 7.1.1 Inventarisasi Aset

Risiko :
Usia aset tidak lama sehingga cepat terjadi kerusakan jika tidak dipelihara.

Rekomendasi :
a. Segera merencanakan pemeliharaan dengan personil lainya yaitu menggerakkan bagian personil di Instalasi SIM-RS dan IPS secepatnya.
b. Segera melaksanakan pemeliharaan secara berkala pada aset informasi (file data dan manual pengguna), aset pendukung (meja komputer, lemari arsip dan rak server) , aset layanan komunikasi dan peralatan UPS.</td><td>Tanggapan :
Memang suatu pemeliharaan masih kurang karena sebagian masih fokus dalam hal perbaikan jika ada kondisi kerusakan.

Komitmen Penyelesaian :
Kami akan menyimpan sebagai suatu masukan dan meninjau ulang untuk diimplementasikan lagi apakah hal ini bisa dilaksanakan secepatnya atau tidaknya.</td></tr>
</table>

3.4.3 Persetujuan Draft Laporan Audit

Draft laporan audit yang telah disusun harus dimintakan persetujuan terlebih dahulu oleh auditee sebelum diterbitkan sebagai laporan audit yang resmi atau formal. Persetujuan *draft* laporan audit dilakukan antara kedua belah pihak berupa notulen persetujuan *draft* laporan audit.

3.4.4 Pertemuan Penutup atau Pelaporan Hasil Audit

Pertemuan penutup audit dilakukan untuk melaporkan hasil audit kepada manajemen, memberikan penjelasan kepada manajemen tentang kondisi khususnya kelemahan untuk objek audit, memberikan rekomendasi utama yang perlu ditindak lanjuti. Output yang dihasilkan adalah dokumentasi dalam bentuk risalah atau notulen pertemuan penutup audit.