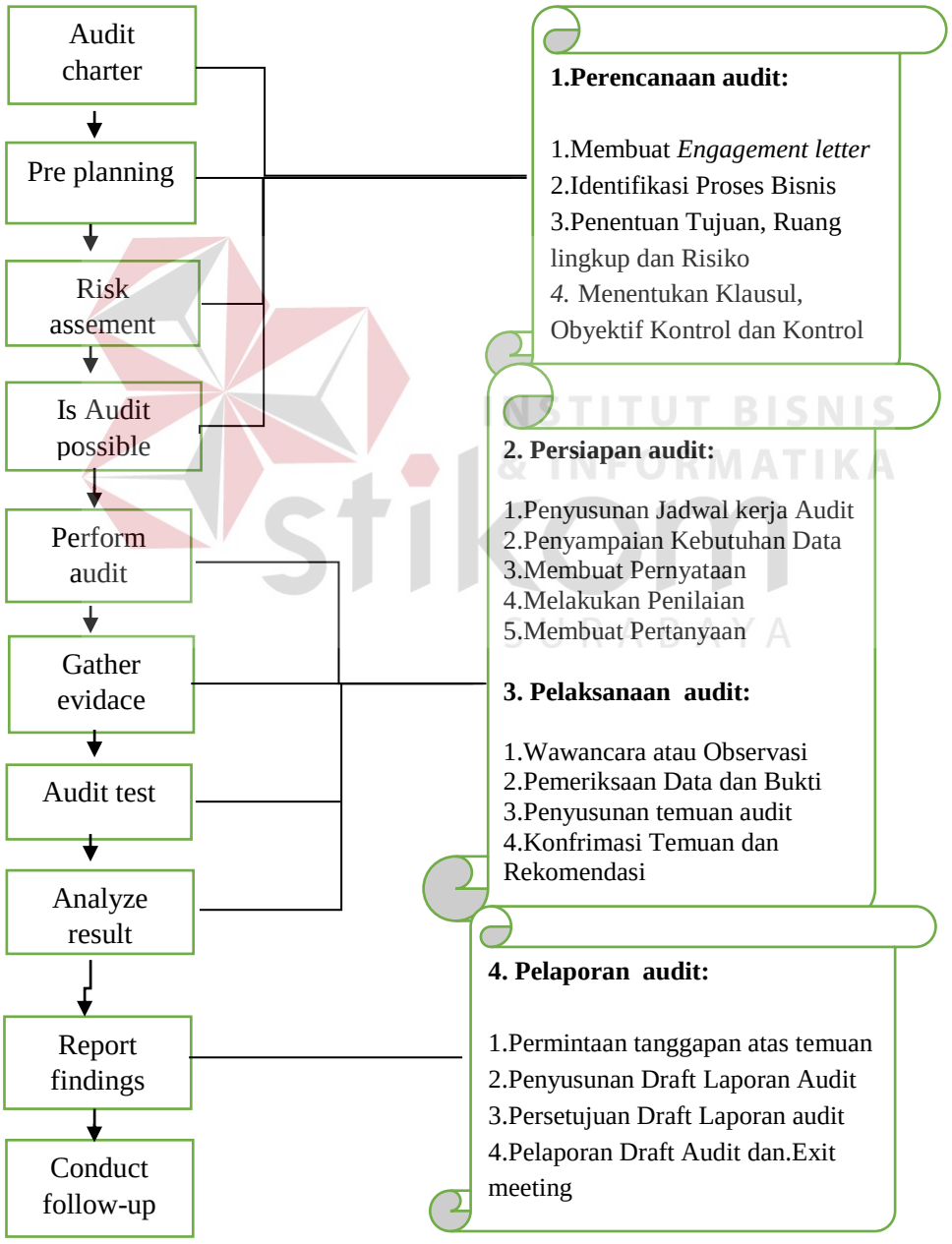
BAB III

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.



Gambar 3.1 Metode Penelitian Audit Keamanan Sistem Informasi

3.1 Tahap Perencanaan Audit

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Membuat *Engagement letter*, 2. Melakukan identifikasi proses bisnis, 3. Melakukan penentuan ruang lingkup, tujuan audit dan risiko, 4. Menentukan Klausul, Obyektif Kontrol dan Kontrol. Tahap ini akan menghasilkan pengetahuan tentang proses bisnis TI perusahaan, ruang lingkup dan tujuan yang telah ditentukan serta klausul yang telah ditentukan.

3.1.1 Membuat *Engagement letter*

Pada tahap ini seorang auditor membuat surat kesepakatan atau keterikatan dengan klien untuk berkomitmen menjaga dan mentaati persetujuan dan peraturan yang telah dibuat selama audit dilakukan. Surat perjanjian tersebut dinamakan *enggagement letter*. Keluaran pada tahap ini adalah *enggagement letter* yang berisi :

a. Pendahuluan
b. Peran Auditor
c. Tujuan
d. Tugas dan Tanggung jawab auditor (*responsibility*)
e. Kewenangan dan Kode etik
f. Ruang Lingkup
g. Pengesahan dan Waktu Pelaksanaan Audit

3.1.2 Identifikasi Proses Bisnis

Dalam perencanaan proses audit, auditor harus melakukan pemahaman proses bisnis dan TI perusahaan yang akan diaudit. Pemahaman dilakukan dengan cara mempelajari dokumen-dokumen yang terkait dengan perusahaan, yaitu profil perusahaan, visi dan misi DPPKD Lombok Barat, struktur organisasi DPPKD, gambaran umum Instalasi SIMDA, dan proses bisnis dan TI SIMDA. Auditor juga harus mengetahui apakah sebelumnya perusahaan telah dilaksanakan proses audit. Apabila pernah maka auditor juga mengetahui tentang laporan audit periode sebelumnya.

Untuk identifikasi proses bisnis pada perusahaan langkah yang dilakukan adalah dengan cara mengetahui dan memeriksa dokumen-dokumen yang terkait dengan proses audit, wawancara manajemen dan staf, serta melakukan observasi kegiatan operasional dan teknologi sistem informasi yang digunakan.

Keluaran yang di hasilkan pada tahap ini adalah:

a. Profil perusahaan,
b. Visi, misi, dan prinsip & managemen,
c. Struktur organisasi,
d. Bukti dan pernyataan bahwa auditor telah melihat serta mempelajari dokumen yang terkait dengan perusahaan.

3.1.3 Penentuan Tujuan, Ruang Lingkup dan Risiko

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 Instalasi SIMDA DPPKD Lombok Barat, Pada proses ini, langkah yang

selanjutnya dilakukan adalah mengidentifikasi tujuan yang berhubungan dengan kebutuhan audit keamanan sistem informasi. Keluaran yang dihasilkan pada tahap ini adalah hasil ruang lingkup, objek audit dan tujuan audit.

3.1.4 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 pada DPPKD. Menentukan klausul, obyektif kontrol dan kontrol yang sesuai dengan kendala dan kebutuhan Pada Simda. Klausul, obyektif kontrol dan kontrol yang ditentukan harus berdasarkan kesepakatan antara auditor dengan *auditee*. Keluaran yang dihasilkan pada tahap ini adalah hasil pemilihan klausul, klausul 8 (keamanan sumber daya manusia), klausul 9 (keamanan fisik dan lingkungan), klausul 11 (kontrol akses).

3.2 Tahap Persiapan Audit

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Melakukan penyusunan jadwal kerja audit, 2. Penyampaian kebutuhan data, 3. Membuat pernyataan yang telah dibuat berdasarkan standar ISO 27002, 4. Melakukan pembobotan dan 5. Membuat pertanyaan.

3.2.1 Penyusunan Jadwal Kerja Audit

Audit *working plan* merupakan dokumen yang dibuat oleh auditor dan digunakan untuk merencanakan dan memantau pelaksanaan audit keamanan sistem informasi secara terperinci. Keluaran yang dihasilkan pada tahap ini berupa rincian rencana kerja dari auditor dalam pelaksanaan audit nantinya berupa daftar

susunan jadwal kerja audit. Penyusunan jadwal kerja ini dapat dilihat pada Tabel 3.1

Tabel 3.1. *Working Plan* Secara Keseluruhan

ID	Task Name	Start	Finish
2	Perencanaan Audit Sistem Informasi 1. Membuat engagemet letter 2. Identifikasi proses bisnis 3. Penentuan tujuan, ruang lingkup dan resiko 4.		
10	Persiapan Audit Sistem Informasi 1. Penyusunan jadwal kerja audit 2. Penyampaian kebutuhan data 3. Membuat pertanyaan 4. Melakukan pembobotan 5. Membuat pernyataan		
13	Pelaksanaan Audit Sistem Informasi 1. Wawancara dan observasi 2. Pemeriksaan data dan bukti 3. Penyusunan temuan audit 4. Temuan dan rekomendasi		
21	Pelaporan Audit Sistem Informasi 1. Penyusunan draft laporan audit 2. Persetujuan darft laporan audit 3. Pelaporan darft audit 4. Exit meeting		

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. Keluaran yang dihasilkan pada tahap ini adalah daftar penyampaian kebutuhan data pada instansi. Penyampaian kebutuhan data dapat di lihat pada Tabel 3.2.

Tabel 3.2. 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 *bagian DPPKD*					
3	*Job description* pegawai di DPPKD					
4	Alur proses bisnis insatansi					
5	Dokumen kebijakan keamanan sistem informasi					
6	Dokumen prosedur aplikasi simda					

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. Keluaran yang dihasilkan pada tahap ini adalah contoh pernyataan pada klausul 8 (delapan) Keamanan Sumber Daya

Manusia dengan obyek kontrol 8.1.1 (Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*) dapat dilihat pada Tabel 3.3

Tabel 3.3. Contoh Pernyataan Pada Kontrol Keamanan Sumber Daya Manusia

PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	
Klausul 8.1 Keamanan Sumber Daya Manusia Sebelum Menjadi Pegawai (*Prior to Employement*)	
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)	
Kontrol : Aturan-aturan dan tanggung jawab keamanan dari pegawai, kontraktor dan pengguna pihak ketiga harus didefinisikan, didokumentasikan sesuai dengan kebijakan keamanan informasi organisasi	
No.	PERNYATAAN
1	Terdapat peraturan pada proses penerimaan pegawai
2	Terdapat dokumentasi kebijakan organisasi aturan dan tanggung jawab penerapan keamanan aset
3	Terdapat dokumentasi kebijakan organisasi aturan dan tanggung jawab pemeliharaan keamanan aset
4	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan asset

3.2.4 Melakukan Penilaian

Setelah membuat pernyataan, maka langkah selanjutnya adalah melakukan pengukuran penilaian pada setiap pernyataan. Pada setiap pernyataan yang telah dibuat harus ditentukan nilainya masing-masing, karena setiap pernyataan tersebut tidak bernilai sama dalam penerapannya untuk kontrol keamanan yang telah ditentukan. Metode ini menggunakan penilaian resiko metode kualitatif, karena menurut Sarno dan Iffano (2009: 89) resiko memiliki hubungan dengan keamanan informasi dan resiko merupakan dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi. Keluaran yang dihasilkan pada tahap ini adalah seperti pemberiaan penilaian pada setiap pernyataan yang telah di berikan oleh auditor contoh penilaian pada klausul

11 dengan kontrol 11.5.3 bisa dilihat pada Tabel 3.5 dan contoh Tabel penilaian resiko bisa dilihat pada Tabel 3.4.

Tabel 3.4. Penilaian Resiko

Resiko	Penilaian
Low	0,1-0,3
Medium	0,4-0,6
High	0,7-1,0

Sumber : Niekerk dan Labuschagne dalam Hastin, 2012:39

Tabel 3.5 Contoh Penilaian Pada Klausul 11 Dengan Kontrol 11.5.3 Sistem Manajemen *Password.*

Klausul 11.5 Kontrol Akses Sistem Operasi				
ISO 27002 11.5.3 Sistem Manajemen *Password*				
Kontrol: Sistem yang digunakan untuk mengelola password harus interaktif dan harus dipastikan passwordnya berkualitas.				
No.	PERNYATAAN	Penilaian		
		Low (0,1-0,39)	Medium (0,4-0,69)	High (0,7-1,0)
1.	Terdapat manajemen password dengan cara memastikan pengguna password individu untuk menjaga tingkat kebenarannya		0,4	
2.	Terdapat kepastian dalam pemilihan password yang berkualitas		0,6	
3.	Terdapat pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi untuk memperbolehkan dalam kesalahan inputan		0,6	
4.	Terdapat pernyataan mengenai larangan menampilkan password di layar ketika dimasukkan			0,7
5.	Terdapat penyimpanan files password terpisah dari data sistem aplikasi	0,3		
6.	Terdapat pemilihan password saat melakukan pengubahan pada log-on pertama yang dilakukan pengguna itu sendiri		0,6	
7.	Terdapat penyimpana catatan password pengguna sebelumnya secara aman		0,5	
8.	Terdapat penyimpanan password dalam bentuk enkripsi menggunakan algoritma enkripsi one-way		0,5	

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 bisa dilihat pada Tabel 3.6.

Tabel 3.6 Contoh Pertanyaan Pada Klausul 11 Dengan Kontrol 11.5.3 Sistem Manajemen *Password.*

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)	
ISO 27002 11.5.3 Sistem Manajemen *Password*	
1	Terdapat manajemen password dengan cara memastikan pengguna password individu untuk menjaga tingkat kebenarannya
	P: Apakah manajemen password sudah memastikan pengguna password telah menjaga tingkat kebenarannya? J: P: Apakah terdapat dokumentasi khusus mengenai manajemen password sehingga dapat menjaga tingkat kebenarannya? J: P: Bagaimana mensosialisasikan pentingnya manajemen password individu kepada pengguna sehingga dapat menjaga tingkat kebenarannya? J:
2	Terdapat kepastian dalam pemilihan password yang berkualitas
	P: Apakah terdapat pemilihan password berkualitas? J: P: Apa saja kriteria dalam pemilihan password berkualitas? J: P: Apakah telah dilakukan kepastian tiap penggunanya bahwa dia telah memiliki password yang berkualitas? J:
3	Terdapat pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi untuk memperbolehkan dalam kesalahan inputan
	P: Apakah pengguna diberikan pemilihan password? J:

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)	
ISO 27002 11.5.3 Sistem Manajemen *Password*	
	P: Apakah pengguna diberikan hak dalam pengubahan password? J: P: Apakah ada prosedur konfirmasi dalam memperbolehkan dalam kesalahan inputan? J:
4	Terdapat pernyataan mengenai larangan menampilkan password di layar ketika dimasukkan
	P: Apakah layar sudah sudah tidak menampilkan password ketika dimasukkan? J: P: Apa bukti tidak menampilkan password yang dimasukkan? J: P: Apakah keseluruhan layar pada staf pengguna sudah tidak menampilkan password ketika dimasukkan? J:
5	Terdapat pemilihan password saat melakukan pengubahan pada log-on pertama yang dilakukan pengguna itu sendiri
	P: Apakah terdapat pemilihan password saat melakukan pengubahan pada log-on pertama kali? J: P: Apakah dalam pemilihan password saat melakukan pengubahan pada log-on pertama dilakukan sudah dilakukan oleh keseluruhan pengguna? J: P: Apakah pemilihan password dilakukan pengguna itu sendiri? J:
6	Terdapat penyimpana catatan password pengguna sebelumnya secara aman
	P: Apakah penyimpanan catatan password pengguna sebelumnya sudah dilakukan secara aman? J: P: Bagaimana cara mengamankan penyimpanan catatan password pengguna sebelumnya? J:

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)	
ISO 27002 11.5.3 Sistem Manajemen *Password*	
	P: Apakah pengguna benar benar menjamin bahwa penyimpanan password yang dilakukan sudah benar benar aman? J:
7	Terdapat penyimpanan password dalam bentuk enkripsi menggunakan algoritma enkripsi one-way
	P: Apakah penyimpanan password dalam bentuk enkripsi? J: P: Apakah menggunakan algoritma enkripsi one-way pada penyimpanan password? J: P: Apa alternative lain jika organisasi tidak menggunakan algoritma enkripsi one-way? J:

3.3 Tahap Pelaksanaan Audit

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

3.3.1 Melakukan Wawancara dan Observasi

Pada proses ini langkah yang dilakukan adalah melakukan wawancara berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan terhadap pihak-pihak yang terlibat dalam eksekusi. Proses TI yang dapat terbagi menjadi 4 kelompok, yaitu: pihak yang bertanggung jawab terhadap kesuksesan aktivitas

(*responsible*), pihak yang bertanggung jawab (*accountable)*, pihak yang mengerti aktivitas (*consulted*), dan pihak yang senantiasa diinformasikan perihal perkembangan aktivitas (*informed*). Keluaran yang dihasilkan pada tahap ini adalah dokumen wawancara yang berisi catatan informasi yang diperoleh dan analisis yang dilakukan selama proses audit dapat dilihat pada Tabel 3.7.

Tabel 3.7 Contoh Wawancara Pada Klausul 11 Dengan Kontrol 11.5.3 Sistem Manajemen *Password.*

KUISONER **KLAUSUL 11(KONTROL AKSES)**		**Auditor : Riyadi Atmajaya**
		Auditee : Normansyah, SE **NIP. 19810921 20050011**
		Tanggal : 13 Juli
		Tanda tangan :
AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)		
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)		
ISO 27002 11.5.3 Sistem Manajemen *Password*		
1	Terdapat manajemen password dengan cara memastikan pengguna password individu untuk menjaga tingkat kebenarannya	
	P: Apakah manahemen password memastikan pengguna password individu sudah terjaga tingkat kebenarannya? J: P: Apakah terdapat dokumentasi khusus mengenai manajemen password sehingga dapat menjaga tingkat kebenarannya? J: P: Bagaimana mensosialisasikan pentingnya manajemen password individu kepada pengguna sehingga dapat menjaga tingkat kebenarannya? J:	
2	Terdapat kepastian dalam pemilihan password yang berkualitas	
	P: Apakah terdapat pemilihan password berkualitas? J: P: Apa saja kriteria dalam pemilihan password berkualitas? J: P: Apakah telah dilakukan kepastian tiap penggunanya bahwa dia telah	

KUISONER **KLAUSUL 11(KONTROL AKSES)**	**Auditor : Riyadi Atmajaya**
	Auditee : Normansyah, SE **NIP. 19810921 20050011**
	Tanggal : 13 Juli
	Tanda tangan :
AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)	
ISO 27002 11.5.3 Sistem Manajemen *Password*	
	memiliki password yang berkualitas? J:
3	Terdapat pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi untuk memperbolehkan dalam kesalahan inputan
	P: Apakah pengguna diberikan pemilihan password? J: P: Apakah pengguna diberikan hak dalam pengubahan password? J: P: Apakah ada prosedur konfirmasi dalam memperbolehkan dalam kesalahan inputan? J:
4	Terdapat pernyataan mengenai larangan menampilkan password di layar ketika dimasukkan
	P: Apakah layar sudah sudah tidak menampilkan password ketika dimasukkan? J: P: Apa bukti tidak menampilkan password yang dimasukkan? J: P: Apakah keseluruhan layar pada staf pengguna sudah tidak menampilkan password ketika dimasukkan? J:
5	Terdapat pemilihan password saat melakukan pengubahan pada log-on pertama yang dilakukan pengguna itu sendiri
	P: Apakah terdapat pemilihan password saat melakukan pengubahan pada log-on pertama kali? J: P: Apakah dalam pemilihan password saat melakukan pengubahan pada log-on pertama dilakukan sudah dilakukan oleh keseluruhan pengguna?

KUISONER **KLAUSUL 11(KONTROL AKSES)**	**Auditor : Riyadi Atmajaya**
	Auditee : Normansyah, SE **NIP. 19810921 20050011**
	Tanggal : 13 Juli
	Tanda tangan :

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)	
ISO 27002 11.5.3 Sistem Manajemen *Password*	
	J: P: Apakah pemilihan password dilakukan pengguna itu sendiri? J:
6	Terdapat penyimpana catatan password pengguna sebelumnya secara aman
	P: Apakah penyimpanan catatan password pengguna sebelumnya sudah dilakukan secara aman? J: P: Bagaimana cara mengamankan penyimpanan catatan password pengguna sebelumnya? J: P: Apakah pengguna benar benar menjamin bahwa penyimpanan password yang dilakukan sudah benar benar aman? J:
7	Terdapat penyimpanan password dalam bentuk enkripsi menggunakan algoritma enkripsi one-way
	P: Apakah penyimpanan password dalam bentuk enkripsi? J: P: Apakah menggunakan algoritma enkripsi one-way pada penyimpanan password? J: P: Apa alternative lain jika organisasi tidak menggunakan algoritma enkripsi one-way? J:

3.3.2 Pemeriksaan Data dan Bukti

Pemeriksaan data dilakukan dengan cara melakukan observasi dan melakukan wawancara kepada *auditee* sesuai dengan ruang lingkup simda serta klausul yang telah disepakati oleh kepala bidang terkait. Keluaran yang dihasilkan pada tahap ini adalah untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Bukti-bukti tersebut berupa foto dan data.

3.3.3 Penyusunan Daftar Temuan Audit

Pada proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah memeriksa data profil perusahaan, kebijakan, standar, Prosedur dan portofolio serta mengobservasi *standard operating procedure* dan melakukan wawancara kepada *auditee.* 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. Keluaran yang dihasilkan pada tahap ini adalah daftar temuan masalah yang didapat saat melaksanakan audite dan rekomendasi bagi instansi.

3.3.4 Konfrimasi Temuan 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 instansi.

3.4 Tahap Pelaporan Audit

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. Keluaran yang dihasilkan pada tahap ini adalah 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 ini nantinya akan di susun secara rapi guna untuk dokumentasi pelaporan audit. Keluaran yang dihasilkan pada tahap ini 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

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. Keluaran yang dihasilkan pada tahap ini adalah laporana audit yang sudah terdokumentasi yang siap di terbitkan sebagai laporan audit.

3.4.4 Pertemuan Penutup atau Pelaporan Hasil Audit

Pertemuan penutup audit keamanan sistem informasi dilakukan untuk melaporkan hasil audit keamanan sistem informasi kepada manajemen, meberikan 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. Keluaran yang dihasilkan dari tahap ini adalah dokumentasi dalam bentuk risalah atau notulen pertemuan penutup audit.