BAB IV

HASIL DAN PEMBAHASAN

Bab ini akan menguraikan hasil atau output dari pembahasan pada bab III dari tahap perencanaan, persiapan, pelaksanaan dan tahap pelaporan audit sistem informasi yang ada.

4.1 Tahapan Perencanaan Audit Sistem Informasi

Hasil dari tahapan perencanaan ini berupa: 1. Hasil pemahaman proses bisnis dan TI yang telah dilihat, 2. Hasil ruang lingkup objek audit dan tujuan audit, 3. Hasil penentuan klausul, obyektif kontrol dan kontrol, dan 4 Hasil perjanjian audit berupa surat perjanjian audit atau *Engagement Letter*.

4.1.1 Hasil Pemahaman Proses Bisnis dan TI

Pada perencanaan audit, pemahaman proses bisnis dan TI merupakan hal yang pertama yang harus dilakukan oleh seorang auditor untuk mengetahui seluk beluk perusahaan sebelum dilakukan audit dengan cara memahami dokumen perusahaan, yaitu profil perusahaan, visi dan misi RSUD Bangil, profil Instalasi SIM-RS RSUD Bangil, struktur organisasi fungsional Instalasi SIM-RS. *Job description* pegawai IT di Instalasi SIM-RS, proses bisnis IT di Instalasi SIM-RS.

1. Profil RSUD Bangil

   Rumah Sakit Umum Daerah (RSUD) Bangil Kabupaten Pasuruan merupakan rumah sakit yang berdiri dan diresmikan pada tahun 1981. Tahun 1985 RSUD Bangil menjadi tipe D dan di tahun 1993 berdasarkan SK Menkes No. 20/Menkes/SK/II/1993 menjadi tipe C. Keberadaan RSUD Bangil lebih

bersifat sosiol ekonomi dan lebih menekankan pelayanan sosial kepada masyarakat tidak mampu dan sekaligus sebagai pusat tujuan Puskesmas dan unit-unit kesehatan yaitu di Wilayah Kabupaten Pasuruan. Tujuan RUSD Bangil adalah terwujudnya layanan kesehatan yang prima, merata, terjangkau masyarakat yang didukung dengan SDM yang professional dengan unit kerja yang mandiri.

2. Visi, Misi dan Nilai RSUD Bangil

Visi : Sebagai Rumah Sakit BLUD yang profesional dan beroerientasi kepada pelanggan tahun 2013.

Misi :
a. Menyelenggarakan pelayanan kesehatan prima.
b. Menyelenggarakan pelayanan kesehatan kesejahteraan prima
c. Meningkatkan kompetensi dan kesejahteraan SDM Rumah Sakit
d. Meningkatkan mut sarana dan prasaran rumah sakit
e. Mengelola sumber Daya secara efektif dan efesien.

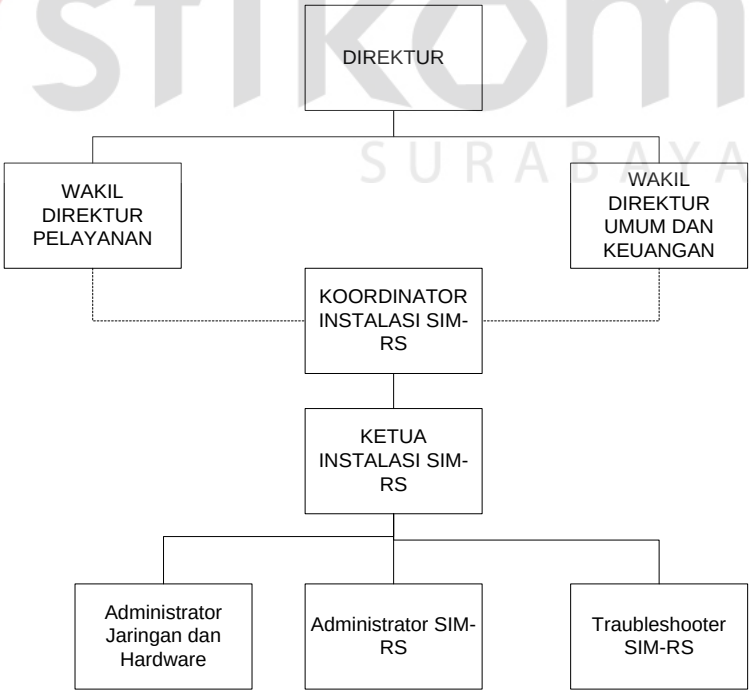
Motto :
a. Sapa, senyum dan sabar
b. Jujur
c. Tanggug Jawab
d. Visioner
e. Kerjasama
f. Adil
g. Peduli

3. Profil Instalasi Sistem Informasi Manajemen Rumah Sakit (SIM-RS) Bangil

   Instalasi SIM-RS terbentuk di tahun 2009 sebagai pendukung kelancaran operasional Sistem Informasi Manajemen Rumah Sakit Umum Daerah (RSUD) Bangil Kabupaten Pasuruan. Instalasi SIM-RS atau disebut dengan Tim Pengelola Data Elektronik bertanggung jawab langsung kepada Direktur dan dalam pelaksanaan tugas sehari-hari berada di bawah koordinasi Wakil Direktur Pelayanan.

4. Struktur Organisasi Fungsional di Instalasi SIM-RS

   Gambar 4.1 adalah gambaran struktur organisasi fungsional Instalasi SIM-RS di RSUD Bangil. Instalasi SIM-RS bekerja di bawah koordinator Instalasi SIM-RS. Adapun jabatan pada Instalasi SIM-RS di bawah pimpinan ketua Instalasi SIM-RS yaitu bagian administator jaringan dan hardware, administrator SIM-RS dan bagian troubleshooter SIM-RS.



Gambar 4.1 Struktur Organisasi Instalasi SIM-RS RSUD Bangil

5. Deskripsi Pekerjaan di Instalasi SIM-RS

Instalasi SIM-RS mempunyai struktur organisasi fungsionalitas dimana pada stuktur didalamnya terdapat keahlian pekerjaan apa saja yang dimiliki oleh setiap bagiannya. Pada Tabel 4.1 menjelaskan job description Instalasi SIM-RS RSUD Bangil.

Tabel 4.1 *Job Description* Instalasi SIM-RS RSUD Bangil

No	Jabatan	Deskripsi Tugas
1	Kepala bagian PDE atau Instalasi SIM-RS	Bertanggung jawab memastikan semua kebutuhan Sistem Informasi Manajemen Rumah Sakit (SM-RS) di seluruh Rumah Sakit Urain Tugas: a. Memberikan keterangan terkait dengan kondisi SIM-RS kepada manajamen RS b. Berkoordinasi dengan manajemen membuat kebijakan terkait dengan SIM-RS c. Mengkoordinir pembuatan perencanaan tahunan untuk perbaikan SIM-RS agar bisa mendukung proses bisnis RS d. Mengkoordinir staf PDE/ Instalsai SIM-RS dalam menalankan tugasnya e. Mengkoordinir inventarisasi alat-alat pendukung SIM-RS yang dimiliki rumah sakit f. Mengkoordinir usulan alat-alat pendukung SIM-RS .
2	Adiministrator jaringan dan Hardware	Bertanggung jawab memastikan seluruh jaringan dan hardware di RS tidak bermasalah. Uraian Tugas: a. Melakukan perbaikan jaringan jika terdapat jaringan yang tidak berfungsi. b. Segera melakukan perbaikan jaringan jia terdapat jaringan yang tidak berfungsi c. Melakukan pemasangan hardware seperti PC atau printer d. Melakukan instalasi software yang dibutuhkan komputer baru yang akan dihubungkan dengan SIM-RS e. Melaporkan dan atau memperbaiki hardware pendukung SIM-RS yang bermasalh f. Membuat perencanaan dan pemasangan jaringan g. jika ada PC atau hardware lain uang perlu terhubung dengan jaringan

Tabel 4.1 *Job Description* Instalasi SIM-RS RSUD Bangil (Lanjutan)

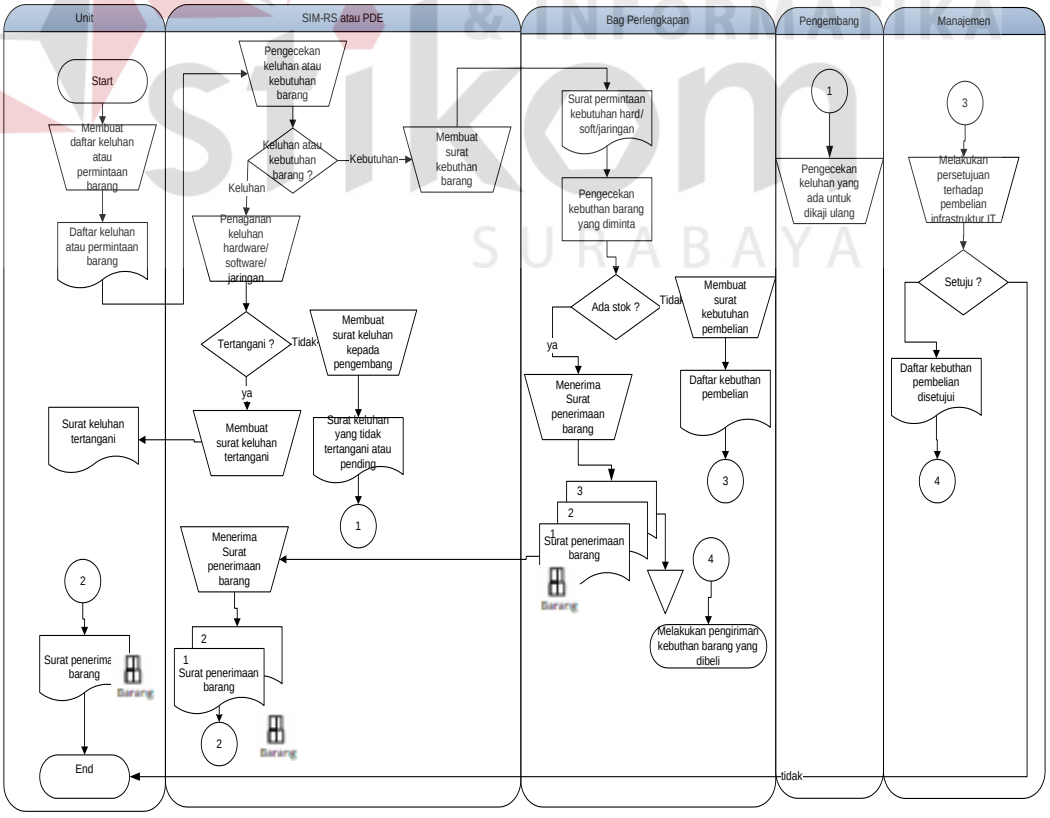
No	Jabatan	Deskripsi Tugas
2		h. Merekomendasikan hal yang berhubungan dengan prencanaan, pemasangan dan perbaikan hardware.
3	Administrator SIM-RS	Bertanggung jawab memastikan bahwa SIM-RS telah mengakomodir kebuthnan RS. Sehingga bisa menjadi sumber informasi untuk pelayanan dan pengemabilan keputusan. Uraian Tugas: a. Membuat laporan/report yang belum bisa diakomodir oleh SIM-RS b. Mengkomunikasikan dengan vendor dan atau memperbaiki hal hal yang dirasa kurang pada SIM-RS c. Melakukan perubahan pengaturan SIM-RS d. Melakukan seting ulang untuk PC setelah diperbaiki oleh admin hardware dan jaringan e. Memastikan keaman data SIM-RS dari serangan orang-orang yang tidak berkepentingan dan orang yang mempunyai niat yang tidak baik f. Memberikan hak akses (otoritas) pada semua pengguna SIM-RS sesuai kebijakan manajemen g. Maintenance software (backup data, backup system) h. Melakukan optimalisasi sistem informasi.
4	Troubleshouter SIM-RS	Bertanggung jawab memastikan semua pengguna SIM-RS telah paham dan mengerti cara menggunakan SIM-RS Uraian Tugas a. Membuat Standard Operation Procedure (SOP) b. Melayani permintaan dan komplain dari pengguna SIM-RS terkait dengan kesulitan pengguna dalam mengoperasikan SIM-RS

6. Proses bisnis dan TI di Instalasi SIM-RS

Proses bisnis pada Instlasi SIM-RS dilakukan saat dilakukan komplain mengenai SIM-RS baik itu komplain pada software, perangkat keras ataupun jaringan yang berasal dari permintaan unit lainnya. Unit yang membutuhkan suatu penanganan akan melakukan permintaan kepada Instalasi SIM-RS. SIM-RS akan melakukan pendataan komplain dari unit. Jika permintaan

tersebut berupa keluhan maka pihak SIM-RS akan melakukan penanganan. Penanganan tersebut jika tak terselesaikan maka akan melakukan tindakan orang kedua yaitu pihak pengembang dengan membuat surat keluhan dan jika terselesaikan maka akan langsung memberikan surat keluhan tertangani. Jika keluhan berupa permintaan barang maka Instalasi SIM-RS akan membuatkan surat permintaan barang yang dibutuhkan kepada bagian perlengkapan. Bagian perlengkapan akan menerima surat permintaan barang dari SIM-RS untuk dilakukan pengecekan barang yang ada. Jika bagian perlengkapan memiliki stok yang diminta maka akan langsung membawa barang dan surat ketersediaan barang kepada bagian manajemen atau unit. Berikut adalah alur proses bisnis Instalasi SIM-RS.

Gambar 4.2 Proses Bisnis dan TI Instalasi SIM-RS RSUD Bangil.



4.1.2 Ruang Lingkup, Objek dan Tujuan Audit

Menentukan ruang lingkup, objek audit dan risiko audit ditentukan dengan cara melakukan observasi, wawancara dan review pada Instalasi SIM-RS. Adapun hasil dari penentuan ruang lingkup, objek audit dan tujuan audit yaitu ruanng lingkup yang akan diaudit membahas mengenai audit keamanan sistem informasi. Objek auditnya pada Instalasi SIM-RS dengan menentukan klausul mana yanag akan dipilih nantinya sesuai dengan kesepakatan bersama kedua belah pihak. Tujuan audit agar dapat mengukur hasil tingkat kedewasaan dengan standar SNI ISO/IEC 27001: 2009 beserta temuan dan rekomendasi yang dilakukan.

4.1.3 Menentukan Klausul, Obyektif Kontrol dan Kontrol

Adapun dalam menetapkan klausul, obyektif kontrol dan kontrol yang ada terdapat pada Tabel 2.2 disesuaikan hasil kesepakatan bersama kedua belah pihak. Sehingga hasil yang didapatkan adalah klausul 7 (manajemen aset), klausul 8 (Keamanan Sumber Daya Manusia), Klausul 9 (Keamanan Fisik dan Lingkungan), Klausul 11 (Kontrol Akses), Klausul 12 (Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan).

4.1.4 Membuat Engagement Letter

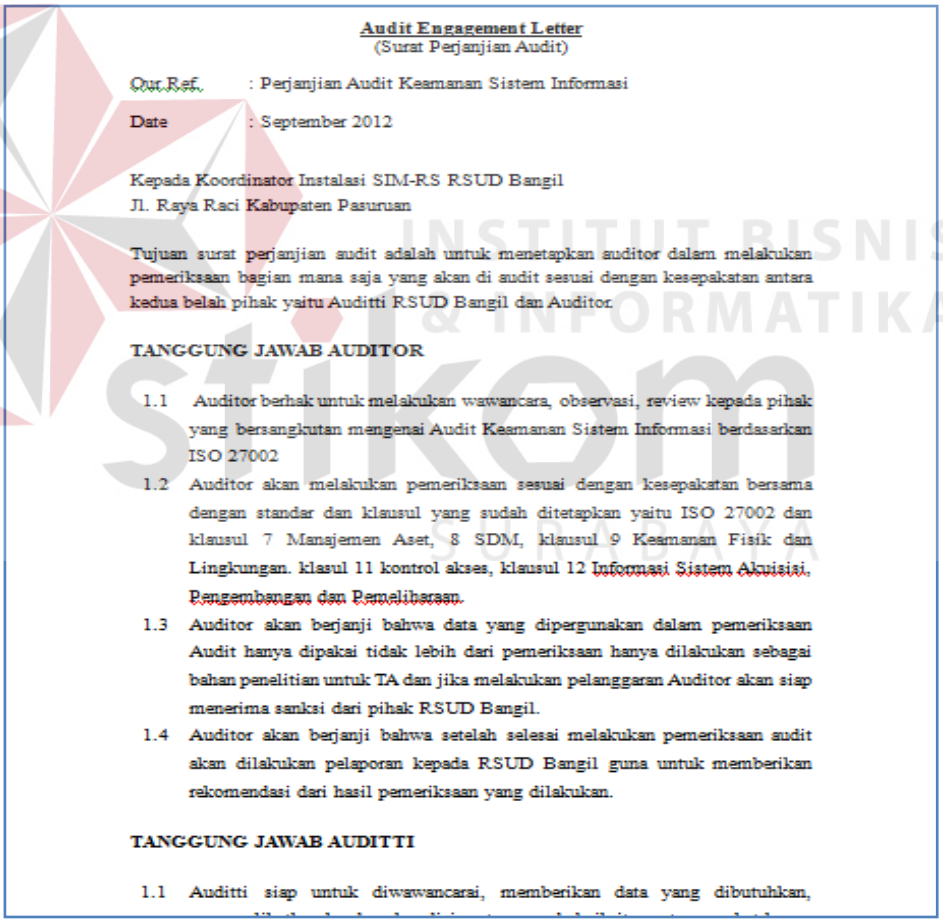
Engagement Letter adalah surat perjanjian kedua belah pihak antara auditor dengan *client* sebagai bentuk kesepakatan. Pada Gambar 4.3 merupakan hasil potongan *Engagement Letter*. Adapun surat perjanjian atau *Engagement Letter* ada pada Lampiran 1 dan berisi poin sebagai berikut.

a. Tanggung jawab auditor.

b. Tanggung jawab auditee.

c. Ruang Lingkup audit sebagai berikut.

1. Tempat melakukan audit.
2. Standar yang digunakan.
3. Waktu dalam pelaksanaan audit.
4. Periode data yang digunakan untuk audit.
5. Klausul yang digunakan audit sesuai dengan hasil pemeriksaan dan kesepakatan.



Audit Engagement Letter
(Surat Perjanjian Audit)

Our Ref. : Perjanjian Audit Keamanan Sistem Informasi

Date : September 2012

Kepada Koordinator Instalasi SIM-RS RSUD Bangil
Jl. Raya Raci Kabupaten Pasuruan

Tujuan surat perjanjian audit adalah untuk menetapkan auditor dalam melakukan pemeriksaan bagian mana saja yang akan di audit sesuai dengan kesepakatan antara kedua belah pihak yaitu Auditti RSUD Bangil dan Auditor.

TANGGUNG JAWAB AUDITOR

1.1 Auditor berhak untuk melakukan wawancara, observasi, review kepada pihak yang bersangkutan mengenai Audit Keamanan Sistem Informasi berdasarkan ISO 27002

1.2 Auditor akan melakukan pemeriksaan sesuai dengan kesepakatan bersama dengan standar dan klausul yang sudah ditetapkan yaitu ISO 27002 dan klausul 7 Manajemen Aset, 8 SDM, klausul 9 Keamanan Fisik dan Lingkungan. klasul 11 kontrol akses, klausul 12 Informasi Sistem Akuisisi, Pengembangan dan Pemeliharaan.

1.3 Auditor akan berjanji bahwa data yang dipergunakan dalam pemeriksaan Audit hanya dipakai tidak lebih dari pemeriksaan hanya dilakukan sebagai bahan penelitian untuk TA dan jika melakukan pelanggaran Auditor akan siap menerima sanksi dari pihak RSUD Bangil.

1.4 Auditor akan berjanji bahwa setelah selesai melakukan pemeriksaan audit akan dilakukan pelaporan kepada RSUD Bangil guna untuk memberikan rekomendasi dari hasil pemeriksaan yang dilakukan.

TANGGUNG JAWAB AUDITTI

1.1 Auditti siap untuk diwawancarai, memberikan data yang dibutuhkan,

Gambar 4.3 Hasil potongan *Engagement Letter*

d. Jadwal kerja

e. Metode kerja

f. Biaya

g. Persetujuan kesepakatan bersama

4.2 Tahap Hasil Persiapan Audit Sistem Informasi

Tahap hasil persiapan Audit Sistem Informasi dilakukan dengan cara menyusun *Audit Working Plan* (AWP), penyampaian kebutuhan data audit, membuat pernyataan, membuat pertanyaan. Penyampaian kebutuhan data sebelum dilakukan audit untuk melakukan kajian dokumen sebelumnya. Selanjutnya dalam membuat pernyataan dan pertanyaan berdasarkan standard ISO 27002.

4.2.1 Hasil Penyusunan *Audit Working Plan* (AWP)

Ouput dari penyusunan *Audit Working Plan* (AWP) berupa jadwal kerja. Jadwal kerja dimulai dari awal kegaitan sampai akhir kegiatan dimana dapat dilihat pada Tabel 4.2.

	Task Name	Start	Finish
1	**Perencanaan Audit**	**Mon 03/09/12**	**Fri 28/09/12**
2	Pemahaman proses bisnis dan TI	Mon 03/09/12	Fri 28/09/12
3	Menentukan ruang lingkup objek audit dan tujuan au	Tue 18/09/12	Wed 19/09/12
4	Menentukan klausul , obyektif kontrol dan kontrol	Tue 11/09/12	Thu 13/09/12
5	Membuat dan menyampaikan engagement letter	Fri 14/09/12	Mon 17/09/12
6	**Persiapan Audit**	**Tue 18/09/12**	**Mon 26/11/12**
7	Penyusunan AWP	Tue 18/09/12	Sat 22/09/12
8	Penyampaian kebutuhan data	Mon 24/09/12	Thu 27/09/12
9	Membuat pernyataan	Mon 24/09/12	Mon 05/11/12
10	Membuat pertanyaan	Tue 06/11/12	Mon 26/11/12
11	**Pelaksanaan Audit**	**Wed 28/11/12**	**Thu 23/05/13**
12	Melakukan pertemuan pendahuluan Audit TI	Wed 28/11/12	Mon 03/12/12
13	Mealkaukan proses pemeriksaan data dan bukti	Sat 05/01/13	Tue 22/01/13
14	Melakukan wawancara dan observasi	Wed 23/01/13	Tue 12/03/13
15	Melakukan uji kematangan	Wed 13/03/13	Wed 20/03/13
16	Penyusunan daftar temuan Audit TI dan rekomenda	Thu 21/03/13	Tue 14/05/13
17	Konfirmasi temuan Audit TI	Wed 15/05/13	Thu 23/05/13
18	**Pelaporan Audit**	**Fri 24/05/13**	**Wed 05/06/13**
19	Permintaan tanggapan atas daftar temuan Audit TI	Fri 24/05/13	Wed 29/05/13
20	Penyusnan draft laporan Audit TI	Thu 30/05/13	Mon 03/06/13
21	Persetujuan draft laopran Audit TI	Tue 04/06/13	Tue 04/06/13
22	Pertemuan penutup / Pelaporan Audit TI	Wed 05/06/13	Wed 05/06/13
23	Pembuatan Laporan TA	Mon 03/09/12	Mon 17/06/13

Tabel 4.2 Hasil *Audit Working Plan.*

4.2.2 Penyampaian Kebutuhan Data

Pada tahap persiapan audit, setelah membuat AWP maka proses selanjutnya adalah menyampaikan kebutuhan data yang diperlukan kepada *auditee* untuk penunjang pemeriksaan auditor. Fungsinya dalam menyampaikan kebutuhan data sebelumnya agar auditor lebih mudah dan lebih cepat dalam memeriksa pada tahap pelaksanaannya sehingga penyampaian kebutuhan data bisa dipersiapkan sebelumnya. Adapun penyampaian kebutuhan data dapat dilihat pada Tabel 4.3 dan lebih detailnya berada pada Lampiran 2.

Tabel 4.3 Daftar Kebutuhan Dokumen

No	Data penunjang yang diperlukan dalam pelaksanaan Audit	Status Data			TTD		Keterangan
		Ada	Tdk	PD	Adr	Adt	
1	Profil perusahaan	√					Ada dokumentasi
2	Struktur Organisasi	√					Ada dokumentasi
3	Job description pegawai	√					Ada di surat keputusan direktur
4	SOP SIM-RS	√					Ada dokumentasi
5	Dokumen inventarisasi aset organisasi	√					Ada daftar inventarisasi
6	Dokumen pencatatan hasil pemeliharaan aset						Ada dokumentasi pemeliharaan aset
7	Dokumen perlindungan terhadap aset	√					Ada dokumentasi
8	Dokumen pertanggung jawaban kepemilikan aset	√					Ada dokumentasi

4.2.3 Pembuatan Pernyataan

Pada tahapan persiapan audit proses selanjutnya adalah membuat pernyataan dengan mengacu pada kontrol keamanan berdasarkan standard ISO 27002. Membuat pernyataan menggambarkan bagaimana implementasi dan pelaksanaan kontrol yang ada. Fungsi untuk membuat pernyataan agar

memudahkan auditor dalam membuat pertanyaan pada proses selanjutnya. Salah satu contoh adalah klausul 7 mengenai manajemen aset sebagai standar acuan dalam memeriksa kondisi manajemen aset yang ada di Instalasi SIM-RS. Berikut adalah pernyataan pada klausul 7 pada Tabel 4.4 adapun lebih lengkapnya berada di Lampiran 3.

Tabel 4.4 Pernyataan pada Klausul 7

Klausul : 7 Pengelolaan Aset	
Objektif Kontrol : 7.1 Tanggung Jawab Aset	
Kontrol : 7.1.1 Inventarisasi Aset	
No.	Pernyataan
1	Terdapat inventarisasi aset organisasi.
2	Terdapat pemeliharaan terhadap aset organisasi
3	Terdapat perlindungan aset organisasi
Klausul : 7 Pengelolaan Aset	
Objektif Kontrol : 7.1 Tanggung Jawab Aset	
Kontrol : 7.1.2 Kepemilikan Aset	
No.	Pernyataan
1	Terdapat pertanggung jawaban atas kepemilikan aset
Klausul : 7 Pengelolaan Aset	
Objektif Kontrol : 7.1 Tanggung Jawab Aset	
Kontrol : 7.1.3 Pengguna Aset yang diterima	
No.	Pernyataan
1	Terdapat aturan dalam penggunaan aset
2	Kesadaran pengguna dalam penggunaan atau memiliki akses ke aset organisasi mengenai batasan penggunaan informasi organisasi

4.2.4 Hasil Membuat Pertanyaan

Setelah membuat pernyataan langkah selanjutnya adalah membuat pertanyaan. Dimana membuat pertanyaan berdasarkan dari pernyataan yang sudah dibuat sebelumnya. Pertanyaan disesuaikan berdasarkan pelaksanaan kontrol yang ada pada standard ISO 27002. Berikut adalah pertanyaan yang dibuat pada klausul 7 mengenai manajemen aset pada Tabel 4.5 halaman 60 dan untuk lebih lengkapnya ada pada Lampiran 4.

Tabel 4.5 Pertanyaan pada Klausul 7

Klausul : 7 Manajemen Aset		
Objektif Kontrol : 7.1 Tanggung Jawab Aset		
Kontrol : 7.1.1 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 dokumentasi mengenai pemilik aset?
		4. Apakah pencatatan inventarisasi aset sudah menjelaskan status kondisi riil aset, pemulihan terhadap bencana dan lokasi aset ?
		5. Apakah pencatatan inventarisasi aset sudah mengandung nilai bisnis untuk organisasi?
2	Terdapat pemeliharaan terhadap aset organisasi	1. Apakah terdapat pemeliharaan aset?
		2. Apa saja jenis aset yang dilakukan pemeliharaan?
		3. Berapa kali pemantauan pemeliharaan aset ?
		4. Siapa saja yang melakukan pemeliharaan tersebut?
		5. Apa buktinya bahwa sudah terdapat pemeliharaan aset?
3	Terdapat perlindungan aset organisasi	1. Apakah terdapat perlindungan terhadap aset ?
		2. Apakah terdapat tingkatan perlindungan aset ?
		3. Apakah terdapat pencatatan perlindungan aset yang dilakukan secara berkala?

4.3 Hasil Pelaksanaan Audit

Pada tahap ini langkah-langkah yang dilakukan yaitu melakukan pertemuan pendahuluan Audit TI, melakukan proses pemeriksaan data dan bukti, melakukan wawancara, melakukan uji kematangan, penyusunan daftar temuan audit TI dan rekomendasi dan konfirmasi temuan audit TI.

4.3.1 Hasil Pertemuan Pendahuluan Audit

Hasil pertemuan pendahuluan audit untuk mendapatkan pemahaman yang sama antara *auditte* dan auditor sebelum pelaksanaan dimana berupa notulen hasil pertemuan pendahuluan audit yang tertera pada Gambar 4.4.

NOTULEN HASIL PERTEMUAN PENDAHULUAN AUDIT

Pertemuan pendahuluan audit bertujuan untuk mendapatkan pemahaman yang sama atas audit SI yang akan dilakukan. Adapun kesimpulan hasil pertemuan pendahuluan audit yang telah disepakati dan dipahami bersama pada tanggal 28 November- 2 Desember 2012 adalah sebagai berikut :

1. Bahwa sebelum dilaksanaan kegaiatan audit menegaskan bahwa kegiatan audit bukan untuk mencari kesalahan akan tetapi menemukan kelemahan agar menjadikannya lebih baik kedepannya dengan adanya rekomendasi yang diberikan oleh auditor.
2. Pelaksanaan audit dilakukan dengan megikutsertakan auditti dengan menyesuaikan topik yang akan diperiksa oleh auditor

Klausul	Deskripsi	*Auditee*
7	Manajemen Aset	Bagian Instalasi SIM-RS Bag Pengadaan Barang
8	Keamanan Sumber Daya Manusia	Bagian SDM Bagian Instalasi SIM-RS
9	Keamanan Fisik dan Lingkungan	Bagian Instalasi SIM-RS Bagian IPS
11	Kontrol Akses	Bagian Instalasi SIM-RS
12	Akuisisisi sistem informasi, pembangunan dan pemeliharaan	Bagian Instalasi SIM-RS

3. Kondisi terakhir yang ada di lapangan sebelum di audit tetap sama dengan sebelumnya dan belum adanya perubahan yang ada, sehingga sekiranya untuk menjadi perhatian dalam dilakukan pemeriksaan audit.

Pasuruan, 3 Desember 2012

Gambar 4.4 Notulen Hasil Pendahuluan Audit.

4.3.2 Hasil Pemeriksaan Data dan Bukti

Hasil pemeriksaan data dan bukti dilaksanakan berdasarkan program audit yang dibuat sebelumnya. Teknik audit yang diperiksa menggunkan *review* atau

pemeriksaan dengan dokumentasi, wawancara dan survei yang tertera pada Tabel 4.6. Untuk selebihnya pemeriksaan data dan bukti pada program audit ini terdapat pada Lampiran 5. Untuk bukti foto, rekaman ataupun dokumen sebagai lampiran pendukung terdapat pada Lampiran 11.

Tabel 4.6 Pemeriksaan Data dan Bukti menggunakan Program Kerja Audit.

	Program Audit Teknologi Informasi		Pemeriksa : Danastri Tanggal : 10 Januari 2013 Auditti : Aqib Halim Penyelia : Bpk. Erwin
	Aspek : Klausul 9 Kontrol Akses		
No	**Pemeriksaan**	**Ref. KKA**	**Catatan Pemeriksaan**	**Catatan Review**
	9.2 Peralatan Keamanan			
9.2.1 Penempatan dan Perlindungan Peralatan				
12	Cek penempatan secara khusus kepada peralatan yang penting Dengan cara: 1. Wawancara 2. Dapatkan dokumen mengenai penempatan peralatan yang penting untuk meminimalkan akses yang tidak sah 3. Survey Ref : ISO 270002 9.1.2 Kontrol Entri Fisik	B.3a B.4.a	Telah dilakukan pemeriksaan bahwa peralatan penempatan sudah dilakukan dengan baik dan tertata. Peralatan penempatan secara khusus terdapat misanya penyimpanan lemari baca untuk dokumen penting, penempatan komputer server yang sensitif dipisahkan penempatannya. Namun aturan peletakan yang aman masih belum ada secara resmi	
13	Identifikasi batasan pengolahan informasi data yang sensitive. Dengan cara: 1. Wawancara 2. Survey Ref : ISO 270002 9.1.2 Kontrol Entri Fisik	B.3.b	Telah dilakukan pemeriksaan bahwa batasan pengolahan informasi ke data yang sensitif sudah dilakukan. Fasilitas penyimpnana untuk menghindari akses yang tidak sah sudah ada misalnya ruangan tersendiri untuk mengamankan peralatan yang berisi informasi yang sensitif.	

4.3.3 Hasil Wawancara

Pada proses wawancara, auditor melakukan wawancara berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan berdasarkan pertanyaan yang telah dibuat oleh auditor. Wawancara ditujukan kepada pihak yang terlibat didalamnya yaiu auditee. Salah satu contoh hasil wawancara terdapat pada klausul 9.2.1 mengenai penempatan dan perlindungan peralatan yang dapat dilihat

pada Tabel 4.7. Untuk lebih lengkapnya hasil wawancara tersebut terdapat padat Kertas Kerja Audit pada Lampiran 6.

Tabel 4.7 Contoh Hasil Wawancara Klausul 7 Manajemen Aset

Klausul 7 : Manajemen Asset		
Objektif Kontrol : 7.1 Tanggung Jawab Aset		Nama dan Jabatan : Aqib/ Professioal TI
Kontrol : 7.1.1 Inventarisasi Aset		Tanggal : 5 Januari 2013
Ref KKA : A.3.a Inventarisasi aset organisasi		TTD :
No	Pertanyaan	Jawaban
1	Apakah sudah dilakukan pendokumentasian inventarisasi aset organisasi?	Sudah dilakukan pendokumentasian iventarisasi aset organisasi. Pendokumentasian dilakukan oleh pihak Gudang.
2	Apakah pencatatan inventarisasi aset telah dilakukan secara berkala?	Pencatatan inventarisasi aset telah dilakukan secara berkala setiap setahun sekali.
3	Apakah pencatatan inventarisasi aset sudah menjelaskan status kondisi riil aset?	Pencatatan inventarisasi aset sudah menjelaskan kondisi real aset. Kondisi rill aset sesuai dengan kenyataan yang ada.
4	Apakah pencatatan inventarisasi aset sudah menjelaskan pemulihan terhadap bencana?	Pencatatan inventarisasi aset belum menjelaskan cara pemulihan terhadap bencana.
5	Apakah pencatatan inventarisasi aset sudah menjelaskan lokasi aset ?	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).

4.3.4 Hasil Pelaksanaan Uji Kematangan

Hasil pelaksanaan uji kematangan diberikan menurut nilai indeks keamanan informasi pada SNI ISO/IEC 27001: 2009. Berikut ini adalah salah satu hasil tabel analisa penilaian uji kematangan dari setiap pertanyaan pada Tabel 4.8 sebagai berikut.

Tabel 4.8 Contoh Salah Satu Hasil Penilaian Uji Kematangan dari Pertanyaan

Klausul : 7 Manajemen 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	6	Nilai	Keterangan
1	Apakah sudah dilakukan pendokumentasian inventarisasi aset organisasi?						√		5	

Tabel 4.8 Contoh Salah Satu Hasil Penilaian Uji Kematangan dari 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	6	Nilai	Keterangan
2	Apakah pencatatan inventarisasi aset telah dilakukan secara berkala?						√		5	
3	Apakah pencatatan inventarisasi aset sudah menjelaskan status kondisi riil aset?						√		5	
4	Apakah pencatatan inventarisasi aset sudah menjelaskan status kondisi riil aset, pemulihan terhadap bencana dan lokasi aset ?			√					2	
5	Apakah pencatatan inventarisasi aset sudah mengandung nilai bisnis untuk organisasi?				√				3	
		Rata-Rata							4	

Setelah dilakukan penilaian dari setiap pertanyaan, maka dihasilkan rata-rata nilai untuk setiap satu pernyataan. Kumpulan dari hasil rata-rata setiap pernyataan tersebut selanjutnya dihitung untuk menghasilkan rata-rata dari setiap kontrol pernyataan. Berikut adalah salah satu hasil penilaian uji kematangan dari pernyataan pada Tabel 4.9 sebagai berikut.

Tabel 4.9 Contoh Salah Satu Hasil Penilaian Uji Kematangan dari Pernyataan

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 penilaian uji kematangan dengan mendapatkan rata-rata dari setiap kontrol yang ada (misal pada klausul 7) maka selanjunya dilakukan penilaian rata-rata objektif kontrol untuk mendapatkan hasil penilaian *maturity level*. Berikut adalah salah satu perhitungan untuk mendapatkan hasil penilaian *maturity level* pada klausul 9 seperti pada Tabel 4.10 sebagai berikut.

Tabel 4.10 Salah Satu Hasil Penilaian Maturity Level Pada Klausul 9.

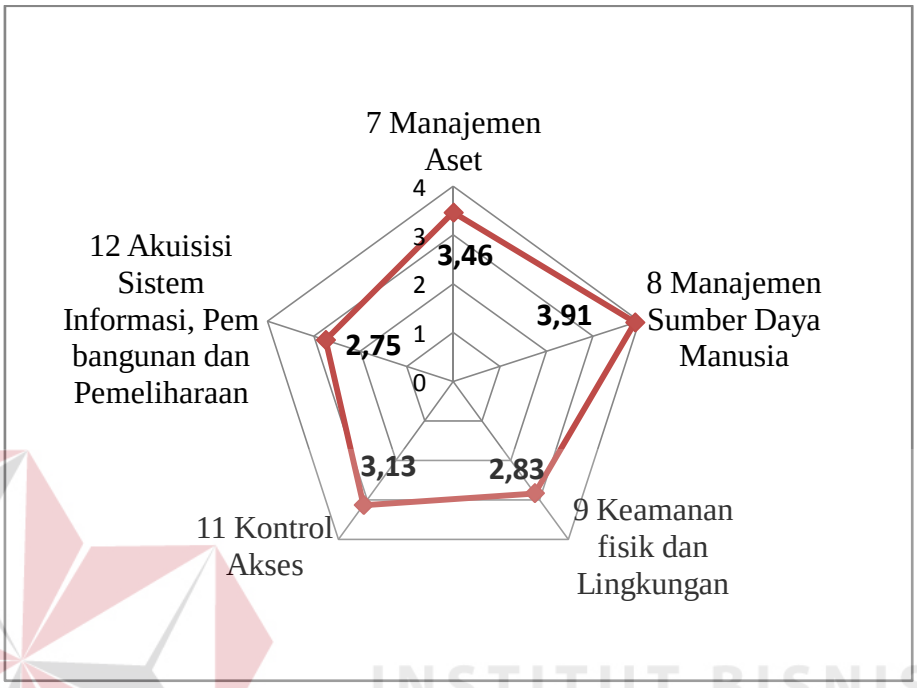
Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Rata-Rata Kontrol Keamanan**	**Rata-Rata Objektif Kontrol Keamanan**
7. Manajemen Aset	7.1 Tanggung Jawab Aset	7.1.1 Inventarisasi Aset	4	4,17
		7.1.2 Kepemilikan Aset	4	
		7.1.3 Penggunaan Aset yang diterima	4,5	
	7.2 Klasifikasi Informasi	7.2.1 Pedoman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

Setelah dilakukan penilaian *maturity level* pada masing-masing klausul, maka langkah selanjutnya dilakukan penilaian akhir pada setiap klausul yang ada. Berikut adalah hasil penilaian akhir yang didapatkan pada Tabel 4.11 sebagai berikut.

Tabel 4.11 Hasil Nilai Rata-Rata Seluruh Klausul

Klausul	**Deskripsi Klausul**	**Hasil**
7	Manajemen Aset	3,46
8	Keamanan Sumber Daya Manusia	3,91
9	Keamanan fisik dan Lingkungan	2,83
11	Kontrol Akses	3,13
12	Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	2,75
Nilai Rata-Rata Seluruh Klausul		3,22

Kesimpulan untuk klausul 7, 8, 9, 11 dan 12 bisa dilihat pada diagram jaring laba-laba pada Gambar 4.5 sebagai berikut.



Gambar 4.5 Gambaran Diagram Jaring Tingkat Kedewasaan Keseluruhan Klausul

Setelah digambarkan dengan model diagram jaring pada Gambar 4.5 terlihat bahwa hasil tertinggi terdapat pada keamanan Sumber Daya Manusia (klausul 8) sebesar 3,91. Bahwa ukuran keamanan informasi menurut SNI ISO/IEC 27001: 2009 berada pada level 3 yaitu pro aktif, artinya keamanan informasi telah dilakukan secara terdefinisi dan konsisten. Hal tersebut dapat dilihat dari adanya penandatanganan perjanjian kerja kepada pegawainya secara konsisten sebelum diberikan akses ke pengolahan informasi.

Sedangkan hasil terendah didapatkan pada Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan (klausul 12) yaitu sebesar 2,75. Bahwa ukuran keamanan informasi menurut SNI ISO/IEC 27001: 2009 berada pada level 2 yaitu aktif artinya proses keamanan sudah diterapkan walaupun sebagian besar masih di

area teknis dan proses pengamanan masih berjalan tanpa dokumentasi atau rekaman resmi. Hal tersebut dapat dilihat dari tidak adanya prosedur yang diterapkan dalam memastikan kebocoran informasi yang terjadi di dalamnya.

Secara keseluruhan, tingkat kontrol keamanan yang diukur mendapatkan nilai sebesar 3,22 yang berarti bahwa ukuran keamanan informasi menurut SNI ISO/IEC 27001: 2009 berada pada level 3 yaitu pro aktif. Hasil ini menunjukkan bahwa sebagai besar proses keamanan informasi telah diterapkan secara konsisten dan terdokumentasi. Efektivitas pengamanan dievaluasi secara berkala walaupun belum melalui proses yang terstruktur. Kerangka kerja pengamanan sudah mematuhi ambang batas minimum standar atau persyaratan hukum yang terkait. Secara umum semua pihak yang terlihat telah menyadari tanggung jawab mereka dalam pengamanan informasi.

4.3.5 Hasil Temuan dan Rekomendasi

Temuan dan rekomendasi dihasilkan pada tabel daftar temuan dan rekomendasi yang dibuat oleh auditor. Hasil tersebut diperoleh dari antara fakta dilapangan dengan beberapa klausul pada ISO 27002: 2005. Adapun temuan yang dihasilkan pada lima klausul yang ditemukan terdapat beberapa kelemahan. Klausul 7 mengenai manajemen aset didapatkan kelemahan, adapun daftar temuan yang didapatkan yaitu pemeliharaan terhadap aset informasi belum direncanakan dengan tepat, belum dilakukan pengontrolan dan mendefinisikan tanggung jawab terhadap aset, tidak ada pertimbangan cara melindungi aset informasi dan cara mengontrol asetnya agar tidak terjadi biaya tambahan.

Klausul 8 mengenai keamanan Sumber Daya Manusia didapatkan kelemahan, adapun daftar temuan yang didapatkan yaitu tidak ada batasan

perjanjian kerja mengenai tanggung jawab pegawai di luar jam kerja, tidak ada pedoman yang dibuat dari pihak manajemen mengenai langkah-langkah dalam mengamankan keamanan informasi yang ada, belum ada bentuk pelatihan khusus pentingnya dalam mengamankan informasi kepada pegawai, tidak ada pencatatan khusus dalam mengembalikan aset pada pegawai yang berhenti atau dipindahkan dalam pekerjaannya, belum terdapatnya prosedur dalam penghapusan aset informasi yang dimiliki pegawai saat pegawai sudah tidak bekerja lagi, belum ada dokumentasi pertimbangan faktor risiko jika akan melakukan penghapusan akses untuk aset dan pengolahan informasinya.

Klausul 9 mengenai keamanan fisik dan lingkungan didapatkan kelemahan, adapun daftar temuan yang didapatkan yaitu belum mendokumentasikan dan mendefinisikan keamanan perimeter bagaimana akses fisik dilakukan agar mencegah kerusakan dari gangguan luar, tidak ada ruangan penerima tamu atau pengunjung dari luar Instalasi SIM-RS agar mengontrol akses dari pihak yang tidak berwenang, tidak adanya alat pendeteksi penyusup pada Instalasi SIM-RS sebagai ruangan pusat pengendalian operasional TI agar mencegah pihak yang tak berwenang masuk, tidak diberikannya buku tamu atau catatan pengujung pada fasilitas pengolahan informasi di Instalasi SIM-RS, pegawai Instalasi SIM-RS, belum memakai tanda pengenal kepegawaian, tidak terdokumentasinya peletakan peralatan penting atau khusus dari jangkauan pihak yang tak berwenang, peletakan alat pemadam kebakaran jauh didekat pintu darurat, saluran listrik dan telekomunikasi pada Instalasi SIM-RS peletakannya masih belum dilindungi dimana peletakannya haruslah di bawah tanah agar tidak terjadi reisko kerusakan dan gangguan saluran listrik dan komunikasinya, posisi

kabel listrik dan komunikasi berdekatan sehingga berisiko terjadi interferensi, belum didokumentasikan keamanan pengkabelan sehingga berisiko terjadi kesalahan pemasangan atau perbaikannya jika ada kerusakan di Instalasi SIM-RS, belum ada pengamanan dan pengontrolan kabel atau pun sistem yang sensitif seperti kabel dan peralatan elektromagnetik lainnya, tidak adanya penyimpanan catatan yang terpelihara secara berkala sehingga berisiko hilangnya keutuhan dan integritas, tidak tersedianya asuransi untuk melindungi peralatan di luar lokasi kerja misalnya di rumah, belum dilakukannya penghapusan dan penghancuran pada peralatan informasi penting yang sudah tidak digunakan lagi sehingga berisiko pihak yang tak berwenang mampu mendapatkan informasi penting tersebut.

Klausul 11 mengenai kontrol akses didapatkan kelemahan, adapun daftar temuan yang didapatkan adalah tidak adanya kebijakan dalam menyampaikan atau menyebarkan informasi yang penting atau tidak adanya kebijakan dalam mengontrol aksesnya, tidak adanya persyaratan dalam melakukan kajian berkala pada kontrol aksesnya, ID pengguna masih mbelum dipasang sesuai dengan kriteria unik, tidak adanya bukti tertulis mengenai kondisi akses pengguna, tidak ada pemeliharaan otorisasi yang dialokasikan kepada pengguna sehingga rawan dalam pembatasan dan pengendalian dalam melindungi aksesnya, belum terdapatnya kerahasiaan password pribadi maupun kelompok pada perjanjian kerja, belum dilakukan pengamanan kata sandi sementara secara aman sehingga rawan diketahui oleh orang yang tak berwenang, penggunaan kata sandi sementara masih tidak sesuai dengan kriteria yang unik sehingga berisiko sandi yang ada mudah ditebak oleh orang lain, belum dilakukan peninjauan hak akses

pengguna secara berkala, tidak ada pendokumentasian tentang peninjauan otorisasi untuk hak akses istimewa secara interval, belum dilakukannya pergantian sandi yang berkualitas, tidak adanya penilai risiko mengenai pengontrolan keamanan peralatan di luar area, belum ada kebijakan mengenai peralatan elektronik, belum ada kebijakan dalam penggunaan layanan jaringan ,tidak adanya prosedur otentiksai pengguna (misalnya kontrol *dial-back*, *call forward*), tidak adanya dokumentasi pengontrolan dan perlindungannya dalam sistem keamanan jaringan, belum ada ketetapan dalam prosedur *log-in* yang benar (misalnya batasan jumlah kegagalan *log-in*, waktu tunggu *login*, tindakan pemutusan koneksi jika *login* beberapa kali gagal, adanya tindakan batasan waktu maksimum dan minumum yang diperbolehkan *log-in*), tidak adanya prosedur tertulis dalam mengidentifikasi dan mengotentikasi *user*, masih lemahnya manajemen *password* yang digunakan, belum adanya dokumentasi prosedur dalam penggunaan fasilitas sistem, belum ada kebijakan format tentang perlindungan fasilitas komputer di luar area, belum ada pertimbangan mengenai *teleworking* atau bekerja dari luar.

Klausul 12 mengenai akuisisi sistem informasi, pembangunan dan pemeliharaan didapatkan kelemahan, adapun daftar temuan yang didapatkan adalah tidak ada dokumentasi mengenai cara mengontrol sistem informasi sehingga sulit untuk melakukan pengontrolan keamanan yang ada, tidak terdapatnya *framework* untuk menganalisis kebutuhan keamanan sistem informasi, belum ada kebijakan ataupun prosedur dalam memanajemen risiko, tidak adanya pemeriksaan jika terdapat adanya kesalahan data yang hilang atau tidak lengkap, tidak adanya dokumentasi mengenai otorisasi data masukan, belum ada prosedur tertulis dalam pengujian kebenaran input data, tidak adanya kajian

risiko keamanan dalam menentukan otentikasi pesan yang dibutuhkan, tidak adanya prosedur tertulis dalam melakukan validasi data output pada sistem informasi yang berjalan saat ini, belum adanya kebijakan dalam penggunaan kontrol kriptografi, belum ada penerapan manajemen kunci, tidak ada penerapan log audit dalam menjaga perpusatkaan program operasional, belum ada pengarsipan versi lama *software* sebagai ukuran kontingensi, tidak ada dokumentasi tertulis mengenai prosedur dalam mengakses kontrol akses pada sistem operasional.

Dari hasil temuan yang didapatkan tersebut maka diberikan suatu rekomendasi agar mampu meminimalisir terjadinya risiko. Hasil rekomendasi yang diberikan bisa dilihat pada Lampiran 8 sebagai salah satu contoh. Pada Tabel 4.12 adalah salah satu contoh daftar temuan dan rekomendasi yang telah diberikan.

Pembahasan pada Tabel 4.12 merupakan salah satu contoh hasil daftar temuan dan rekomenasi pada klausul 9 dengan kontrol 9.1.2 (kontrol entri fisik) maka temuan yang didapatkan adalah peletakan alat pemadam kebakaran yang jauh dari pintu darurat dan letaknya berada kurang lebih 15 meter. Sehingga risiko yang bisa terjadi adalah mempersulit penggunanya jika ada kejadian kebakaran karena peletakannya yang tidak strategis atau jauh dari pintu darurat. Maka rekomendasi yang diberikan adalah merencanakan dan mengkoordinasikan peletakaan kepada pihak IPS untuk mengubah susunan peletakan alat pemadam kebakaran dimana peletakannya tepat berada di daerah pintu darurat. Rekomendasi yang diberikan lainnya adalah membuat pencatatan pengumuman peletakan alat pemadam kebakaran untuk pengguna agar mempermudah dalam

mencari alat pemadam kebakaran tersebut demi terjaganya kondisi lingkungan yang aman dan terhindar dari risiko yang terjadi.

4.4 Hasil Pelaporan Audit Sistem Informasi

Tahap pelaporan adalah tahap untuk melaporkan secara resmi sebagai suatu bentuk penyelesaian proses audit yang dilakukan. Hasil pelaporan audit diserahkan kepada pihak yang berwenang saja dikarenakan bersifat tertutup untuk kalangan umum atau rahasia.

4.4.1 Hasil Permintaan Tanggapan Atas Daftar temuan Audit

Permintaan tanggapan atas daftar temuan audit dilakukan oleh auditor kepada *auditee* dengan memberikan tanggapan atas apa yang telah ditemukan auditor dan memberikan komitmen penyelesaiannya. Hasil permintaan tanggapan atas daftar temuan audit telah dilaksanakan dan dapat dilihat pada Lampiran 8.

4.4.2 Penyusunan dan Persetujuan Draft Laporan Audit TI

Setelah dilakukan penyusunan draft laporan audit TI berupa Kertas Kerja Audit, temuan dan tanggapan a*uditee* sebagai bentuk tanggung jawab atas penugasan Audit TI yang telah selesai dilaksanakan maka dilakukan persetujuan audit. Hasil persetujuan *draft* laporan audit dapat dilihat pada Lampiran 9.

4.4.3 Pertemuan Penutup atau Pelaporan Audit TI

Pertemuan penutup memberikan penjelasan mengenai kondisi yang telah diaudit. Pertemuan penutup dihasilkan berupa *exit meeing* yang dapat dilihat pada Lampiran 10.

Tabel 4.12 Contoh Salah Satu Daftar Temuan Audit pada klausul 9 kontrol 9.1.2 (Kontrol Entri Fisik).

DAFTAR TEMUAN AUDIT TEKNOLOGI INFORMASI				Pemeriksa : Danastri Rasmona W Penyelia : Bpk. Haryanto / Bpk.Erwin
Aspek : Klausul 7 Manajemen Aset (Ref A.4.a)				Auditee : Aqib Halim Tanggal : 21 Maret 2013
No	Pernyataan	Temuan atau Bukti	Referensi, Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
1	Terdapat pemeliharaan terhadap aset	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.	Referensi : Lampiran klausul 7 A.4.a Ref : ISO 270002 7.1.1 Inventarisasi Aset Resiko : 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.	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.

INSTITUT BISNIS
& INFORMATIKA
stikom
SURABAYA