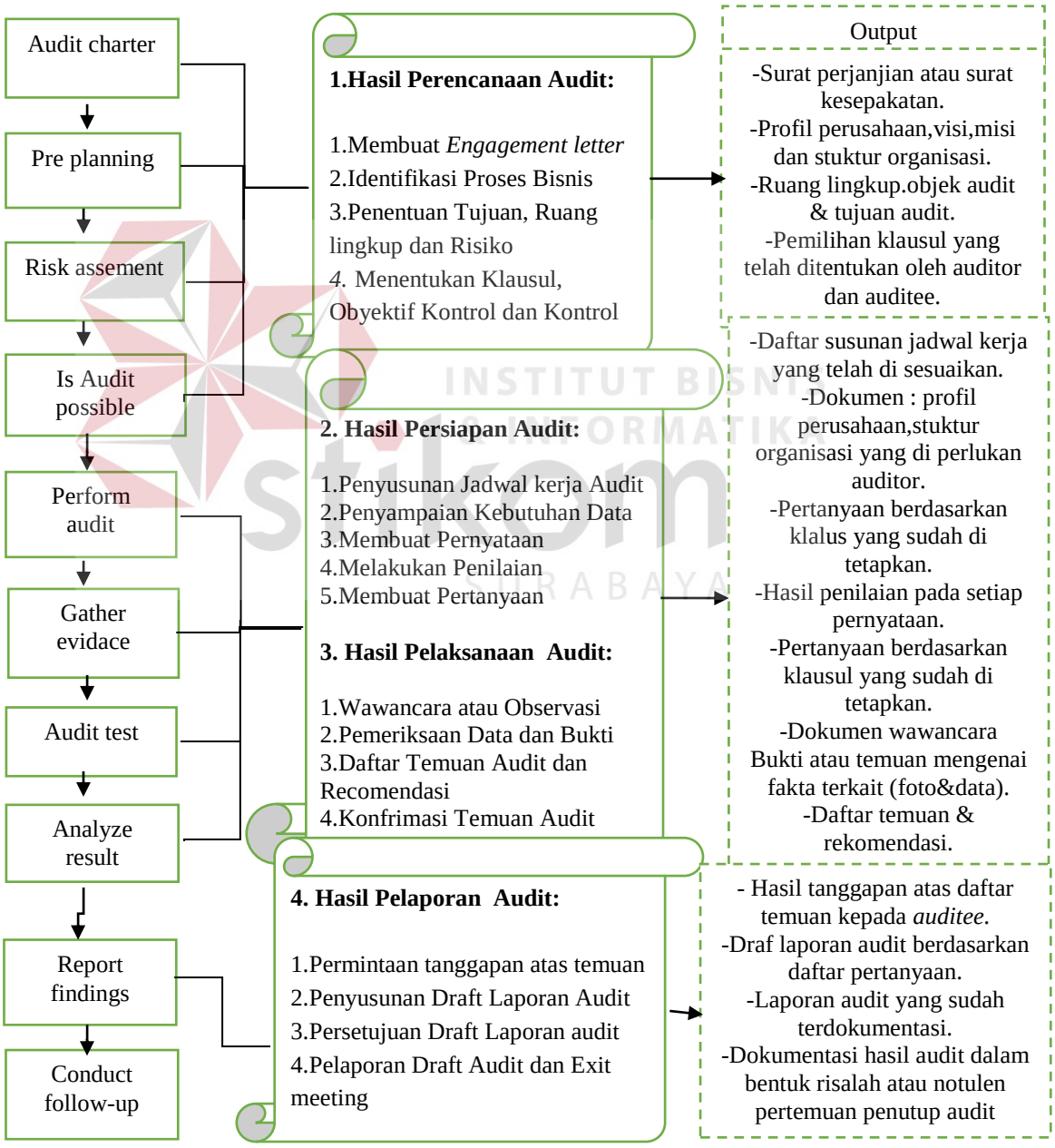
BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini akan diuraikan tentang hasil dan pembahasan bab III dari tahap perencanaan audit, tahap persiapan audit, tahap pelaksanaan, serta tahap pelaporan audit keamanan sistem informasi. Dapat dilihat pada Gambar 4.1



Gambar 4.1 Metode Penelitian Audit Keamanan Sistem Informasi

4.1 Tahap Perencanaan Audit Keamanan Sistem Informasi

Hasil dari tahapan perencanaan ini berupa: 1. Hasil perjanjian audit berupa surat perjanjian audit atau *Engagement Letter*, 2. Hasil pemahaman proses bisnis yang telah dilihat, 3. Hasil penentuan ruang lingkup objek audit & tujuan audit, 4.) Hasil penentuan klausul, objektif kontrol.

4.1.1 Hasil Surat Perjanjian Audit atau Engagement Letter

Hasil dari surat perjanjian kontrak kerja audit yang telah di sepakati oleh auditor dan auditee atau *Engagement Letter* ini berisi beberapa poin di dalamnya selengkapnya dapat dilihat pada Lampiran 1 dan berisi poin sebagai berikut.

a. Peran auditor
b. Tujuan auditor
c. Tugas dan tanggung jawab auditor
d. Kewenangan dan kode etik auditor
e. Ruang lingkup auditor
f. Bentuk laporan
g. Akses auditor
h. Pengesahan dan waktu pelaksanaan

4.1.2 Hasil Identifikasi Proses Bisnis

Hasil pada pemahaman proses bisnis ini adalah seorang auditor harus mengetahui segala kegiatan yang berlangsung di perusahaan sebelum dilakukan audit dengan cara memahami dokumen perusahaan, Hasil yang didapat setelah melakukan identifikasi proses bisnis yaitu profil Nusa Tenggara Barat, visi dan misi DPPKD Lombok Barat, profil Dinas Pendapatan Dan Pengelolaan Keuangan

Daerah, struktur organisasi DPPKD Lombok Barat, *Job description* pegawai DPPKD Lombok Barat, proses bisnis DPPKD Lombok Barat.

1. Profil Lombok Barat

   Pada tahun 1968 dalam situasi yang masih belum menggembirakan sebagai akibat berbagai krisis nasional yang membias ke daerah, gubernur pertama AR. Moh. Ruslan Tjakraningrat digantikan oleh HR.Wasita Kusuma. Dengan mulai bergulirnya program pembangunan lima tahun tahap pertama (pelita I) langkah perbaikan ekonomi, sosial, politik mulai terjadi. Pada tahun 1978 H.R.Wasita Kusuma digantikan H.Gatot Soeherman sebagai Gubernur Provinsi NTB yang ketiga. Dalam masa kepemimpinannya, usaha-usaha pembangunan kian dimantapkan dan Provinsi NTB yang dikenal sebagai daerah minus, berubah menjadi daerah swasembada. Pada tahun 1988 Drs. H. Warsito, SH terpilih memimpin NTB menggantikan H. Gatot Soeherman. Drs.H.Warsito, SH mengendalikan tampuk pemerintahan di Provinsi NTB untuk masa dua periode, sebelum digantikan Drs. H. Harun Al Rasyid, M.Si pada tanggal 31 Agustus 1998.

   Drs. H. Harun Al Rasyid M.Si berjuang membangun NTB dengan berupaya meningkatkan kualitas sumber daya manusia melalui Program Gema Prima. Tahun 2003 hingga 1 september 2008 Drs. H. Lalu Serinatadan wakil Gubernur Drs.H.B. Thamrin Rayes memimpin NTB. Pada masa ini berbagai macam upaya dilakukan dalam membangun NTB dan mengejar ketertinggalan diberbagai bidang dan sektor. Di zaman ini, Sejumlah program diluncurkan, seperti Gerbang E-Mas dengan Program Emas Bangun Desa. Selain itu, pada

masa ini pembangunan Bandara Internasional Lombok di Lombok Tengah mulai terealisasi dan ditargetkan rampung pertengahan 2009.

Dalam usianya yang ke-52 Provinsi NTB kini dipimpin oleh salah satu putra terbaiknya yaitu Gubernur Dr. KH. M. Zainul Majdi dan Wakil Gubernur Ir. H. Badrul Munir, MM. Pada tahun 2010 ini, kedua pasangan pemimpin menggenapkan dua tahun pemerintahannya di ProvinsiNTB untuk mengemban amanah dan harapan masyarakat Nusa Tenggara Barat dalam mencapai kesejahteraan dan pembangunan daerah menuju NTB yang Beriman dan Berdaya Saing.

2. Visi, Misi DPPKD Lombok Barat

Visi :

Terwujudnya Kemandirian Keuangan Daerah Menuju Lombok Barat Bangkit Dilandasi Nilai-Nilai Patut Patuh Patju.

Misi :

a. Menguatkan kapasitas kelembagaan dan operasi Dinas Pendapatan dan Pengelolaan Keuangan Daerah Kab. Lombok Barat.
b. Meningkatkan pendapatan daerah.
c. Memantapkan pengelolaan keuangan daerah

3. Profil DPPKD Lombok Barat

Dinas Pendapatan Dan Pengelolaan Keuangan Daerah merupakan salah satu bagian dari SKPD di lombok barat. Dalam melaksakan tugas pokok dan fungsinya, khusuusnya dlm pengelolaan keuangan DPPKD menggunakan apkilasi SIMDA. Pada tahun 2014 entitas akuntansi dan entitas pelaporan telah terdesentralisasi pada tiap Satuan Kerja Perangkat Daerah Kabupaten

Lombok Barat. Dengan diberlakukannya Permendagri No. 21 Tahun 2011 dan Peraturan Daerah Nomor 9 Tahun 2011 tentang Pembentukan Susunan Organisasi Perangkat Daerah, maka entitas akuntansi diberlakukan pada 17 (tujuh belas) dinas, 2 (dua) sekretariat, 10 (sepuluh) badan, 5 (lima) kantor, 1 (satu) Rumah Sakit Umum Daerah dan 10 (sepuluh) unit kerja kecamatan. Dimana entitas tersebut telah terdesentralisasi pada tiap Satuan Kerja Perangkat Daerah Kabupaten Lombok Barat. Sehingga pelaporan keuangan merupakan konsolidasian dari laporan keuangan entitas-entitas akuntansi tersebut bisa dilihat pada Tabel 4.1. dokumen ini juga di perkuat oleh dokumen pendukung lainnya selengkapnya dapat dilihat pada Lampiran 2.

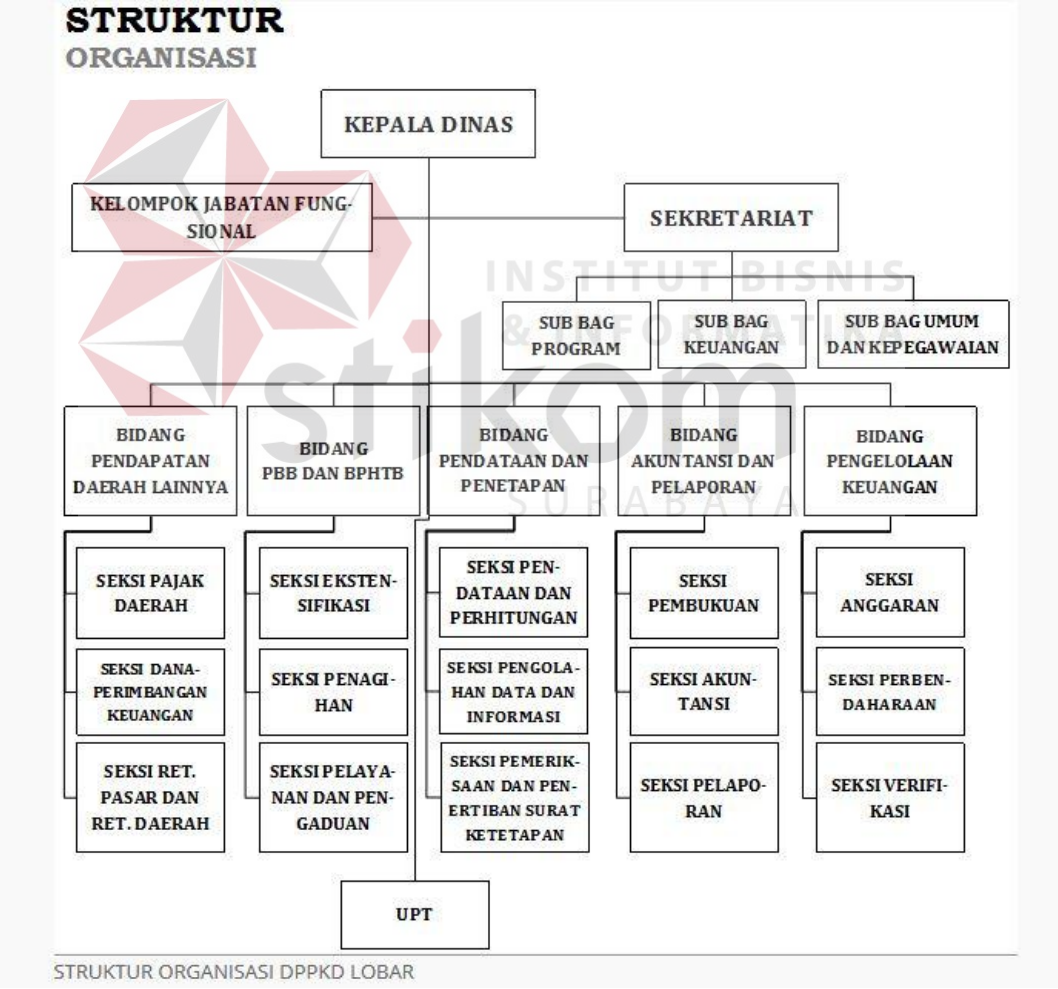
Tabel 4.1 Entitas Akuntansi Lombok Barat

TABLE ENTITAS AKUNTANSI			
NO.	**URAIAN**	**NO.**	**URAIAN**
1	Dinas Pendidikan dan Kebudayaan	24	Kecamatan Lembar
2	Dinas Kesehatan	25	Kecamatan Gerung
3	Rumah Sakit Umum Daerah	26	Kecamatan Labuapi
4	Dinas Pekerjaan Umum	27	Kecamatan Kediri
5	Dinas Tata Kota, Pertamanan dan Kebersihan	28	Kecamatan Kuripan
6	Badan Perencana Pembangunan Daerah	29	Kecamatan Narmada
7	Dinas Perhubungan Komunikasi dan Informatika	30	Kecamatan Lingsar
8	Badan Lingkungan Hidup	31	Kecamatan Gunungsari

TABLE ENTITAS AKUNTANSI			
NO.	**URAIAN**	**NO.**	**URAIAN**
9	Dinas Kependudukan dan Catatan Sipil	32	Kecamatan Batu Layar
10	Badan Keluarga Berencanan dan Pemberdayaan Perempuan	33	Kantor Ketahanan Pangan Daerah
11	Dinas Sosial Tenaga Kerja dan Transmigrasi	34	Badan Pelaksana Penyuluhan
12	Dinas Koperasi dan UMKM	35	BPMPD
13	Badan Penanaman Modal dan Perizinan Terpadu	36	Kantor Perpustakaan dan Arsip Daerah
14	Badan Kesatuan Bangsa dan Politik	37	Dinas Pertanian
15	Polisi Pamong Praja	38	Dinas Kehutanan
16	Badan Penanggulangan Bencana Daerah	39	Dinas Pertambangan
17	Sekretariat Daerah	40	Dinas Pariwisata
18	Sekretariat DPRD	41	Dinas Kelautan
19	Dinas Pendapatan dan Pengelolaan Keuangan Daerah	42	Dinas Perindustrian dan Perdagangan
20	Badan Kepegawaian Daerah	43	PPKD
21	Inspektorat	44	DPRD
22	Kantor Aset Daerah	45	Kepala Daerah
23	Kecamatan Sekotong		

Pada bagian DPPKD ini belum pernah dilakukan audit sebelumnya dan berdasarkan rekomendasi pihak instansi untuk dilakukan audit pada bagian DPPKD. Maka bagian DPPKD perlu diaudit dan diperkuat oleh dokumen Perbub No.3/2009 Pembangunan dan Pengembangan Sistem Informasi Manajemen Peraturan Bupati tentang SIMDA, dan peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja dinas pendapatan dan pengelolaan keuangan daerah lombok barat.

4. Struktur Organisasi diri DPPKD



Gambar 4.2 Struktur Organisasi DPPKD Lombok Barat

DPPKD memiliki struktur organisasi dimana didalamnya terdapat sub-sub bag yang memiliki beberapa bagian pada bidangnya masing-masing. Susunan organisasi pada DPPKD yaitu :

(1) Susunan Organisasi Dinas Pendapatan dan Pengelolaan Keuangan Daerah terdiri dari :

a. Kepala.

b. Sekretariat terdiri dari :

1. Sub Bagian Program;
2. Sub Bagian Keuangan;
3. Sub Bagian Umum dan Kepegawaian.

c. Bidang Pendapatan Daerah Lainnya terdiri dari :

1. Seksi Pajak Daerah;
2. Seksi Retribusi Pasar dan Retribusi Daerah;
3. Seksi Dana Perimbangan Keuangan.

d. Bidang PBB dan BPHTB terdiri dari :

1. Seksi Ekstensifikasi;
2. Seksi Pelayanan dan Pengaduan;
3. Seksi Penagihan.

e. Bidang Pendataan dan Penetapan terdiri dari :

1. Seksi Pendataan dan Perhitungan;
2. Seksi Pemeriksaan dan Penertiban Surat Ketetapan;
3. Seksi Pengolahan Data dan Informasi.

f. Bidang Akuntansi dan Pelaporan terdiri dari :

1. Seksi Pembukuan;

2. Seksi Akuntansi;
3. Seksi Pelaporan.

g. Bidang Pengelolaan Keuangan Daerah terdiri dari :

1. Seksi Anggaran;
2. Seksi Perbendaharaan;
3. Seksi Verifikasi.

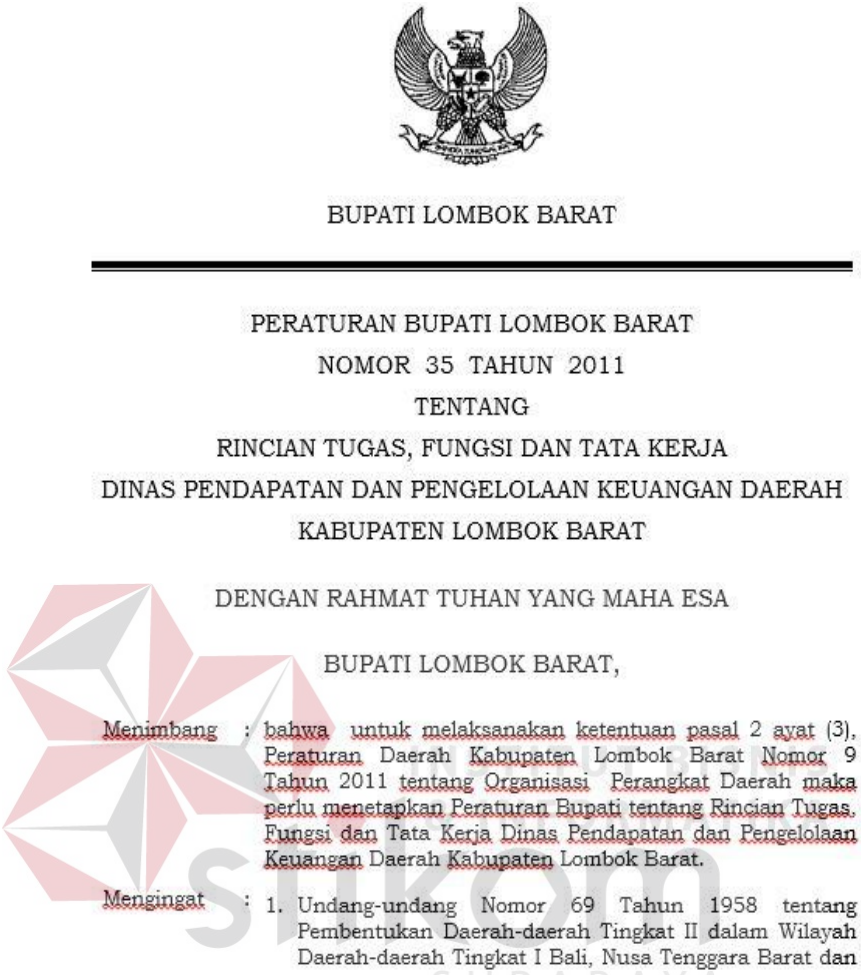
h.Unit Pelaksana Teknis (UPT).

i. Kelompok Jabatan Fungsional.

Sekretariat, Kepala Bidang dan UPT dipimpin oleh seorang Kepala yang berada di bawah dan bertanggung jawab langsung kepada Kepala Dinas.

5. Deskripsi Pekerjaan di DPPKD

Dinas Pendapatan Dan Pengelolaan Keuangan Daerah memiliki tugas dan fungsi dari setiap bagian yang tertuang pada dokumen peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja. Kilasan cotoh gambar deskripsi pekerjaan bisa dilihat pada Gambar 4.3 selengkapnya dapat dilihat pada Lampiran 2 menjelaskan job description pada DPPKD Lombok Barat.



BUPATI LOMBOK BARAT

PERATURAN BUPATI LOMBOK BARAT
NOMOR 35 TAHUN 2011
TENTANG
RINCIAN TUGAS, FUNGSI DAN TATA KERJA
DINAS PENDAPATAN DAN PENGELOLAAN KEUANGAN DAERAH
KABUPATEN LOMBOK BARAT

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI LOMBOK BARAT,

Menimbang : bahwa untuk melaksanakan ketentuan pasal 2 ayat (3), Peraturan Daerah Kabupaten Lombok Barat Nomor 9 Tahun 2011 tentang Organisasi Perangkat Daerah maka perlu menetapkan Peraturan Bupati tentang Rincian Tugas, Fungsi dan Tata Kerja Dinas Pendapatan dan Pengelolaan Keuangan Daerah Kabupaten Lombok Barat.

Mengingat : 1. Undang-undang Nomor 69 Tahun 1958 tentang Pembentukan Daerah-daerah Tingkat II dalam Wilayah Daerah-daerah Tingkat I Bali, Nusa Tenggara Barat dan

Gambar 4.3 *Job Description* DPPKD Lombok Barat

6. Proses Bisnis di DPPKD

Proses bisnis pada DPPKD ini secara garis besar yaitu : di mulai dari proses penyusunan anggaran dimulai dari proses penyusunan RPJP (rencana pembangunan jangka panjang) Daerah yang memuat visi, misi serta arah pembangunan daerah dan ditetapkan dengan Peraturan Daerah, RPJM (rencana pembangunan jangga menengah) Daerah ditetapkan dengan peraturan daerah paling lambat 3 (tiga) bulan sejak kepala daerah dilantik berdasarkan Undang-undang Nomor 25 Tahun 2004 Pasal 19 ayat (3). Setelah

itu dilanjutkan dengan penetapan RKPD (rencana kerja pemerintah daerah) yang ditetapkan setiap tahunnya bedasarkaan acuan RPJMD (rencana pembangunan jangga menengah daerah) rencana strategi, rencana kerja dan memperhatikan RKP dengan Peraturan Kepala Daerah sebagai dasar untuk penyusunan APBD. Proses perencanaan dari RPJP Daerah, RPJM Daerah sampai dengan RKP Daerah sesuai dengan Undang-undang Nomor 25 Tahun 2005 berada di BAPEDA. Dilanjutkan dengan proses penatausahaan yang melibatkan bendahara di dalamnya memerlukan peraturan tersendiri, dalam rangka pengelolaan keuangan yang lebih transparan dan tertib administrasi, maka harus menghadirkan proses penatausahaan pertanggungjawaban yang benar dan tertib. Prosedur akuntansi dan pelaporan juga harus sesuai Standar Akuntansi Pemerintahan untuk menjamin penyusunan laporan keuangan yang akuntabel dan proses yang terhakhir adalah pembukuan dan pelaporan keuangan fungsi Pembukuan meliputi serangkaian proses mulai dari pencatatan, pengikhtisaran, sampai dengan pelaporan keuangan dalam rangka pertanggungjawaban pelaksanaan APBD yang dapat dilakukan secara manual atau menggunakan aplikasi komputer. Pelaporan dan Pertanggungjawaban akan menekankan pada bahasan bagaimana menyiapkan Laporan Keuangan dengan Aplikasi Simda Versi 2.1. Laporan Keuangan akan tersaji secara otomatis oleh Program Aplikasi, namun terdapat proses dan langkah-langkah yang harus dilakukan oleh fungsi pembukuan atau akuntansi agar Laporan Keuangan tersaji secara akurat dengan menampilkan data yang sebenarnya pada tanggal tertentu. Fungsi Pembukuan pada SKPKD meliputi :

1. Pencatatan transaksi Jurnal

2. Pencatatan transaksi Penyesuaian Pendapatan

3. Input Saldo Awal

4. Posting Data dan

5. Ekspor Impor Saldo Awal dan Posting Jurnal

Dalam proses bisnis ini dibantu oleh aplikasi SIMDA dimana ke 3 proses dimulai dari penyusunan anggaran, proses penatausahaan serta proses pembukuan dan pelaporan keuangan menggunakan aplikasi.

4.1.3 Hasil Penentuan Tujuan, Ruang Lingkup dan Resiko

Hasil dari penentuan ruang lingkup objek audit dan tujuan audit di dapatkan melalui wawancara , review permasalahan apa yang terjadi di DPPKD hasilnya yaitu ditentukan ruang lingkup yang akan diaudit ruang lingkup yang akan dibahas adalah kepatuhan pegawai terhadap kebijakan yang terdapat di DPPKD, keamanan fisik dan lingkungan yang terdapat di bagian DPPKD dan kontrol akses informasi di DPPKD. Objek auditnya yaitu pada bagian DPPKD Lombok Barat.

Hasil ruang lingkup yang akan diaudit tersebut berdasar kondisi permasalahan dari bagian DPPKD, terdapat beberapa kondisi permasalahan tersebut yaitu pegawai yang tidak memenuhi ketentuan dokumen Kebijakan Sekuriti Sistem Informasi, maka ruang lingkup yang perlu diaudit adalah keamanan sumber daya manusia yang terdapat di klausul 8. Lalu kurangannya perawatan perangkat keras seperti CPU, monitor, *keyboard* atau fisik yang kurang dilindungi dengan maksimal, maka ruang lingkup yang perlu diaudit adalah keamanan fisik dan lingkungan yang terdapat di klausul 9. Informasi di DPPKD yang seharusnya terlindungi, dapat dilihat oleh pegawai lain di bagian yang sama

namun sebenarnya pegawai tersebut tidak memiliki akses untuk melihat informasi khusus yang bukan haknya. Karena setiap pegawai telah memiliki hak akses yang berbeda untuk melihat informasi yang dibutuhkan sesuai jobnya, maka ruang lingkup yang perlu diaudit adalah kontrol akses yang terdapat di klausul 11. Pemilihan ruang lingkup tersebut juga telah sesuai dengan kesepakatan bersama kedua belah pihak yaitu auditor dan auditee dengan tujuan dapat mengurangi terjadinya resiko keamanan informasi dan mengetahui keamanan sistem informasi yang sedang berlangsung.

Tabel 4.2 Pemetaan Permasalahan dan Ruang Lingkup Audit Keamanan Sistem Informasi

.	Table Pemetaan Permasalahan dan Ruang Lingkup Audit		
No	Permasalahan	Ruang Lingkup	Penjelasan
1.	Pegawai tidak memenuhi beberapa ketentuan yang telah terdapat pada peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja dinas pendapatan dan pengelolaan keuangan daerah kabupaten lombok barat	Kepatuhan Pegawai Terhadap Kebijakan yang Terdapat di Bagian DPPKD	Berdasarkan permasalahan ketidak patuhan Pegawai tersebut maka ruang lingkup yang harus diaudit adalah keamanan sumber daya manusia yang terdapat di klausul 8.
2.	Perawatan perangkat keras atau fisik dalam bagian DPPKD yang kurang dilindungi dengan maksimal	Keadaan Fisik dan Lingkungan yang Terdapat di DPPKD	Berdasarkan permasalahan kurangnya perlindungan pada penempatan fisik tersebut maka ruang lingkup yang

.	Table Pemetaan Permasalahan dan Ruang Lingkup Audit		
No	Permasalahan	Ruang Lingkup	Penjelasan
			harus diaudit adalah keamanan fisik dan lingkungan yang terdapat di klausul 9.
3.	Informasi DPPKD yang harusnya terlindungi dengan baik, dapat dilihat oleh karyawan yang tidak memiliki hak akses untuk melihatnya	Kontrol Akses Informasi di DPPKD	Berdasarkan permasalahan kurangnya perlindungan untuk akses informasi tersebut maka ruang lingkup yang harus diaudit adalah kontrol akses yang terdapat di klausul 11.

4.1.4 Hasil Menentukan Klausul, Objektif Kontrol dan Kontrol

Hasil dalam menentukan klausul, Objektif kontol dan kontrol menghasilkan penentuan ruang lingkup auditor serta penentuan klausul yang digunakan untuk melakukan audit di dalam tahap perencanaan ini. Adapun dalam menetapkan klausul, objektif kontrol dan kontrol berdasarkan beberapa permasalahan dan ruang lingkup yang telah ditetapkan dan disesuaikan berdasarkan kesepakatan bersama kedua belah pihak, Yang telah tertuang dalam surat perjanjian kontrak kerja audit. Sehingga didapatkan klausul 8 (Keamanan Sumber Daya Manusia), Klausul 9 (Keamanan Fisik dan Lingkungan) dan Klausul 11 (Kontrol Akses) sebagai klausul yang di gunakan dalam melakukan audit keamanan sistem informasi. Pemetaan Tabel pada klausul yang di gunakan bisa dilihat pada Tabel 4.3.

Tabel 4.3 Pemetaan Klausul, Objektif Kontrol dan Kontrol yang Digunakan

No.	Klausul	Objektif Kontrol	Kontrol
1.	Klausul 8 Keamanan Sumber Daya Manusia	a. 8.1 Sebelum Menjadi Pegawai b. 8.2 Selama Menjadi Pegawai c. 8.3 Pemberhentian atau pemindahan pegawai	a. 8.1.1 Aturan dan tanggung jawab keamanan b. 8.1.2 Seleksi c. 8.1.3 Persyaratan dan kondisi yang harus dipenuhi oleh pegawai d. 8.2.1 Tanggung jawab manajemen e. 8.2.2 Pendidikan dan pelatihan keamanan informasi f. 8.2.3 Proses Kedisiplinan g. 8.3.1 Tanggung jawab pemberhentian h. 8.3.2 Pengembalian aset i. 8.3.3 Penghapusan hak akses
2.	Klausul 9 Keamanan Fisik dan Lingkungan	a. 9.1 Wilayah Aman b. 9.2 Keamanan Peralatan	a. 9.1.1 Pembatasan keamanan fisik b. 9.1.2 Kontrol masuk fisik c. 9.1.3 Keamanan kantor, ruang dan fasilitasnya d. 9.1.4 Perlindungan terhadap ancaman dari luar dan lingkungan sekitar e. 9.1.5 Bekerja di wilayah aman f. 9.1.6 Akses publik, tempat pengiriman dan penurunan barang g. 9.2.1 Letak peralatan dan pengamanannya h. 9.2.2 Utilitas pendukung

No.	Klausul	Objektif Kontrol	Kontrol
			i. 9.2.3 Keamanan pengkabelan j. 9.2.4 Pemeliharaan Peralatan k. 9.2.5 Keamanan peralatan di luar tempat yang tidak disyaratkan l. 9.2.6 Keamanan untuk pembuangan atau pemanfaatan kembali peralatan m. 9.2.7 Hak pemanfaatan
3.	Klausul 11 Kontrol akses	a. 11.1 Persyaratan Bisnis Untuk Akses Kontrol b. 11.2 Manajemen Akses User c. 11.3 Tanggung Jawab Pengguna d. 11.4 Kontrol Akses Jaringan e. 11.5 Kontrol Akses Sistem Operasi f. 11.6 Kontrol Akses Informasi dan Aplikasi g. 11.7 Komputasi Bergerak dan Bekerja Dari Lain Tempat	a. 11.1.1 Kebijakan kontrol akses b. 11.2.1 Registrasi pengguna c. 11.2.2 Manajemen hak istimewa d. 11.2.3 Manajemen *password user* e. 11.2.4 Tinjauan terhadap hak akses user f. 11.3.1 Penggunaan *password* g. 11.3.2 Peralatan penggunaan yang tanpa penjagaan h. 11.3.3 Kebijakan *Clear desk* dan *clear screen* i. 11.4.1 Kebijakan penggunaan layanan jaringan j. 11.4.2 Otentikasi pengguna untuk melakukan koneksi keluar k. 11.4.3 Identifikasi peralatan di dalam jaringan l. 11.4.4 Perlindungan *remote diagnostic* dan konfigurasi

No.	Klausul	Objektif Kontrol	Kontrol
			port m. 11.4.5 Pemisahan dengan jaringan n. 11.4.6 Kontrol terhadap koneksi jaringan o. 11.4.7 Kontrol terhadap koneksi jaringan p. 11.5.1 Prosedur Log-On yang aman q. 11.5.2 Identifikasi dan autentikasi pengguna r. 11.5.3 Sistem Manajemen Password s. 11.5.4 Penggunaan utilitas sistem t. 11.5.5 Sesi *time-out* u. 11.5.6 Batasan waktu koneksi v. 11.6.1 Pembatasan akses informasi w. 11.6.2 Pengisolasian sistem yang sensitif x. 11.7.1 Komunikasi dan terkomputerisasi yang bergerak y. 11.7.2 Teleworking

4.2 Tahap Hasil Persiapan Audit

Tahap hasil persiapan Audit Keamanan Sistem Informasi dilakukan dengan cara, 1. Penyusunan Jadwal kerja Audit, 2. Penyampaian kebutuhan data audit, 3. Membuat pernyataan, 4. Melakukan pembobotan, 5. Membuat pertanyaan. Pernyataan yang telah dibuat berdasarkan standar ISO 27002:2005 dan pertanyaan yang telah dibuat berdasarkan pernyataan.

4.2.1 Hasil Penyusunan Jadwal Kerja Audit

Hasil dari penyusunan *Audit Working Plan* (AWP) berupa jadwal kerja. Jadwal kerja dimulai dari awal kegaitan sampai akhir kegiatan dimana penyusunan jadwal keerja ini berisi daftar tahapan audit yang akan dilakukan selengkapnya dapat dilihat pada Tabel 4.4.

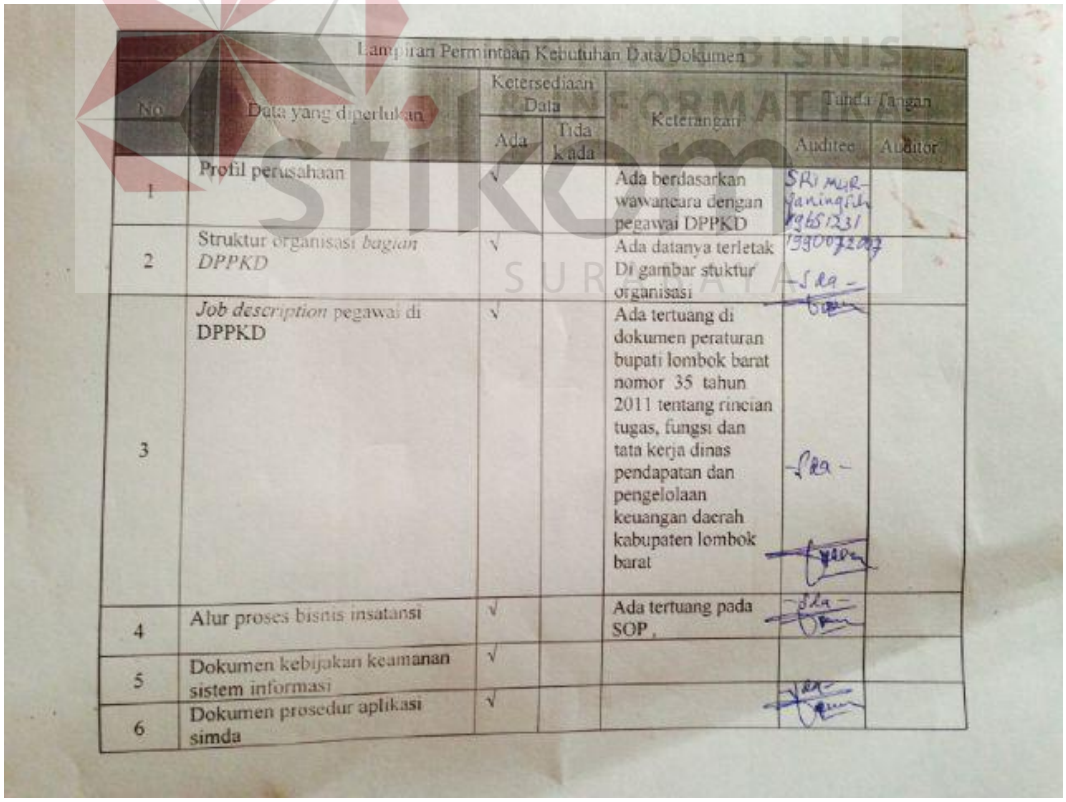
Tabel 4.4 Hasil *Audit Working Plan*

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. Menentukan Klausul, Obyektif Kontrol dan Kontrol	Fri 6/16/15 (16days)	Wed 7/2/15
10	Persiapan Audit Sistem Informasi 1. Penyusunan jadwal kerja audit 2. Penyampaian kebutuhan data 3. Membuat pertanyaan 4. Melakukan pembobotan 5. Membuat pernyataan	Wed 7/5/15 (47days)	Wed 8/20/15
13	Pelaksanaan Audit Sistem Informasi 1. Wawancara dan observasi 2. Pemeriksaan data dan bukti 3. Penyusunan temuan audit 4. Temuan dan rekomendasi	Thu 8/25/15 (15days)	Wed 9/10/15
21	Pelaporan Audit Sistem Informasi 1. Penyusunan draft laporan audit 2. Persetujuan darft laporan audit 3. Pelaporan darft audit 4. Exit meeting	Wed 9/11/15 (19days)	Tue 9/30/15
	Total	97 Days	

4.2.2 Hasil Penyampaian Kebutuhan Data

Pada tahap penyampaian kebutuhan data ini proses yang dilakukan adalah menyampaikan kebutuhan data yang diperlukan kepada *auditee* untuk penunjang pemeriksaan auditor. Hasilnya agar mempermudah auditor dalam melaksanakan tugasnya dalam melakukan auditor dan lebih cepat dalam memeriksa pada tahap pelaksanaannya sehingga penyampaian kebutuhan data bisa dipersiapkan sebelumnya.

Selain data penunjang yang terdapat pada Gambar 4.4 mengenai Lampiran kebutuhan audit, ada beberapa data yang telah dikumpulkan dan selengkapnya berada pada Lampiran 2 berupa 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	√		Ada berdasarkan wawancara dengan pegawai DPPKD		
2	Struktur organisasi *bagian DPPKD*	√		Ada datanya terletak Di gambar stuktur organisasi		
3	*Job description* pegawai di DPPKD	√		Ada tertuang di dokumen peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja dinas pendapatan dan pengelolaan keuangan daerah kabupaten lombok barat		
4	Alur proses bisnis insatansi	√		Ada tertuang pada SOP,		
5	Dokumen kebijakan keamanan sistem informasi	√				
6	Dokumen prosedur aplikasi simda	√				

Gambar 4.4 Lampiran Kebutuhan Data Penunjang yang Diperlukan Dalam Pelaksanaan Audit

4.2.3 Hasil Pernyataan

Pada Proses selanjutnya pada tahapan persiapan audit 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.

Beberapa contoh pernyataan yaitu pada klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*), klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 pembatas keamanan fisik (*Physical security perimeter*) dan klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.5.3 Sistem Manajemen *Password* dapat dilihat pada Tabel 4.4, Tabel 4.5, Tabel 4.6 dan untuk selengkapnya dapat dilihat pada Lampiran 3.

Dalam memenuhi kontrol audit pada klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 (Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*) yaitu berupa proses tanggung jawab selama menjadi pegawai secara formal bagi seluruh pegawai instansi serta memiliki komitmen dalam menjalani aturan dan tanggungjawabnya menjaga keamanan informasi, maka dibutuhkan beberapa pernyataan yang sesuai. Untuk itu auditor harus mengetahui beberapa hal tentang proses aturan dan tanggung. jawab pegawai diantaranya yaitu :

a. Harus mengetahui bagaimana prosedur peraturan dan tanggung jawab seluruh pegawai khususnya untuk bagian DPPKD.

b. Harus mengetahui beberapa kebijakan dan tanggung jawab yang berlaku di DPPKD.
c. Harus mengetahui konsekuensi untuk semua pegawai yang kurang memperhatikan prosedur keamanan informasi dalam instansi.
d. Harus mengetahui role dan kebijikan dalm perlindungan aset instansi.

Dari beberapa hal yang harus diketahui untuk memenuhi kontrol audit pada klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 (Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*) di atas, maka didapatkan pernyataan seperti yang ada pada Tabel 4.5.

Tabel 4.5 Pernyataan Klausul 8 Dengan Kontrol 8.1.1 Proses Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)

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 asset
3	Terdapat dokumentasi kebijakan organisasi aturan dan tanggung jawab pemeliharaan keamanan asset
4	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan asset

Dalam memenuhi kontrol audit pada klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (pembatas keamanan fisik (*Physical security perimeter*)) yaitu pembatasan keamanan (dinding pembatas, kontrol kartu akses, atau penjaga) harus disediakan untuk melindungi wilayah atau ruang

penyimpanan informasi dan perangkat pemrosesan informasi. Untuk itu auditor harus mengetahui banyak hal tentang pembatas keamanan tersebut diantaranya :

a. Harus mengetahui batas perimeter yang jelas dan aman khususnya pada tempat fasilitas pemrosesan informasi
b. Harus mengetahui bahwa pada akses menuju tempat kerja harus dibatasi hanya untuk personil dengan otorisasi
c. Harus mengetahui bahwa pada pintu darurat harus terpasang tanda bahaya dan benar benar tertutup rapat
d. Harus mengetahui bahwa setiap pengunjung atau orang yang menuju wilayah aman harus diawasi

Dari beberapa hal yang harus diketahui untuk memenuhi kontrol audit pada klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (pembatas keamanan fisik (*Physical security perimeter*)) di atas, maka akan didapatkan pernyataan seperti yang ada pada Tabel 4.6.

Tabel 4.6 Pernyataan Klausul 9 Dengan Kontrol 9.1.1 Pembatas Keamanan Fisik (*Physical security perimeter*)

PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	
Klausul 9.1 Wilayah Aman	
9.1.1 Pembatasan keamanan fisik	
Kontrol : Pembatasan keamanan (dinding pembatas, kontrol kartu akses, atau penjaga) harus disediakan untuk melindungi wilayah atau ruang penyimpanan Informasi dan perangkat pemrosesan Informasi.	
No.	PERNYATAAN
1.	Terdapat batas perimeter yang jelas pada tempat fasilitas informasi yang aman secara fisik
2.	Akses menuju tempat kerja harus dibatasi hanya untuk pesonil dengan otorisasi.
3.	Semua pintu darurat dalam batas parimeter keamanan harus dipasang tanda bahaya dan tertutup rapat.
4.	Pengunjung ke wilayah aman harus diawasi

Dalam memenuhi kontrol audit pada klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.5.3 Sistem Manajemen *Password* yaitu pengguna harus mengikuti praktek keamanan yang baik dalam pemilihan dan manajemen *password*, maka dibutuhkan beberapa pernyataan yang sesuai. Untuk itu auditor harus mengetahui banyak hal tentang penggunaan *password* tersebut diantaranya :

a. Harus mengetahui seberapa besar kesadaran pegawai guna menjaga tingkat kebenaran *password*
b. Harus mengetahui sikap pegawai untuk menjaga kepastiannya dalam pemilihan password yang berkualitas
c. Harus mengetahui bahwa pegawai telah mematuhi manajemen *password* agar tidak terjadi kesalahan dalam pengimputan *password*
d. Harus mengetahui kedisiplinan pegawai dalam penginputan sandi agar tidak menampilkan sandi saat log on ke applikasi bisnis.
e. Harus mengetahui bahwa pegawai telah melakukan pergantian password sementara pada saat pertama kali log-on
f. Harus mengetahui bahwa pegawai mengetahui resiko apabila menyimpan catatan password secara tidak aman
g. Harus mengetahui bahwa pegawai telah mengerti akan cara penyimpanan *password* dengan menggunakan *algoritma enkripsi one-way*

Dari beberapa hal yang harus diketahui untuk memenuhi kontrol audit pada klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.5.3 Sistem Manajemen *Password* di atas, maka akan didapatkan pernyataan seperti yang ada pada Tabel 4.7

Tabel 4.7 Pernyataan Klausul 11 Dengan Kontrol 11.3.1 Penggunaan Password (*Password Use*)

PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	
Klausul 11.5 Kontrol Akses Sistem Operasi	
11.5.3 Sistem Manajemen Password	
Kontrol : Sistem yang digunakan untuk mengelola password harus interaktif dan harus dipastikan passwordnya berkualitas.	
No.	PERNYATAAN
1.	Terdapat manajemen password dengan cara memastikan pengguna password individu untuk menjaga tingkat kebenarannya
2.	Terdapat kepastian dalam pemilihan password yang berkualitas
3.	Terdapat pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi untuk memperbolehkan dalam kesalahan inputan
4.	Terdapat pernyataan mengenai larangan menampilkan password di layar ketika dimasukkan
5.	Terdapat pemilihan password saat melakukan pengubahan pada log-on pertama yang dilakukan pengguna itu sendiri
6.	Terdapat penyimpana catatan password pengguna sebelumnya secara aman
7.	Terdapat penyimpanan password dalam bentuk enkripsi menggunakan algoritma enkripsi one-way

Pernyataan berdasarkan standar ISO 27002:2005 digunakan untuk memudahkan auditor sebagai acuan membuat pertanyaan untuk wawancara audit keamanan sistem informasi dari beberapa contoh klausul yaitu klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 proses Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*) membahas proses aturan dan tanggungjawab sehingga bila semua aturan dan tanggungjawab terdapat pada bagian DPPKD maka dapat menjadi standar uturan dan tanggungjawab sumber daya manusia pada DPPKD, klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (pembatas keamanan fisik (*Physical security perimeter*)) membahas tentang pembatas keamanan fisik sehingga bila semua aspek pembatas keamanan fisik terdapat pada bagian DPPKD maka dapat menjadi standar pembatas keamanan fisik pada DPPKD, klausul 11

(Sebelas) Kontrol Akses dengan kontrol Sistem Manajemen Password membahas tentang manajemen password sehingga bila semua aspek manajemen password terdapat pada bagian DPPKD maka dapat menjadi standar kontrol akses pada DPPKD. Keseluruhan pernyataan dari klausul 8, 9, dan 11 bisa dilihat pada Lampiran 3.

4.2.4 Hasil Penilaian Pernyataan

Setelah membuat pernyataan, maka langkah selanjutnya adalah melakukan pengukuran penilaian pada setiap pernyataan. Penilaian dilakukan berdasarkan perhitungan, dengan membagi tingkat penilaian dalam manajemen menjadi 3 (tiga), yaitu: rendah, cukup dan tinggi yang telah disesuaikan dengan kondisi DPPKD saat ini dan kesepakatan dengan pihak yang terkait dengan kreteria penilaiannya dapat dilihat pada Tabel 4.8.

Tabel 4.8 Tingkat Kepentingan dalam Penilaian Pernyataan

Resiko	Penilaian	Keterangan
Rendah (*Low*)	0,00 - 0,39	Pernyataan tersebut mempunyai peranan kurang penting dalam proses sistem informasi
Cukup (*Medium*)	0,40 - 0,69	Pernyataan tersebut mempunyai peranan cukup penting dalam proses sistem informasi
Tinggi (*High*)	0,70 - 1,00	Pernyataan tersebut mempunyai peranan sangat penting dalam proses sistem informasi

(Sumber: Niekerk dan Labuschagne dalam Hastin, 2012:39)

Hasil penilaian ini didapatkan dengan cara memberikan angket kepada pihak auditee dengan posisi jabatan officer 1 administrasi dan monitoring. Beberapa contoh penilaian yang ada dalam klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 (Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)), klausul 9 (sembilan) Keamanan Fisik dan

Lingkungan dengan kontrol 9.1.1 (pembatasan keamanan fisik (*Physical security perimeter*)) dan klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.5.3 Sistem Manajemen *Password*, dapat dilihat pada Tabel 4.9, Tabel 4.10 Tabel 4.11 dan untuk selengkapnya dapat dilihat pada Lampiran 4.

Penilaian pada klausul 8 dengan kontrol 8.1.1 proses tanggungjawab, didapatkan beberapa nilai dari pihak auditee yang disesuaikan dengan kondisi DPPKD diantaranya yaitu :

a. Pernyataan nomor 1 (satu) mendapatkan nilai 0,6 dimana nilai 0,6 tersebut memiliki peranan cukup penting dalam proses sistem informasi. Berdasarkan keterangan dari pihak auditee, bahwa pegawai harus mematuhi aturan dan tanggungjawab yang ada karena saat proses penerimaan pegawai wajib mematuhi aturan dan tanggungjawab sebagai pegawai di ikat dalam ikrar sumpah pegawai. Oleh karena itu diberikan nilai 0,6 dalam pernyataan nomor 1 tersebut.
b. Pernyataan nomor 2 (dua) mendapatkan nilai 0,6 dimana nilai 0,6 tersebut memiliki peranan cukup penting dalam proses sistem informasi, menurut pihak auditee perlindungan aset juga cukup penting dan perlu diterapkan di DPPKD.
c. Pernyataan nomor 3 (tiga) mendapatkan nilai 0,8 dimana nilai 0,8 memiliki peranan sangat penting dalam proses sistem informasi, menurut auditee peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada saat ini belum berjalan secara optimal. Jadi harus menerapkan konsekuensi bagi pegawai yang mengabaikan prosedur tanggungjawab keamanan sistem informasi.

d. Pernyataan no 4 (empat) mendapatkan nilai 0,8 dimana nilai 0,8 memiliki peranan sangat penting dalam proses sistem informasi, menurut auditee kepastian tanggungjawab keamanan sistem informasi cukup penting namun masih melekat dan tertuang dalam tupoksi, belum ada kepastian dokument yang mengatur kepastian untuk melindungi keamanan informasi.

Tabel 4.9 Penilaian Klausul 8 Dengan Kontrol 8.1.1 Proses Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	Auditor: Riyadi Atmajaya
	Auditee: Dra. Sri Muryaningsih. MM NIP. 19651231 199007 2 007
	Tanggal : 27 juli 2015
	Tanda tangan:

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				
Klausul 8.1 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	Penilaian		
		Rendah (0,1-0,39)	Cukup (0,4-0,69)	Tinggi (0,7-1,0)
1.	Terdapat peraturan pada proses penerimaan pegawai pada DPPKD		0,6	
2.	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan asset		0,6	
3.	Terdapat peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada			0,8
4.	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi			0,8

Penilaian pada klausul 9 dengan kontrol 9.1.1 pembatasan keamanan fisik, didapatkan beberapa nilai dari pihak auditee yang disesuaikan dengan kondisi DPPKD yaitu :

a. Pernyataan nomor 1 (satu) mendapatkan nilai 0,8 dimana nilai 0,8 memiliki peranan sangat penting dalam proses sistem informasi. Berdasarkan keterangan dari pihak auditee, telah terdapat batas fisik yang jelas bahwa area aman harus diberi batas sekuriti fisik untuk melindungi area pemprosesan informasi namun masih dirasa kurang optimal karena tidak dilengkapi cctv di ruang pemrosesan informasi.
b. Pernyataan nomor 2 (dua) mendapatkan nilai 0,6 dimana nilai 0,6 memiliki peranan cukup penting dalam proses sistem informasi. Berdasarkan keterangan pihak auditee untuk masuk menuju ke tempat tertentu harus dengan otorisasi khusus dan masih belum terdapat cctv menuju ke tempat tertentu (pemprosesan informasi), sedangkan pada ruang DPPKD dan sepanjang jalan menuju ruang DPPDK juga masih belum terdapat cctv. Sehingga pihak instansi harus menerapkan akses menuju tempat kerja dibatasi hanya untuk pesonil dengan otorisasi khusus.
c. Pernyataan nomor 3 (tiga) mendapatkan nilai 0,6 dimana nilai 0,6 memiliki peranan cukup penting dalam proses sistem informasi. Berdasarkan keterangan pihak auditee untuk semua pintu darurat belum terpasang tanda bahaya di karenakan tidak terdapat pintu darurat di instansi hanya sebatas pintu keluar masuk instansi. Jadi instansi DPPKD perlu menerapkan semua pintu darurat dalam batas parimeter keamanan harus dipasang tanda bahaya dan tertutup rapat.

d. Pernyataan nomor 4 (empat) mendapatkan nilai 0,6 dimana nilai 0,6 memiliki peranan cukup penting dalam proses sistem informasi. Berdasarkan keterangan pihak auditee harus ada pengawasan dari petugas sekuriti untuk orang lain yang akan masuk ke wilayah aman, namun dirasa kurang optimal karena terkadang tidak memeriksa setiap orang lain selain pegawai yang masuk ke wilayah aman. Jadi harus menerapkan pengawasan terhadap orang yang akan ke wilayah.

Tabel 4.10 Penilaian Klausul 9 Dengan Kontrol 9.1.1 Pembatasan Keamanan Fisik (*Physical security perimeter*)

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)		Auditor: Riyadi Atmajaya		
		Auditee: Ikhwania safitri, SE NIP. 19790723 200501 2 017		
		Tanggal: 27 juli 2015		
		Tanda Tangan:		
Klausul 9.1 Wilayah Aman				
9.1.1 Pembatasan keamanan fisik				
Kontrol : Pembatasan keamanan (dinding pembatas, kontrol kartu akses, atau penjaga) harus disediakan untuk melindungi wilayah atau ruang penyimpanan Informasi dan perangkat pemrosesan Informasi.				
No.	PERNYATAAN	Penilaian		
		Rendah (0,1-0,39)	Cukup (0,4-0,69)	Tinggi (0,7-1,0)
1.	Terdapat batas perimeter yang jelas pada tempat fasilitas informasi yang aman secara fisik			0,8
2.	Akses menuju tempat kerja harus dibatasi hanya untuk pesonil dengan otorisasi		0,6	
3.	Semua pintu darurat dalam batas parimeter keamanan harus dipasang tanda bahaya dan tertutup rapat.		0,6	
4.	Orang yang akan ke wilayah aman harus diawasi		0,6	

Penilaian pada klausul 11 dengan kontrol 11.5.3 sistem manajemen *password*, didapatkan beberapa nilai dari pihak auditee yang disesuaikan dengan kondisi DPPKD diantaranya yaitu:

a. Pernyataan nomor 1 (satu) mendapatkan nilai 0,4 dimana nilai 0,4 memiliki peranan cukup penting dalam proses sistem informasi. Berdasarkan keterangan dari pihak auditee, bahwa kesadaran pegawai sendiri untuk menjaga kebenarannya dan sudah tertuang dalam tupoksi peraturan bupati lombok barat no 35 tahun 2011 wajib, namun masih saja ada pegawai yang melanggar atau lalai dalam tugasnya.
b. Pernyataan nomor 2 (dua) mendapatkan nilai 0,6 dimana nilai 0,6 memiliki peranan sangat penting dalam proses sistem informasi. Berdasarkan keterangan pihak auditee untuk saat ini pemilihan kata sandi yang berkualitas dengan mengkombinasikan angka dan huruf tidak dilakukan oleh pegawai itu sendiri namun pada umumnya mengenai pemilihan sandi yang berkualitas hanya dilakukan oleh administrator saja.
c. Pernyataan nomor 3 (tiga) mendapatkan nilai 0,6 dimana nilai 0,6 memiliki peranan sangat penting dalam proses sistem informasi. Berdasarkan keterangan pihak *auditee* pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi hanya dilakukan oleh administrator ataupun pengubahan sandi dilakukan juga oleh administrator.
d. Pernyataan nomor 4 (empat) mendapatkan nilai 0,7 dimana nilai 0,7 memiliki peranan sangat penting dalam proses sistem informasi. Berdasarkan keterangan dari pihak *auditee*, terdapat pernyataan mengenai larangan menampilkan *password* di layar ketika dimasukkan namun hanya secara lisan

saja yang dilakukan oleh admin kepada para pegawai untuk melarang pegawai menampilkan *password* saat *log on*.

e. Pernyataan nomor 5 (lima) mendapatkan nilai 0,6 dimana nilai 0,6 memiliki peranan sangat penting dalam proses sistem informasi. Berdasarkan keterangan dari pihak *auditee* tidak terdapat pemilihan password saat melakukan pengubahan pada log-on pertama yang dilakukan pegawai itu sendiri karna pada umumnya hanya admin yang melakukannya.

f. Pernyataan nomor 6 (enam) mendapatkan nilai 0,5 dimana nilai 0,5 memiliki peranan sangat penting dalam proses sistem informasi. Berdasarkan keterangan pihak auditee pegawai tidak pernah menyimpan catatan *password*, karena pada umumnya semua pegawai mengetahui password masuk ke dalam aplikasi simda , namun hanya untuk pegawai yang memang tugasnya menggunakan aplikasi simda ini.

g. Pernyataan nomor 7 (tujuh) mendapatkan nilai 0,6 dimana nilai 0,6 memiliki peranan sangat penting dalam proses sistem informasi. Berdasarkan keterangan pihak auditee, sudah dilakukannya penyimpanan password dalam bentuk enkripsi dengan menggabungkan antara huruf dan angka dalam pembuatan password yang dilakukan oleh admin.

Tabel 4.11 Penilaian Klausul 11 Dengan Kontrol 11.5.3 Sistem Manajemen *Password*

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	Auditor: Riyadi Atmajaya
	Auditee: Normansyah, SE NIP. 19810921 200501 1 006
	Tanggal: 27 juli 2015
	Tanda Tangan:

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		
		Rendah (0,1-0,39)	Cukup (0,4-0,69)	Tinggi (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 pemilihan password saat melakukan pengubahan pada log-on pertama yang dilakukan pengguna itu sendiri		0,6	
6.	Terdapat penyimpana catatan password pengguna sebelumnya secara aman		0,5	
7.	Terdapat penyimpanan password dalam bentuk enkripsi menggunakan algoritma enkripsi one-way		0,5	

Dari hasil penilaian untuk klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 (Aturan dan tanggung jawab keamanan (*Roles and*

Responsibilities)) didapatkan pentingnya Aturan dan tanggung jawab pegawai untuk bagian DPPKD, sehingga pihak instansi harus lebih memperhatikan proses aturan dan tanggung jawab. Untuk klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (pembatas keamanan fisik (*Physical security perimeter*)) didapatkan pentingnya pembatas keamanan fisik untuk bagian DPPKD, sehingga pihak instansi harus lebih memperhatikan pembatas keamanan fisik yang ada di kantor baik berupa bahan yang di gunakan dalam skat pembatas dan lingkungan sekitar kantor. Untuk klausul 11 (Sebelas) Kontrol Akses dengan kontrol 11.5.3 Sistem Manajemen *Password* didapatkan pentingnya manajemen *password* bagi pegawai di dinas pendapatan dan pengelolaan keuangan daerah, sehingga pihak instansi harus lebih memperhatikan kembali mengenai manajemen *password.* Pernyataan yang digunakan tersebut sesuai dengan permintaan auditee yang sebelumnya juga telah mengetahui nilai beserta makna dari tingkat kepentingan dalam pembobotan pernyataan dan juga menyesuaikan dengan kondisi sebenarnya pada bagian DPPKD maka yang digunakan adalah tingkat resiko cukup/*medium* (0,4-0,69) dan tinggi/*high* (0,7-1,0). Apabila terdapat nilai yang tingkat resikonya rendah/*low* maka pihak auditee sepakat tidak menggunakannya karena berdasarkan tingkat kepentingan dalam penilaian pernyataan, pernyataan tersebut mempunyai peranan kurang penting dalam proses sistem informasi. Hasil penilaiannya dapat dilihat pada Tabel 4.12, Tabel 4.13, Tabel 4.14 dan selengkapnya dapat dilihat Lampiran 5.

Tabel 4.12 Hasil Penilaian Klausul 8 Dengan Kontrol 8.1.1 Aturan dan Tanggung Jawab Keamanan (*Roles and Responsibilities*) Dengan Nilai *Medium* (0,4-0,69) dan *High*(0,7-1,0)

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	Auditor: Riyadi Atmajaya
	Auditee: Dra. Sri Muryaningsih. MM NIP. 19651231 199007 2 007
	Tanggal : 27 juli 2015
	Tanda tangan:

Klausul 8.1 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	Penilaian		
		Rendah (0,1-0,39)	Cukup (0,4-0,69)	Tinggi (0,7-1,0)
1.	Terdapat peraturan pada proses penerimaan pegawai pada DPPKD		0,6	
2.	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan aset		0,6	
3.	Terdapat peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada			0,8
4.	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi			0,8

Tabel 4.13 Hasil Penilaian Klausul 9 Dengan Kontrol 9.1.1 Pembatasan Keamanan Fisik (*Physical security perimeter*) Dengan Nilai *Medium* (0,4-0,69) dan *High*(0,7-1,0)

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	Auditor: Riyadi Atmajaya
	Auditee: Ikhwania safitri, SE NIP. 19790723 200501 2 017
	Tanggal: 27 juli 2015
	Tanda Tangan:

Klausul 9.1 Wilayah Aman

9.1.1 Pembatasan keamanan fisik

Kontrol : Pembatasan keamanan (dinding pembatas, kontrol kartu akses, atau penjaga) harus disediakan untuk melindungi wilayah atau ruang penyimpanan Informasi dan perangkat pemrosesan Informasi.

No.	PERNYATAAN	Penilaian		
		Rendah (0,1-0,39)	Cukup (0,4-0,69)	Tinggi (0,7-1,0)
1.	Terdapat batas perimeter yang jelas pada tempat fasilitas informasi yang aman secara fisik			0,8
2.	Akses menuju tempat kerja harus dibatasi hanya untuk pesonil dengan otorisasi		0,6	
3.	Semua pintu darurat dalam batas parimeter keamanan harus dipasang tanda bahaya dan tertutup rapat.		0,6	
4.	Orang yang akan ke wilayah aman harus diawasi		0,6	

Tabel 4.14 Hasil Penilaian Klausul 11 Dengan Objektif Kontrol Sistem Manajemen Password Dengan Nilai *Medium* (0,4-0,69) dan *High*(0,7-1,0)

PEMBOBOTAN PERNYATAAN AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 11 (KONTROL AKSES)	Auditor: Riyadi Atmajaya
	Auditee: Normansyah, SE NIP. 19810921 200501 1 006
	Tanggal: 27 juli 2015
	Tanda Tangan:

Klausul 11.3 Tanggung Jawab Pengguna (*user*)				
11.3.1 Penggunaan *password*				
Kontrol : Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan password.				
No.	PERNYATAAN	Penilaian		
		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		0,6	
2.	Terdapat penggantian kata password setiap kali ada kemungkinan sistem atau password dalam keadaan bahaya		0,6	
3.	Terdapat larangan dalam pembuatan catatan password		0,6	
4.	Terdapat larangan untuk tidak membagi satu password kepada pengguna lain			0,8
5.	Terdapat pergantian password sementara pada saat pertama kali log-on			0,8
6.	Terdapat pemilihan password secara berkualitas yang mudah diingat	0,3		
7.	Terdapat perubahan kata sandi/password berkala atau berdasarkan jumlah akses dan larangan menggunakan password yang lama			0,8

4.2.5 Hasil Pertanyaan

Setelah melakukan pembobotan pernyataan langkah selanjutnya adalah membuat pertanyaan. Pertanyaan yang dibuat mengacu pada pernyataan yang ada dimana satu pernyataan bisa memiliki lebih dari satu pertanyaan, hal tersebut dikarenakan setiap pertanyaan harus mewakili pernyataan pada saat dilakukan wawancara. Pertanyaan pada tabel didasarkan pada pernyataan yang telah

disesuaikan dengan standar ISO 27002. Beberapa pertanyaan pada klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*), klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (pembatasan keamanan fisik (*Physical security perimeter*)) dan klausul 11 (sebelas) Kontrol Akses dengan kontrol Sistem Manajemen Password, Dapat dilihat pada Tabel 4.15, Tabel 4.16, Tabel 4.17 dan untuk selengkapnya dapat dilihat pada Lampiran 5.

Berdasarkan beberapa hasil pernyataan dari klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*) maka didapatkan pertanyaan yang disesuaikan dengan kebutuhan yang terdapat pada setiap pernyataan, diantaranya yaitu :

a. Pernyataaan nomor 1 (satu), dibutuhkan peraturan khusus pada penerimaan pegawai dan dokument yang mengatur proses pemerimaan pegawai di DPPKD, maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.15 nomor 1 (satu).
b. Pernyataan nomor 2 (dua), dibutuhkan perlindungan asset pada peran dan tanggung jawab pegawai DPPKD maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.15 nomor 2 (dua).
c. Pernyataan nomor 3 (tiga), dibutuhkan peran dan tanggung jawab yang mengatur tentang keamanan informasi khususnya mengenai peran dan tanggung jawab pegawai maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.15 nomor 3 (tiga).

d. Pertanyaan nomer 4 (empat), tidak hanya di butuhkan peran dan tanggung jawab dari pegawai namun juga kepastian dari peran dan tanggung jawab benar – benar sudah di berikan demi melindungi kemanan instansi, maka di dapatkan beberapa pertanyaan seperti yang ada pada Table 4.15 nomer 4 (empat)

Tabel 4.15 Hasil Pertanyaan Klausul 8 Dengan Kontrol 8.1.1 Aturan dan Tanggung Jawab Keamanan (*Roles and Responsibilities*)

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)	
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)	
1	Terdapat peraturan pada proses penerimaan pegawai pada DPPKD
	P: Adakah peraturan khusus pada proses penerimaan pegawai pada DPPKD? J: Peraturan penerimaan pegawai pada DPPKD terpusat pada BKD kab Lobar P: Bagaimana peraturan pada proses penerimaan pegawai pada DPPKD ? J: Peraturan berlaku secara umum untuk semua SKPD dan telah di atur oleh BKD P: Adakah dokumentasi peraturan pada proses penerimaan pegawai pada DPPKD? J: Ada di BKD (nama dokumennya atau contoh foto dokumennya) Sk penetapan pengangkatan K2
2	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan aset
	P: Apakah organisasi telah melakukan perlindungan terhadap aset pada peran dan tanggung jawab pegawai di DPPKD? J: Iya P: Siapakah yang membuat perlindungan aset yang sesuai dengan peran dan tanggung jawab pegawai tersebut? J: Aset menjadi tanggung jawab semua pegawai secara umum & bendahara barang secara khusus dengan berkordinasi dengan badan aset daerah P: Apakah ada dokumentasinya dari perlindungan asset tersebut ? J: Ada di kantor aset daerah

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)	
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)	
3	Terdapat peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada
	P: Apakah peran dan tanggung jawab pegawai sudah sesuai dengan kebijakan keamanan informasi yang diterapkan instansi? J: Secara umum sudah P: Siapa yang membuat kebijakan keamanan informasi yang mengatur peran dan tanggung jawab pegawai tersebut? J: BKD P: Apakah terdapat dokumentasi kebijakan keamanan informasi insatansi yang khusus mengatur peran dan tanggung jawab pegawai? J: Iya ada sudah melekat , pada tugas pokok dan fungsi masing-masing . doc pada peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja dinas pendapatan dan pengelolaan keuangan daerah kabupaten lombok barat
4	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi
	P: Apakah telah dilakukan pelaporan apabila ada suatu ancaman yang beresiko bagi keamanan organisasi instansi? J: Belum ada P: Siapa yang bertanggung jawab atas laporan peristiwa yang memiliki potensi resiko pada keamanan informasi yang ada? J: Pada umumnya BKD P: Apakah terdapat dokumentasi atas laporan peristiwa yang berpotensi beresiko pada keamanan informasi yang ada? J: Iya ada sudah melekat ,Pada tugas pokok dan fungsi masing-masing. doc pada peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja dinas pendapatan dan pengelolaan keuangan daerah kabupaten lombok barat

Berdasarkan beberapa hasil pernyataan dari klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (Pembatasan Keamanan

Fisik (*Physical security perimeter*)) maka didapatkan pertanyaan yang disesuaikan dengan kebutuhan yang terdapat pada setiap pernyataan, diantaranya yaitu :

a. Pernyataaan nomor 1 (satu), dibutuhkan kepastian bahwa batas perimeter yang terdapat pada tempat fasilitas informasi DPPKD benar-benar terjamin keamanannya sesuai standar keamanan serta dibutuhkan data atau prosedur keamanan yang mengatur tentang batas fisik tersebut, maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.16 nomor 1 (satu)
b. Pernyataan nomor 2 (dua), dibutuhkan kepastian bahwa akses menuju tempat kerja dan pada saat di tempat kerja harus terjamin keamanannya dengan membatasi personil yang memiliki otorisasi saja yang diperbolehkan masuk selain itu dibutuhkan data keamanan lingkungan yang mengatur akses menuju tempat pemprosesan informasi dibatasi hanya untuk personil dengan otorisasi, maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.16 nomor 2 (dua)
c. Pada pernyataan nomor 3 (tiga), dibutuhkan kepastian bahwa seluruh pintu darurat dalam batas perimeter keamanan harus tertutup rapat dan dalam pengawasan pihak keamanan yang bersangkutan, maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.16 nomor 3 (tiga)
d. Pada pernyataan nomor 4 (empat), dibutuhkan kepastian bahwa orang yang akan ke wilayah aman benar benar harus diawasi dan terjamin keamanannya, maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.16 nomor 4 (empat)

Tabel 4.16 Hasil Pertanyaan Klausul 9 Dengan Kontrol 9.1.1 Pembatasan Keamanan Fisik (*Physical security perimeter*)

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.1 Pembatas keamanan fisik	
1	Terdapat batas perimeter yang jelas pada tempat fasilitas informasi yang aman secara fisik
	P: Apakah terdapat batas fisik dan seperti apa batas yang terdapat di dalam ruangan DPPKD untuk melindungi pemrosesan informasi yang sedang berlangsung? J: Iya , tembok, sekat ruangan, akses pintu keluar masuk P: Apakah batas fisik tersebut terjamin keamanannya secara optimal untuk melindungi kegiatan pemrosesan informasi yang sedang berlangsung? J: Iya , karena akses pintu keluar masuk dapat terkontrol atau terlihat siapa saja yg masuk keruangan tersebut P: Apakah batas fisik tersebut telah dibuat sesuai standar keamanan yang layak? Terbuat dari bahan apakah pembatas fisik tersebut? J: Iya , dinding, kaca dan pintu dari bahan standart P: Apakah ada prosedur keamanan yang mengatur tentang batas fisik tersebut? J: tidak secara tertulis P: Apakah di ruangan DPPKD terdapat kaca yang memiliki pandangan keluar gedung dan apakah kaca tersebut terbuat dari bahan yang kuat dan tidak mudah pecah? J: Iya, bahan tersebut standart dan mudah pecah P: Apakah selama ini pernah terjadi insiden pelemparan kaca kantor DPPKD? Apakah ada standar khusus untuk kaca harus terbuat dari apa untuk ruang DPPKD ini? J: Tidak pernah terjadi , karena lingkungan kantor selalu dijaga baik , penjaga malam maupun sat pol pp
2	Akses menuju tempat kerja harus dibatasi hanya untuk pesonil dengan otorisasi.
	P: Siapakah yang menempati ruangan pemrosesan informasi di sini? J: Personil/pengguna pemprosesan data dan informasi P: Perlindungan seperti apakah yang digunakan untuk melindungi tempat kerja yang khusus hanya personil dengan otorisasi saja yang boleh

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.1 Pembatas keamanan fisik	
	masuk?(pintu,kartu akses,penjaga pintu,dll) J: Pintu, dan otoritas / password masing-masing personil P: Apakah terdapat cctv (close circuit tele vision) yang ditempatkan di lokasi yang ideal untuk merekam keluar masuknya pegawai? Apakah di dalam ruang kerja atau pemrosesan informasi juga ada cctv? J: Tidak terdapat CCTV di kedua tempat yang di maksud P: Apakah ada dokumen yang mengatur bahwa untuk akses menuju tempat kerja dibatasi hanya untuk personil dengan otorisasi? J: Belum ada dokumen
3	Semua pintu darurat dalam batas parimeter keamanan harus dipasang tanda bahaya dan tertutup rapat.
	P: Apakah pintu darurat telah dipasang sesuai standar keamanan dan tertutup rapat? J: Tidak terdapat pintu darurat P: Standar yang dimaksud di sini seperti apa ? Mungkin bisa dijelaskan? (missal kalau pintu darurat, khusus pintu darurat harus memiliki criteria khusus bahwa pegangan pintunya harus terbuat dari bahan apa dan bentuknya harus seperti apa, dll) J: - P: Bagaimana kontrol pengawasan apabila terjadi bencana mendadak seperti kebakaran, banjir atau gempa? J: Tidak pernah dilakukan simulasi, ataupun kontrol pengamanan P: Apakah setiap pegawai mengetahui di mana saja pintu darurat berada? J: Tidak kanera hanya memiliki pintu keluar masuk yang sifatnya bukan darurat P: Apakah pintu darurat tersebut hanya dapat dibuka dari dalam atau juga dapat dibuka dari luar? (Kalaupun dapat dibuka dari luar , hanya dengan menggunakan kunci yang dimiliki oleh orang-orang yang telah ditunjuk misalnya personal keamanan gedung) J: -
4	Orang yang akan ke wilayah aman harus diawasi
	P: Apakah ada peraturan/persyaratan khusus untuk orang lain selain pegawai yang akan mengunjungi wilayah aman seperti ruang server dan wilayah aman lainnya? Seperti apakah persyaratan/peraturan tersebut?

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.1 Pembatas keamanan fisik	
	J: Iya , namun tidak tertulis . yang dapat masuk hanya vendor dan admin P: Apakah ada pencatatan khusus apabila ada yang keluar masuk ruangan DPPKD? J: Tidak ada P: Adakah cctv yang mengawasi siapa saja yang masuk dan keluar ke wilayah aman? J: tidak ada

Berdasarkan beberapa hasil pernyataan dari klausul 11 (sebelas) Kontrol Akses dengan kontrol Sistem Manajemen Password maka didapatkan pertanyaan yang disesuaikan dengan kebutuhan yang terdapat pada setiap pernyataan, diantaranya yaitu :

a. Pernyataaan nomor 1 (satu), dibutuhkan kepastian bahwa pegawai telah menjaga dan memastikan pengguna password individu sudah terjaga tingkat kebenarannya maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.17 nomor 1 (satu)
b. Pernyataan nomor 2 (dua), dibutuhkan kepastian mengenai dalam pemilihan password yang berkualitas maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.17 nomor 2 (dua)
c. Pernyataan nomor 3 (tiga), dibutuhkan kepastian pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi untuk memperbolehkan dalam kesalahan inputan media lainnya maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.17 nomor 3 (tiga)

d. Pernyataan nomor 4 (empat), dibutuhkan kepastian bahwa pernyataan mengenai larangan menampilkan password di layar ketika dimasukkan maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.17 nomor 4 (empat)

e. Pernyataan nomor 5 (lima), dibutuhkan kepastian bahwa pemilihan password saat melakukan pengubahan pada log-on pertama yang dilakukan pengguna itu sendiri maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.17 nomor 5 (lima)

f. Pernyataan nomor 6 (enam), dibutuhkan kepastian bahwa pegawai tidak menyimpan catatan password di kertas maupun di *handphone* atau media lainnya maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.17 nomor 6 (enam)

g. Pernyataan nomor 7 (tujuh), dibutuhkan kepastian bahwa pegawai telah melakukan penyimpanan password dalam bentuk enkripsi menggunakan algoritma enkripsi one-way maka didapatkan beberapa pertanyaan seperti yang ada pada Tabel 4.17 nomor 7

Tabel 4.17 Hasil Pertanyaan 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 manahemen password memastikan pengguna password individu sudah terjaga tingkat kebenarannya? J: Pada umumnya sudah P: Apakah terdapat dokumentasi khusus mengenai manajemen password sehingga dapat menjaga tingkat kebenarannya?

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: Tidak terdapat dokumentasi mengenai manajemen password P: Bagaimana mensosialisasikan pentingnya manajemen password individu kepada pengguna sehingga dapat menjaga tingkat kebenarannya? J: Hanya sebatas pemberitahuan lisan
2	Terdapat kepastian dalam pemilihan password yang berkualitas
	P: Apakah terdapat pemilihan password berkualitas? J: Iya P: Apa saja kriteria dalam pemilihan password berkualitas? J: Dengan mengkombinasikan angka dan huruf P: Apakah telah dilakukan kepastian tiap penggunanya bahwa dia telah memiliki password yang berkualitas? J: Pada umumnya sudah
3	Terdapat pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi untuk memperbolehkan dalam kesalahan inputan
	P: Apakah pengguna diberikan pemilihan password? J: Tidak karena password yang membuat admin, untuk pemilihan password di serahkan hanya ke pada admin saja. P: Apakah pengguna diberikan hak dalam pengubahan password? J: Hanya admin yang memiliki hak merubah password P: Apakah ada prosedur konfirmasi dalam memperbolehkan dalam kesalahan inputan? J: Ada dengan munculnya pesan di layar password salah
4	Terdapat pernyataan mengenai larangan menampilkan password di layar ketika dimasukkan
	P: Apakah layar sudah tidak menampilkan password ketika dimasukkan? J: iya P: Apa bukti tidak menampilkan password yang dimasukkan? J: Dengan mengganti form password menjadi lambang titik-titik

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 keseluruhan layar pada staf pengguna sudah tidak menampilkan password ketika dimasukkan? J: Sudah
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: Tidak ada P: Apakah dalam pemilihan password saat melakukan pengubahan pada log-on pertama dilakukan sudah dilakukan oleh keseluruhan pengguna? J: Tidak pernah karena password sudah tinggal di pakai , untuk perubahan password itu otoritas admin terkait P: Apakah pemilihan password dilakukan pengguna itu sendiri? J: Tidak dilakukan oleh admin
6	Terdapat penyimpana catatan password pengguna sebelumnya secara aman
	P: Apakah penyimpanan catatan password pengguna sebelumnya sudah dilakukan secara aman? J: Tidak ada penyimpanan catatan password, karena pada umumnya semua pegawai mengetahui password masuk ke dalam aplikasi simda, namun hanya untuk pegawai yang memang tugasnya menggunakan aplikasi simda ini. P: Bagaimana cara mengamankan penyimpanan catatan password pengguna sebelumnya? J: Tidak pernah membuat catatan password, namun mungkin ada beberapa pegawai yang menyimpan password dalam ponselnya sendiri 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: Iya

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 menggunakan algoritma enkripsi one-way pada penyimpanan password? J: Iya kombinasi angka dan huruf / karakter unik P: Apa alternative lain jika organisasi tidak menggunakan algoritma enkripsi one-way? J: tidak ada

4.3 Hasil Pelaksanaan Audit

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. Tahap ini akan menghasilkan temuan dan bukti, dokumen wawancara, hasil daftar temuan dan rekomendasi audit.

4.3.1 Hasil Wawancara dan observasi

Pada proses wawancara, auditor melakukan wawancara berdasarkan pertanyaan yang telah dibuat. Sebelum melakukan wawancara auditor harus mengevaluasi dulu, Objek auditnya bagaimana, Objek pemeriksaannya gimana barulah wawancara dilakukan berdasarkan pertanyaan yang telah dibuat oleh auditor. Wawancara ditujukan kepada staf kepegawaian yang terlibat di dalamnya diharapkan dari hasil wawancara ini didapatkan temuan bukti mengenai permasalahan yang ada di dinas dppkd. Beberapa contoh hasil wawancara terdapat pada klausul 8 (Delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*), klausul 9 (Sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1

(Pembatasan Keamanan Fisik (*Physical security perimeter*)) dan klausul 11 (sebelas) Kontrol Akses dengan control 11.5.3 Sistem Manajemen *Password* dapat dilihat pada Tabel 4.18, Tabel 4.19, Tabel 4.20 dan selengkapnya pada Lampiran 6.

Tabel 4.18 Wawancara Klausul 8 Dengan Kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)

KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	**Auditor : Riyadi Atmajaya**
	Auditee : Dra. Sri Muryaningsih.MM **NIP. 19651231 199007 2 007**
	Tanggal : 13 juli 2015
	Tanda tangan :
AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)	
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)	
1	Terdapat peraturan pada proses penerimaan pegawai pada DPPKD
	P: Adakah peraturan khusus pada proses penerimaan pegawai pada DPPKD? J: Peraturan penerimaan pegawai pada DPPKD terpusat pada BKD kab Lobar P: Bagaimana peraturan pada proses penerimaan pegawai pada DPPKD ? J: Peraturan berlaku secara umum untuk semua SKPD dan telah di atur oleh BKD P: Adakah dokumentasi peraturan pada proses penerimaan pegawai pada DPPKD?

KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	**Auditor : Riyadi Atmajaya**
	Auditee : Dra. Sri Muryaningsih.MM **NIP. 19651231 199007 2 007**
	Tanggal : 13 juli 2015
	Tanda tangan :

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)

Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)

ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)

	 BUPATI LOMBOK BARAT KEPUTUSAN BUPATI LOMBOK BARAT Nomor : 161.A /800/102.1/BKD/2014 PENETAPAN KELULUSAN PESERTA SELEKSI CPNS TAHUN 2013 DARI TENAGA HONORER KATEGORI II PEMERINTAH KABUPATEN LOMBOK BARAT BUPATI LOMBOK BARAT, Menimbang : a. bahwa surat Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor B/789/M.PAN/2/2014 tanggal 9 Februari 2014 Perihal Pengumuman Kelulusan Peserta Seleksi CPNS Tahun 2013 Dari Tenaga Honorer Kategori II, perlu ditindaklanjuti dengan menetapkan keputusan bupati; b. bahwa berdasarkan pertimbangan sebagaimana dimaksud huruf a, perlu menetapkan Keputusan Bupati tentang Penetapan Kelulusan Peserta Seleksi CPNS Tahun 2013 Dari Tenaga Honorer Kategori II Pemerintah Kabupaten Lombok Barat. J: Ada di BKD => Sk penetapan pengangkatan K2
2	Terdapat prosedur kebijakan tanggung jawab pegawai terhadap perlindungan aset
	P: Apakah organisasi telah melakukan perlindungan terhadap aset pada peran dan tanggung jawab pegawai di DPPKD? J: Iya P: Siapakah yang membuat perlindungan aset yang sesuai dengan peran dan tanggung jawab pegawai tersebut? J: Aset menjadi tanggung jawab semua pegawai secara umum & bendahara barang secara khusus dengan berkordinasi dengan badan aset daerah P: Apakah ada dokumentasinya dari perlindungan aset tersebut ? J: ada di kantor aset daerah
3	Terdapat peran dan tanggung jawab dalam melaksanakan dan bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada
	P: Apakah peran dan tanggung jawab pegawai sudah sesuai dengan kebijakan keamanan informasi yang diterapkan instansi? J: Secara umum sudah

KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	**Auditor : Riyadi Atmajaya**
	Auditee : Dra. Sri Muryaningsih.MM **NIP. 19651231 199007 2 007**
	Tanggal : 13 juli 2015
	Tanda tangan :

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)

Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)

ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)

	P: Siapa yang membuat kebijakan keamanan informasi yang mengatur peran dan tanggung jawab pegawai tersebut? J: BKD P: Apakah terdapat dokumentasi kebijakan keamanan informasi insatansi yang khusus mengatur peran dan tanggung jawab pegawai? J: Iya ada sudah melekat , pada tugas pokok dan fungsi masing-masing . doc pada peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja dinas pendapatan dan pengelolaan keuangan daerah kabupaten lombok barat
4	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi
	P: Apakah telah dilakukan pelaporan apabila ada suatu ancaman yang beresiko bagi keamanan organisasi instansi? J: belum ada P: Siapa yang bertanggung jawab atas laporan peristiwa yang memiliki potensi resiko pada keamanan informasi yang ada? J: BKD P: Apakah terdapat dokumentasi atas laporan peristiwa yang berpotensi beresiko pada keamanan informasi yang ada? J: Iya ada sudah melekat , pada tugas pokok dan fungsi masing-masing. doc pada peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja dinas pendapatan dan pengelolaan keuangan daerah kabupaten lombok barat

Tabel 4.19 Wawancara Klausul 9 Dengan Kontrol 9.1.1 Pembatasan Keamanan Fisik (*Physical security perimeter*)

KLAUSUL 9(KEAMANAN FISIK DAN LINGKUNGAN)	**Auditor : Riyadi Atmajaya**
	Auditee : Ikhwania safitri, SE **NIP. 19790723 200501 2 017**
	Tanggal : 27 juli 2015
	Tanda tangan :
AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.1 Pembatas keamanan fisik	
1	Terdapat batas perimeter yang jelas pada tempat fasilitas informasi yang aman secara fisik
	P: Apakah terdapat batas fisik dan seperti apa batas yang terdapat di dalam ruangan DPPKD untuk melindungi pemrosesan informasi yang sedang berlangsung? J: Iya , tembok, sekat ruangan, akses pintu keluar masuk P: Apakah batas fisik tersebut terjamin keamanannya secara optimal untuk melindungi kegiatan pemrosesan informasi yang sedang berlangsung? J: Iya , karena akses pintu keluar masuk dapat terkontrol atau terlihat siapa saja yg masuk keruangan tersebut P: Apakah batas fisik tersebut telah dibuat sesuai standar keamanan yang layak? Terbuat dari bahan apakah pembatas fisik tersebut? J: Iya , dinding, kaca dan pintu dari bahan standart P: Apakah ada prosedur keamanan yang mengatur tentang batas fisik tersebut? J: tidak secara tertulis P:Apakah di ruangan DPPKD terdapat kaca yang memiliki pandangan keluar gedung dan apakah kaca tersebut terbuat dari bahan yang kuat dan tidak mudah pecah? J: Iya, bahan tersebut standart dan mudah pecah P: Apakah selama ini pernah terjadi insiden pelemparan kaca kantor DPPKD? Apakah ada standar khusus untuk kaca harus terbuat dari apa untuk ruang DPPKD ini? J: Tidak pernah terjadi , karena lingkungan kantor selalu dijaga baik , penjaga malam maupun sat pol pp
2	Akses menuju tempat kerja harus dibatasi hanya untuk pesonil dengan otorisasi.
	P: Siapakah yang menempati ruangan pemrosesan informasi di sini? J: Personil/pengguna pemprosesan data dan informasi

KLAUSUL 9(KEAMANAN FISIK DAN LINGKUNGAN)	**Auditor : Riyadi Atmajaya**
	Auditee : Ikhwania safitri, SE NIP. 19790723 200501 2 017
	Tanggal : 27 juli 2015
	Tanda tangan :

AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)

Klausul 9.1 Wilayah Aman (*Secure Areas*)

ISO 27002 9.1.1 Pembatas keamanan fisik

	P: Perlindungan seperti apakah yang digunakan untuk melindungi tempat kerja yang khusus hanya personil dengan otorisasi saja yang boleh masuk?(pintu,kartu akses,penjaga pintu,dll) J: Pintu, dan otoritas / password masing-masing personil P: Apakah terdapat cctv (close circuit tele vision) yang ditempatkan di lokasi yang ideal untuk merekam keluar masuknya pegawai? Apakah di dalam ruang kerja atau pemrosesan informasi juga ada cctv? J: Tidak terdapat CCTV di kedua tempat yang di maksud P: Apakah ada dokumen yang mengatur bahwa untuk akses menuju tempat kerja dibatasi hanya untuk personil dengan otorisasi? J: belum ada dokumen
3	Semua pintu darurat dalam batas parimeter keamanan harus dipasang tanda bahaya dan tertutup rapat.
	P: Apakah pintu darurat telah dipasang sesuai standar keamanan dan tertutup rapat? J: Tidak terdapat pintu darurat P: Standar yang dimaksud di sini seperti apa ? Mungkin bisa dijelaskan? (missal kalau pintu darurat, khusus pintu darurat harus memiliki criteria khusus bahwa pegangan pintunya harus terbuat dari bahan apa dan bentuknya harus seperti apa, dll) J: P: Bagaimana kontrol pengawasan apabila terjadi bencana mendadak seperti kebakaran, banjir atau gempa? J: Tidak pernah dilakukan simulasi, ataupun kontrol pengamanan P: Apakah setiap pegawai mengetahui di mana saja pintu darurat berada? J: Tidak kanera hanya memiliki pintu keluar masuk yang sifatnya bukan darurat P: Apakah pintu darurat tersebut hanya dapat dibuka dari dalam atau juga dapat

KLAUSUL 9(KEAMANAN FISIK DAN LINGKUNGAN)	**Auditor : Riyadi Atmajaya**
	Auditee : Ikhwania safitri, SE NIP. 19790723 200501 2 017
	Tanggal : 27 juli 2015
	Tanda tangan :
AUDIT KEAMANAN SISTEM INFORMASI KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)	
Klausul 9.1 Wilayah Aman (*Secure Areas*)	
ISO 27002 9.1.1 Pembatas keamanan fisik	
	dibuka dari luar? (Kalaupun dapat dibuka dari luar , hanya dengan menggunakan kunci yang dimiliki oleh orang-orang yang telah ditunjuk misalnya personal keamanan gedung) J:
4	Orang yang akan ke wilayah aman harus diawasi
	P: Apakah ada peraturan/persyaratan khusus untuk orang lain selain pegawai yang akan mengunjungi wilayah aman seperti ruang server dan wilayah aman lainnya? Seperti apakah persyaratan/peraturan tersebut? J: Iya , namun tidak tertulis . yang dapat masuk hanya vendor dan admin P: Apakah ada pencatatan khusus apabila ada yang keluar masuk ruangan DPPKD? J: Tidak ada P: Adakah cctv yang mengawasi siapa saja yang masuk dan keluar ke wilayah aman? J: Tidak ada

Tabel 4.20 Wawancara Klausul 11 Dengan Kontrol 11.5.3 Sistem Manajemen *Password*

KLAUSUL 11(KONTROL AKSES)	Auditor: Riyadi Atmajaya
	Auditee: Normansyah, SE NIP. 19810921 200501 1 006
	Tanggal: 27 juli 2015
	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*	

KLAUSUL 11(KONTROL AKSES)	Auditor: Riyadi Atmajaya
	Auditee: Normansyah, SE NIP. 19810921 200501 1 006
	Tanggal: 27 juli 2015
	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: Pada umumnya sudah P: Apakah terdapat dokumentasi khusus mengenai manajemen password sehingga dapat menjaga tingkat kebenarannya? J: Tidak terdapat dokumentasi mengenai manajemen password P: Bagaimana mensosialisasikan pentingnya manajemen password individu kepada pengguna sehingga dapat menjaga tingkat kebenarannya? J: Hanya sebatas pemberitahuan lisan
2	Terdapat kepastian dalam pemilihan password yang berkualitas
	P: Apakah terdapat pemilihan password berkualitas? J: Iya P: Apa saja kriteria dalam pemilihan password berkualitas? J: Dengan mengkombinasikan angka dan huruf P: Apakah telah dilakukan kepastian tiap penggunanya bahwa dia telah memiliki password yang berkualitas? J: Pada umumnya sudah
3	Terdapat pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi untuk memperbolehkan dalam kesalahan inputan
	P: Apakah pengguna diberikan pemilihan password? J: Tidak karena password yang membuat admin , untuk pemilihan password di serahkan hanya ke pada admin saja. P: Apakah pengguna diberikan hak dalam pengubahan password? J: Hanya admin yang memiliki hak merubah password P: Apakah ada prosedur konfirmasi dalam memperbolehkan dalam kesalahan inputan? J: Ada dengan munculnya pesan di layar password salah

KLAUSUL 11(KONTROL AKSES)	Auditor: Riyadi Atmajaya
	Auditee: Normansyah, SE NIP. 19810921 200501 1 006
	Tanggal: 27 juli 2015
	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*	
4	Terdapat pernyataan mengenai larangan menampilkan password di layar ketika dimasukkan
	P: Apakah layar sudah tidak menampilkan password ketika dimasukkan? J: iya P: Apa bukti tidak menampilkan password yang dimasukkan? J: Dengan mengganti form password menjadi lambang titik-titik P: Apakah keseluruhan layar pada staf pengguna sudah tidak menampilkan password ketika dimasukkan? J: Sudah
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: Tidak ada P: Apakah dalam pemilihan password saat melakukan pengubahan pada log-on pertama dilakukan sudah dilakukan oleh keseluruhan pengguna? J: Tidak pernah karena password sudah tinggal di pakai , untuk perubahan password itu otoritas admin terkait P: Apakah pemilihan password dilakukan pengguna itu sendiri? J: Tidak dilakukan oleh admin
6	Terdapat penyimpana catatan password pengguna sebelumnya secara aman
	P: Apakah penyimpanan catatan password pengguna sebelumnya sudah dilakukan secara aman? J: Tidak ada penyimpanan catatan password , karena pada umumnya semua pegawai mengetahui password masuk ke dalam aplikasi simda , namun hanya untuk pegawai yang memang tugasnya menggunakan aplikasi simda ini. P: Bagaimana cara mengamankan penyimpanan catatan password pengguna sebelumnya? J: Tidak pernah membuat catatan password, namun mungkin ada beberapa

KLAUSUL 11(KONTROL AKSES)	Auditor: Riyadi Atmajaya
	Auditee: Normansyah, SE NIP. 19810921 200501 1 006
	Tanggal: 27 juli 2015
	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*	
	pegawai yang menyimpan password dalam ponselnya sendiri 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: Iya P: Apakah menggunakan algoritma enkripsi one-way pada penyimpanan password? J: Iya kombinasi angka dan huruf / karakter unik P: Apa alternative lain jika organisasi tidak menggunakan algoritma enkripsi one-way? J: tidak ada

4.3.2 Hasil Pemeriksaan Data Bukti

Setiap langkah pemeriksaan yang ada dalam program audit dilaksanakan oleh auditor TI dengan menggunakan satu atau lebih teknik audit yang sesuai dan disertai data /bukti pendukung yang memadai / mencukupi. Wawancara dan observasi, serta pengujian fisik secara langsung dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Hasilnya berupa bukti-bukti berupa foto, dokumen, rekaman dan data-data pendukung lainnya di dinas DPPKD. Beberapa contoh dokumen pemeriksaan pada klausul 8

(Delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*), klausul 9 (Sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (Pembatasan Keamanan Fisik (*Physical security perimeter*)) dan klausul 11 (Sebelas) Kontrol Akses dengan kontrol 11.5.3 Sistem Manajemen *Password* dapat dilihat pada Tabel 4.21, Tabel 4.22 dan Tabel 4.23 untuk bukti foto, dokumen selengkapnya dapat dilihat pada Lampiran 9, untuk dokumen pemeriksaan data audit dapat dilihat di Lampiran 7.

Tabel 4.21 Dokumen Pemeriksaan Data Pada Klausul 8 Dengan Kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)		Pemeriksa : Bpk Haryanto Tanuwijaya/Bpk Erwin Sutomo	
		Auditor : Riyadi Atmajaya	
		Auditee : Dra Sri Muryaningsih	
		Tanggal : 29 juli – 21agustus 2015	
		Tanda Tangan :	
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)			
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)			
No.	Pemeriksaan	Catatan Pemeriksa	Catatan Review
1.	Identifikasi peraturan pada proses penerimaan pegawai Dengan cara: 1. Wawancara untuk proses penerimaan pegawai 2. Dapatkan dokumen mengenai peraturan pada proses penerimaan pegawai	Telah dilakukan pemeriksaan bahwa terdapat peraturan khusus pada proses penerimaan pegawai di dinas pendapatan dan pengolaan keuangan daerah, penerimaan pegawai terpusat di kantor bupati lombok barat (BKD) , lalu di lakukan seleksi penerimaan pegawai dan di atur dalam dokumen keputusan bupati lombok barat no	Telah terdapat peraturan khusus penerimaan PNS, di dinas DPPKD lombok barat serta terdapat pula dokument yang mengatur tentang penerimaan pegawai di dinas pendapatan dan pengelolaan keuangan daerah lombok barat.

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	Pemeriksa : Bpk Haryanto Tanuwijaya/Bpk Erwin Sutomo
	Auditor : Riyadi Atmajaya
	Auditee : Dra Sri Muryaningsih
	Tanggal : 29 juli – 21agustus 2015
	Tanda Tangan :

Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)

ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)

No.	Pemeriksaan	Catatan Pemeriksa	Catatan Review
		: 503 .B / 800/25274/BKD/2014	
2.	Identifikasi prosedur kebijakan mengenai tanggung jawab pegawai terhadap perlindungan aset Dengan cara: 1. Wawancara mengenai tanggung jawab pegawai terhadap perlindungan aset 2. Dapatkan dokumen mengenai perlindungan aset	Telah diperiksa bahwa dilakukan perlindungan aset oleh kantor asset daerah lombok barat. Dan dokumentasinya juga berada di kantor aset daerah.	Terdapat dokumen tanggung jawab pegawai dalam melindungi aset oleh dinas aset daerah lombok barat
3.	Identifikasi peran dan tanggung jawab dalam bertindak sesuai dengan kebijakan keamanan informasi organisasi yang ada Dengan cara: 1. Wawancara mengenai peran dan tanggung jawab sesuai kebijakan yang berlaku	Telah dilakukan pemeriksaan bahwa peran dan tanggung jawab karyawan telah tertuang pada topuksi pegawai di dalam dokumen peraturan bupati lombok barat NO 35 TAHUN 2011 TENTANG RINCIAN TUGAS, FUNGSI DAN TATA KERJA tentang tanggung jawab yang dimiliki masing masing pihak seperti	Peran dan tanggung jawab pegawai di dinas DPPKD sudah tertuang dalam dokumen peraturan bupati lombok barat. NO 35 TAHUN 2011 TENTANG RINCIAN TUGAS, FUNGSI DAN TATA KERJA tentang tanggung jawab yang dimiliki masing masing pihak seperti karyawan, pekerja kontrak, dan mitra kerja.

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)	Pemeriksa : Bpk Haryanto Tanuwijaya/Bpk Erwin Sutomo
	Auditor : Riyadi Atmajaya
	Auditee : Dra Sri Muryaningsih
	Tanggal : 29 juli – 21agustus 2015
	Tanda Tangan :

Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)

ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)

No.	Pemeriksaan	Catatan Pemeriksa	Catatan Review
	2. Dapatkan dokumentasi mengenai kebijakan keamanan informasi perusahaan yang khusus mengatur peran dan tanggung jawab karyawan	karyawan, pekerja kontrak, dan mitra kerja.	
4.	Identifikasi tentang kepastian mengenai tanggung jawab pegawai sudah diberikan demi melindungi keamanan informasi Dengan cara: 1. Wawancara mengenai tanggung jawab pegawai demi perlindungan keamanan informasi 2. Dapatkan dokumentasi atau laporan mengenai peristiwa yang berpotensi beresiko pada	Telah dilakukan pemeriksaan pada pelaporan jika terjadi suatu peristiwa yang memiliki resiko pada keamanan informasi yang ada oleh pihak yang terkait, dan dokumentasinya tertuang dalam tupoksi.	Dokumentasi tentang kepastian tanggung jawab pegawai dalam melindungi keamanan informasi tertuang dalam tupoksi pegawai masing-masing.

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)		Pemeriksa : Bpk Haryanto Tanuwijaya/Bpk Erwin Sutomo	
		Auditor : Riyadi Atmajaya	
		Auditee : Dra Sri Muryaningsih	
		Tanggal : 29 juli – 21agustus 2015	
		Tanda Tangan :	
Klausul 8.1 Sebelum Menjadi Pegawai (*Prior to Employement*)			
ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*)			
No.	Pemeriksaan	Catatan Pemeriksa	Catatan Review
	keamanan informasi		

Tabel 4.22 Dokumen Pemeriksaan Data Pada Klausul 9 Dengan Kontrol 9.1.1 Pembatas Keamanan Fisik (*Physical security perimeter*)

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)		Pemeriksa : Bpk Haryanto Tanuwijaya/Bpk Erwin Sutomo	
		Auditor : Riyadi Atmajaya	
		Auditee : Ikhwania safitri, SE	
		Tanggal : 4 Agustus – 27agustus 2015	
		Tanda Tangan :	
Klausul 9.1 Wilayah Aman (*Secure Area*)			
ISO 27002 9.1.1 Pembatasan keamanan fisik			
No.	Pemeriksaan	Catatan Auditor	Catatan Review
1.	Identifikasi batas perimeter yang jelas pada tempat fasilitas informasi yang aman secara fisik Dengan cara 1. Wawancara 2. Dapatkan dokumen atau prosedur keamanan yang mengatur tentang batas fisik tersebut 3. Survey	Telah diperiksa bahwa ada batas fisik yang terdapat di dalam ruangan DPPKD yaitu berupa sekat ,tembok, Namun bahan sekat , kaca, dan pintu terbuat dari bahan standart Tidak terdapat dokumen yang mengatur tentang prosedur keamanan batas fisik , namun terdapat peraturannya hanya sebatas lisan.	Terdapat batas parameter Di dalam ruang kerja DPPKD, bahan sekat , kaca, pintu terbuat dari bahan standart dan tidak terdapat dokumen yang mengatur tentang prosedur keamanan fisik dan lingkungan.
2	Identifikasi akses menuju	Telah diperiksa bahwa	Tidak memiliki kartu

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)		Pemeriksa : Bpk Haryanto Tanuwijaya/Bpk Erwin Sutomo Auditor : Riyadi Atmajaya Auditee : Ikhwania safitri, SE Tanggal : 4 Agustus – 27agustus 2015 Tanda Tangan :	
Klausul 9.1 Wilayah Aman (*Secure Area*)			
ISO 27002 9.1.1 Pembatasan keamanan fisik			
No.	Pemeriksaan	Catatan Auditor	Catatan Review
.	tempat kerja harus dibatasi hanya untuk pesonil dengan otorisasi Dengan cara 1. Wawancara 2. Dapatkan dokumen yang mengatur bahwa untuk akses menuju tempat kerja dibatasi hanya untuk personil dengan otorisasi.	setiap pegawai memiliki kartu tanda pengenal tetapi tidak memiliki kartu akses khusus yang digunakan untuk masuk ke beberapa ruangan dengan otoritas tertentu dan. Tidak terdapat dokumen yang mengatur untuk akses menuju tempat kerja, tidak terdapat CCTV disetiap ruangan	akses khusus hanya sebatas kartu tanda pengenal pegawai saja dan tidak ada dokumen yang mengatur bahwa untuk akses menuju tempat kerja di batasi hanya untuk personil degan otoritas tertentu. Tidak terdapat CCTV di setiap ruang akses menuju dinas pendapatan dan pengelolaan keuangan daerah lombok barat.
3.	Identifikasi pintu darurat dalam batas parimeter keamanan harus dipasang sesuai standar Dengan cara 1. Wawancara 2. Survey	Telah diperiksa bahwa tidak terdapat pintu darurat di dinas DPPKD ini. Dan tidak pernah di lakukan simulasi jika sewaktu-waktu terjadi bencana atau kontrol keamanan .	Tidak terdapat pintu darurat di DPPKD dan tidak pernah dilakukan simulasi jika sewaktu-waktu terjadi bencana atau kontrol keamanan.
4.	Identifikasi orang yang akan masuk ke wilayah aman harus diawasi Dengan cara 1. Wawancara 2. Survey	Telah diperiksa bahwa terdapat persyaratan khusus untuk orang yg memasuki wilayan aman tapi tidak secara tertulis bagi orang atau pegawai yang memasuki ruangan pemprosesan informasi, hanya admin dan	Terdapat persyaratan kshusus bagi orang yang memasuki wilayah aman (ruang server) tetapi tidak tertulis yang dapat masuk hanya vendor dan admin dan tidak terdapat CCTV

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 9 (KEAMANAN FISIK & LINGKUNGAN)		Pemeriksa : Bpk Haryanto Tanuwijaya/Bpk Erwin Sutomo	
		Auditor : Riyadi Atmajaya	
		Auditee : Ikhwania safitri, SE	
		Tanggal : 4 Agustus – 27agustus 2015	
		Tanda Tangan :	
Klausul 9.1 Wilayah Aman (*Secure Area*)			
ISO 27002 9.1.1 Pembatasan keamanan fisik			
No.	Pemeriksaan	Catatan Auditor	Catatan Review
		vendor. Tidak terdapat CCTV di ruangan pegawai dan ruang menuju wilayah aman.	diruangan pegawai maupun wilayah aman(ruang server).

Tabel 4.23 Dokumen Pemeriksaan Data Pada Klausul 11 Dengan Kontrol 11.5.3 Sistem Manajemen *Password*

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 11 (KONTROL AKSES)		Pemeriksa : Dr. Haryanto Tanuwijaya, S.Kom, M.MT/ Erwin Sutomo, S.Kom, M.Eng	
		Auditor : Riyadi Atmajaya	
		Auditee : Normansyah, SE	
		Tanggal : 4 Agustus – 27agustus 2015	
		Tanda Tangan :	
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)			
ISO 27002 11.5.3 Sistem Manajemen *Password*			
No.	Pemeriksaan	Catatan Pemeriksa	Catatan Review
1	Terdapat manajemen password dengan cara memastikan pengguna password individu untuk menjaga tingkat kebenarannya Dengan cara 1. wawancara 2. dapatkan dokumen manajemen password	Telah dilakukannya pemeriksaan mengenai manajemen password untuk memastikan pengguna password individu sudah terjaga tingkat kebenarannya, namun tidak terdapat dokumentasi khusus mengenai manajemen password sehingga dapat menjaga tingkat kebenarannya, pensosialisasian mengenai pentingnya	Sudah dilakukan pemeriksaan manajemen password indovidu

PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 11 (KONTROL AKSES)		Pemeriksa : Dr. Haryanto Tanuwijaya, S.Kom, M.MT/ Erwin Sutomo, S.Kom, M.Eng	
		Auditor : Riyadi Atmajaya	
		Auditee : Normansyah, SE	
		Tanggal : 4 Agustus – 27agustus 2015	
		Tanda Tangan :	
Klausul 11.5 Kontrol Akses Sistem Operasi (*Operating system access control*)			
ISO 27002 11.5.3 Sistem Manajemen *Password*			
No.	Pemeriksaan	Catatan Pemeriksa	Catatan Review
		manajemen password individu dilakukan sebatas pemberitahuan lisan saja.	
2	Terdapat kepastian dalam pemilihan *password* yang berkualitas Dangan cara 1. wawancara 2. *survey*	Telah dilakaukan pemeriksaan kepastian pemilihan *password* yang berkualitas dengan mengkombinasikan angka dan huruf.	Di dapatkan kepastian dalam pemilihan *password*
3	Terdapat pemilihan dan pengubahan password kepada penggunanya termasuk prosedur konfirmasi untuk memperbolehkan dalam kesalahan inputan Dengan cara 1. wawancara 2. dapatkan dokumen tentang pemilihan password	Telah diperiksa bahwa untuk pemilihan password dan perubahan password dilakaukan oleh administrator saja tidak untuk pengguna / pegawai	Telah diperiksa untuk perubahan dan pemilihan sandi dilakukan hanya oleh admin
4	Terdapat pernyataan mengenai larangan menampilkan password di layar ketika dimasukkan Dangan cara 1. wawancara 2. survey	Telah dilakukan pemeriksaan, terdapat larangan agar tidak menampilkan password di layar saat di inputkan agar terhindar dari	
5	Terdapat pemilihan password saat melakukan pengubahan pada log-on pertama yang dilakukan pengguna itu sendiri Dengan cara 1. wawancara	Telah dilakukan pemeriksaan tidak terdapat pemilihan password saat log on pertama dan tidak ada pemilihan password saat melakukan pengubahan	Di daptkan bahwa tidak terdapat pilihan pengubahan password saat log on pertama oleh pengguna

<table>
<tr><td colspan="2" rowspan="4">PROGRAM PEMERIKSAAN AUDIT KEAMANAN SISTEM INFORMASI ASPEK : KLAUSUL 11 (KONTROL AKSES)</td><td colspan="2">Pemeriksa : Dr. Haryanto Tanuwijaya, S.Kom, M.MT/ Erwin Sutomo, S.Kom, M.Eng</td></tr>
<tr><td colspan="2">Auditor : Riyadi Atmajaya</td></tr>
<tr><td colspan="2">Auditee : Normansyah, SE</td></tr>
<tr><td colspan="2">Tanggal : 4 Agustus – 27agustus 2015</td></tr>
<tr><td colspan="4">Tanda Tangan :</td></tr>
<tr><td colspan="4">Klausul 11.5 Kontrol Akses Sistem Operasi (Operating system access control)</td></tr>
<tr><td colspan="4">ISO 27002 11.5.3 Sistem Manajemen Password</td></tr>
<tr><td>No.</td><td>Pemeriksaan</td><td>Catatan Pemeriksa</td><td>Catatan Review</td></tr>
<tr><td></td><td>2. dokumen tentang perubahan password</td><td>pada log-on pertama dilakukan oleh pengguna dikarenakan password sudah tinggal di pakai , untuk perubahan password itu otoritas admin terkait</td><td></td></tr>
<tr><td>6</td><td>Terdapat penyimpana catatan password pengguna sebelumnya secara aman
Dengan cara
1. wawancara
2. dapatkan dokumen penyimpanan catatan password user secara aman</td><td>Telah diperiksa tidak ada penyimpanan catatan password oleh pengguna/ pegawai dan tidak ada dokumen yang mengatur mengenai penyimpanan catatan password.</td><td>Tidak terdapat penyimpanan catatan password oleh pegawai</td></tr>
<tr><td>7</td><td>Terdapat penyimpanan password dalam bentuk enkripsi menggunakan algoritma enkripsi one-way
Dengan cara
1. wawancara
2. survey</td><td>Telah diperksa terdapat penyimpanan password dalam bentuk enkripsi dan menggunkanan algoritma</td><td></td></tr>
</table>

4.3.3 Hasil Temuan dan Rekomendasi

Penyusunan temuan dan rekomendasi sebagai hasil evaluasi dari pelaksanaan audit keamanan sistem informasi ini muncul setelah dilakukan pembandingan antara apa yang seharusnya dilakukan dengan proses yang sedang berlangsung pada perusahaan. Dari hasil temuan tersebut kemudian dilaksanakan

rekomendasi yang merupakan rincian temuan serta rekomendasi yang diberikan untuk perbaikan proses keamanan sistem informasi ke depannya. Beberapa contoh temuan dan rekomendasi pada Klausul 8 Dengan Kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*), klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (pembatas keamanan fisik) serta klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.5.3 Sistem Manajemen *Password* dapat dilihat pada Tabel 4.24, Tabel 4.25, Tabel 4.26 dan untuk selengkapnya dapat dilihat pada Lampiran 8.

Tabel 4.24 Daftar Temuan dan Rekomendasi Pada Klausul 8 Dengan Kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities)*

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI				Auditor : Riyadi Atmajaya Auditee : Dra.Sri muryaningsih. MM **NIP. 19651231 199007 2 007**
ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				Tanggal : 13 juli 2015 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
1	Terdapat kepastian bahwa tanggung jawab pegawai benar benar sudah diberikan demi melindungi keamanan informasi	Terdapat dokumentasi mengenai tanggung jawab pegawai dalam menjaga keamanan informasi khususnya mengenai pentingnya menjaga keamanan sistem informasi agar tidak terjadi peristiwa/ ancaman yang berpotensi mengganggu keamanan informasi yang ada. Namun masi saja ada pegawai yang lalai	Ref : ISO 27002 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities* Resiko : Jika masih ada beberapa pegawai yang lalai dalam tanggung jawabnya dalam menjaga atau melindungi keamanan sistem informasi hal ini sangat merugikan instansi DPPKD apabila terjadi kesalahan informasi yang berpotensi menjadi ancaman tidak langsung dilaporkan. Tentu saja hal ini akan berpengaruh kepada pembuatan laporan aset daerah atau laporan keuangan serta terbitnya pembuatan APBD.	Tanggapan : Memang tidak ada prosedur atau dokumen khusus untuk pegawai yang melanggar peraturan mengelai tanggung jawab pegawai dalam menjaga keamanan sitem informasi yang telah ditetapkan oleh instansi. Namun untuk dokumen tugas pokok pegawai untuk tanggung jawabnya setelah menjadi pegawai sudah tertuang dalam tupoksi masing-masing .

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI				Auditor : Riyadi Atmajaya Auditee : Dra.Sri muryaningsih. MM **NIP. 19651231 199007 2 007**
ASPEK : KLAUSUL 8 (KEAMANAN SUMBER DAYA MANUSIA)				Tanggal : 13 juli 2015 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
		dalam tanggung jawabnya menjaga keamanan sistem informasi seperti sering menitipkan pasword pada pegawai lain dan data yang harusnya terlindungi bisa di ketahui oleh pihak luar ini menandakan kurangnya tanggung jawab pegawai dalam keamanan sistem informasi hal ini tentu saja akan merugikan	Rekomendasi : - Seharusnya terdapat sanksi bagi pegawai apabila lalai dalam tanggung jawabnya demi melindungi keamanan informasi yang sudah tertuang pada doc pada peraturan bupati lombok barat nomor 35 tahun 2011 tentang rincian tugas, fungsi dan tata kerja dinas pendapatan dan pengelolaan keuangan daerah kabupaten lombok barat.	

Tabel 4.25 Daftar Temuan dan Rekomendasi Pada Klausul 9 Dengan Kontrol 9.1.1 Pembatas Keamanan Fisik

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI				Auditor : Riyadi Atmajaya Auditee : Ikhwania safitri, SE **NIP. 19790723 200501 2 017**
ASPEK : KLAUSUL 9 (KEAMANAN FISIK DAN LINGKUNGAN)				Tanggal : 27 juli 2015 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
1.	Akses menuju tempat kerja harus dibatasi hanya untuk pesonil dengan otorisasi.	Tidak terdapat dokumen yang mengatur untuk akses menuju tempat kerja ataupun cctv di ruang kerja/ pemrosesan informasi di DPPKD	Ref : ISO 27002 9.1.1 Pembatas keamanan fisik Resiko : Apabila tidak terdapat cctv di ruang kerja/pemrosesan informasi pada dinas DPPKD, maka kegiatan memonitoring tidak dapat dilakukan untuk para pegawai saat sedang bekerja atau bukan pegawai yang memasuki lingkungan kantor dari dinas pendapatan dan pengelolaan keuangan daerah Lombok barat. Rekomendasi : - Segera merencanakan untuk memasang cctv yang sesuai standar pada umumnya khususnya di ruangan kerja/ arah menuju tempat pemrosesan informasi di DPPKD	Tanggapan : Memang tidak terdapat Cctv di semua ruangan baik diruangan server, jalan menuju ruang server ,ruang pemprosesan informasi serta di tempat menaik turunkan barang tangga menuju gudang Komitmen Penyelesaian : Kami akan mengusulkan untuk segera mengadakan dan memasang cctv di ruangan kerja/pemrosesan informasi yang ada di DPPKD.

Tabel 4.26 Daftar Temuan dan Rekomendasi Pada Klausul 11 Dengan Kontrol 11.5.3 Sistem Manajemen *Password*

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI				Auditor : Riyadi Atmajaya Auditee : Normansyah, SE
ASPEK : KLAUSUL 11 (KONTROL AKSES)				Tanggal : 27 Agustus 2015 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
1.	Terdapat larangan agar tidak penyimpana catatan *password* pengguna sebelumnya secara tidak aman	Masih ada saja beberapa pegawai yang melanggar dan menyimpan cataan password pada kertas/ handphone Namun tidak terdapat dukumen mengenai manajemen *password*. Tidak ada konsekuensi khusus, hanya\ berupa teguran secara lisan.	Ref : ISO 27002 11.5.3 Sistem Manajemen *Password* Resiko : Password yang seharusnya tidak diketahui oleh yang bukan haknya bisa diketahui dengan melihap alat kumunikasi dimana tempat penyimpanan catatan password disimpan dan lupa membuang kertas dimana catatan password di tulis.Hal ini sangat merugikan pihak instansi apabila tidak di benahi. Rekomendasi : - Segera merencanakan konsekuensi khusus bagi pegawai yang belum sadar akan pentingnya untuk tidak membuat catatan salinan password dan instansi harus konsisten dengan peraturan yang dibuat	Tanggapan : Meskipun sudah ada peraturan atau kebijakan mengenai larangan untuk tidak membuat catatan password namun tingkat kesadaran manajemen keamanannya pegawai masih kurang. Tidak semua pegawai namum ada beberapa pegawai yang kurang akan hal tersebut Komitmen Penyelesaian :

TEMUAN AUDIT KEAMANAN SISTEM INFORMASI				Auditor : Riyadi Atmajaya Auditee : Normansyah, SE
ASPEK : KLAUSUL 11 (KONTROL AKSES)				Tanggal : 27 Agustus 2015 Tanda Tangan :
No	Pernyataan	Temuan	Referensi, Penyebab Risiko dan Rekomendasi	Tanggapan dan Komitmen Penyelesaian
			karena tidak ada gunanya peraturan dibuat namun tidak diterapkan/ dipraktikkan.	

Dari hasil wawancara dengan pegawai dari DPPKD dan bukti foto serta wawancara maka didapatkan temuan pada klausul 8 (delapan) Keamanan Sumber Daya Manusia dengan kontrol 8.1.1 Aturan dan tanggung jawab keamanan (*Roles and Responsibilities*) masih terdapat pegawai yang tidak menjalankan tanggung jawabnya yang telah ditetapkan dalam topuksi pegawai, yaitu masi saja ada pegawai yang saling menitipkan password yang sudah jelas bersifat rahasia dan beresiko bagi keamanan informasi instansi, untuk klausul 9 (sembilan) Keamanan Fisik dan Lingkungan dengan kontrol 9.1.1 (pembatas keamanan fisik) yaitu tidak ada cctv di hampir semua ruang kerja/ dalam ruang pemrosesan informasi dan tidak terdapat pintu darurat apabila sewaktu- waktu terjadi bencana di DPPKD dan untuk klausul 11 (sebelas) Kontrol Akses dengan kontrol 11.5.3 Sistem Manajemen *Password* terdapat temuan yaitu masih ada pegawai yang menyimpan catatan password pada kertas / smartphone hal ini jelas menandakan kurang disiplin dalam menjaga kerahasiaan passwordnya. Dari hasil temuan yang didapatkan pada klausul 8 dengan kontrol 8.1.1 maka rekomendasi yang dapat diberikan adalah dengan memberikan konsekuensi kepada pegawai apabila memberitahukan password kepada orang lain atau lalai dalam tanggung jawabnya sebagai pegawai , walaupun tidak ada dokumen khusus mengenai kebijikan keamanan informasi namun peraturan mengenai pentingnya tanggung jawab menjaga keamanan telah tertuang pada tupoksi pegawai.. Untuk rekomendasi pada temuan klausul 9 dengan kontrol 9.1.1 yaitu segera merencanakan untuk memasang cctv yang sesuai standar pada umumnya khususnya di ruangan kerja/pemrosesan informasi serta membuatkan pintu darurat di dinas pendapatan dan pengelolaan keuangan daerah. Untuk rekomendasi klausul 11 dengan kontrol

11.5.3 yaitu pihak perusahaan segera memberi konsekuensi khusus kepada pegawai yang dengan sengaja menitipkan password atau membuat salinan password pada kerta atau smartphone tersebut, dan dibuatkan dokumentasi khusus mengenai manajemen password.

4.4 Hasil Pelaporan Audit Keamanan Sistem Informasi

Tahap pelaporan adalah tahap untuk melaporkan secara resmi sebagai suatu bentuk penyelesaian proses audit yang dilakukan. Hasil pelaporan audit diserahkan kepada pihak yang berwenang saja dikarenakan bersifat tertutup untuk kalangan umum atau rahasia.

4.4.1 Hasil Permintaan Tanggapan Atas Daftar Temuan Audit Keamanan Sistem Informasi

Permintaan tanggapan atas daftar temuan audit dilakukan oleh auditor kepada *auditee* dengan memberikan tanggapan atas apa yang telah ditemukan auditor dan memberikan komitmen penyelesaiannya. Hasil permintaan tanggapan atas daftar temuan audit telah dilaksanakan dan dapat dilihat pada Lampiran 10.

4.4.2 Penyusunan dan Persetujuan Draft Laporan Audit Keamanan Sistem Informasi

Setelah dilakukan penyusunan draft laporan audit keamanan sistem informasi berupa kertas kerja audit, temuan dan tanggapan a*uditee* sebagai bentuk tanggung jawab atas penugasan audit keamanan sistem informasi yang telah selesai dilaksanakan maka dilakukan persetujuan audit. Hasil persetujuan *draft* laporan audit dapat dilihat pada Lampiran 10.

4.4.3 Pertemuan Penutup atau Pelaporan Audit Keamanan Sistem Informasi

Pertemuan penutup memberikan penjelasan mengenai kondisi yang telah diaudit. Pertemuan penutup dihasilkan berupa *exit meeing* yang dapat dilihat pada Lampiran 11.