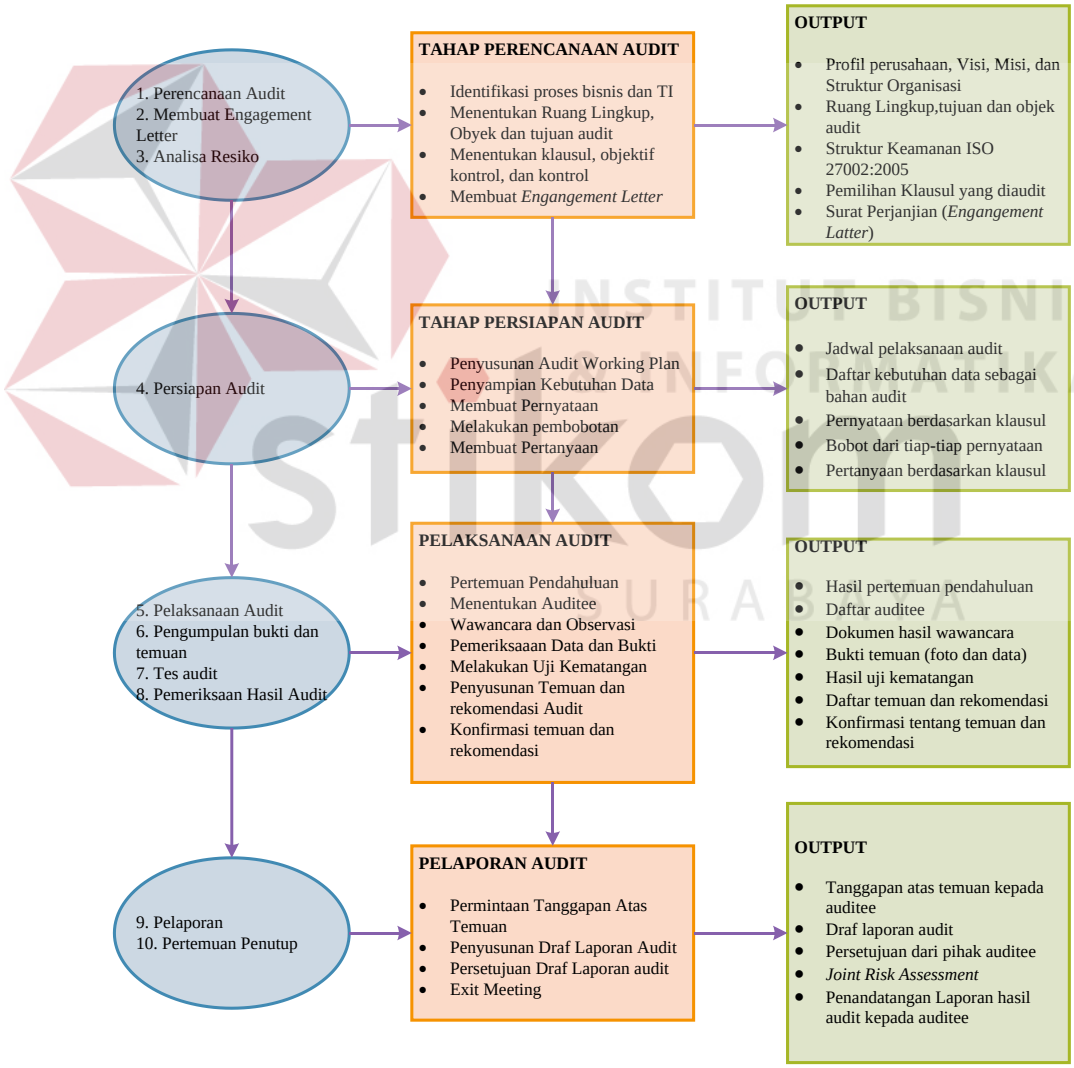
BAB III

METODE PENELITIAN

Pada bab ini membahas tentang tahapan-tahapan yang digunakan dalam melakukan audit keamanan sistem informasi parahita berdasarkan ISO 27002:2005 pada Parahita *Diagnostic Center*. Agar lebih jelasnya tahapan-tahapan yang digunakan dalam audit ini dapat dilihat pada Gambar 3.1.



Gambar 3. 1 Tahapan Audit yang Digunakan

3.1. Tahap Perencanaan Audit

Pada tahap perencanaan ini terdapat beberapa langkah-langkah yang dilakukan yaitu : 1. Identifikasi proses bisnis dan TI, 2. Menentukan ruang lingkup, tujuan dan resiko, 3. Menentukan klausul, obyektif kontrol dan kontrol, dan 4. Membuat *Engagement Letter*. Tahapan ini akan menghasilkan pengetahuan tentang proses bisnis dan TI perusahaan, ruang lingkup, tujuan dan resiko yang telah ditentukan serta klausul yang telah ditentukan sebelumnya dari permasalahan dan kesepakatan kedua belah pihak. Selain itu tahapan ini juga menghasilkan *Engagement Letter* yang merupakan surat perjanjian antara kedua belah pihak.

3.1.1 Identifikasi Proses Bisnis dan TI

Tahapan perencanaan audit ini yang dilakukan dengan cara observasi dan wawancara. Observasi dilakukan dengan mempelajari proses bisnis dan TI pada perusahaan yang akan diaudit (*auditee*) dengan cara mempelajari dokumen-dokumen perusahaan yang dibutuhkan. Dokumen tersebut adalah berupa profil perusahaan, visi dan misi perusahaan, struktur organisasi perusahaan, proses bisnis perusahaan, alur sistem informasi parahita serta *job description* karyawan Parahita *Diagnostic Center*. Langkah selanjutnya dilakukannya wawancara untuk memastikan apakah pernah dilakukan audit sebelumnya dikarenakan auditor perlu mengetahui dan memeriksa laporan audit sebelumnya.

Pada tahapan ini menghasilkan *output* berupa profil perusahaan, visi dan misi perusahaan, struktur organisasi perusahaan, proses bisnis perusahaan, alur sistem informasi parahita serta *job description* karyawan Parahita *Diagnostic Center*. Contoh proses identifikasi proses bisnis dengan melakukan wawancara dapat dilihat pada Tabel 3.1.

Tabel 3. 1 Contoh Proses Identifikasi Proses Bisnis

Wawancara Permasalahan Pada Bagian Teknologi dan Sistem Informasi Parahita Diagnostic Center	Auditor : Nama Auditor
	Auditee : Nama Auditee
	Tanggal : Tanggal Dilaksanakan
Pertanyaan	**Jawaban**
1. Bagaimana alur proses bisnis yang ada pada Parahita Diagnostic Center ?	
dst.	dst.

3.1.2. Menentuan Ruang Lingkup, Obyek dan Tujuan Audit

Tahapan perencanaan selanjutnya adalah menentukan ruang lingkup, obyek dan tujuan audit yang akan dilakukan pada audit kali ini. Penentuan ruang lingkup ini dilakukan dengan cara observasi dan wawancara pada bagian TI Parahita Diagnostic Center. Proses selanjutnya adalah menentukan tujuan yang berkaitan dengan kebutuhan audit keamanan sistem informasi. *Output* yang dihasilkan pada tahapan ini adalah ruang lingkup, obyek dan tujuan audit.

Tabel 3. 2 Contoh Hasil dari proses penentuan ruang lingkup

Hasil Penentuan Ruang Lingkup, Obyektif dan tujuan audit	Auditor : Nama Auditor	
	Auditee : Nama Auditee	
	Tanggal : Tanggal Dilaksanakan	
Ruang Lingkup	**Obyek**	**Tujuan Audit**

3.1.3. Menentukan Klausul, Obyektif Kontrol dan Kontrol

Tahapan selanjutnya pada tahapan perencanaan adalah menentukan klausul, obyektif kontrol dan kontrol. Tahap ini ditentukan setelah tahap sebelumnya dilakukan. Pemilihan klausul, obyektif kontrol dan kontrol ini disesuaikan dengan

kesepakatan bersama kedua belah pihak dimana pemilihan klausul ini disesuaikan dengan standar keamanan ISO 27002:2005. Dalam menentukan klausul harus ada bukti tertulis dari pihak yang bersangkutan. *Output* yang dihasilkan pada tahap ini adalah pemilihan klausul yang akan dilakukan audit, obyektif kontrol dan kontrol sesuai ISO 27002:2005. Contoh proses menentuan klausul dapat dilihat pada Tabel 3.3.

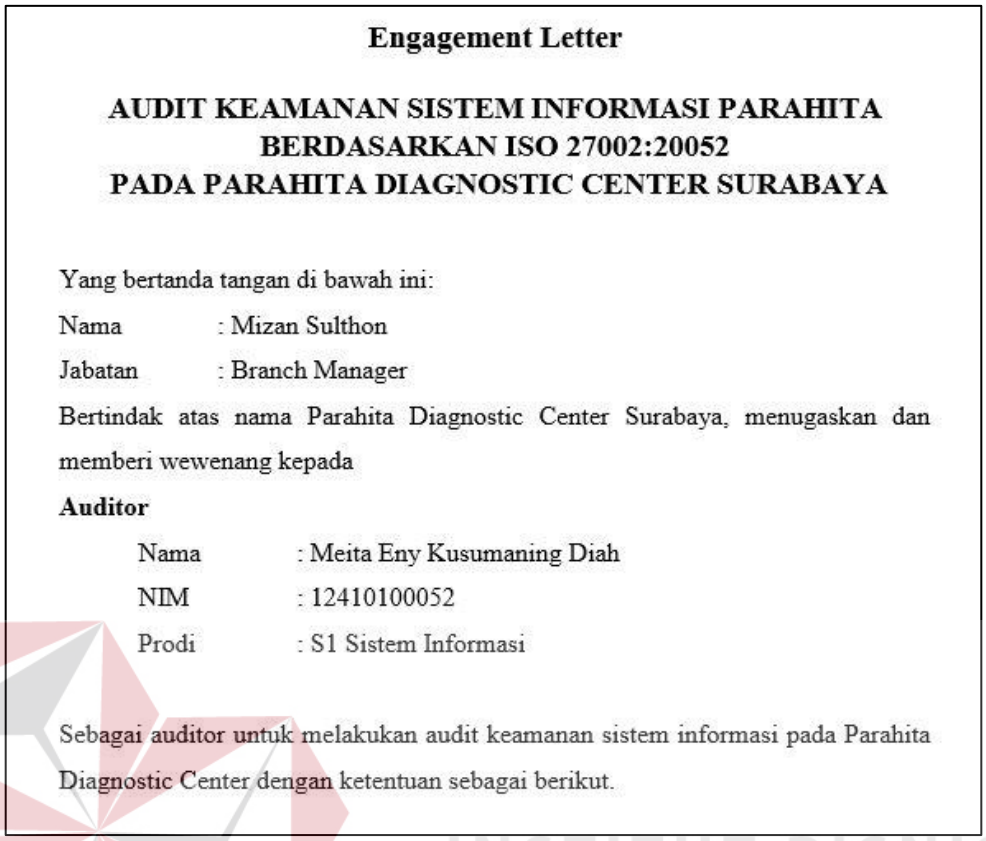
Tabel 3. 3 Contoh Proses Menentukan Klausul, Obyektif Kontrol dan Kontrol

Klausul yang digunakan atas kesepakatan kedua belah pihak	Auditor : Nama Auditor
	Auditee : Nama Auditee
	Tanggal : Tanggal Dilaksanakan

NO	**Klausul yang digunakan**
1	Klausul 10 Manajemen Komunikasi dan Operasi
2	Klausul 12 Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan

3.1.4. Membuat *Engagement Letter*

Tahapan ini digunakan untuk membuat surat perjanjian atau *engagement letter*. *Engagement letter* adalah surat persetujuan antara *auditee* dan auditor tentang syarat-syarat pekerjaan audit yang akan dilakukan oleh auditor. Isi dari *Engagement letter* yakni tanggung jawab manajemen dan auditor, lingkup audit dan ketentuan perjanjian audit. *Output* yang dihasilkan dalam tahapan ini adalah berupa dokumen surat perjanjian atau *Engagement letter* yang disepakti oleh kedua belah pihak. Dapat dilihat pada Gambar 3.2 contoh surat perjanjian atau *engagement letter*.



Engagement Letter

AUDIT KEAMANAN SISTEM INFORMASI PARAHITA BERDASARKAN ISO 27002:20052 PADA PARAHITA DIAGNOSTIC CENTER SURABAYA

Yang bertanda tangan di bawah ini:

Nama : Mizan Sulthon

Jabatan : Branch Manager

Bertindak atas nama Parahita Diagnostic Center Surabaya, menugaskan dan memberi wewenang kepada

Auditor

Nama : Meita Eny Kusumaning Diah

NIM : 12410100052

Prodi : S1 Sistem Informasi

Sebagai auditor untuk melakukan audit keamanan sistem informasi pada Parahita Diagnostic Center dengan ketentuan sebagai berikut.

Gambar 3. 2 Contoh Surat Perjanjian atau Engagement Letter

3.2. Tahap Persiapan Audit

Pada tahapan persiapan ini ada beberapa langkah yang dilakukan yakni menyusun audit *working plan*, penyampaian kebutuhan data, membuat pernyataan, melakukan pembobotan dan membuat pertanyaan. Tahap persiapan akan menghasilkan tabel audit *working plan*, surat penyampaian kebutuhan data, pernyataan yang sesuai dengan standar ISO 27002:2005, hasil pembobotan dan daftar pertanyaan yang telah dibuat berdasarkan pernyataan.

3.2.1. Penyusunan Audit Working Plan (AWP)

Penyusunan *Audit Working Plan* atau AWP merupakan salah satu tahap yang terdapat pada persiapan audit. Pada tahapan ini menggunakan *tools* yaitu Microsoft Excel atau Microsoft Project yang digunakan dalam membantu

pembuatan AWP. AWP merupakan dokumen yang dibuat oleh Auditor yang digunakan dalam merencanakan dan memantau pelaksanaan audit. *Output* yang dihasilkan pada tahapan ini adalah daftar susunan *Audit Working Plan*. Contoh AWP dapat dilihat pada Tabel 3.4.

Tabel 3. 4 Contoh Audit Working Plan

No	Kegiatan	Maret				April				Mei			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Pembuatan dan Pengajuan Proposal TA												
2	Perencanaan Audit												
	a. Membuat Engagement Letter												
	b. Identifikasi Proses Bisnis												
	c. Penetuan Tujuan, Ruang Lingkup, dan Risiko												
	d. Membuat Klausul, Objektif Kontrol dan Kontrol												
3	Persiapan Audit												
	a. Penyusunan Audit Working Plan												
	b. Penyampaian Kebutuhan Dana												
	c. Membuat Pernyataan												
	d. Melakukan Pembobotan												
	e. Membuat Petanyaan												
4	Pelaksanaan Audit												

3.2.2. Penyampaian Kebutuhan Data

Tahapan penyampaian kebutuhan data ini sangat diperlukan auditor untuk menyampaikan data apa saja yang dibutuhkan dalam melaksanakan audit. Kebutuhan data ini disampaikan kepada *auditee* terlebih dahulu. Setelah itu *Field work* dilaksanakan auditor setelah *auditee* menyetujui ketersediaan semua data yang diperlukan auditor, sehingga *field work* dapat dilaksanakan oleh auditor secara efektif dan efisien. *Output* yang dihasilkan dari tahapan ini adalah daftar penyampaian kebutuhan data perusahaan. Contoh daftar penyampaian kebutuhan data perusahaan dapat dilihat pada Tabel 3.5.

Tabel 3. 5 Contoh Daftar penyampaian kebutuhan data perusahaan

Lampiran Permintaan Kebutuhan Data/Dokumen						
No.	Data Yang Diperlukan	Ketersediaan Data		Keterangan	Tanda Tangan	
		Ada	Tidak Ada		*Auditee*	Auditor
1	Profil Perusahaan					
2	Struktur organisasi PDC					
3	*Job description* Karyawan					

3.2.3. Membuat Pernyataan

Tahapan selanjutnya adalah membuat pernyataan berdasarkan standar ISO 27002:2005. Pada setiap kontrol keamanan dapat ditentukan pernyataan yang menjelaskan implementasi dan pengontrolan yang dilakukan. *Output* yang dihasilkan adalah melakukan pembuatan pernyataan seperti pada Tabel 3.6.

Tabel 3. 6 Contoh Pernyataan

Klausul 10 Manajemen Komunikasi Operasi	
10.1 Tanggung Jawab dan Prosedur Operasional	
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**	
10.1.1 Pendokumentasian Prosedur Operasi	
No	**Pernyataan**
1	Terdapat dokumentasi terhadap prosedur operasi
2	Terdapat pemeliharaan terhadap prosedur operasi

3.2.4. Melakukan Pembobotan

Tahapan selanjutnya setelah membuat pernyataan adalah melakukan pembobotan untuk masing-masing pernyataan. Bobot dari masing-masing pernyataan berbeda karena disesuaikan dalam penerapannya untuk kontrol keamanan yang ditentukan. Metode ini menggunakan bobot pada penilaian risiko metode kualitatif, karena menurut Sarno dan Iffano, (2009) risiko memiliki hubungan dengan keamanan informasi dan risiko merupakan dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi. pembobotan penilaian risiko dapat dilihat pada Tabel 3.7

Tabel 3. 7 Pembobotan Penilaian Risiko

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

(Sumber: Sarno dan Iffano, 2009)

Pembobotan ini ditentukan dari panduan implementasi dan tingkat seberapa penting dari tiap perusahaan. Pernyataan yang mendapatkan pembobotan dengan risiko *high* berarti pernyataan tersebut sangat penting untuk diterapkan pada perusahaan. Untuk pernyataan dengan bobot risiko *medium* berarti pernyataan tersebut tetap diterapkan meskipun risiko yang akan terjadi apabila ada ancaman keamanan tidak sebesar dengan bobot resiko high. Pernyataan dengan risiko *low* berarti pernyataan tersebut tidak terlalu wajib untuk diterapkan namun apabila diterapkan akan menambah keamanan pada sistem. *Output* yang dihasilkan pada tahapan ini adalah bobot dari masing-masing pernyataan. Contoh pembobotan dari setiap pernyataan dapat dilihat pada Tabel 3.8.

Tabel 3. 8 Contoh Pembobotan dari setiap pernyataan

Klausul 10 Manajemen Komunikasi Operasi		
10.1 Tanggung Jawab dan Prosedur Operasional		
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**		
10.1.1 Pendokumentasian Prosedur Operasi		
No	**Pernyataan**	**Pembobotan**
1	Terdapat dokumentasi terhadap prosedur operasi	1
2	Terdapat pemeliharaan terhadap prosedur operasi	0.8
dst.		

3.3.5. Membuat Pertanyaan

Tahapan membuat pertanyaan ini dilakukan setelah menentukan pernyataan yang telah dibuat sebelumnya. Satu pernyataan bisa memiliki lebih dari satu pertanyaan karena setiap pertanyaan mewakili pernyataan pada saat dilakukannya wawancara, observasi, survei dan identifikasi dokumen. Output yang dihasilkan pada tahapan ini adalah daftar pertanyaan dari pernyataan yang ada pada Tabel 3.9.

Tabel 3. 9 Contoh pertanyaan yang dihasilkan dari pernyataan

Klausul 10 Manajemen Komunikasi Operasi		
10.1 Tanggung Jawab dan Prosedur Operasional		
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**		
10.1.1 Pendokumentasian Prosedur Operasi		
No	**Pernyataan**	**Pertanyaan**
1	Terdapat dokumentasi terhadap prosedur operasi	1. Apakah terdapat dokumentasi semua prosedur operasi yang ada saat ini ?
		2. Dokumentasi disimpan dalam format apa ?

Tabel 3. 9 (Lanjutan)

Klausul 10 Manajemen Komunikasi Operasi		
10.1 Tanggung Jawab dan Prosedur Operasional		
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**		
10.1.1 Pendokumentasian Prosedur Operasi		
No	**Pernyataan**	**Pertanyaan**
		3. Sejak kapan dokumentasi prosedur operasi tersebut dilakukan ?
		4. Siapa yang membuat dokumentasi prosedur tersebut ?

3.3. Tahap Pelaksanaan Audit

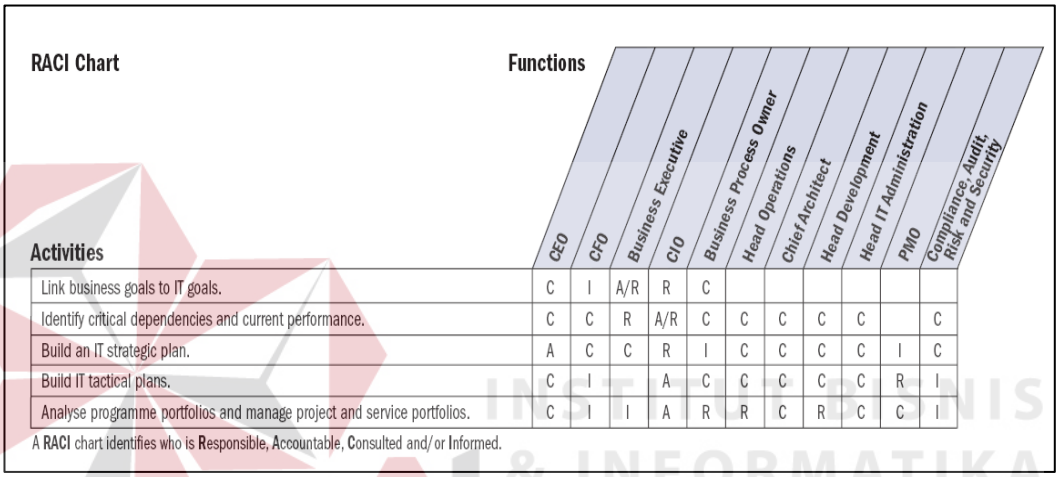
Pada tahapan pelaksanaan audit ada beberapa langkah-langkah yaitu melakukan pertemuan pendahuluan audit, pemeriksaan data dan bukti, melakukan wawancara, melakukan uji kematangan, menyusun temuan dan rekomendasi audit, dan konfirmasi temuan audit. Tahapan ini akan menghasilkan hasil pertemuan pendahuluan audit, hasil temuan atau bukti, hasil uji kematangan, penyusunan daftar temuan dan rekomendasi, dan konfirmasi temuan audit.

3.3.1. Pertemuan Pendahuluan Audit

Pada tahapan ini dilakukan pertemuan pendahuluan audit yang digunakan untuk mendapatkan kesepakatan bersama dan mendapatkan pemahaman yang sama sebelum dilakukannya proses pelaksanaan aduit dimulai. Pertemuan ini dilakukan oleh auditor dan *auditee.*

3.3.2. Menentukan *Auditee*

Pada tahapan menentukan *auditee*, langkah yang digunakan yaitu memilih *auditee* yang sesuai dengan klausul yang digunakan. Pemilihan *auditee* ini dilakukan berdasarkan RACI. RACI sendiri merupakan singkatan dari *Responsible, Accountable, Consulted,* dan *Informed.* Contoh RACI dapat dilihat pada Gambar 3.3.



RACI Chart

Functions

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Link business goals to IT goals.	C	I	A/R	R	C						
Identify critical dependencies and current performance.	C	C	R	A/R	C	C	C	C	C		C
Build an IT strategic plan.	A	C	C	R	I	C	C	C	C	I	C
Build IT tactical plans.	C	I		A	C	C	C	C	C	R	I
Analyse programme portfolios and manage project and service portfolios.	C	I	I	A	R	R	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Gambar 3. 3 RACI Chart
(Sumber: IT Governance Institute, 2007)

Output yang dihasilkan pada tahapan ini yaitu hasil *auditee* yang akan diwawancari pada tahapan wawancara sebagai sumber informasi yang dibutuhkan pada audit keamanan sistem informasi. Contoh menentukan auditee dapat dilihat pada Tabel 3.10.

Tabel 3. 10 Contoh Penentuan Auditee

Klausul		Kepala Cabang	Staff Bagian TI
Klausul 10	Manajemen Komunikasi dan Operasi		
dst.			

3.3.3. Melakukan Wawancara

Tahapan wawancara ini dilaksanakan setelah membuat pertanyaan yang sudah dibuat oleh auditor. Wawancara dilakukan kepada *auditee* yang terlibat dalam proses audit. *Output* pada tahap ini adalah dokumen wawancara yang berisikan hasil wawancara yang telah dilakukan selama proses audit berlangsung. Berikut contoh wawancara yang dilakukan dapat dilihat pada Tabel 3.11.

Tabel 3. 11 Contoh wawancara

Klausul 10 Manajemen Komunikasi Operasi			
10.1 Tanggung Jawab dan Prosedur Operasional			
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**			
10.1.1 Pendokumentasian Prosedur Operasi			
No	**Pernyataan**	**Pertanyaan**	**Jawaban**

3.3.4 . Pemeriksaan Data dan Bukti

Pemeriksaan data dan bukti ini dilakukan dengan observasi dan wawancara kepada *auditee* sesuai dengan rang lingkup dan klausul yang telah disepakati oleh pihak perusahaan yaitu klausul 10, klausul 12, klausul 13, klausul 14, dan klausul 15. Hasil yang diperoleh pada tahap ini adalah penemuan bukti dan temuan tentang permasalahan yang ada. Bukti atau temuan berupa foto ataupun data. Contoh dokumen pemeriksaan data dan bukti tersebut ada pada Tabel 3.12.

3.3.5. Melakukan Uji Kematangan

Langkah selanjutnya dilakukan uji kematangan, dalam proses ini langkah yang dilakukan adalah memberi nilai tingkat kepatutan pada setiap pernyataan yang sesuai dengan hasil pemeriksaan yang menggunakan kriteria penilaian yang ada dalam standar peniaian *maturity level*. Penilaian yang digunakan meliputi non-

eksisten yang memiliki nilai 0 (nol) hingga ke tingkat optimal yang memiliki nilai 5 (lima). Jumlah kriteria nilai yang ada dibagi dengan jumlah seluruh pernyataan dalam satu kontrol keamanan untuk mendapatkan nilai maturity level pada kontrol keamanan tersebut.

Selanjutnya setelah *maturity level* setiap kontrol keamanan ISO diketahui, maka akan dilanjutkan dengan menghitung *maturity level* pada setiap obyektif kontrol yang telah diambil rata-rata *maturity level* setiap kontrol keamanan yang ada. Setiap rata-rata *maturity level* keseluruhan objektif kontrol yang ada pada klausul bersangkutan merupakan *maturity level* pada klausul tersebut. Hasil dari proses ini adalah hasil uji *maturity level*. Berikut contoh perhitungan tingkat kematangan pada klausul 10 dapat dilihat pada Tabel 3.12

Tabel 3. 12 Contoh perhitungan maturity level

Klausul 10 Manjemen dan Komunikasi Operasional										
Klausul 10.1 Tanggung jawab dan prosedur operasional										
Kontrol: 10.1.1 Pendokumentasian prosedur operasi				Penilaian						Nilai
No	Pernyataan	Hasil Pemeriksaan	Bobot	0	1	2	3	4	5	

3.3.6. Penyusunan Temuan dan Rekomendasi Audit

Pada tahapan penyusunan temuan dan rekomendasi, langkah yang dilakukan adalah memeriksa data profil perusahaan, standar yang digunakan, prosedur yang ada, kebijakan perusahaan dan melakukan wawancara, *review* dan observasi kepada *auditee*. Seluruh langkah diatas menghasilkan bukti (*evidence*) yang terkait dengan sistem yang digunakan oleh perusahaan. *Output* yang dihasilkan adalah daftar temuan dan rekomendasi, seperti pada Tabel 3.13.

Tabel 3. 13 Contoh dokumen temuan dan rekomendasi

Klausul 10 Manajemen Komunikasi Operasi					
10.1 Tanggung Jawab dan Prosedur Operasional					
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**					
10.1.1 Pendokumentasian Prosedur Operasi					
No	**Pernyataan**	**Temuan**	**Bukti**	**Rekomendasi**	**Tanggapan**

3.3.7. Konfirmasi Temuan dan Rekomendasi

Sebelum dilaporan secara formal kepada *auditee* temuan harus dikonfirmasikan terlebih dahulu. *Output* yang dihasilkan dari konfirmasi temuan ini adalah dokumentasi dalam bentuk notulen konfirmasi temuan.

3.4. Tahap Pelaporan

Pada tahap pelaporan ini terdapat beberapa langkah yang dilakukan yaitu melakukan permintaan tanggapan atas dafatar temuan audit, penyusunan dan persetujuan draft pelaporan audit, serta pertemuan penutup atau pelaporan hasil audit. Output yang dihasilkan pada tahapan ini adalah hasil permintaan tanggapan atas daftar temuan audit, haisl penyusunan *draft* laporan untuk perusahaan, hasil persetujuan draft laporan audit, hasil pertemuan penutup berupa *exit meeting*.

3.4.1. Permintaan Tanggapan Atas Temuan

Auditee harus memberikan tanggapannya dan komitmen penyelesaiannya oleh karena itu diperlukannya tahapan permintaan tanggapan atas temuan yang disampaikan oleh auditor. Tanggapan ini diperlukan untuk penyusunan laporan sehingga dapat menjadi acuhan pemantauan tindak lanjut penyelesaian temuan audit. *Output* yang dihasilkan adalah hasil tanggapan atas daftar temuan kepada *auditee*.

3.4.2. Penyusunan Draf Laporan Audit

Pada tahapan penyusunan draf laporan audit ini terdiri atas daftar pertanyaan, temuan dan tanggapan oleh karena itu auditor harus menyusun draf laporan yang telah selesai dilaksanakan. Laporan ini disusun dengan efektif, obyektif, lengkap, jelas dan lugas. *Output* yang dihasilkan adalah draf laporan audit yang berdasarkan daftar pertanyaan, temuan dan tanggapan oleh karena itu auditor harus menyusun draf laporan audit yang telah selsai dilaksanakan oleh auditor.

3.4.3. Persetujuan Draf Laporan Audit

Draf laporan yang telah disusun perlu untuk dimintakan persetujuan terlebih dahulu kepada *auditee* sebelum diterbitkan sebagai laporan audit yang resmi atau formal. Persetujuan ini dilakukan oleh kedua belah pihak berupa notulen persetujuan draf laporan audit.

3.4.4 Pertemuan Penutup atau *Exit Meeting*

Pertemuan penutup dilakukan untuk melaporkan hasil audit yang telah dilakukan auditor kepada manajemen, memberikan penjelasan kepada manajemen tentang kondisi yang ada khususnya kelemahan untuk obyek audit, memberikan rekomendasi yang perlu ditindak lanjuti. *Output* yang dihasilkan adalah dokumentasi dalam bentuk notulen pertumuan penutup audit.