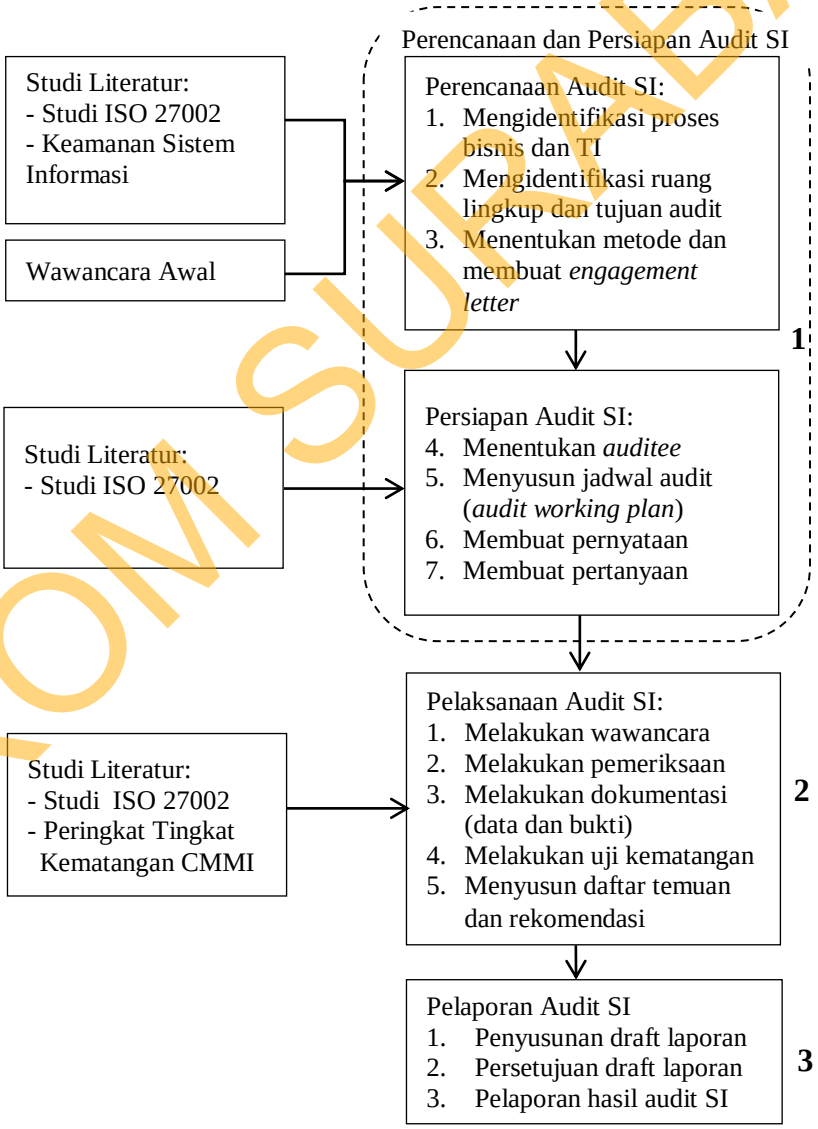
BAB III

METODE PENELITIAN

Pada Bab III ini akan membahas tentang perencanaan dalam melaksanakan audit keamanan sistem informasi. Pembahasan mencakup semua aktivitas auditor dari awal kegiatan hingga hasil akhir audit yang didapat. Gambar 3.1 merupakan alur dari serangkaian kegiatan audit.



Gambar 3.1 Langkah-Langkah Kegiatan Audit Sistem Informasi

Langkah-langkah kegiatan audit sistem informasi yang akan dilakukan telah dipaparkan pada Gambar 3.1 di halaman 29. Penomoran digunakan untuk menunjukkan langkah-langkah kegiatan inti, sedangkan aktivitas lain merupakan inputan yang digunakan untuk kegiatan inti tersebut. Untuk penjabaran dari aktivitas kegiatan yang lebih detail akan dijelaskan pada sub bab metode penelitian ini.

3.1 Perencanaan dan Persiapan Audit Sistem Informasi

Tahap perencanaan dan persiapan ini adalah tahap awal yang dilakukan pada proses audit. Langkah ini dilakukan untuk memastikan bahwa pihak perusahaan yang akan diaudit telah memberikan kewenangan dan mempersiapkan segala sesuatu demi kelancaran pelaksanaan audit yang akan dilakukan. Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Melakukan identifikasi proses bisnis dan TI, 2. Mengidentifikasi ruang lingkup dan tujuan audit, 3. Menentukan metode dan membuat *engagement letter*, 4. Menentukan *auditee*, 5. Menyusun jadwal audit (*audit working plan*), 6. Membuat pernyataan, dan 7. Membuat pertanyaan. Tahap ini akan menghasilkan pengetahuan tentang proses bisnis dan TI perusahaan, ruang lingkup dan tujuan yang telah ditentukan, klausul yang digunakan, tabel *auditee* dan *audit working plan*, pernyataan yang telah dibuat berdasarkan standar ISO 27002, dan pertanyaan yang telah dibuat berdasarkan pernyataan. Hasil dari tahap perencanaan dan persiapan audit sistem informasi ini akan dituangkan ke dalam surat perjanjian audit (*engagement letter*), lampiran perencanaan audit, dan kertas kerja audit.

3.1.1 Mengidentifikasi Proses Bisnis dan TI

Pada tahapan perencanaan audit, proses pertama yang dilakukan adalah melakukan pemahaman proses bisnis dan TI perusahaan yang diaudit (*auditee*). Pemahaman dilakukan dengan cara mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen tersebut berupa profil perusahaan, *standard operating procedure*, kebijakan, standar, prosedur, portopolio, arsitektur, infrastruktur, dan aplikasi sistem informasi. 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 *auditee* langkah yang dilakukan adalah dengan cara mengetahui dan memeriksa dokumen-dokumen yang terkait dengan proses audit, wawancara manajemen dan staff, serta melakukan observasi kegiatan operasional dan teknologi sistem informasi yang digunakan. *Output* yang dihasilkan pada proses ini adalah profil perusahaan, visi dan misi perusahaan, struktur organisasi, serta gambaran umum teknologi informasi yang selengkapnya akan dipaparkan pada Bab IV.

3.1.2 Mengidentifikasi Ruang Lingkup dan Tujuan Audit

Proses kedua pada tahapan perencanaan ini adalah mengidentifikasi ruang lingkup dan tujuan yang berhubungan dengan kebutuhan audit keamanan sistem informasi ini. Ruang lingkup audit keamanan sistem informasi ini tidak hanya pada sistem informasi yang ada pada perusahaan, tetapi juga berdasarkan keamanan dalam memanajemen seluruh kemungkinan kelemahan informasi yang

dapat dimungkinkan berasal dari faktor di luar sistem itu sendiri. Penentuan ruang lingkup dilakukan dengan cara melakukan observasi sekaligus menentukan klausul, obyektif kontrol dan kontrol yang sesuai dengan permasalahan dan kebutuhan PT. AJBS. Klausul, obyektif kontrol, dan kontrol yang ditentukan harus berdasarkan kesepakatan antara auditor dengan *auditee*. Proses ini akan menghasilkan pemetaan klausul, objektif kontrol serta kontrol yang telah ditentukan dan disepakati oleh auditor dengan *auditee*. Contoh klausul, objektif kontrol, dan kontrol keamanan yang tidak digunakan dapat dilihat pada Tabel 3.1 sedangkan contoh klausul, objektif kontrol, dan kontrol keamanan yang telah ditetapkan dapat dilihat pada Tabel 3.2.

Tabel 3.1 Contoh Klausul, Objektif Kontrol, dan Kontrol Keamanan ISO 27002:2005 yang Tidak Digunakan

Klausul	Kontrol Keamanan	Alasan
5 Kebijakan Keamanan	Semua	Perusahaan tidak memiliki dokumen khusus untuk kebijakan keamanan.
6 Organisasi Keamanan Informasi	Semua	Perusahaan tidak memiliki organisasi khusus untuk keamanan informasi.
Dan seterusnya		

Tabel 3.2 Contoh Klausul, Objektif Kontrol, dan Kontrol Keamanan ISO 27002 yang Telah Dipetakan

No	Klausul	Objektif Kontrol	Kontrol Keamanan
1	8 Keamanan Sumber Daya Manusia	8.1 Keamanan sumber daya manusia sebelum menjadi pegawai	8.1.1 Aturan dan tanggung jawab
2			8.1.2 Seleksi
3			8.1.3 Persyaratan dan kondisi yang harus dipenuhi oleh pegawai
Dan seterusnya			

3.1.3 Menentukan Metode dan Membuat *Engagement Letter*

Setelah melakukan survei awal untuk memperoleh gambaran umum perusahaan, mengidentifikasi ruang lingkup dan tujuan audit, langkah selanjutnya adalah menentukan metode apa yang digunakan dalam pelaksanaan audit. Setelah seluruh perencanaan telah selesai dibuat selanjutnya dituliskan di dalam dokumen *engagement letter* yang berisi kesepakatan antara auditor dengan pihak perusahaan dan mengajukan permintaan kebutuhan data.

3.1.4 Menentukan *Auditee*

Pada proses menentukan *auditee*, langkah yang dilakukan yaitu memilih *auditee* berdasarkan klausul yang telah ditetapkan. Contoh tabel penentuan *auditee* berdasarkan klausul ISO yang digunakan dapat dilihat pada Tabel 3.3.

Tabel 3.3 Contoh Penentuan *Auditee*

Klausul	Deskripsi	*Auditee*
8	Keamanan Sumber Daya Manusia	Bagian HRD
9	Keamanan Fisik dan Lingkungan	Bagian MIS/TI
10	Manajemen Operasi dan Komunikasi	Bagian MIS/TI
Dan seterusnya		

3.1.5 Menentukan Jadwal Audit (*Audit Working Plan*)

Pada proses membuat audit *working plan* langkah yang dilakukan adalah membuat daftar semua kegiatan yang akan dilakukan dalam melakukan proses audit mulai dari proses awal hingga proses pelaporan audit, kemudian memasukkan daftar kegiatan tersebut di dalam tabel. Contoh dari *audit working plan* dapat dilihat pada Tabel 3.4 di halaman 34.

Tabel 3.4 Contoh *Audit Working Plan*

No	Kegiatan	Bulan													
		April				Mei				Juni				Juli	
		1	2	3	4	1	2	3	4	1	2	3	4	1	2
1	Studi Literatur														
2	Penentuan ruang lingkup														
Dan seterusnya.															

3.1.6 Membuat Pernyataan

Proses selanjutnya pada tahapan persiapan audit ini dilakukan dengan membuat pernyataan berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah ditentukan. Kontrol keamanan dapat dilihat pada panduan implementasi ISO 27002. Pada tiap kontrol keamanan dapat ditemukan pernyataan yang mendeskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut. Salah satu contoh kontrol keamanan yaitu Pembatas Keamanan Fisik yang ada dalam Klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dan beberapa pernyataannya dapat dilihat pada Tabel 3.5.

Tabel 3.5 Contoh Pernyataan pada Kontrol Keamanan Pembatas Keamanan Fisik

Klausul 9: Keamanan Fisik dan Lingkungan	
Kategori Keamanan Utama: 9.1 Wilayah Aman	
Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik	
No	Pernyataan
1	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)
2	Terdapat perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi
Dan seterusnya	

3.1.7 Membuat Pertanyaan

Setelah dilakukan pembobotan pernyataan pada tiap proses TI, maka selanjutnya auditor membuat pertanyaan berdasarkan pernyataan tersebut. Pada tiap pernyataan tidak selalu menghasilkan satu pertanyaan bahkan mungkin menghasilkan lebih dari satu pertanyaan. Pertanyaan tersebut akan dijadikan acuan dalam melakukan wawancara kepada pihak yang telah ditentukan sebelumnya. Tabel 3.6 adalah contoh beberapa pertanyaan yang dihasilkan dari pernyataan kontrol keamanan Pembatas Keamanan Fisik yang ada dalam Klausul 9 (sembilan) Keamanan Fisik dan Lingkungan.

Tabel 3.6 Contoh Pertanyaan pada Kontrol Keamanan Pembatas Keamanan Fisik

Klausul 9: Keamanan Fisik dan Lingkungan		
Kategori Keamanan Utama: 9.1 Wilayah Aman		
Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik		
No	Pernyataan	Pertanyaan
1	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)	Apakah ada perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)?
2	Terdapat perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi	Apakah ada perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi?
Dan seterusnya		

3.2 Pelaksanaan Audit Sistem Informasi

Pelaksanaan audit keamanan sistem informasi ini menggunakan jenis audit kepatutan atau audit kesesuaian. Menurut Sarno dan Iffano (2009: 172) audit kepatutan yang dilaksanakan untuk tujuan dalam menegaskan apakah kontrol-kontrol keamanan yang ditentukan telah diimplementasi, dipelihara, memenuhi syarat pada panduan implementasi dan berjalan sesuai dengan yang diharapkan.

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Melakukan wawancara, 2. Melakukan pemeriksaan, 3. Melakukan dokumentasi (data dan bukti), 4. Melakukan uji kematangan, dan 5. Menyusun daftar temuan dan rekomendasi. Tahap ini akan menghasilkan dokumen wawancara, temuan dan bukti, nilai kematangan, dan rekomendasi.

3.2.1 Melakukan Wawancara

Pada proses ini langkah yang dilakukan adalah melakukan wawancara berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan terhadap pihak-pihak yang terlibat dalam eksekusi. Salah satu contoh dokumen wawancara dengan kontrol keamanan yaitu Pembatas Keamanan Fisik yang ada dalam Klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dapat dilihat pada Tabel 3.7.

Tabel 3.7 Contoh Dokumen Wawancara pada Kontrol Keamanan Pembatas Keamanan Fisik

Klausul 9: Keamanan Fisik dan Lingkungan			
Kategori Keamanan Utama: 9.1 Wilayah Aman			
Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik			
No	Pernyataan	Pertanyaan	Jawaban
1	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)	Apakah ada perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)?	
2	Terdapat perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi	Apakah ada perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi?	
Dan seterusnya			

3.2.2 Melakukan Pemeriksaan

Pada proses ini langkah yang dilakukan adalah melakukan pemeriksaan. Pemeriksaan dilakukan dengan cara melakukan wawancara dan observasi kepada *auditee* sesuai dengan ruang lingkup serta klausul yang telah disepakati oleh PT. AJBS. Wawancara dan observasi dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Pada saat observasi berlangsung untuk beberapa kasus dapat dilakukan pengujian baik secara *compliance test* maupun *substantive test.* Contoh format pendokumentasian hasil pemeriksaan beserta bukti dapat dilihat pada Tabel 3.8.

3.2.3 Melakukan Dokumentasi (Data dan Bukti)

Pada tahap ini langkah yang dilakukan adalah melakukan dokumentasi baik berupa data maupun bukti-bukti atas temuan atau fakta yang ada. Bukti-bukti tersebut dapat berupa foto, rekaman, data atau video. Contoh format pendokumentasian fakta dan bukti yang didapatkan dilihat pada Tabel 3.8.

Tabel 3.8 Contoh Hasil Pemeriksaan Pernyataan Pada Kontrol Keamanan Pembatas Keamanan Fisik

Klausul 9: Keamanan Fisik dan Lingkungan		
Kategori Keamanan Utama: 9.1 Wilayah Aman		
Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik		
No	Pernyataan	Hasil Pemeriksaan
1	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)	
2	Terdapat perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi	
Dan seterusnya		

3.2.4 Melakukan Uji Kematangan

Setelah melakukan pemeriksaan dan mendokumentasikan bukti-bukti audit, maka langkah berikutnya yaitu melakukan perhitungan *maturity level*. Setiap pernyataan dinilai tingkat kepatutannya sesuai dengan hasil pemeriksaan yang ada menggunakan kriteria penilaian yang ada dalam standar penilaian *maturity level*. Tingkat kriteria 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. Contoh kerangka kerja perhitungan *maturity level* dapat dilihat pada Tabel 3.9.

Tabel 3.9 Contoh Kerangka Kerja Perhitungan *Maturity Level*

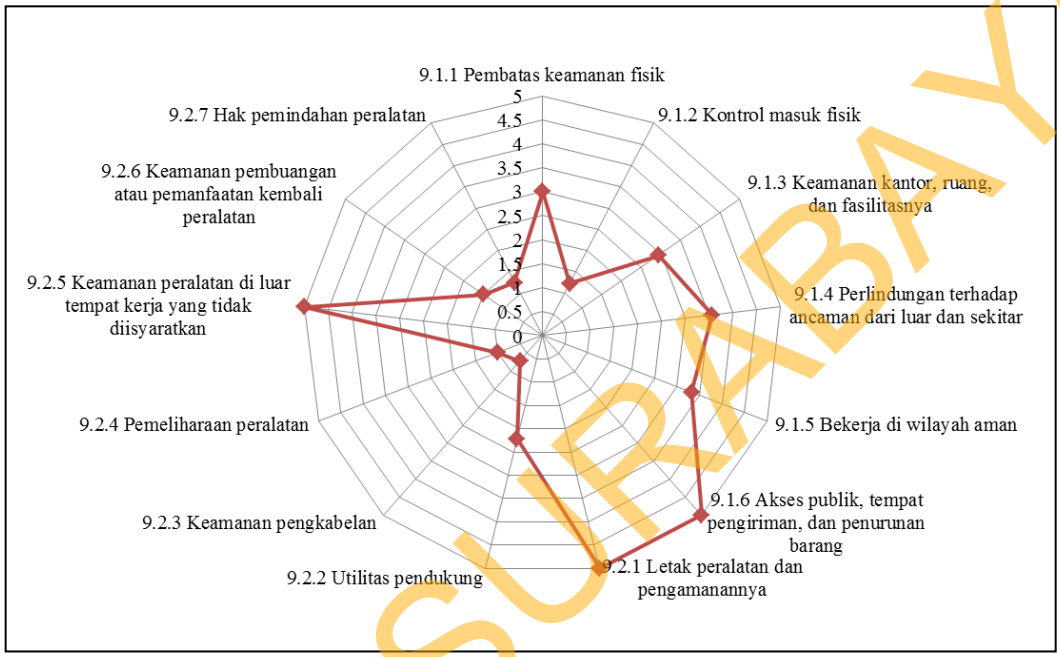
Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik										
No	Pernyataan	Hasil Pemeriksaan	Apakah?						
			0	1	2	3	4	5	Nilai
1	Terdapat perlindungan keamanan fisik.	Perlindungan keamanan fisik telah dikendalikan dengan baik. Terdapat pagar besi harmonika, dinding, sekat, penjaga pintu, resepsionis berawak, kartu tanda pengenal, dan ruangan server memiliki batasan akses masuk dan kunci tersendiri. Bukti: - Pagar besi harmonika - Dinding dan sekat - Penjaga pintu - Resepsionis berawak - Kartu tanda pengenal - Ruangan server memiliki batasan akses masuk dan kunci tersendiri.							

Setelah *maturity level* setiap kontrol keamanan ISO diketahui, maka langkah selanjutnya adalah menghitung *maturity level* setiap objektif kontrol yang diambil dari rata-rata *maturity level* setiap kontol keamanan yang ada. Dan rata-rata *maturity level* keseluruhan objektif kontrol yang ada pada klausul bersangkutan merupakan *maturity level* pada klausul tersebut. Contoh tabel penentuan *maturity level* ISO 27002 dapat dilihat pada Tabel 3.10.

Tabel 3.10 Contoh Tabel Penentuan *Maturity Level* ISO 27002

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-rata Objektif Kontrol**
9 Keamanan Fisik dan Lingkungan	9.1 Wilayah aman	9.1.1 Pembatas keamanan fisik	3.00	3.18
		9.1.2 Kontrol masuk fisik	1.22	
		9.1.3 Keamanan kantor, ruang dan fasilitasnya	2.94	
		9.1.4 Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar	3.56	
		9.1.5 Bekerja di wilayah aman	3.33	
		9.1.6 Akses publik, area pengiriman dan penurunan barang	5.00	
	9.2 Keamanan peralatan	9.2.1 Penempatan peralatan dan perlindunganya	5.00	2.38
		9.2.2 Utilitas pendukung	2.22	
		9.2.3 Keamanan pengkabelan	0.71	
		9.2.4 Pemeliharaan peralatan	1.00	
		9.2.5 Keamanan peralatan di luar tempat kerja yang tidak diisyaratkan	5.00	
		9.2.6 Keamanan pembuangan atau pemanfaatan kembali peralatan	1.50	
		9.2.7 Hak pemindahan peralatan	1.25	
***Marturity level* Klausul 9**				**2.78**

Setelah dihasilkan nilai *maturity level* yang didapat dari seluruh rata-rata nilai tingkat kemampuan kontrol keamanan, selanjutnya nilai-nilai tersebut akan direpresentasikan ke dalam diagram jaring yang ada pada Gambar 3.3.



Gambar 3.2 Contoh Representatif Nilai *Maturity Level* Klausul 9

3.2.5 Penyusunan Daftar Temuan dan Rekomendasi

Pada proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah memeriksa data profil perusahaan, kebijakan, standar, prosedur dan portopolio serta mengobservasi *standard operating procedure*, melakukan wawancara kepada *auditee* hingga melakukan pemeriksaan atau pengujian baik secara *compliance test* maupun *substantive test*. Seluruh aktivitas tersebut menghasilkan bukti *(evidence)* yang berarti terkait dengan sistem yang berlangsung diperusahaan. Masih dibutuhkannya banyak evaluasi dan perbaikan yang harus dijalankan untuk meningkatkan keamanan informasi pada perusahaan, serta menjadi acuan untuk memperoleh ISMS *certification* dengan standar ISO

27002. Ada proses yang telah dilakukan dengan baik, namun terdapat juga beberapa temuan yang masih perlu diperbaiki. Diadakan analisa sebab dan akibat untuk temuan tersebut, serta diberikan rekomendasi untuk perusahaan agar penerapan kontrol keamanan dapat diterapkan dengan lebih baik dan sesuai dengan standar ISO 27002. Contoh format dari laporan hasil audit keamanan sistem informasi dapat dilihat pada Tabel 3.11.

Tabel 3.11 Contoh Hasil Temuan dan Rekomendasi

Klausul	Obyektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
9 Keamanan Fisik dan Lingkungan	9.1 Wilayah Aman	9.1.1 Pembatas Keamanan Fisik		
		9.1.2 Kontrol Masuk Fisik		
Dan seterusnya				

3.3 Pelaporan Audit Sistem Informasi

Berdasarkan seluruh kertas kerja audit, temuan, dan tanggapan *auditee*, maka *audite* harus menyusun *draft* laporan audit keamanan sistem informasi sebagai pertanggungjawaban atas penugasan audit keamanan sistem informasi yang telah dilaksanakan. Selanjutnya laporan audit harus ditunjukan kepada pihak yang berhak saja karena laporan audit keamanan sistem informasi merupakan dokumen yang bersifat rahasia. Tahap pelaporan audit sistem informasi yang dilakukan dimulai dengan penyusunan *draft* laporan hasil audit, persetujuan *draft* laporan hasil audit, dan pelaporan hasil audit.