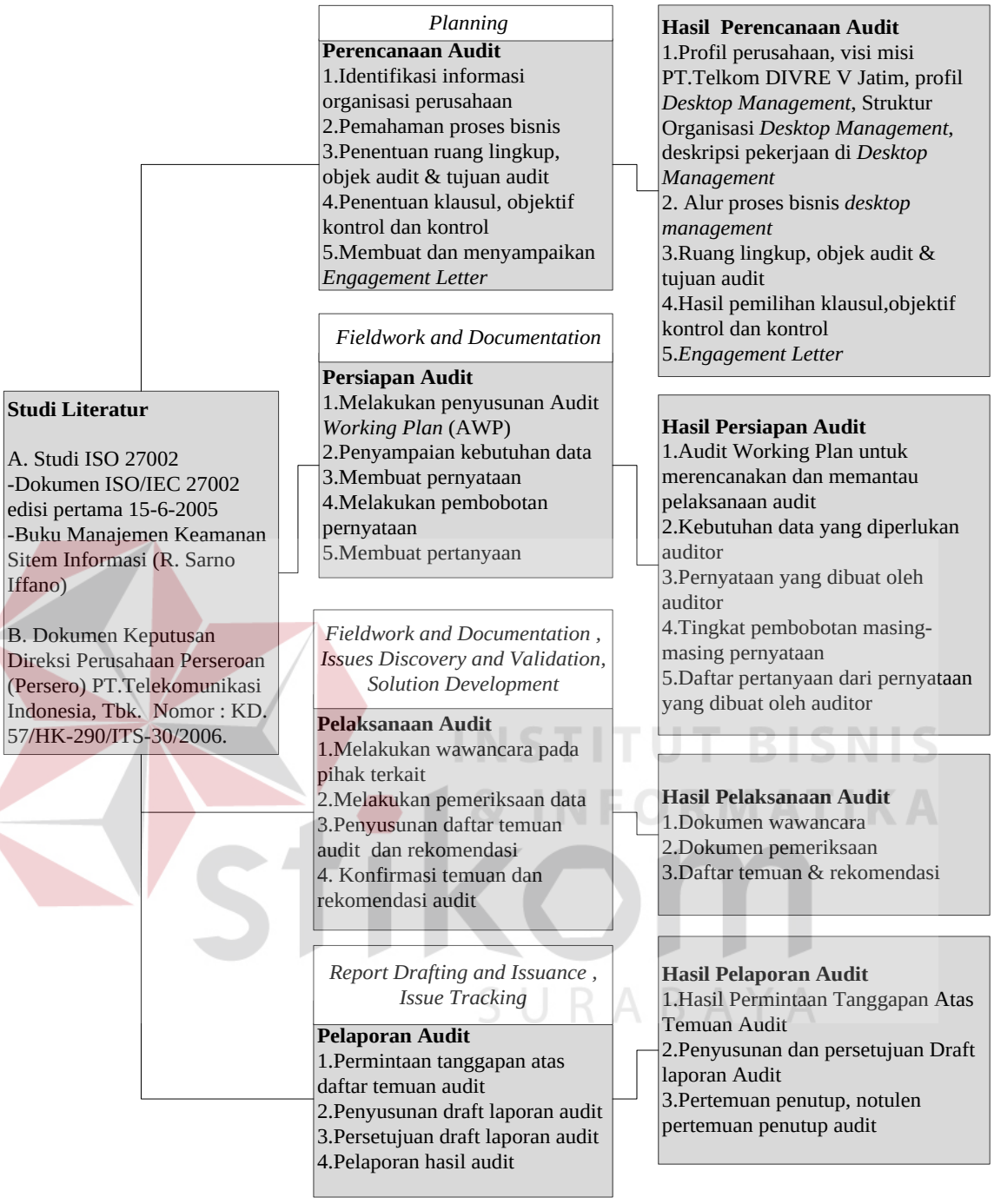
BAB III

METODE PENELITIAN

Pada Bab III akan dilakukan pembahasan dimulai dengan profil perusahaan, gambaran struktur organisasi, dan dilanjutkan dengan tahapan-tahapan audit yang akan dilaksanakan. Dapat dilihat pada Gambar 3.1.

Studi literartur yang digunakan dalam metode penelitian ini adalah ISO 27002:2005 dan regulasi dari perusahaan yaitu dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006. Pada standar ISO 27002 dan dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 terdapat beberapa kesamaan dalam panduan implementasi audit yang dapat dilihat pada Tabel 3.1.

Setelah standar audit sudah ditetapkan pada proses studi literatur maka terdapat suatu gambaran tahapan dalam audit keamanan sistem informasi. Berdasarkan referensi dari Davis dengan memperhatikan juga referensi dari (Windriya, 2013:35) maka gambaran tahapan dalam audit keamanan sistem informasi dapat dikembangkan dan disederhanakan menjadi beberapa tahap audit seperti pada Tabel 3.2.



Gambar 3.1 Tahapan-Tahapan dalam Audit Keamanan Sistem Informasi

Tabel 3.1 Pemetaan Standar ISO 27002:2005 dan Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006

No	Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor : KD.57/HK-290/ITS-30/2006	ISO 27002:2005
1.	**Bab V** **Sekuriti Sumber Daya Manusia** **Pasal 13** **Sebelum Penugasan** Dalam pasal 13 ini mengatur tentang pengelolaan SDM serta proses *screening* pada calon karyawan serta pekerja kontrak dan mitra kerja yang harus menandatangani *Term and Conditions.*	**Klausul 8 Keamanan Sumber Daya Manusia** **Kategori Keamanan Utama: 8.1 (Berelasi dengan Pasal 13 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)** Sebelum menjadi pegawai Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga memahami akan tanggung jawabnya dan bisa menjalankan aturan yang mereka dapatkan untuk meminimalkan resiko pencurian atau kesalahan dalam penggunaan fasilitas informasi. 8.1.1 Aturan dan tanggung jawab keamanan 8.1.2 Seleksi 8.1.3 Persyaratan dan Kondisi yang harus dipenuhi oleh pegawai
	Pasal 14 **Selama Penugasan** Dalam pasal 14 ini mengatur tentang pemahaman *Security Awareness* yang cukup untuk menjalani prosedur sekuriti dalam pekerjaannya dan untuk meminimalisir terjadinya *human eror.*	**Kategori Keamanan Utama: 8.2 (Berelasi dengan Pasal 14 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)** Selama Menjadi Pegawai Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga

Tabel 3.1 Pemetaan Standar ISO 27002:2005 dan Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 (Lanjutan)

No	Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor : KD.57/HK-290/ITS-30/2006	ISO 27002:2005
1.	**Pasal 15** **Pemutusan atau Penggantian Tugas** Dalam pasal 15 ini mengatur tentang tata cara pemberhentian atau penggantian tugas karyawan, hak akses yang diberikan pada karyawan, serta pengembalian aset apabila sudah tidak bekerja.	memahami Keamanan Informasi yang telah ditetapkan oleh organisasi demi mengurangi terjadinya kesalahan kerja (*human error*) dan resiko yang dihadapi oleh organisasi. 8.2.1 Tanggung jawab manajemen 8.2.2 Pendidikan dan pelatihan Keamanan Informasi 8.2.3 Proses kedisiplinan **Kategori Keamanan Utama: 8.3 (Berelasi dengan Pasal 15 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)** Pemberhentian atau pemindahan pegawai Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga yang diberhentikan atau dipindah dilakukan sesuai prosedur yang benar. 8.3.1 Tanggung jawab pemberhentian 8.3.2 Pengembalian aset-aset 8.3.3 Penghapusan hak akses
2.	**Bab VI** **Sekuriti Fisik dan Lingkungan Aset Informasi** **Pasal 16** **Area Aman**	**Klausul 9 Keamanan Fisik dan Lingkungan** **Kategori Keamanan Utama: 9.1 (Berelasi dengan Pasal 16 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)**

Tabel 3.1 Pemetaan Standar ISO 27002:2005 dan Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 (Lanjutan)

No	Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor : KD.57/HK-290/ITS-30/2006	ISO 27002:2005
	Dalam pasal 16 ini mengatur tentang area aman harus diberi batas fisik, hanya dapat dimasuki oleh personil yang memiliki hak akses serta didesain dengan mempertimbangkan aspek sekuriti.	Wilayah Aman Objektif Kontrol: Untuk mencegah akses fisik tanpa hak, kerusakan dan ganguan terhadap Informasi dan perangkatnya dalam organisasi. 9.1.1 Pembatasan Keamanan Fisik 9.1.2 Kontrol Masuk Fisk 9.1.3 Keamanan kantor, ruang dan fasilitasnya 9.1.4 Perlindungan terhadap ancaman dari luar dan lingkungan sekitar 9.1.5 Bekerja di wilayah aman 9.1.6 Akses publik, tempat pengiriman dan penurunan barang
2.	**Pasal 17** **Sekuriti Perangkat Teknologi Informasi** Dalam pasal 17 ini mengatur tentang perangkat teknologi informasi harus ditempatkan di lokasi yang aman, serta kabel daya dan kabel komunikasi harus dilindungi dari kerusakan	**Kategori Keamanan Utama: 9.2 (Berelasi dengan Pasal 17 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)** Keamanan Peralatan 9.2.1 Letak peralatan dan pengamanannya 9.2.2 Utilitas pendukung 9.2.3 Keamanan pengkabelan 9.2.4 Pemeliharaan peralatan 9.2.5 Keamanan peralatan diluar tempat yang tidak disyaratkan 9.2.6 Keamanan untuk pembuangan atau pemanfaatan kembali peralatan 9.2.7 Hak pemanfaatan

Tabel 3.1 Pemetaan Standar ISO 27002:2005 dan Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 (Lanjutan)

No	Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor : KD.57/HK-290/ITS-30/2006	ISO 27002:2005
3.	**Bab VIII** **Kontrol Akses** **Pasal 34** **Manajemen Akses Pengguna** Dalam pasal 34 ini mengatur tentang prosedur kontrol akses sistem informasi, pemberian dan pencabutan hak akses, serta alokasi *password* yang harus dikelola untuk memaksimumkan perlindungan terhadap sistem, aplikasi dan data. **Pasal 35** **Tanggung Jawab Pengguna** Dalam pasal 35 ini mengatur tentang tanggung jawab pengguna untuk melindungi aset informasi, pengguna harus bertanggung jawab untuk memelihara kontrol akses yang diberikan serta pengguna harus menjamin bahwa perangkat yang sedang tidak dikontrol memiliki proteksi yang memadai.	**Klausul 11 Kontrol Akses** **Kategori Keamanan Utama: 11.1** Persyaratan bisnis untuk akses kontrol Objektif Kontrol: Untuk mengontrol akses informasi. 11.1.1 Kebijakan kontrol akses **Kategori Keamanan Utama: 11.2 (Berelasi dengan Pasal 34 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)** Manajemen akses *user* Objektif Kontrol: Untuk memastikan pengguna yang mempunyai hak akses ke Sistem Informasi dan yang tidak. 11.2.1 Registrasi pengguna 11.2.2 Manajemen hak istimewa 11.2.3 Manajemen *password user* 11.2.4 Tinjauan terhadap hak akses user **Kategori Keamanan Utama: 11.3 (Berelasi dengan Pasal 35 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)** Tanggung jawab pengguna (*user*) Objektif Kontrol: Untuk mencegah akses user tanpa hak atau pencurian Informasi dan fasilitas

Tabel 3.1 Pemetaan Standar ISO 27002:2005 dan Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 (Lanjutan)

No	Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor : KD.57/HK-290/ITS-30/2006	ISO 27002:2005
		pemrosesan Informasi. 11.3.1 Penggunaan *password* 11.3.2 Peralatan penggunaan yang tanpa penjagaan 11.3.3 Kebijakan *clear desk* dan *clear screen*
3.	**Pasal 36** **Kontrol Akses Layanan Jaringan** Dalam pasal 36 ini mengatur tentang harus dilakukannya pengendalian akses ke layanan jaringan internal dan eksternal, unit pengelola teknologi informasi bertanggung jawab untuk menyusun prosedur implementasi layanan jaringan.	**Kategori Keamanan Utama: 11.4 (Berelasi dengan Pasal 36 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)** Kontrol Akses Jaringan Objektif Kontrol: Untuk mencegah akses tanpa hak ke dalam layanan jaringan. 11.4.1 Kebijakan penggunaan layanan jaringan 11.4.2 Otentikasi pengguna untuk melakukan koneksi keluar 11.4.3 Identifikasi peralatan di dalam jaringan 11.4.4 Perlindungan *remote diagnostic*dan konfigurasi *port* 11.4.5 Pemisahan dengan jaringan 11.4.6 Kontrol terhadap koneksi jaringan 11.4.7 Kontrol terhadap *routing* jaringan
	Pasal 37 **Kontrol Akses Sistem Operasi** Dalam pasal 37 ini mengatur tentang pengendalian akses sistem operasi dilakukan dengan prosedur log-on untuk mengurangi akses yang tidak	**Kategori Keamanan Utama: 11.5 (Berelasi dengan Pasal 37 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)**

Tabel 3.1 Pemetaan Standar ISO 27002:2005 dan Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 (Lanjutan)

No	Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor : KD.57/HK-290/ITS-30/2006	ISO 27002:2005
	terotorisasi.	Kontrol Akses Sistem Operasi Objektif Kontrol: Untuk mencegah akses tanpa hak ke sistem operasi. 11.5.1 Prosedur Log-On yang aman 11.5.2 Identifikasi dan autentikasi pengguna 11.5.3 Sistem Manajemen Password 11.5.4 Penggunaan utilitas sistem *diagnostic*dan konfigurasi *port* 11.5.5 Sesi *time-out* 11.5.6 Batasan waktu koneksi
3.	**Pasal 38** **Kontrol Akses Aplikasi dan Informasi** Dalam pasal 38 ini mengatur tentang akses terhadap informasi dan aplikasi harus diatur berdasarkan prosedur.	**Kategori Keamanan Utama: 11.6 (Berelasi dengan Pasal 38 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)** Kontrol Akses Informasi dan aplikasi Objektif Kontrol: Untuk mencegah akses tanpa hak terhadap Informasi yang terdapat di dalam aplikasi. 11.6.1 Pembatasan akses informasi 11.6.2 Pengisolasian sistem yang sensitif
	Pasal 39 ***Mobile Computing* dan *Teleworking*** Dalam pasal 39 ini mengatur tentang seluruh perangkat mobile computing sedapat mungkin harus mengikuti prosedur keamanan yang berlaku.	**Kategori Keamanan Utama: 11.7 (Berelasi dengan Pasal 39 dari Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006)**

Tabel 3.1 Pemetaan Standar ISO 27002:2005 dan Dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 (Lanjutan)

No	Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk. Nomor : KD.57/HK-290/ITS-30/2006	ISO 27002:2005
3.		Komputasi bergerak dan bekerja dari lain tempat *(teleworking)* Objektif Kontrol: Untuk memastikan Keamanan Informasi saat menggunakan fasilitas komputasi bergerak atau bekerja darilaintempat. 11.7.1 Komunikasi dan terkomputerisasi yang bergerak 11.7.2 *Teleworking*

Tabel 3.2 Pemetaan Gambaran Proses Audit Menurut Davis dan Tahap Audit yang Dikembangkan

No	Davis	Proses Pengembangannya
1	*Planning*	Pada tahap *planning* ini masuk ke dalam tahap perencanaan audit
2	*Fieldwork and Documentation*	Pada tahap *Fieldwork and Documentation* ini masuk ke dalam tahap persiapan audit dan pelaksanaan audit
3	*Issues Discovery and Validation*	Pada tahap *Issues Discovery and Validation* masuk ke dalam tahap pelaksanaan audit
4	*Solution Development*	Pada tahap *Solution Development* ini masuk ke dalam tahapan pelaksanaan audit
5	*Report Drafting and Issuance*	Pada tahap *Report Drafting and Issuance* masuk ke dalam tahap pelaporan audit
6	*Issue Tracking*	Pada tahap *Issue Tracking* masuk ke dalam tahap pelaporan audit

3.1 Tahap Perencanaan Audit Keamanan Sistem Informasi

Pada tahap ini langkah-langkah yang dilakukan yakni 1.) Identifikasi Informasi organisasi perusahaan 2.) Pemahaman proses bisnis, 3.) Menentukan ruang lingkup, objek audit dan tujuan audit, 4.) Penentuan klausul, objektif kontrol dan kontrol, 5.) Membuat dan menyampaikan *engagement letter*. Dari tahapan tersebut akan menghasilkan pengetahuan tentang proses bisnis

perusahaan, ruang lingkup dan tujuan yang telah ditentukan serta klausul yang telah ditentukan oleh kedua belah pihak.

3.1.1 Identifikasi Informasi Organisasi Perusahaan

Pada tahapan perencanaan audit, proses pertama yang dilakukan adalah mengidentifikasi informasi organisasi perusahaan yang diaudit dengan mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen tersebut berupa profil perusahaan PT Telkom Divre V Jatim, visi misi PT Telkom Divre V Jatim, profil bagian *Desktop Management*, struktur organisasi *Desktop Management* serta deskripsi pekerjaan di *Desktop Management.* 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 informasi organisasi perusahaan langkah yang dilakukan adalah dengan cara mengetahui dan memeriksa dokumen-dokumen yang terkait dengan proses audit, wawancara manajemen dan staff, serta melakukan observasi. Salah satu contoh proses identifikasi informasi organisasi perusahaan dengan wawancara manajemen dan staff dapat dilihat pada Tabel 3.3.

Tabel 3.3 Contoh Wawancara dengan Manajemen dan Staf

Wawancara Permasalahan Pada *Desktop Management*	Auditor : Dian Ayu P
	Auditee : Bpk Agus Widodo (Bagian Officer 2 administrasi & monitoring) & Pak Uyud (Bagian Officer 1 Desktop Operation & Lisensi)
	Tanggal : 10 Desember 2012
1. T: Apakah pada perusahaan ini khususnya di bagian Desktop Management PT Telkom Divre V Jatim memiliki suatu regulasi khusus	

Tabel 3.3 Contoh Wawancara dengan Manajemen dan Staf (Lanjutan)

Wawancara Permasalahan Pada *Desktop Management*	Auditor : Dian Ayu P
	Auditee : Bpk Agus Widodo (Bagian Officer 2 administrasi & monitoring) & Pak Uyud (Bagian Officer 1 Desktop Operation & Lisensi)
	Tanggal : 10 Desember 2012
2. 1. untuk audit atau keterikatan, misalnya seperti Bank regulasinya adalah PBI/BI, apabila saham berdasarkan BEI/Bapepam? Apabila tidak ada regulasi khusus, dapatkah saya nantinya mengaudit pada bagian tertentu berdasarkan SOP atau kebijakan atau peraturan yg berlaku pada perusahaan ini? 3. J: Mengenai SOP (Standard Operating Procedure), hampir seluruh alur proses bisnis datanya tidak di sini tapi terdapat di Telkom Bandung. Namun terdapat satu bagian yang dapat anda audit karena masih bisa dilihat secara langsung proses kerjanya yaitu di bagian Desktop Management. Pada bagian tersebut terdapat aplikasi penyimpanan dokumen, serta prosedur standard keamanan untuk penggunaan password. 4. 2. T : Pada setiap perusahaan pasti terdapat beberapa aset berharga, contoh : aset informasi, aset piranti lunak, aset fisik, aset layanan. Pada bagian Desktop Management , terdapat aset apa saja? 5. J : Ya aset-aset tersebut semuanya ada di sini. Di antaranya yaitu : Aset informasi :berupa dokumentasi prosedur standard keamanan untuk penggunaan password, Aset fisik :berupa fasilitas dari perusahaan yaitu PC, printer dan perabotan kantor lainnya, Aset piranti lunak :berupa aplikasi CNEMAS (Computer & Network Equipment Management System), Aset layanan :berupa pencahayaan, AC, dll 6. 3. T: Bagaimana penjelasan secara umum mengenai fungsi aplikasi tersebut? 7. J: CNEMAS merupakan suatu aset piranti lunak yang berfungsi untuk mengontrol pergerakan fasilitas kerja pegawai	

3.1.2 Pemahaman Proses Bisnis

Proses kedua pada tahapan perencanaan audit ini adalah mengetahui proses bisnis perusahaan sebelum dilakukan audit dengan cara memahami proses bisnis yang ada pada bagian *Desktop Management. Output* yang dihasilkan dalam proses ini adalah alur proses bisnis bagian *Desktop Management*.

3.1.3 Penentuan Ruang Lingkup, Objek Audit dan Tujuan Audit

Proses ketiga pada tahapan perencanaan ini adalah mengidentifikasi ruang lingkup dan tujuan yang akan dibahas dalam audit kali ini. Penentuan ruang lingkup dilakukan dengan cara melakukan observasi, wawancara dan kuesioner pada bagian *Desktop management*. Pada proses ini, langkah yang selanjutnya dilakukan adalah mengidentifikasi tujuan yang berhubungan dengan kebutuhan audit keamanan sistem informasi. *Output* yang dihasilkan adalah hasil ruang lingkup, objek audit dan tujuan audit.

3.1.4 Menentukan Klausul, Objektif Kontrol dan Kontrol

Pada proses ini langkah yang dilakukan adalah menentukan objek mana saja yang akan diperiksa sesuai dengan permasalahan yang ada dan kebutuhan perusahaan. Menentukan klausul, objektif kontrol dan kontrol yang sesuai dengan kendala dan kebutuhan *Desktop management*. Klausul, objektif kontrol dan kontrol yang ditentukan harus berdasarkan kesepakatan antara auditor dengan *auditee* dan disesuaikan dengan standar ISO 27002:2005. *Output* yang dihasilkan adalah hasil pemilihan klausul yang akan diperiksa, objektif kontrol dan kontrol sesuai ISO 27002:2005 yang juga tertuang pada *engagement letter*.

3.1.5 Membuat dan Menyampaikan *Engagement Letter*

Pada tahap ini adalah membuat dan menyampaikan *Engagement Letter* atau surat perjanjian audit. Surat perjanjian audit adalah surat persetujuan antara kedua belah pihak yang bersangkutan yaitu auditor dengan manager *Desktop Management* tentang syarat-syarat pekerjaan audit yang akan dilakukan oleh auditor. Adapun isi dari *engagement letter* yakni berisi tanggung jawab komite

manajemen dan auditor, lingkup audit dan ketentuan audit. *Output* yang dihasilkan adalah berupa dokumen *Engagement Letter* yang disepakati oleh kedua belah pihak.

3.2 Tahap Persiapan Audit Keamanan Sistem Informasi

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1.) Melakukan penyusunan audit *working plan,* 2.) Penyampaian kebutuhan data, 3.) Membuat pernyataan, 4.) Melakukan pembobotan pernyataan dan 5.) Membuat pertanyaan.

3.2.1 Penyusunan Audit *Working Plan*

Audit *working plan* merupakan dokumen yang dibuat oleh auditor dan digunakan untuk merencanakan dan memantau pelaksanaan audit keamanan sistem informasi secara terperinci. *Output* yang dihasilkan adalah daftar susunan AWP dan dapat dilihat pada tabel 3.4

Tabel 3.4 Audit *Working Plan* Secara Keseluruhan

ID	Task Name	Duration	Start	Finish
1	Total Hari Audit	355 days	Thu 3/27/14	Fri 7/31/15
2	Perencanaan Audit Sistem Informasi	113 days	Thu 3/2714	Fri 8/29/14
7	Persiapan Audit Sistem Informasi	200 days	Wed 8/6/14	Thu 5/7/15
13	Pelaksanaan Audit Sistem Informasi	238 days	Fri 9/5/14	Fri 7/31/15
18	Pelaporan Audit Sistem Informasi	65 days	Mon 5/4/15	Fri 7/31/15

3.2.2 Penyampaian Kebutuhan Data

Penyampaian kebutuhan data yang diperlukan auditor dapat disampaikan terlebih dahulu kepada *auditee* agar dapat dipersiapkan terlebih dahulu. *Fieldwork* dilaksanakan auditor setelah *auditee* menginformasikan ketersediaan semua data yang diperlukan auditor sehingga *fieldwork* dapat dilaksanakan oleh auditor

secara efektif. *Output* yang dihasilkan adalah daftar penyampaian kebutuhan data perusahaan pada tampilan Tabel 3.5.

Tabel 3.5 Contoh Lampiran Kebutuhan Data Penunjang yang Diperlukan Dalam Pelaksanaan Audit

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 *Desktop Management*					
3	*Job description* pegawai di *Desktop Management*					
4	Alur proses bisnis perusahaan					
5	Dokumen kebijakan keamanan sistem informasi					
6	Dokumen prosedur *Desktop Management*					

3.2.3 Membuat Pernyataan

Proses selanjutnya pada tahapan persiapan audit ini dilakukan dengan membuat pernyataan berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah ditetapkan berdasarkan standar ISO 27002. Pada setiap kontrol keamanan dapat ditentukan pernyataan yang mendiskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut. *Output* yang dihasilkan adalah salah satu contoh pernyataan pada klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.3.1 (penggunaan password (*Password Use*)) dapat dilihat pada Tabel 3.6.

Tabel 3.6 Contoh Pernyataan Pada Klausul 11 Dengan Kontrol 11.3.1 Penggunaan Password (*Password Use*)

PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon sibilities*)	
ISO 27002 11.3.1 Penggunaan *Password* (*Password Use*)	
Kontrol : Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan *password*.	
No.	PERNYATAAN
1.	Adanya kesadaran dari diri sendiri untuk menjaga kerahasiaan password
2.	Terdapat penggantian kata password setiap kali ada kemungkinan sistem atau password dalam keadaan bahaya
3.	Terdapat larangan dalam pembuatan catatan *password*
4.	Terdapat larangan untuk tidak membagi satu *password* kepada pengguna lain
5.	Terdapat pergantian *password* sementara pada saat pertama kali log-on
6.	Terdapat pemilihan *password* secara berkualitas yang mudah diingat
7.	Terdapat perubahan kata sandi/*password* berkala atau berdasarkan jumlah akses dan larangan menggunakan *password* yang lama

3.2.4 Melakukan Pembobotan Pernyataan

Setelah membuat pernyataan, maka langkah selanjutnya adalah melakukan pengukuran pembobotan pada setiap pernyataan. Pembobotan dilakukan berdasarkan perhitungan yang dilakukan oleh (Niekerk dan Labuschagne dalam hastin 2012: 39), dengan membagi tingkat pembobotan dalam manajemen menjadi 3 (tiga), yaitu: rendah, cukup dan tinggi. *Output* yang dihasilkan adalah contoh tingkat kepentingan dalam pembobotan pernyataan pada Tabel 3.7 dan salah satu contoh pembobotan yang ada dalam klausul 11 (sebelas) Kontrol Akses dapat dilihat pada Tabel 3.8.

Tabel 3.7 Tingkat Kepentingan dalam Pembobotan Pernyataan (Sumber: Niekerk dan Labuschagne dalam Hastin, 2012:39)

Resiko	Bobot	Keterangan
Rendah	0,00 - 0,39	Pernyataan tersebut mempunyai peranan kurang penting dalam proses sistem informasi

Tabel 3.7 Tingkat Kepentingan dalam Pembobotan Pernyataan (Lanjutan)
(Sumber: Niekerk dan Labuschagne dalam Hastin, 2012:39)

Resiko	Bobot	Keterangan
Cukup	0,40 - 0,69	Pernyataan tersebut mempunyai peranan cukup penting dalam proses sistem informasi
Tinggi	0,70 - 1,00	Pernyataan tersebut mempunyai peranan sangat penting dalam proses sistem informasi

Tabel 3.8 Contoh Pembobotan Pada Klausul 11 Dengan Kontrol 11.3.1 Penggunaan Password (*Password Use*)

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)				
Klausul 11.3 Tanggung Jawab Pengguna (*user*)				
ISO 27002 11.3.1 Penggunaan *password*				
Kontrol : Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan password.				
No.	PERNYATAAN	Bobot		
		Rendah (0,1-0,39)	Cukup (0,4-0,69)	Tinggi (0,7-1,0)
1.	Adanya kesadaran dari diri sendiri untuk menjaga kerahasiaan password			1
2.	Terdapat penggantian kata password setiap kali ada kemungkinan sistem atau password dalam keadaan bahaya		0,6	
3.	Terdapat larangan dalam pembuatan catatan password			0,8
4.	Terdapat larangan untuk tidak membagi satu password kepada pengguna lain			1
5.	Terdapat pergantian password sementara pada saat pertama kali log-on			1
6.	Terdapat pemilihan password secara berkualitas yang mudah diingat		0,6	
7.	Terdapat perubahan kata sandi/password berkala atau berdasarkan jumlah akses dan larangan menggunakan password yang lama			0,7

3.2.5 Membuat Pertanyaan

Pada proses ini langkah yang dilakukan adalah membuat pertanyaan dari pernyataan yang telah ditentukan sebelumnya. Pada satu pernyataan bisa memiliki lebih dari satu pertanyaan, hal tersebut dikarenakan setiap pertanyaan harus

mewakili pernyataan pada saat dilakukan wawancara, observasi dan identifikasi dokumen. *Output* yang dihasilkan dalam membuat pertanyaan adalah daftar pertanyaan dari pernyataan yang ada pada Tabel 3.9.

Tabel 3.9 Contoh Pertanyaan Pada Klausul 11 Dengan Kontrol 11.3.1 Penggunaan *Password*

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon Sibilities*)	
ISO 27002 11.3.1 Penggunaan *password*	
1	Adanya kesadaran dari diri sendiri untuk menjaga kerahasiaan password
	P: Apakah karyawan *Desktop Management* telah menyadari mengenai pentingnya kerahasiaan password masing-masing? J: P: Apakah ada perintah tertulis yang menangani pentingnya menjaga kerahasiaan password? J:
2	Terdapat penggantian kata password setiap kali ada kemungkinan sistem atau password dalam keadaan bahaya
	P: Apakah karyawan yang bersangkutan sering melakukan pergantian password jika dirasa sistem dalam keadaan bahaya? J: P: Apakah terdapat aturan secara tertulis atau secara lisan mengenai perintah pergantian sandi setiap kali ada kemungkinan keadaan bahaya? J: P: Apakah ada pencatatan perintah dalam pergantian password setiap kali ada kemungkinan sistem atau password dalam keadaan bahaya? J:
3	Terdapat larangan dalam pembuatan catatan password

Tabel 3.9 Contoh Pertanyaan Pada Klausul 11 Dengan Kontrol 11.3.1 Penggunaan *Password* (Lanjutan)

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon Sibilities*)	
ISO 27002 11.3.1 Penggunaan *password*	
	P: Apakah ada larangan dalam pembuatan catatan password? J: P: Siapa yang membuat larangan pembuatan catatan password? J: P: Apakah karyawan memiliki metode penyimpanan yang aman dalam peletakan passwordnya? J:

3.3 Tahap Pelaksanaan Audit Keamanan Sistem Informasi

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1.) Melakukan wawancara, 2.) Melakukan proses pemeriksaan data, 3.) Penyusunan daftar temuan audit keamanan sistem informasi dan rekomendasi dan 4.) Konfirmasi daftar temuan audit keamanan sistem informasi dan rekomendasi Tahap ini akan menghasilkan temuan dan bukti, dokumen wawancara, hasil daftar temuan dan rekomendasi, dan hasil konfirmasi temuan audit.

3.3.1 Melakukan Wawancara

Wawancara dilaksananakan setelah membuat pertanyaan yang sudah dibuat sebelumnya. Wawancara dilakukan terhadap pihak yang berkepentingan sesuai dengan pertanyaan yang ada. *Output* yang dihasilkan adalah dokumen wawancara yang berisi catatan informasi yang diperoleh dan analisis yang dilakukan selama proses audit. Berikut adalah salah satu hasil wawancara pada

klausul 11 (Sebelas) Kontrol Akses dengan kontrol 11.3.1 (Penggunaan Password (*Password Use*)) Tabel 3.10.

Tabel 3.10 Contoh Wawancara Klausul 11 Dengan Kontrol 11.3.1 Penggunaan *Password*

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	Auditor : Dian Ayu P Auditee : Bpk Setiyobudi Tanggal :
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon Sibilities*)	
ISO 27002 11.3.1 Penggunaan *password*	
1	Adanya kesadaran dari diri sendiri untuk menjaga kerahasiaan password
	P: Apakah karyawan *Desktop Management* telah menyadari mengenai pentingnya kerahasiaan password masing-masing? J: Sudah P: Apakah ada perintah tertulis yang memberitahukan pada karyawan tentang pentingnya menjaga kerahasiaan password? J: Ada, yaitu berupa larangan menyebarkan password. Di dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 Bab VIII Pasal 34 ayat (4)d
2	Terdapat penggantian kata password setiap kali ada kemungkinan sistem atau password dalam keadaan bahaya
	P: Apakah karyawan yang bersangkutan sering melakukan pergantian password jika dirasa sistem dalam keadaan bahaya? J: Selama ini masih belum melakukan pergantian password, karena masih belum ada sistem yang berbahaya P: Apakah terdapat aturan secara tertulis atau secara lisan mengenai perintah pergantian sandi setiap kali ada kemungkinan keadaan bahaya? J: Kalau memang ada perintah ya biasanya secara lisan
3	Terdapat larangan dalam pembuatan catatan password
	P: Apakah ada larangan dalam pembuatan catatan password di laptop kerja tanpa perlindungan khusus? J: Ada P: Siapa yang membuat larangan pembuatan catatan password tersebut? J: Pihak direksi, larangan tersebut terdapat di dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 Pasal 34 ayat (4)k P: Apakah karyawan memiliki metode penyimpanan yang aman dalam peletakan passwordnya?

Tabel 3.10 Contoh Wawancara Klausul 11 Dengan Kontrol 11.3.1 Penggunaan *Password* (Lanjutan)

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	Auditor : Dian Ayu P
	Auditee : Bpk Setiyobudi
	Tanggal :
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon Sibilities*)	
ISO 27002 11.3.1 Penggunaan *password*	
1	J: Iya , melalui perangkat pribadi masing masing, seperti perangkat mobile

3.3.2 Proses Pemeriksaan Data

Pada Pemeriksaan data dilakukan dengan cara melakukan observasi dan melakukan wawancara kepada *auditee* sesuai dengan ruang lingkup serta klausul yang telah disepakati oleh Manager *Desktop management*. Wawancara dan observasi dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Bukti-bukti tersebut berupa foto dan data. Berikut adalah contoh dokumen pemeriksaan fakta dan bukti yang dapat dilihat pada Tabel 3.11.

Tabel 3.11 Contoh Dokumen Pemeriksaan Data Audit Pada Klausul 11 Dengan Kontrol 11.3.1 Penggunaan *Password*

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 11 (KONTROL AKSES)		Pemeriksa : Bpk Erwin Sutomo/Bpk Teguh Sutanto	
		Auditor : Dian Ayu P	
		Auditee : Bpk Setyo Budi	
		Tanggal :	
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon Sibilities*)			
ISO 27002 11.3.1 Penggunaan *Password*			
No.	Pemeriksaan	Catatan Auditor	Catatan Review
1.	Identifikasi kesadaran dari diri sendiri untuk menjaga kerahasiaan password Dengan cara 1. Wawancara 2. Dapatkan dokumen yang memberitahukan	Telah diperiksa bahwa terdapat kesadaran dari para karyawan akan pentingnya untuk menjaga password dan telah sesuai dengan dokumen yang ada di	

Tabel 3.11 Contoh Dokumen Pemeriksaan Data Audit Pada Klausul 11 Dengan Kontrol 11.3.1 Penggunaan *Password* (Lanjutan)

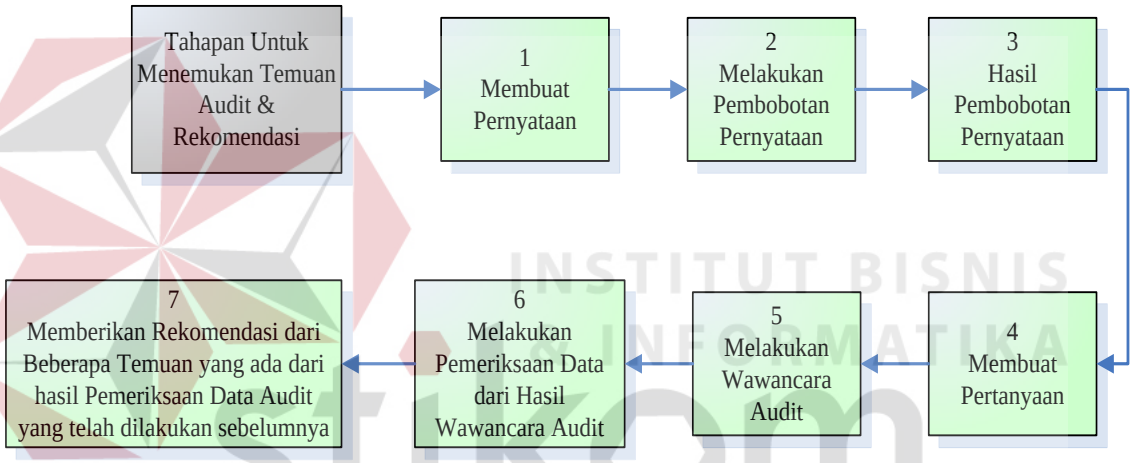
PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 11 (KONTROL AKSES)		Pemeriksa : Bpk Erwin Sutomo/Bpk Teguh Sutanto	
		Auditor : Dian Ayu P	
		Auditee : Bpk Setyo Budi	
		Tanggal :	
Klausul 11.3 Tanggung Jawab Pengguna (*User Respon Sibilities*)			
ISO 27002 11.3.1 Penggunaan *Password*			
No.	Pemeriksaan	Catatan Auditor	Catatan Review
	larangan untuk menyebarluaskan password dan menjaga kerahasiaannya	perusahaan yaitu di dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 bab VIII pasal 34 ayat (4)d.	

3.3.3 Penyusunan Daftar Temuan Audit Keamanan Sistem Informasi dan Rekomendasi

Pada proses penentuan temuan dan rekomendasi terdapat beberapa langkah yang dilakukan yaitu dari proses membuat pernyataan, melakukan pembobotan pernyataan, hasil pembobotan pernyataan yang digunakan, membuat pertanyaan, melakukan wawancara audit, melakukan pemeriksaan data dari hasil wawancara audit, memberikan rekomendasi dari beberapa temuan yang ada dari hasil pemeriksaan data audit seperti yang terlihat pada gambar 3.2. Seluruh aktivitas tersebut menghasilkan bukti *(evidence)* yang berarti terkait dengan sistem yang berlangsung di perusahaan. Berdasarkan temuan dan bukti-bukti tersebut dihasilkan rekomendasi untuk perusahaan agar penerapan kontrol keamanan dapat diterapkan lebih baik. *Output* yang dihasilkan adalah daftar temuan dan rekomendasi seperti pada tabel 3.12.

Tabel 3.12 Contoh Lampiran Temuan dan Rekomendasi Pada Klausul 11 (Sebelas) Kontrol Akses

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI				Auditor : Dian Ayu P Auditee : Bpk Setyo Budi
ASPEK : KLAUSUL 11 (KONTROL AKSES) ISO 27002 11.3.1 Penggunaan Password (*Password Use*)				Tanggal :
No	Pernyataan	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian



Gambar 3.2 Tahapan dalam Menentukan Temuan Audit dan Rekomendasi

Beberapa langkah untuk mendapatkan temuan audit dan rekomendasi seperti yang terlihat pada gambar 3.2, akan dijelaskan sebagai berikut :

a. Membuat Pernyataan

Untuk membuat pernyataan, lebih dominan menggunakan referensi dari ISO 27002 dibanding dengan dokumen yang menjadi regulasi perusahaan yaitu dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk nomor : KD.57/HK-290/ITS-30/2006 atau

yang sering disebut dengan dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006. Karena di dalam ISO 27002 lebih detail dalam menjelaskan panduan implementasi untuk audit.

b. Melakukan Pembobotan Pernyataan

Setelah membuat pernyataan langkah untuk menemukan temuan audit yaitu melakukan pembobotan pernyataan. Pembobotan pernyataan dilakukan dengan cara memberikan angket kepada pihak auditee yang nantinya akan menilai pada setiap pernyataan yang telah dibuat auditor, dan ada beberapa ketentuan nilai yaitu rendah (0,1-0,39), cukup (0,4-0,69) serta tinggi (0,7-1,0). Ketentuan nilai tersebut menggunakan referensi dari Niekerk dan Lambuscgahne dalam Hastin, 2012 : 39.

c. Hasil Pembobotan Pernyataan yang Digunakan

Setelah melakukan pembobotan pada setiap pernyataan, maka akan muncul hasil nilai pembobotan pernyataan. Sesuai kesepakatan dengan pihak auditee yang terlampir dalam berita acara hasil penilaian pembobotan pernyataan audit untuk nilai kategori yang rendah maka pernyataan tersebut tidak digunakan dalam proses audit selanjutnya, yang digunakan adalah nilai cukup dan tinggi saja.

d. Membuat Pertanyaan

Setelah memperoleh pernyataan dari hasil pembobotan pernyataan, maka langkah selanjutnya adalah membuat beberapa pertanyaan dari setiap pernyataan yang terpilih. Pertanyaan disesuaikan dengan beberapa hal yang

harus diketahui oleh auditor untuk memenuhi kontrol yang ada pada setiap pernyataan.

e. Melakukan Wawancara Audit

Pernyataan dan pertanyaan telah dibuat, maka langkah selanjutnya adalah melakukan wawancara audit. Wawancara audit ini dilakukan dengan beberapa narasumber. Untuk wawancara pada proses perencanaan audit yang meliputi pertanyaan mengenai profil perusahaan, visi misi PT Telkom, profil *Desktop Management*, struktur organisasi *Desktop Management* dan deskripsi pekerjaan dilakukan dengan bapak Agus Widodo bagian *Officer* 2 administrasi dan *monitoring*. Untuk alur proses bisnis *Desktop Management* dilakukan wawancara dengan bapak Uyud bagian *Officer* 1 *Desktop Operation* dan Lisensi. Untuk wawancara persiapan audit sampai pelaksanaan audit dilakukan dengan bapak Setiyobudi Eko bagian *Officer* 1 Administrasi dan *Monitoring*. Wawancara disertai juga dengan melihat langsung keadaan di sekitar ruang *Desktop Management* yang disertai foto dalam wawancara.

f. Melakukan Pemeriksaan Data dari Hasil Wawancara Audit

Setelah wawancara audit, maka auditor perlu memeriksa hasil wawancara audit guna menemukan suatu temuan pada hasil wawancara yang sudah dilakukan. Auditor memeriksa data berdasarkan hasil wawancara dan apa yang telah dilihat langsung di sekitar ruang lingkup *Desktop Management* dan akan menuliskan hasil pemeriksaannya dalam catatan auditor. Setelah menuliskan hasil pemeriksaannya pada kolom catatan auditor, langkah selanjutnya adalah memberikan catatan *review* yang merupakan kesimpulan dari hasi pemeriksaan yang telah dituliskan di catatan auditor. Dalam

kesimpulan yang dituliskan di catatan review tersebut bisa didapatkan suatu temuan audit.

g. Memberikan Rekomendasi dari Beberapa Temuan Audit

Dari hasil wawancara audit yang telah diperiksa maka akan teridentifikasi beberapa temuan audit dan dalam temuan audit tersebut akan diberitahukan kepada pihak auditee. Adapun dokumen terkait yang digunakan untuk memberi rekomedasi yaitu berdasarkan regulasi yang dimiliki perusahaan Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk nomor : KD.57/HK-290/ITS-30/2006 atau yang sering disebut dengan dokumen Keputusan Direksi Perusahaan Perseroan (Persero) PT Telekomunikasi Indonesia, Tbk Nomor : KD.57/HK-290/ITS-30/2006 dan standar ISO 27002.

3.3.4 Konfrimasi Daftar Temuan Audit keamanan Sistem Informadi dan Rekomendasi

Temuan harus dikonfirmasikan terlebih dahulu kepada *auditee* sebelum dilaporkan secara formal. Konfirmasi temuan didokumentasikan dalam bentuk risalah atau Notulen konfirmasi temuan.

Pada proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah memeriksa data profil perusahaan, kebijakan, standar, prosedur dan portopolio serta mengobservasi standard operating procedure dan melakukan wawancara kepada auditti. Seluruh aktivitas tersebut menghasilkan bukti (*evidence)* yang berarti terkait dengan sistem yang berlangsung di perusahaan.

3.4 Tahap Pelaporan Audit Keamanan Sistem Informasi

Tahap pelaporan ada beberapa langkah yang dilakukan yaitu: 1.) Melakukan permintaan tanggapan atas temuan audit keamanan sistem informasi, 2.) Penyusunan draft laporan audit keamanan sistem informasi, 3.) Persetujuan draft laporan audit keamanan sistem informasi dan 4.) Pertemuan penutup atau pelaporan hasil audit keamanan sistem informasi.

3.4.1 Permintaan Tanggapan Atas Temuan

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

3.4.2 Penyusunan *Draft* Laporan Audit keamanan sistem informasi

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

3.4.3 Persetujuan Draft Laporan Audit keamanan sistem informasi

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

3.4.4 Pertemuan Penutup atau Pelaporan Hasil Audit keamanan sistem informasi

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