BAB III

METODE PENELITIAN

Pada Bab III ini akan disajikan pembahasan tahapan-tahapan audit mulai perencanaan audit, persiapan audit, pelaksanaan audit, hingga tahap pelaporan audit yang dilaksanakan pada PT. Karya Karang Asem Indonesia.

Gambar 3.1 Tahapan-Tahapan Kerja Audit

Tahapan-tahapan kerja audit sistem informasi yang akan dilakukan telah dipaparkan pada Gambar 3.1 di halaman 51. 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 ini adalah tahap awal yang dilakukan pada proses audit. Tahap ini dimulai dari permintaan ijin kepada pihak perusahaan yang akan diaudit. Selain itu, perusahaan akan mempersiapkan segala sesuatu demi kelancaran pelaksanaan audit yang akan dilakukan. Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Melakukan identifikasi proses bisnis dan IT, 2. Menentukan ruang lingkup dan tujuan audit, dan 3. Menentukan metode dan membuat proposal ke perusahaan, 4. Menentukan *auditee*, 5. Menyusun jadwal audit (*audit working plan*), 6. Membuat pernyataan, dan 7. Membuat pertanyaan. Tahap ini akan menghasilkan pengetahuan tentang proses dan TI perusahaan, ruang lingkup dan tujuan yang telah ditentukan, klausul yang digunakan, tabel *auditee* dan rencana kerja audit, 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 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 dan TI perusahaan yang diaudit dengan mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen

tersebut berupa profil perusahaan, prosedur standar operasi, kebijakan, prosedur, portofolio, 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, misi, dan prinsip manajemen, struktur organisasi, serta gambaran umum teknologi informasi yang selengkapnya akan dipaparkan pada Bab IV.

3.1.2 Menentukan Ruang Lingkup dan Tujuan Audit

Proses kedua pada tahapan perencanaan ini adalah mengidentifikasi ruang lingkup dan tujuan yang yang berhubungan dengan kebutuhan audit kontrol akses sistem informasi ini. Ruang lingkup audit kontrol akses 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 pada PT. Karya Karang Asem Indonesia sekaligus menentukan klausul, obyektif kontrol dan kontrol yang sesuai dengan permasalahan dan kebutuhan. Klausul, obyektif kontrol, dan kontrol yang ditentukan harus berdasarkan kesepakatan antara auditor dengan

perusahaan. Proses ini akan menghasilkan pemetaan klausul, objektif kontrol serta kontrol yang telah ditentukan dan disepakati oleh auditor dengan perusahaan. Contoh klausul, objektif kontrol, dan kontrol keamanan yang telah ditetapkan dapat dilihat pada Tabel 3.1.

Tabel 3.1 Contoh Klausul, Objektif Kontrol, dan Kontrol Keamanan ISO 27002 yang Telah Dipetakan

No	Klausul	Objektif Kontrol	Kontrol Keamanan
1	11 Kontrol akses	11.1 Persyaratan bisnis untuk kontrol akses	11.1.1 Kebijakan kontrol akses

3.1.3 Menentukan Metode dan Membuat Proposal ke Perusahaan

Setelah melakukan survei awal untuk memperoleh gambaran umum perusahaan, ruang lingkup dan tujuan audit, langkah yang dilakukan selanjutnya adalah menentukan klausul, obyektif kontrol dan metode apa yang digunakan dalam pelaksanaan audit yang sesuai dengan permasalahan dan kebutuhan PT. Karya Karang Asem Indonesia. Setelah seluruh perencanaan telah selesai dibuat selanjutnya menuangkan seluruh perencanaan audit yang telah dibuat dalam proposal yang langsung diberikan ke pihak perusahaan. Proses ini akan menghasilkan klausul, obyektif kontrol serta metode apa yang digunakan dalam pelaksanaan audit yang sesuai dengan permasalahan dan kebutuhan PT. Karya Karang Asem Indonesia yang telah ditentukan.

Apabila perusahaan telah menyetujui proposal yang telah dibuat langkah selanjutnya adalah membuat proposal yang berisi kesepakatan antara auditor dengan pihak perusahaan dan menandatanganinya.

3.1.4 Menentukan *Auditee*

Pada proses menentukan *auditee*, langkah yang dilakukan yaitu memilih *auditee* berdasarkan klausul yang telah ditetapkan. Menurut ISACA (2010) RACI dibagi empat sebagai berikut.

a. *Responsibility*: bagian yang bertanggung jawab atas pekerjaan yang dilakukan.
b. *Accountable*: bagian yang bertanggung jawab untuk setiap aktivitas, kualitas dan akhir dari proses.
c. *Consulted*: bagian yang memberi masukan pengetahuan dan informasi.
d. *Informed* : bagian penerimaan informasi tentang proses eksekusi dan kualitas.

Contoh tabel penentuan *auditee* berdasarkan klausul ISO yang digunakan dapat dilihat pada Tabel 3.2.

Tabel 3.2 Contoh Penentuan *Auditee*

Klausul	Deskripsi	*Auditee*	Keterangan
11	Kontrol Akses	Bagian pengembang aplikasi	*Responsible*

3.1.5 Menentukan Jadwal Audit

Pada proses membuat rencana kerja audit 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 rencana kerja audit dapat dilihat pada Tabel 3.3.

Tabel 3.3 Contoh Rencana Kerja Audit

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														

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 Kebijakan kontrol akses yang ada dalam Klausul 11 (sebelas) Kontrol akses dan beberapa pernyataannya dapat dilihat pada Tabel 3.4

Tabel 3.4 Contoh Pernyataan pada Kontrol Keamanan Kebijakan Kontrol Akses

Klausul 11 Kontrol Akses	
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol	
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses	
No	Pernyataan
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.
2	Terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.

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 3.5 adalah contoh beberapa pertanyaan yang dihasilkan dari pernyataan kontrol keamanan yaitu Kebijakan kontrol akses yang ada dalam Klausul 11 (sebelas) Kontrol akses.

Tabel 3.5 Contoh Pertanyaan pada Kontrol Keamanan Kebijakan Kontrol Akses

Klausul 11 Kontrol Akses		
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol		
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses		
No	Pernyataan	Pertanyaan
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.	Apakah terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan?
2	Terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.	Apakah terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses?

3.2 Pelaksanaan Audit Sistem Informasi

Pelaksanaan audit kontrol akses 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 Kebijakan kontrol akses yang ada dalam Klausul 11 (sebelas) Kontrol akses dapat dilihat pada Tabel 3.6.

Tabel 3.6 Contoh Dokumen Wawancara pada Kontrol Kebijakan Kontrol Akses

Klausul 11 Kontrol Akses			
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol			
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses			
No	Pernyataan	Pertanyaan	Jawaban
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.	Apakah terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan?	
2	Terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.	Apakah terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses?	

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. KKAI. 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 3.7.

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 3.7.

Tabel 3.7 Contoh Hasil Pemeriksaan Pernyataan Pada Kontrol Kebijakan Kontrol Akses

Klausul 11 Kontrol Akses		
Kategori Keamanan Utama: 11.1 Persyaratan bisnis untuk akses kontrol		
Kontrol Keamanan: 11.1.1 Kebijakan Kontrol Akses		
No	Pernyataan	Hasil Pemeriksaan
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.	
2	Terdapat peraturan dan hak kontrol akses untuk setiap pengguna yang telah dinyatakan dengan jelas dalam suatu pernyataan kebijakan tentang akses.	

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 3.8.

Tabel 3.8 Contoh Kerangka Kerja Perhitungan *Maturity Level*

Kontrol Keamanan: 11.1.1 Pembatas keamanan fisik									
No	Pernyataan	Hasil Pemeriksaan	Apakah?						
			0	1	2	3	4	5	Nilai
1	Terdapat persyaratan bisnis kontrol akses yang telah ditetapkan dan didokumentasikan.	Persyaratan bisnis kontrol akses terdokumentasi dengan baik. Terdapat persyaratan bisnis kontrol akses didalam peraturan perusahaan dan telah terdefinisi.							

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

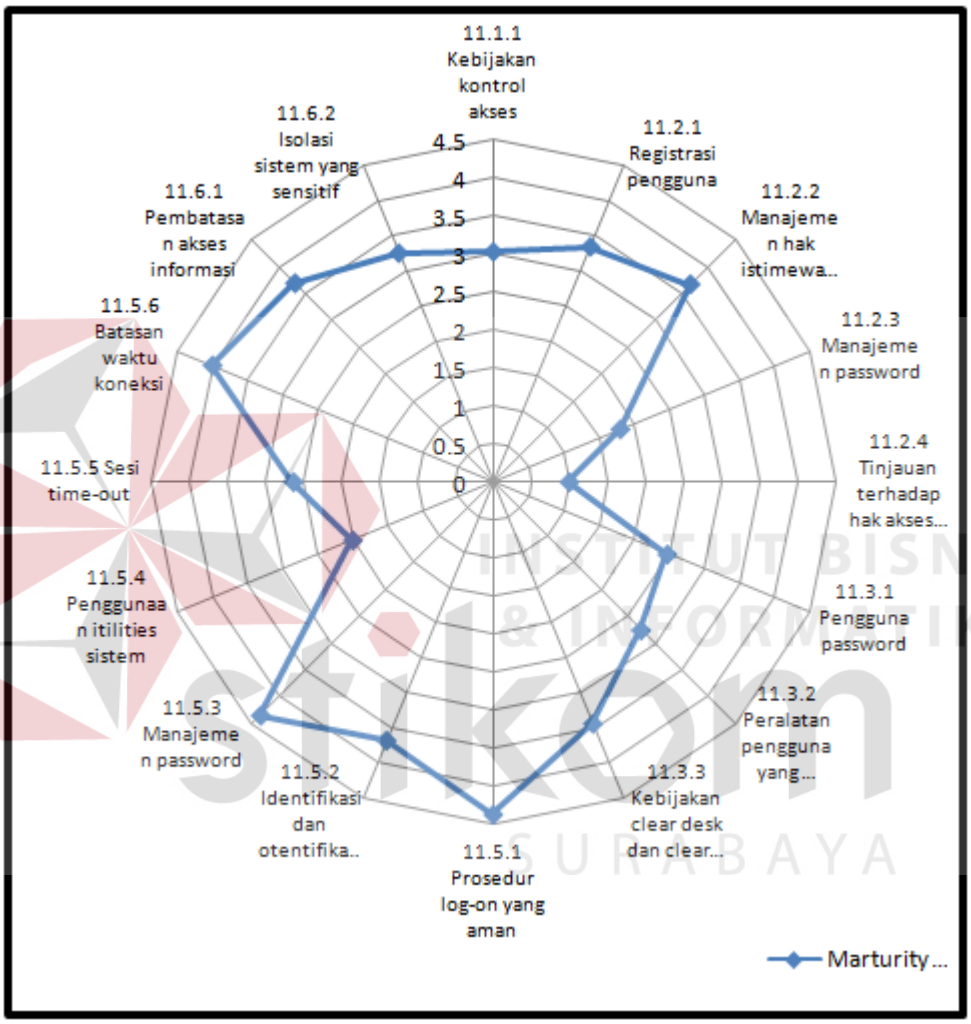
bersangkutan merupakan *maturity level* pada klausul tersebut. Contoh tabel penentuan *maturity level* ISO 27002 dapat dilihat pada Tabel 3.9.

Tabel 3.9 Contoh Tabel Penentuan *Maturity Level* ISO 27002

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-rata Objektif Kontrol**
11 Kontrol akses	11.1 Persyaratan bisnis untuk kontrol akses	11.1.1Kebijakan kontrol akses		
	11.2 Manajemen akses *user*	11.2.1 Registrasi pengguna		
		11.2.2 Manajemen hak istimewa atau khusus		
		11.2.3 Manajemen *password*		
		11.2.4 Tinjauan terhadap hak akses *user*		
	11.3 Tanggung jawab pengguna	11.3.1 Pengguna *password*		
		11.3.2 Peralatan pengguna yang tidak dijaga		
		11.3.3 Kebijakan *clear desk* dan *clear screen*		
	11.5 Kontrol akses sistem operasi	11.5.1 Prosedur log-on yang aman		
		11.5.2 Identifikasi dan otentifikasi *user*		
		11.5.3 Manajemen *password*		
		11.5.4 Penggunaan utilities sistem		
		11.5.5 Sesi time-out		
		11.5.6 Batasan waktu koneksi		
	11.6 Kontrol akses informasi dan aplikasi	11.6.1 Pembatasan akses informasi		
		11.6.2 Isolasi sistem yang sensitif		

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 3.2

.



Gambar 3.2 Contoh Representatif Nilai *Maturity Level* Klausul 11

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 prosedur standart operasi, melakukan wawancara

kepada pihak perusahaan 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 kontrol akses sistem informasi dapat dilihat pada Tabel 3.10.

Tabel 3.10 Contoh Hasil Temuan dan Rekomendasi

Klausul	Obyektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
11 Kontrol akses	11.1 Persyaratan bisnis untuk kontrol akses.	11.1.1 Kebijakan kontrol akses.		

3.3 Pelaporan Audit Sistem Informasi

Berdasarkan seluruh kertas kerja audit, temuan, dan tanggapan pihak perusahaan, maka *auditor* harus menyusun *draft* laporan audit kontrol akses sistem informasi sebagai pertanggung jawaban atas penugasan audit kontrol akses sistem informasi yang telah dilaksanakan. Selanjutnya laporan audit harus ditunjukan kepada pihak yang berhak saja karena laporan audit kontrol akses

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.