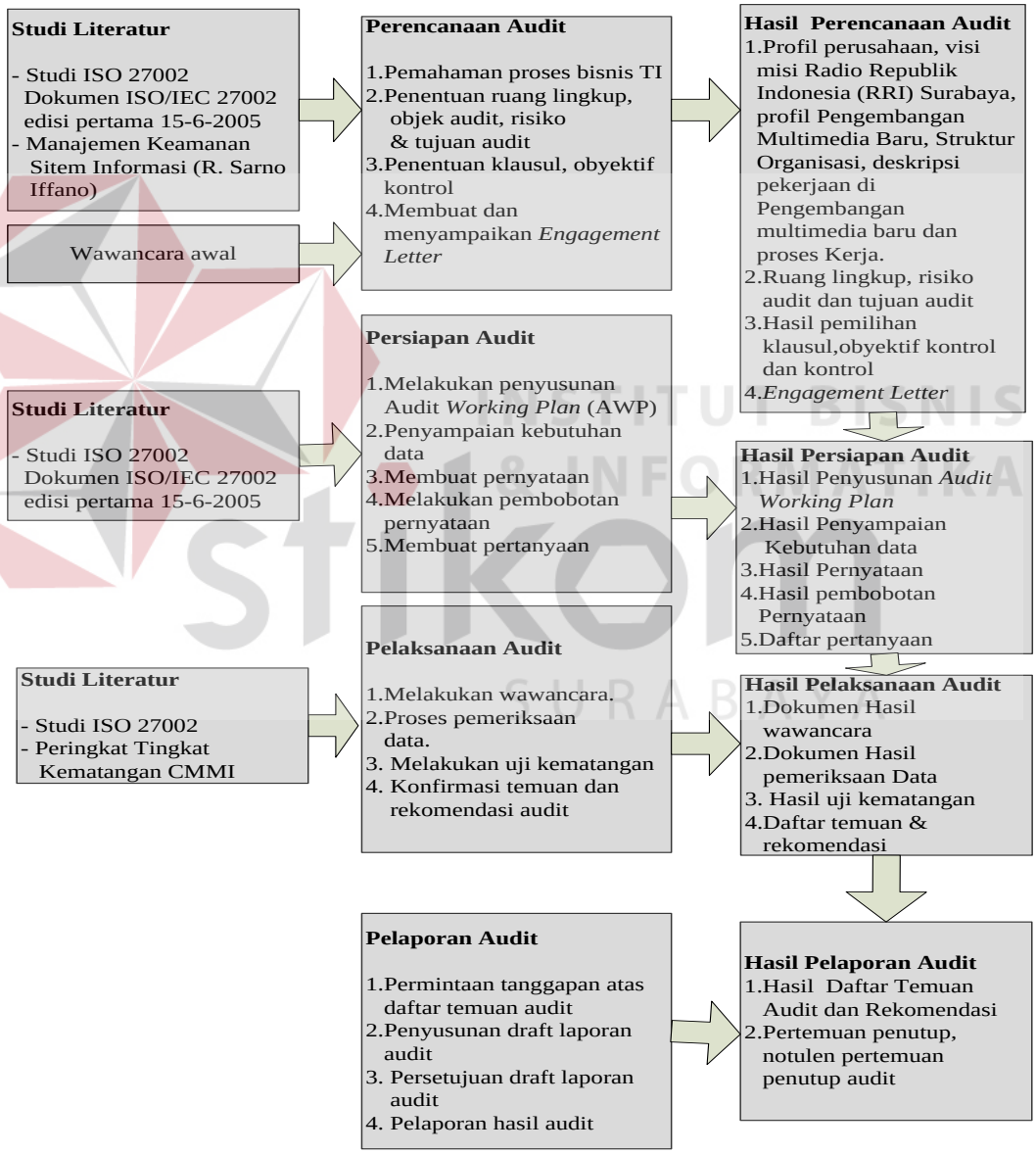
BAB III

METODE PENELITIAN

Pada Bab III akan dilakukan pembahasan dimulai dari tahapperencanaan audit, persiapan audit,pelaksanaan, dan dilanjutkan dengan tahap pelaporan auditseperti terdapat pada Gambar 3.1.



Gambar 3.1Tahapandalam Audit Keamanan InformasiPada Pagian Pengembangan Multimedia Baru
(Sumber: Davis, 2011)

3.1 Tahap Perencanaan Audit Keamanan Informasi

Pada tahap ini langkah-langkah yang dilakukan yakni 1. Pemahaman proses bisnis TI, 2.Menentukan ruang lingkup,risiko dan tujuan audit,3.Penentuan klausul, obyektif kontrol, 4. Membuat dan menyampaikan *engagement letter*. Dari tahapan tersebut akan menghasilkan Profil perusahaan, visi dan misi Radio Republik Indonesia (RRI) Surabaya,profil Pengembangan Multimedia Baru,Struktur Organisasi, deskripsi pekerjaan di Pengembangan multimedia baru dan proses Kerja, ruang lingkup obyek audit dan tujuan audit, hasil pemilihan klausul, obyektif kontrol dan kontrol, dan *Engagement Letter*.

3.1.1 Pemahaman ProsesBisnis TI

Pada tahapan perencanaan audit, proses pertama yang dilakukan adalah pemahaman proses bisnis dan TI perusahaan yang diaudit (*auditee*) dengan mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen tersebut berupa profil perusahaan, tugas pokok dan fungsi (tupoksi), 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 proses TI dibagian PMB maka *auditor* menyususn langkah-langkah yang dilakukan untuk mengetahui dan memeriksa dokumen-dokumen yang terkait dengan proses audit, wawancara Kepala Seksi dan pelaksana, serta melakukan observasi kegiatan operasional dan teknologi informasi yang digunakan.

Dalam hal ini diharapkan definisi dari pemahaman proses informasi di bagian PMB menghasilkan dokumen berupa profil RRI Surabaya, visi, misi dan tujuan Radio Republik Indonesia Surabaya, profil pengembangan multimedia baru (PMB) pada RRI Surabaya, struktur organisasi fungsional di pengembangan multimedia baru, deskripsi pekerjaan di PMB serta hasil observasi kegiatan operasional dan siaran yang digunakan dapat menjadi pengetahuan dalam proses kerja instansi. Salah satu contoh proses identifikasi proses bisnis dengan wawancara kepada Kepala Seksi PMB dapat dilihat pada Tabel 3.1.

Tabel 3.1 Contoh Wawancara dengan Kepala Seksi PMB

Wawancara Permasalahan Pada Pengembangan Multimedia Baru	Auditor : Dewangga Putra Sejati
	Auditee : Bpk Tauchid Harsono
	Tanggal : 1 Oktober2015
	Tanda Tangan :

1. T: Apakah pada perusahaan ini khususnya di bagian Pengembangan Multimedia Baru RRI Surabaya memiliki suatu regulasi khusus untuk audit atau keterikatan, misalnya seperti penyiaranumum adalah KPI, 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 instansi ini?
   J: Mengenai SOP (Standard Operating Procedure), hampir seluruh alur proses bisnis diberi arahan oleh RRI pusat untuk masing-masing bagian dinamakan tupoksi (tugas pokok siaran). Namun terdapat satu bagian yang dapat anda audit karena masih bisa dilihat secara langsung proses kerjanya yaitu di bagian Pengembangan Multimedia Baru (PMB). Pada bagian tersebut terdapat penyimpanan berita, lagu, siaran.
2. T : Pada setiap perusahaan pasti terdapat beberapa aset berharga, contoh : aset informasi, aset piranti lunak, aset fisik, aset layanan. Pada bagian PMB , terdapat aset apa saja?
   J : Ya aset-aset tersebut semuanya ada di sini. Di antaranya yaitu : Aset informasi :berupa dokumentasi dilapangan, iklan, lagu, Aset fisik :berupa fasilitas dari instansi yaitu PC, alat transmisi, pemancar, dan peralatanpenyiaran lainnya, Aset piranti lunak:berupa aplikasi pengolahan lagu, berita serta iklanAset layanan :berupa studio, peralatan siaran, kendaraan siaran bergerak, AC, dll
3. T: Bagaimana penjelasan secara umum mengenai fungsi aplikasi tersebut?
   J: PMB adalah bagian di RRI Surabaya yang bertugas mengatur jalanya siaran serta mengelola informasi.

3.1.2 Penentuan Ruang Lingkup,Risiko dan Tujuan Audit

Proses kedua 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 bagianPMB. Pada proses ini, langkah yang selanjutnya dilakukan adalah mengidentifikasi tujuan yang berhubungan dengan kebutuhan audit keamanan informasi. Output yang dihasilkan adalah tujuan audit keamanan informasi PMB RRI Surabaya, ruang lingkup, penilaian risiko.

3.1.3 Menentukan Klausul, Obyektif 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, obyektif kontrol dan kontrol yang sesuai dengan kendala dan kebutuhan bagian PMB. Klausul, obyektif kontrol dan kontrol yang ditentukan harus berdasarkan kesepakatan antara auditor dengan *auditee*. Keluaran yang diharapkan dari proses ini dapat menjadi acuan dalam menentukan klausul yang digunakan dalam audit keamanan sistem informasi.

3.1.4 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 Kepala seksi PMBtentang 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 Informasi

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Melakukan penyusunan audit *working plan*(AWP), 2. Penyampaian kebutuhan data, 3. Membuat pernyataan, 4. Melakukan pembobotan pernyataan, dan 5. Membuat pertanyaan.Dari tahapan tersebut menghasilkan hasil penyusunan *Audit Working Plan*, hasil penyampaian kebutuhan data, hasil pernyataan, hasil pembobotan pernyataan, dan daftar 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 3.2

Tabel 3.2*Working Plan* Secara Keseluruhan

No.	Nama Pekerjaan	Durasi	Mulai	Selesai
1.	Total Hari Audit	317hari	Kamis10/01/15	Senin,09/23/16
2.	Perencanaan Audit	152hari	Kamis10/01/15	Senin, 03/14/16
3.	Persiapan Audit	17hari	Selasa 03/15/16	Kamis,03/31/16
4.	Pelaksanaan Audit	21hari	Jumat04/01/16	Kamis,04/21/16
5.	Pelaporan Audit	106hari	Jumat04/22/16	Jumat,09/23/16

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 3.3.

Tabel3.3 Contoh Lampiran Kebutuhan Data 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 RRI Surabaya					
3	*Job description* pegawai di Pengembangan Multimedia Baru					
4	Alur proses bisnis Instansi					
5	Dokumen kebijakan keamanan informasi					
6	Dokumen prosedur Pengembangan Multimedia Baru					

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 27002:2005. Pada setiap kontrol keamanan dapat ditentukan pernyataan yangmendiskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut. Output yang dihasilkan adalah salah satu contoh pernyataan padaklausul 11 (sebelas) Kontrol aksesdengan obyek kontrol 11.3tanggung jawab pengguna (*user*)dapat dilihat pada Tabel3.4.

Tabel3.4Contoh PernyataanPada Klausul 11 Kontrol Akses

PERNYATAAN AUDIT KEAMANAN INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.3Tanggung Jawab Pengguna (*user*)	
ISO 27002:200511.3.1Penggunaan *Password*	
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 Pembobotan Pernyataan

Setelah membuat pernyataan, maka langkah selanjutnya adalah melakukan pengukuran pembobotan pada setiap pernyataan.Pada setiap pernyataan yang telah dibuat harus ditentukan nilai bobotnya masing-masing, karena setiap pernyataan tersebut bisa jadi tidak bernilai sama dalam penerapannya untuk kontrol keamanan yang telah ditentukan.Metode ini menggunakan bobot pada penilaian resiko metode kualitatif, resiko memiliki hubungan dengan keamanan informasi dan resiko merupakan dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi (Sarno dan Iffano, 2009). Output yang dihasilkan adalahcontoh tingkat pembobotanpada Tabel 3.5 dan salah satu contoh pembobotan yang ada dalam klausul 9 (sembilan) Keamanan Fisik dan Lingkungandapat dilihat pada Tabel 3.6.

Tabel 3.5 Pembobotan Penilaian Risiko

Resiko	Bobot
Rendah(*Low*)	0,1-0,3
Cukup(*Medium*)	0,4-0,6
Tinggi(*High*)	0,7-1,0

(Sumber: Sarno, 2009)

Pembobotan ditentukan dari panduan implementasi dan tingkat kepentingannya bagi organisasi. Pernyataan yang mendapatkan pembobotan dengan resiko *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 risiko *high*. Pernyataan dengan risiko *low*berarti pernyataan tersebut tidak terlalu wajib untuk diterapkan namun apabila diterapkan akan menambah keamanan pada sistem.

Tabel3.6Contoh Pembobotan Pada Kontrol Keamanan Fisik dan Lingkungan

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)				
Klausul 9.1 Wilayah Aman				
ISO 27002 9.1.2 Kontrol masuk fisik				
Kontrol : Wilayah aman (*secure*) harus dilindungi dengan kontrol akses masuk yang memadai untuk memastikan hanya orang yang berhak saja dibolehkan masuk.				
No.	PERNYATAAN	Bobot		
		Rendah (0,1-0,3)	Cukup (0,4-0,6)	Tinggi (0,7-1,0)
1.	Terdapat pengawasan terhadap orang yang datang (Tanggal dan waktu berkunjung ke wilayah aman harus dicatat)			0,7
2.	Orang yang memasuki wilayah aman hanya diberikan akses untuk tujuan dan otorisasi tertentu		0,5	
3.	Setiap personil diwajibkan memakai tanda pengenal yang jelas.			0,8
4.	Orang tidak dikenal, tanpa pemandu dan tidak mempunyai tanda pengenal, harus ditanyai tentang keperluan dan identitasnya.			0,7

Tabel3.6 (Lanjutan)

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)				
Klausul 9.1 Wilayah Aman				
ISO 27002 9.1.2 Kontrol masuk fisik				
Kontrol : Wilayah aman (*secure*) harus dilindungi dengan kontrol akses masuk yang memadai untuk memastikan hanya orang yang berhak saja dibolehkan masuk.				
No.	PERNYATAAN	Bobot		
		Rendah (0,1-0,3)	Cukup (0,4-0,6)	Tinggi (0,7-1,0)
5.	Hak akses ke wilayah aman harus dikaji ulang		0,4	
6.	Desain wilayah aman telah memperhitungkan terjadinya kerusakan akibat dari bencana alam, lingkungan atau ulah manusia	0,2		

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 Tabel3.7.

Tabel3.7Contoh PertanyaanPada Kontrol Keamanan Fisik dan Lingkungan

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)			
	Auditor	: Dewangga Putra Sejati	
	Auditee	: Bpk. Basuki Bpk. Gilang	
	Tanggal	:	
	Tanda Tangan	:	
Klausul 9.1 Wilayah Aman (*Secure Areas*)			
ISO 27002 9.1.2 Kontrol masuk fisik			
1	Terdapat pengawasan terhadap orang yang datang (Tanggal dan waktu berkunjung ke wilayah aman harus dicatat)		

Tabel 3.7 (Lanjutan)

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	Auditor	: Dewangga Putra Sejati
	Auditee	: Bpk. Basuki Bpk. Gilang
	Tanggal	:
	Tanda Tangan	:
Klausul 9.1 Wilayah Aman (*Secure Areas*)		
ISO 27002 9.1.2 Kontrol masuk fisik		
	P: Bagaimana kontrol pengamanan terhadap orang lain/bukan karyawan yang datang? Bagaimana antisipasi terhadap orang yang berkunjung di luar jam kerja? J:	
2	Orang yang memasuki wilayah aman hanya diberikan akses untuk tujuan dan otorisasi tertentu	
	P: Pada tempat atau wilayah yang aman , orang lain selain karyawan hanya dibolehkan melakukan kegiatan apa saja? J: P: Apabila orang selain karyawan tersebut melakukan suatu hal yang melanggar tujuan dan otoritas tertentu, bagaimana pihak perusahaan menanggapinya? Apakah ada sanksi khusus bagi orang luar yang melanggar tersebut? J:	

3.3 Tahap Pelaksanaan Audit

Pada tahap ini langkah-langkah yang dilakukan yaitu:1.Melakukan wawancara pada pihak terkait, 2.Melakukanpemeriksaan data danpenyusunan daftar temuan audit dan rekomendasi,3. Melakukan uji kematangan, 4.Konfirmasi temuan dan rekomendasi audit. Pada tahap ini akan menghasilkan dokumen hasil wawancara,dokumen hasil pemeriksaan data, hasil uji kematangan, daftar temuan dan rekomendasi.

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 hasil wawancara yang berisi catatan informasi yang diperoleh dan analisis yang dilakukan selama proses audit. Berikut adalah salah satu hasil wawancara pada klausul 9 (Sembilan) Keamanan Fisik dan Lingkungan dengan obyek kontrol 9.1.1 Pembatas keamanan fisik (*Physical security perimeter*)Tabel 3.8.

Tabel 3.8Hasil Wawancara Klausul 9 (Sembilan) Keamanan Fisik dan Lingkungan

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)		**Auditor : Dewangga Putra Sejati** **Auditee : TAUCHID HARSONO, SPt** **NIP. 196510181985031003** **Tanggal : 04 April 2016** **Tanda tangan :**
Klausul 9.1 Wilayah Aman (*Secure Areas*)		
ISO 27002 9.1.2 Kontrol masuk fisik		
1	Terdapat pengawasan terhadap orang yang datang (Tanggal dan waktu berkunjung ke wilayah aman harus dicatat)	
	P: Bagaimana kontrol pengamanan terhadap orang lain/bukan karyawan yang datang? Bagaimana antisipasi terhadap orang yang berkunjung di luar jam kerja? J: Setiap tamu/pengunjung yang masuk ke wilayah aman RRI selalu di dampingi, diawasi CCTV, bila pengunjung datang diluar jam kerja maka harus menunggu diluar dan menunggu sampai admin datang.	

Tabel 3.8 (Lanjutan)

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	**Auditor : Dewangga Putra Sejati** **Auditee : TAUCHID HARSONO, SPt NIP. 196510181985031003** **Tanggal : 04 April 2016** **Tanda tangan :**
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.2 Kontrol masuk fisik	
2	Orang yang memasuki wilayah aman hanya diberikan akses untuk tujuan dan otorisasi tertentu
	P: Pada tempat atau wilayah yang aman , orang lain selain karyawan hanya dibolehkan melakukan kegiatan apa saja? J: Hanya sebatas meminta pengajaran (kepentingan magang untuk SMK/Perguruan tinggi). Bila sangat mendesak maka didampingi serta diawasi kepentinganya. P: Apabila orang selain karyawan tersebut melakukan suatu hal yang melanggar tujuan dan otoritas tertentu, bagaimana pihak perusahaan menanggapinya? Apakah ada sanksi khusus bagi orang luar yang melanggar tersebut? J: Mendapat teguran keras atau dilaporkan pihak berwajib.

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 Kepala Seksi PMB. 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 3.9.

Tabel 3.9 Contoh Dokumen Pemeriksaan Data Audit Pada Kontrol Keamanan Fisik dan Lingkungan

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	Pemeriksa : Dr. Haryanto Tanuwijaya, S.Kom., M.MT. Auditor : Dewangga Putra Sejati Auditee : Gilang Setio Nugroho Tanggal : 22 Maret – 30 Maret 2016 Tanda Tangan :		
Klausul 9.1 Wilayah Aman (*Secure Area*)			
ISO 27002 9.1.2 Kontrol masuk fisik			
No.	Pemeriksaan	Catatan Pemeriksa	Catatan Review
1.	Identifikasi pengawasan terhadap orang yang datang Dengan cara 1. Wawancara 2. Survey	Telah diperiksa bahwa ada kontrol bagi orang yang datang di luar jam kerja, yaitu harus menemui pihak security dan akan ditanyai apa keperluannya.	
2.	Identifikasi orang yang memasuki wilayah aman hanya diberikan akses untuk tujuan dan otorisasi tertentu Dengan cara 1. Wawancara 2. Survey	Telah diperiksa bahwa selain karyawan hanya diperbolehkan melakukan kegiatan yang berkaitan dengan urusan dinas saja. Apabila ada orang-lain yang melakukan di luar urusan dinas maka akan berurusan langsung dengan pihak keamanan.	

3.3.3 Melakukan Uji Kematangan

Setelah melakukan pemeriksaan dan mendokumentasikan bukti-bukti audit, maka langkah selanjutnya yaitu melakukan perhitungan *maturity level*. Setiap pernyataan dinilai tingkat kepatutanya sesuai dengan hasil pemeriksaan yang ada menggunakan kriteria penilaian yang ada dalam standar penilaian

maturity level. Tingkat kriteria yang digunakan meliputi *initial* yang memiliki nilai 1 (satu), *managed*yang memiliki nilai 2 (dua), *defined* yang memiliki nilai 3 (tiga), *quantitatively managed* yang memiliki nilai 4 (empat), dan *optimizing* yang memiliki nilai 5 (lima).Contoh kerangka kerja perhitungan *maturity level* dapat dilihat pada Tabel 3.10.Perhitungan tersebut dilakukan secara bertahap, berikut tahapan yang harus dilakukan adalah:

a. Setiap pernyataan pada kontrol keamanan diberikan angka bobot yang sesuai.
b. Dari hasil wawancara didapatkan nilai tingkat kematangan pada setiap pernyataan yaitu angka 1 (satu) sampai angka 5 (lima).
c. Nilai Pada setiap pernyataan bobot dikalikan dengan tingkat kematangan masing-masing.
d. Tingkat kematangan dihasilkan dari perhitungan total nilai dari perkalian bobot dan tingkat kematangan dibagi dengan jumlah bobot yang ada pada seluruh pernyataan dalam satu kontrol keamanan.
e. Hasil dari tahapan sebelumnya merupakan nilai tingkat kematangan pada kontrol keamanan tersebut.

Tabel3.10 Contoh penentuan tingkat kematangan pada klausul 8 KeamananSumber Daya Manusia

Klausul 8 (keamanan sumber daya manusia)										
Klausul 8.3 Pemberhentian atau pemindahan pegawai										
ISO 27002 8.3.1 Tanggung jawab pemberhentian				Tingkat kematangan						
				1	2	3	4	5		
No	Pernyataan	Hasil Pemeriksaan	Bobot	Initial	Managed	Defined	Quantitaively Managed	Optimized	Nilai	
1.	Terdapat pertanggung jawaban dalam mengkomunikasikan terminasi	Dokumentasi mengenai mengkomunikasikan terminasi di tinjau kembali dengan melihat peraturan TUPOKSI. Lampiran: tupoksi	0,6			√			1,8	
Total bobot			0,6	Tingkat Kematangan		3		Total nilai	1,8	

3.3.4 Konfirmasi Temuan dan Rekomendasi Audit

Pada proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah menentukan nilai bobot dari hasil temuan dengan kategori rendah (0,1-0,3), cukup (0,4-0,6), dan tinggi (0,7-1,0) yang sudah disepakati oleh auditor dan *auditee*, nilai tingkat kematangan yang dihasilkan selanjutnya dipadukan dengan keterkaitan refrensi antar klausul pada ISO 27002:2005, maka dibuatlah rekomendasi berdasarkan 3 kategori, yaitu: manajemen, teknikal, dan operasional mengacu pada ISO 27002:2005 untuk proses perbaikan keamanan informasi di bagian PMB RRI Surabaya. Seluruh aktivitas tersebut menghasilkan bukti *(evidence)* yang berarti terkait dengan sistem yang berlangsung di instansi.

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 3.11.

Tabel 3.11Contoh Lampiran Temuan dan Rekomendasi Pada Klausul 9 (Sembilan) Kemanan Fisik dan Lingkungan

<table>
<tr><td colspan="5">TEMUAN AUDIT KEAMANAN SISTEM INFORMASI</td><td>Auditor: Dewangga
Auditee:TAUCHID HARSONO</td></tr>
<tr><td colspan="5">ASPEK : KLAUSUL 8 (KEAMANAN FISIK DAN LINGKUNGAN)
ISO 27002 9.1.1 Pembatas Keamanan Fisik (Physical Security Perimeter)</td><td>Tanggal :
Tanda tangan :</td></tr>
<tr><td>No</td><td>Pernyataan</td><td>Temuan</td><td>Ref</td><td>Referensi, Penyebab Risiko dan Rekomendasi</td><td>Tanggapan dan Komitmen Penyelesaian</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

3.4 Tahap Pelaporan Audit Keamanan Sistem Informasi

Tahap pelaporan ada beberapa langkah yang dilakukan yaitu: 1. Permintaan tanggapan atas daftar temuan audit, 2. Penyusunan draft laporan audit, 3. Persetujuan draft laporan audit, dan 4.pelaporan hasil audit. Pada tahap ini akan menghasilkan hasil daftar temuan audit dan rekomendasi, dan pertemuan penutup, notulen pertemuan penutup audit.

3.4.1 Permintaan Tanggapan Atas Daftar Temuan Audit

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

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, obyektif, lengkap, jelas, dan lugas.Output yang dihasilkan adalah draft laporan audit yang berdasarkan daftar pertanyaan, temuan dan tanggapan maka auditorharus menyusunan *draft* laporan audit yang telah selesai dilaksanakan oleh auditor.

3.4.3 Persetujuan *Draft* Laporan Audit

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 Pelaporan Hasil Audit

Pertemuan penutup audit keamanan sistem informasi dilakukan untuk melaporkan hasil audit keamanan sistem informasi kepada pihak PMB, memberikan penjelasan kepada pihak PMB 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.