BAB IV

HASIL DAN PEMBAHASAN

Pada Bab IV ini akan membahas hasil analisa dan evaluasi yang dilaksanakan mulai dari tahap perencanaan audit dan persiapan audit sistem informasi, tahap pelaksanaan audit sistem informasi, serta tahap pelaporan hasil audit sistem informasi.

4.1 Hasil Perencanaan dan Persiapan Audit Sistem Informasi

Tahap perencanaan dan persiapan ini adalah tahap awal yang dilakukan pada proses audit. Langkah ini dilakukan untuk memastikan bahwa pihak perusahaan yang akan diaudit telah memberikan kewenangan dan mempersiapkan segala sesuatu demi kelancaran pelaksanaan audit yang akan dilakukan.

4.1.1 Hasil Identifikasi Proses Bisnis dan TI

Dari hasil identifikasi proses bisnis dan TI yang telah dilakukan maka diperoleh gambaran umum perusahaan mulai dari profil perusahaan, visi dan misi perusahaan, struktur organisasi, serta gambaran umum lingkungan TI yang ada.

1. Profil Perusahaan

Perseroan Terbatas Aneka Jaya Baut Sejahtera (PT. AJBS) adalah sebuah perusahaan swasta nasional yang berkonsentrasi pada pengadaan perlengkapan dan peralatan pendukung industri. PT. AJBS terus berupaya untuk meningkatkan pelayanan, sejak pendiriannya pada tahun 1966. Sejalan dengan peningkatan volume usaha dan semakin luasnya wilayah usaha, PT. AJBS mengembangkan

sebuah pola manajemen menuju ke arah pengelolaan usaha memperhatikan ketepatan dan kelengkapan pelayanan terhadap pelanggan. Hal ini berarti kualitas sumber daya manusia PT. AJBS menjadi ujung tombak penyediaan kualitas pelayanan yang prima.

PT. AJBS memiliki jenis dan jumlah produk yang besar, hal ini yang mengharuskan PT. AJBS untuk menerapkan teknologi informasi yang memadai. Pengelolaan inventori, transaksi, data pelanggan, dan data supplier, serta keseluruhan pelaporan dan analisa keuangan ditangani dalam sistem operasional yang terintegrasi. Upaya PT. AJBS untuk selalu lebih efisien telah membuahkan koleksi lengkap aneka perlengkapan dan peralatan pendukung industri dengan harga bersaing, dan sesuai dengan tujuan usaha pelanggan PT. AJBS. Dengan kesungguhan untuk mendukung para pelanggan mencapai keberhasilan usaha, PT. AJBS berharap dapat menjadi partner kemajuan industri di Indonesia dan mancanegara.

2. Visi dan Misi PT. Aneka Jaya Baut Sejahtera (PT. AJBS)

Dengan didukung staf karyawan yang berpengalaman di bidang perlengkapan industri dan peralatan pendukung industri, perusahaan senantiasa mengutamakan kepuasan dan kepercayaan pelanggan, dengan menjamin bahwa produk yang dipasarkan dapat memenuhi mutu yang dipersyaratkan, kelengkapan dan jumlah produk yang terjamin, penyerahan produk tepat waktu, serta harga yang bersaing maka ditetapkan visi dan misi perusahaan sebagai berikut.

VISI

Menjadi perusahaan yang terbaik dan terbesar di bidang perlengkapan industri dan peralatan pendukung industri.

MISI

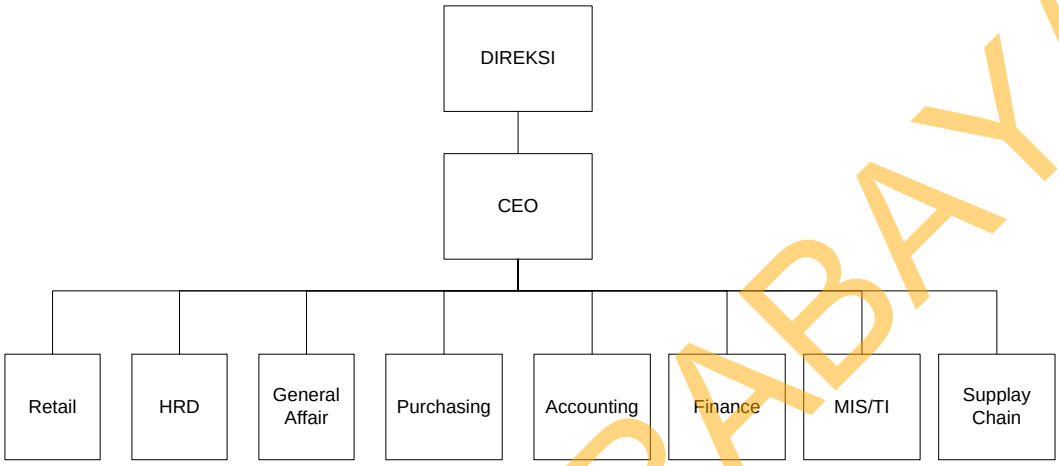
1. Meningkatkan pelayanan dengan jumlah dan kelengkapan stok pendukung penjualan yang terjamin.
2. Meningkatkan efektifitas dan efisiensi dalam semua bidang.
3. Membangun dan mengembangkan kompetensi Sumber Daya Manusia.

3. Struktur Organisasi PT. Aneka Jaya Baut Sejahtera (PT. AJBS)

Secara fungsional struktur organisasi PT. AJBS akan dijabarkan sebagai berikut.

1. Direksi: dalam pelaksanaan pada PT. AJBS ini, dewan direksi diduduki oleh *owner* dari PT. AJBS sendiri.
2. *Chief Executive Officer* (CEO): jabatan tertinggi di bawah Direksi dan mempunyai tugas untuk memimpin suatu perusahaan dan bertanggung jawab untuk kestabilan dan kemajuan PT. AJBS.
3. Departemen-departemen yang memiliki fungsi masing-masing. Departemen-departemen tersebut dibagi menjadi 8 (delapan) departemen yaitu: *Retail*, *Human Resource Development* (HRD), *General Affair*, *Purchasing*, *Accounting*, *Finance*, *Management Information System* (MIS), *Supply Chain*. Dalam tiap departemen masing-masing dikepalai oleh seorang manajer yang bertugas mengatur dan mengarahkan orang lain untuk mencapai tujuan dari departemen tersebut, dibantu oleh para staf dan supervisor yang melakukan supervisi terhadap para staf pelaksanan rutinitas aktivitas bisnis perusahaan sehari-hari.

Gambar bagan struktur organisasi yang ada pada PT. AJBS dapat dilihat pada Gambar 4.1.



Gambar 4.1 Struktur Organisasi PT. AJBS

4. Gambaran Umum Lingkungan Teknologi Informasi

PT. AJBS berlokasi di Jl. Semarang 116 D-E Surabaya. Pengelolaan inventori, transaksi, data pelanggan, dan data supplier, serta keseluruhan pelaporan dan analisa keuangan ditangani dalam sistem operasional yang terintegrasi yang bernama *Integrated Trading System* (ITS). PT. AJBS memiliki 5 (lima) *server* yang beroperasi, yaitu 2 (dua) *server* untuk data aplikasi, 1 (satu) *server* untuk *router* dan *proxy*, 1 (satu) *server* untuk *domain controller*, dan 1 (satu) *server* untuk *mail server*.

4.1.2 Hasil Identifikasi Ruang Lingkup dan Tujuan Audit

Setelah dilakukan observasi maka hasil yang diperoleh adalah penetapan ruang lingkup audit yaitu keamanan sistem informasi dan standar yang digunakan adalah ISO 27002. Dari tahap identifikasi ini dihasilkan juga pemetaan klausul,

objektif kontrol, dan kontrol keamanan yang telah disepakati oleh PT. AJBS. Klausul yang digunakan adalah Klausul 8 tentang Keamanan Sumber Daya Manusia, Klausul 9 tentang Keamanan Fisik dan Lingkungan, Klausul 10 tentang Manajemen Komunikasi dan Operasi kecuali manajemen layanan oleh pihak ketiga, manajemen keamanan jaringan, layanan *e-commerce*, dan hal-hal yang tidak sesuai dengan proses bisnis yang ada pada PT. AJBS, Klausul 11 tentang Kontrol Akses kecuali bagian *teleworking*, Klausul 12 tentang Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan, Klausul 13 tentang Manajemen Kejadian Keamanan Informasi, dan Klausul 14 tentang Manajemen Kelangsungan Bisnis.

Klausul, objektif kontrol, dan kontrol keamanan yang tidak digunakan dapat dilihat pada Tabel 4.1 sedangkan klausul, objektif kontrol, dan kontrol keamanan yang telah ditetapkan dapat dilihat pada Tabel 4.2 di halaman 48. Penentuan ruang lingkup yang telah disepakati ini juga dituangkan ke dalam *engagement letter*.

Tabel 4.1 Klausul, Objektif Kontrol dan Kontrol Keamanan ISO 27002 yang Tidak Digunakan

Klausul	Kontrol Keamanan	Alasan
5 Kebijakan Keamanan	Pada seluruh kontrol keamanan	Perusahaan belum memiliki kebijakan khusus tentang keamanan informasi.
6 Organisasi Keamanan Informasi	Pada seluruh kontrol keamanan	Perusahaan belum memiliki pengaturan untuk menangani keamanan informasi.
7 Manajemen Aset	Pada seluruh kontrol keamanan	Kontrol keamanan yang ada dalam Klausul 7 auditor tidak diijinkan untuk mengaudit manajemen aset perusahaan.

Tabel 4.1 Klausul, Objektif Kontrol dan Kontrol Keamanan ISO 27002 yang Tidak Digunakan (Lanjutan)

Klausul	Kontrol Keamanan	Alasan
10 Manajemen Komunikasi dan Operasi	Seluruh kontrol keamanan dalam objektif kontrol 10.2 Manajemen layanan pengiriman oleh pihak ketiga	Objektif kontrol 10.2 tidak digunakan karena perusahaan tidak menggunakan layanan pengiriman oleh pihak ketiga.
	10.4.2 Kontrol terhadap *mobile code*	Perusahaan tidak menggunakan *mobile code.*
	Seluruh kontrol keamanan dalam objektif kontrol 10.6 Manajemen keamanan jaringan	Objektif kontrol 10.6 tidak digunakan karena auditor tidak mendapatkan ijin untuk mengaudit bagian jaringan dan pengkabelan.
	10.8.2 Perjanjian pertukaran	Kontrol keamanan 10.8.2 tidak digunakan karena perusahaan tidak berhubungan dengan pihak ketiga untuk pertukaran informasi
	10.8.3 Pemindahan media secara fisik	Kontrol keamanan 10.8.3 tidak digunakan karena perusahaan tidak berhubungan dengan pihak ketiga dan tidak terjadi pemindahan media di luar organisasi
	Seluruh kontrol keamanan dalam objektif kontrol 10.9 *Layanan e-commerce*	Objektif kontrol 10.9 tidak digunakan karena perusahaan tidak menggunakan layanan *e-commerce.*
11 Kontrol Akses	11.4.3 Identifikasi peralatan di dalam jaringan	Kontrol keamanan 11.4.3 tidak digunakan karena auditor tidak diijinkan mengaudit peralatan di dalam jaringan.
	11.4.4 Perlindungan *remote diagnostic* dan konfigurasi *port*	Kontrol keamanan 11.4.4 tidak digunakan karena perusahaan tidak menggunakan fasilitas tersebut.
	11.7.2 *Teleworking*	Kontrol keamanan 11.7.2 tidak digunakan karena perusahaan tidak menggunakan *teleworking*

Tabel 4.1 Klausul, Objektif Kontrol dan Kontrol Keamanan
ISO 27002 yang Tidak Digunakan (Lanjutan)

Klausul	Kontrol Keamanan	Alasan
12 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	12.2.3 Integritas pesan	Kontrol keamanan 12.2.3 tidak digunakan karena auditor tidak diijinkan untuk mengaudit bagian tersebut.
	Seluruh kontrol keamanan dalam objektif kontrol 12.3 Kontrol kriptografi	Objektif kontrol 12.3 tidak digunakan karena perusahaan tidak menggunakan kriptografi
	Seluruh kontrol keamanan dalam objektif kontrol 12.4 Keamanan *file* sistem	Objektif kontrol 12.3 tidak digunakan karena auditor tidak mendapatkan ijin untuk mengaudit *file* sistem yang bersifat sangat sensitif dan sangat rahasia.
	12.5.2 Tinjauan teknis aplikasi setelah dilakukan perubahan sistem operasi	Kontrol keamanan 12.5.2 tidak digunakan karena perusahaan tidak melakukan perubahan sistem operasi
	12.5.5 Pembangunan *software* yang di-*outsource*-kan	Kontrol keamanan 12.5.5 tidak digunakan karena perusahaan tidak melakukan *outsource* pembangunan *software*.
15 Kepatutan	Pada seluruh kontrol keamanan	Perusahaan belum pernah melakukan proses audit atau uji kepatutan dalam bentuk apapun.

Tabel 4.2 Klausul, Objektif Kontrol dan Kontrol Keamanan
ISO 27002 yang Telah Ditetapkan

No	Klausul	Objektif Kontrol	Kontrol Keamanan
1	8 Keamanan Sumber Daya Manusia	8.1 Keamanan sumber daya manusia sebelum menjadi pegawai	8.1.1 Aturan dan tanggung jawab
			8.1.2 Seleksi
			8.1.3 Persyaratan dan kondisi yang harus dipenuhi oleh pegawai
		8.2 Selama menjadi pegawai	8.2.1 Tanggung jawab manajemen
			8.2.2 Pendidikan dan pelatihan keamanan informasi
			8.2.3 Proses kedisiplinan

Tabel 4.2 Klausul, Objektif Kontrol dan Kontrol Keamanan
ISO 27002 yang Telah Ditetapkan (Lanjutan)

No	Klausul	Objektif Kontrol	Kontrol Keamanan
	8 Keamanan Sumber Daya Manusia (Lanjutan)	8.3 Pemberhentian atau pemindahan pegawai	8.3.1 Tanggung jawab pemberhentian
			8.3.2 Pengembalian aset
			8.3.3 Penghapusan hak akses
2	9 Keamanan Fisik dan Lingkungan	9.1 Wilayah aman	9.1.1 Pembatas keamanan fisik
			9.1.2 Kontrol masuk fisik
			9.1.3 Keamanan kantor, ruang, dan fasilitasnya
			9.1.4 Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar
			9.1.5 Bekerja di wilayah aman
			9.1.6 Akses publik, area pengiriman, dan penurunan barang
		9.2 Keamanan peralatan	9.2.1 Penempatan peralatan dan perlindungannya
			9.2.2 Utilitas pendukung
			9.2.3 Keamanan pengkabelan
			9.2.4 Pemeliharaan peralatan
			9.2.5 Keamanan peralatan di luar tempat kerja yang tidak diisyaratkan
			9.2.6 Keamanan pembuangan atau pemanfaatan kembali peralatan
			9.2.7 Hak pemindahan peralatan

Tabel 4.2 Klausul, Objektif Kontrol dan Kontrol Keamanan
ISO 27002 yang Telah Ditetapkan (Lanjutan)

No	Klausul	Objektif Kontrol	Kontrol Keamanan
3	10 Manajemen Komunikasi dan Operasi	10.1 Prosedur dan tanggung jawab operasional	10.1.1 Dokumentasi prosedur operasi
			10.1.2 Manajemen pertukaran
			10.1.3 Pemisahan tugas
			10.1.4 Pemisahan pengembangan, pengujian dan operasional fasilitas
		10.3 Perencanaan dan penerimaan sistem	10.3.1 Manajemen kapasitas
			10.3.2 Penerimaan sistem
		10.4 Perlindungan terhadap malicious dan *mobile code*	10.4.1 Kontrol terhadap kode bahaya
		10.5 *Back-up*	10.5.1 *Back-up* sistem informasi
		10.7 Penanganan media	10.7.1 Manajemen pemindahan media
			10.7.2 Pemusnahan atau pembuangan media
			10.7.3 Prosedur penanganan informasi
			10.7.4 Keamanan dokumentasi sistem
		10.8 Pertukaran informasi	10.8.1 Kebijakan dan prosedur pertukaran informasi
			10.8.4 Pesan elektronik
			10.8.5 Sistem informasi bisnis
		10.10 Monitoring	10.10.1 Rekaman audit
			10.10.2 Monitoring penggunaan sistem
			10.10.3 Proteksi catatan informasi
			10.10.4 Catatan administrator dan operator
			10.10.5 Catatan kesalahan
			10.10.6 Sinkronisasi waktu

Tabel 4.2 Klausul, Objektif Kontrol dan Kontrol Keamanan
ISO 27002 yang Telah Ditetapkan (Lanjutan)

No	Klausul	Objektif Kontrol	Kontrol Keamanan
4	11 Kontrol Akses	11.1 Persyaratan bisnis untuk kontrol akses	11.1.1 Kebijakan kontrol akses
		11.2 Manajemen akses *user*	11.2.1 Registrasi pengguna
			11.2.2 Manajemen hak istimewa atau khusus
			11.2.3 Manajemen *password user*
			11.2.4 Tinjauan terhadap hak akses *user*
		11.3 Tanggung jawab pengguna	11.3.1 Penggunaan *password*
			11.3.2 Peralatan pengguna yang tidak dijaga
			11.3.3 Kebijakan *clear desk* dan *clear screen*
		11.4 Kontrol akses jaringan	11.4.1 Kebijakan penggunaan layanan jaringan
			11.4.2 Otentikasi pengguna untuk melakukan koneksi keluar
			11.4.5 Pemisahan dengan jaringan
			11.4.6 Kontrol terhadap koneksi jaringan
			11.4.7 Kontrol terhadap *routing* jaringan
		11.5 Kontrol akses sistem operasi	11.5.1 Prosedur *log-on* yang aman
			11.5.2 Identifikasi dan otentifikasi *user*
			11.5.3 Sistem manajemen *password*
			11.5.4 Penggunaan utilitas sistem
			11.5.5 Sesi *time-out*
			11.5.6 Batasan waktu koneksi
		11.6 Kontrol akses informasi dan aplikasi	11.6.1 Pembatasan akses informasi
			11.6.2 Isolasi sistem yang sensitif
		11.7 Komputasi bergerak dan *teleworking*	11.7.1 Komunikasi dan terkomputerisasi yang bergerak

Tabel 4.2 Klausul, Objektif Kontrol dan Kontrol Keamanan
ISO 27002 yang Telah Dipetakan (Lanjutan)

No	Klausul	Objektif Kontrol	Kontrol Keamanan
5	12 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	12.1 Persyaratan keamanan untuk sistem informasi	12.1.1 Analisa dan spesifikasi persyaratan keamanan
		12.2 Pemrosesan yang benar dalam aplikasi	12.2.1 Validasi data *input*
			12.2.2 Kontrol untuk pemrosesan internal
			12.2.4 Validasi data o*utput*
		12.5 Keamanan dalam pembangunan dan proses-proses pendukung	12.5.1 Prosedur tambahan kontrol
			12.5.3 Pembatasan perubahan paket *software*
			12.5.4 Kelemahan informasi
		12.6 Manajemen teknik kelemahan (*Vurnerability*)	12.6.1 Kontrol terhadap kelemahan secara teknis (*Vurnerability*)
6	13 Manajemen Kejadian Keamanan Informasi	13.1 Pelaporan kejadian dan kelemahan keamanan informasi	13.1.1 Pelaporan kejadian keamanan informasi
			13.1.2 Pelaporan kelemahan keamanan
		13.2 Manajemen kejadian keamanan informasi dan pengembanganya	13.2.1 Tanggung jawab dan prosedur
			13.2.2 Belajar dari kejadian keamanan informasi
			13.2.3 Pengumpulan bukti
7	14 Manajemen Kelangsungan Bisnis	14.1 Aspek keamanan informasi dalam manajemen kelangsungan bisnis	14.1.1 Memasukkan keamanan informasi dalam proses manajemen kelangsungan bisnis
			14.1.2 Kelangsungan bisnis dan penilaian resiko
			14.1.3 Pembangunan dan implementasi rencana kelangsungan yang didalamnya meliputi keamanan informasi
			14.1.4 Kerangka kerja rencana kelangsungan bisnis
			14.1.5 Pengujian, pemeliharaan dan pengkajian ulang rencana kelangsungan bisnis

4.1.3 Hasil Penentuan Metode dan Pembuatan *Engagement Letter*

Pada audit keamanan sistem informasi di PT. AJBS ini menggunakan metode audit kepatutan dengan acuan ISO 27002 sebagai pedomannya serta melakukan wawancara, observasi, dan pemeriksaan sebagai teknik pelaksanaan audit. Setelah menentukan metode dan merancang perencanaan audit, selanjutnya membuat *engagement letter* yang berisi kesepakatan antara auditor dengan pihak perusahaan dan mengajukan permintaan kebutuhan data. Lampiran *engagement letter* yang telah disetujui oleh PT. AJBS dapat dilihat pada Lampiran 2. Lampiran surat pernyataan mengenai hal-hal yang tidak diijinkan yang menjadi keterbatasan dalam audit ini dapat dilihat pada Lampiran 3 dan lampiran beserta permintaan kebutuhan data dapat dilihat pada Lampiran 4.

4.1.4 Hasil Penentuan *Auditee*

Sebelum audit keamanan sistem informasi dilakukan terlebih dahulu menentukan bagian mana di perusahaan yang akan diaudit atau yang disebut *auditee*. Tabel 4.3 menunjukkan bagian yang akan diwawancara berdasarkan klausul yang telah ditentukan.

Tabel 4.3 Hasil Penentuan *Auditee*

Klausul	Deskripsi	*Auditee*
8	Keamanan Sumber Daya Manusia	Bagian HRD
9	Keamanan Fisik dan Lingkungan	Bagian MIS/TI
10	Manajemen Operasi dan Komunikasi	Bagian MIS/TI
11	Kontrol Akses	Bagian MIS/TI
12	Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	Bagian MIS/TI
13	Manajemen Kejadian Keamanan Informasi	Bagian MIS/TI
14	Manajemen Kelangsungan Bisnis	Bagian MIS/TI

4.1.5 Hasil Penentuan Jadwal Audit (*Audit Working Plan*)

Hasil dari proses penyusunan *audit working plan* berupa tabel yang berisi tentang aktifitas yang dilakukan selama audit berlangsung. Pelaksanaan audit keamanan sistem informasi dilakukan secara bertahap sesuai dengan jadwal yang dapat dilihat pada Tabel 4.4 dan detil perencanaan dapat dilihat pada Lampiran 5.

Tabel 4.4 Jadwal Kegiatan Audit (*Audit Working Plan*)

No	Kegiatan	Bulan													
		April				Mei				Juni				Juli	
		1	2	3	4	1	2	3	4	1	2	3	4	1	2
1	Studi Literatur														
2	Penentuan ruang lingkup														
3	Pengumpulan Bukti: • Peninjauan Struktur Organisasi														
	• Peninjauan kebijakan dan prosedur yang terkait dengan TI														
	• Peninjauan standar yang terkait dengan TI														
	• Peninjauan dokumentasi pengelolaan SI/TI														
	• Wawancara														
	• Pengobservasian proses dan kinerja karyawan														
4	Pelaksanaan uji kepatutan														
5	Penentuan tingkat kematangan														
6	Penentuan hasil audit														
7	Penyusunan laporan audit														

4.1.6 Hasil Pembuatan Pernyataan

Hasil dari proses membuat pernyataan berupa tabel yang berisi rincian pernyataan yang sesuai dengan standar ISO 27002. Pernyataan yang telah dibuat dapat dilihat pada Tabel 4.5 dan selanjutnya dapat dilihat pada Lampiran 6.

Tabel 4.5 Hasil Pernyataan pada Kontrol Keamanan Pembatas Keamanan Fisik

Klausul 9: Keamanan Fisik dan Lingkungan	
Kategori Keamanan Utama: 9.1 Wilayah Aman	
Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik	
No	Pernyataan
1	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)
2	Terdapat perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi
Dan seterusnya	

4.1.7 Hasil Pembuatan Pertanyaan

Hasil dari proses pembuatan pertanyaan ini adalah tabel yang berisi pertanyaan sesuai dengan pernyataan yang telah dibuat pada proses sebelumnya. Pertanyaan yang telah dibuat akan diperlukan dan mendukung saat wawancara. Pertanyaan yang telah dibuat dapat dilihat pada Tabel 4.6 dan selengkapnya dapat dilihat pada Lampiran 6.

Tabel 4.6 Hasil Pertanyaan pada Kontrol Keamanan Pembatas Keamanan Fisik

Klausul 9: Keamanan Fisik dan Lingkungan		
Kategori Keamanan Utama: 9.1 Wilayah Aman		
Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik		
No	Pernyataan	Pertanyaan
1	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)	Apakah ada perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)?
2	Terdapat perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi	Apakah ada perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi?
Dan seterusnya		

4.2 Hasil Pelaksanaan Audit Keamanan Sistem Informasi

4.2.1 Hasil Wawancara

Setelah dilakukan proses wawancara maka hasil yang diperoleh adalah dokumen wawancara. Dokumen wawancara merupakan tabel yang berisi pernyataan, pertanyaan, dan jawaban *auditee*. Untuk hasil wawancara yang telah dilakukan dapat dilihat pada Tabel 4.7 dan selengkapnya dapat dilihat pada Lampiran 6.

Tabel 4.7 Dokumen Wawancara pada Kontrol Keamanan Pembatas Keamanan Fisik

Klausul 9: Keamanan Fisik dan Lingkungan			
Kategori Keamanan Utama: 9.1 Wilayah Aman			
Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik			
No	Pernyataan	Pertanyaan	Jawaban
1	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)	Apakah ada perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)?	Terdapat dinding, penjaga pintu, dan resepsionis berawak, namun kartu akses masuk tidak ada. Hanya server yang dibatasi akses masuknya dan terdapat kunci tersendiri.
2	Terdapat perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi	Apakah ada perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi?	Perlindungan fisik berupa dinding, pagar besi harmonika untuk pintu terluar, sekat, kaca, dan ruangan pemrosesan informasi yang dibatasi aksesnya.
Dan seterusnya			

4.2.2 Hasil Pemeriksaan

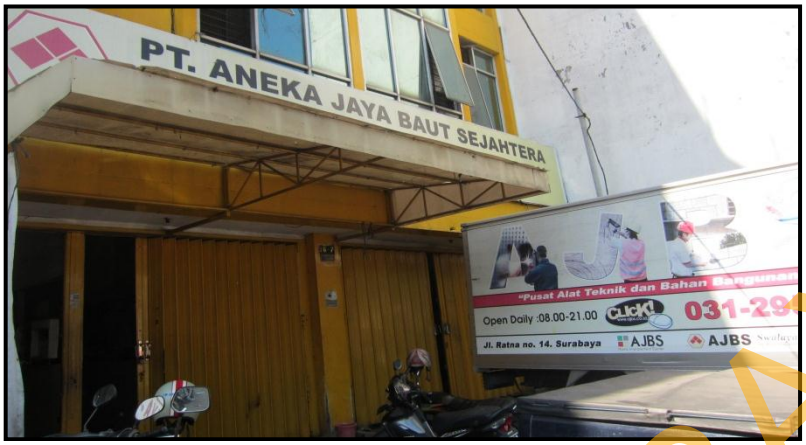
Setelah proses wawancara selesai maka dilakukan pemeriksaan baik melalui observasi maupun pengujian untuk mengetahui dan memastikan secara langsung kebenaran proses yang ada. Daftar percobaan yang dilakukan dapat dilihat pada Lampiran 7. Hasil dari proses pemeriksaan adalah temuan beserta bukti yang dapat dilihat pada Tabel 4.8 dan selanjutnya dapat dilihat pada Lampiran 10.

4.2.3 Hasil Dokumentasi (Data dan Bukti)

Hasil dokumentasi berisi data maupun bukti yang ada mengenai temuan-temuan yang ditemukan saat pelaksanaan audit. Bukti-bukti tersebut dapat berupa foto, rekaman, data atau video. Hasil dokumentasi dapat dilihat pada Tabel 4.8 dan selengkapnya dapat dilihat pada Lampiran 10, sedangkan bukti audit yang berupa dokumentasi foto dapat dilihat pada Gambar 4.2 di halaman 58 dan selengkapnya dapat dilihat pada Lampiran 8. Lampiran daftar akses *user* dapat dilihat pada Lampiran 9.

Tabel 4.8 Hasil Pemeriksaan Pernyataan Pada Kontrol Keamanan Pembatas Keamanan Fisik

Kontrol Keamanan: 9.1.1 Pembatas Keamanan Fisik		
No	Pernyataan	Hasil Pemeriksaan
1	Terdapat perlindungan keamanan fisik seperti dinding, kartu akses masuk atau penjaga pintu.	Perlindungan keamanan fisik telah dikendalikan dengan baik. Bukti: - Terdapat pagar besi harmonika - Terdapat dinding - Terdapat penjaga pintu - Terdapat resepsionis berawak - Tidak terdapat kartu akses masuk - Terdapat kartu tanda pengenal - Ruangan server memiliki batasan akses masuk dan kunci tersendiri.



Gambar 4.2 Pembatas Keamanan Fisik Pagar Besi Harmonika

4.2.4 Hasil Pelaksanaan Uji Kematangan

Berdasarkan analisa dari wawancara dengan *auditee*, pemeriksaan, dan pengumpulan bukti, maka diperoleh hasil uji kepatutan dari tingkat kematangan untuk masing-masing kontrol. Adapun tingkat kematangan tersebut diperoleh dari masing-masing analisa yang dapat dilihat pada kerangka kerja perhitungan *maturity level* pada Lampiran 10. Hasil perhitungan tingkat kematangan hasil audit keamanan sistem informasi adalah sebagai berikut.

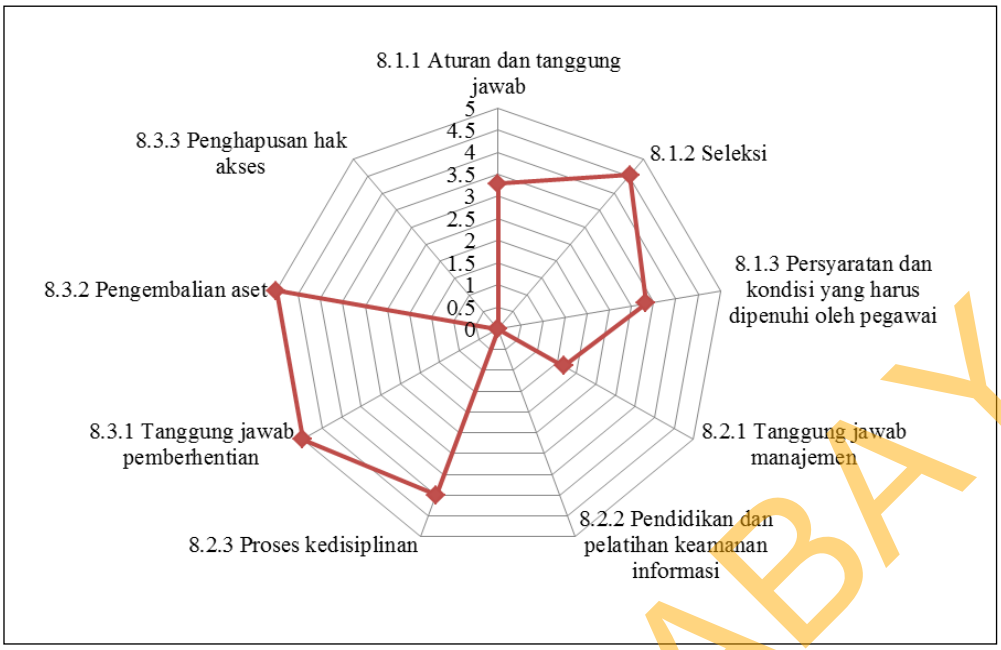
a. Hasil *Maturity Level* Klausul 8 Keamanan Sumber Daya Manusia

Hasil dari proses perhitungan *maturity level* pada klausul 8 keamanan sumber daya manusia adalah 2.98 yaitu *limited/repeatable*. Hasil tersebut menunjukkan bahwa proses keamanan sumber daya manusia yang ada masih dalam pengembangan dan dokumentasi masih terbatas. Hal tersebut dapat dilihat dengan adanya beberapa prosedur yang belum terdokumentasi dan masih banyak kontrol yang belum dilakukan misalnya belum dilakukannya pemeriksaan referensi dan kelayakan karekter, belum ada pelatihan-pelatihan

mengenai prosedur keamanan informasi, perjanjian kerahasiaan belum dijabarkan secara detail dan spesifik. dan lain-lain. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.9. Hasil perhitungan *maturity level* pada klausul 8 keamanan sumber daya manusia dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 8 keamanan sumber daya manusia dapat dilihat pada Gambar 4.3 di halaman 60.

Tabel 4.9 Hasil *Maturity Level* Klausul 8 Keamanan Sumber Daya Manusia

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
8 Keamanan Sumber Daya Manusia	8.1 Keamanan sumber daya manusia sebelum menjadi pegawai	8.1.1 Aturan dan tanggung jawab	3.29	3.72
		8.1.2 Seleksi	4.55	
		8.1.3 Persyaratan dan kondisi yang harus dipenuhi oleh pegawai	3.33	
	8.2 Selama menjadi pegawai	8.2.1 Tanggung jawab manajemen	1.67	1.89
		8.2.2 Pendidikan dan pelatihan keamanan informasi	0.00	
		8.2.3 Proses kedisiplinan	4.00	
	8.3 Pemberhentian atau pemindahan pegawai	8.3.1 Tanggung jawab pemberhentian	5.00	3.33
		8.3.2 Pengembalian aset	5.00	
		8.3.3 Penghapusan hak akses	0.00	
***Marturity level* Klausul 8**				**2.98**



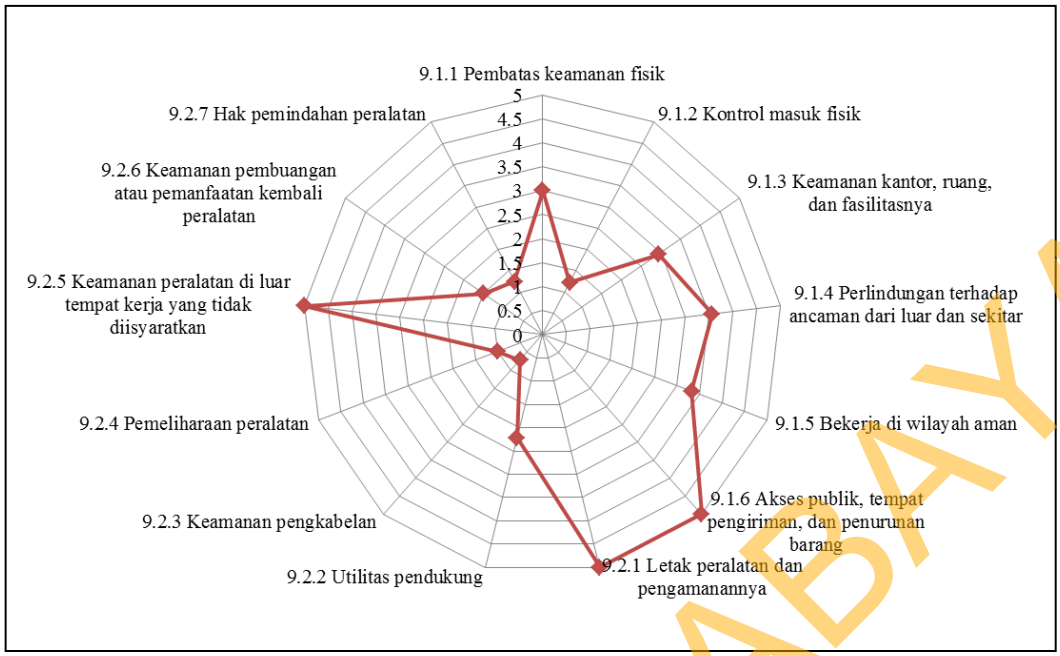
Gambar 4.3 Representasi Nilai *Maturity Level* Klausul 8 Keamanan Sumber Daya Manusia

b. Hasil *Maturity Level* Klausul 9 Wilayah Aman

Hasil dari proses perhitungan *maturity level* pada klausul 9 wilayah aman adalah 2.78 yaitu *limited/repeatable*. Hasil tersebut menunjukkan bahwa proses keamanan wilayah yang ada masih dalam pengembangan dan ada dokumentasi terbatas. Hal tersebut dapat dilihat dengan adanya beberapa prosedur yang belum terdokumentasi dan masih banyak kontrol yang belum dilakukan misalnya pemasangan tanda bahaya, log datang dan perginya pengunjung, pemeliharaan peralatan yang terabaikan, tidak adanya catatan peminjaman peralatan, dan lain-lain. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.10 di halaman 61. Hasil perhitungan *maturity level* pada klausul 9 wilayah aman dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 9 wilayah aman dapat dilihat pada Gambar 4.4 di halaman 62.

Tabel 4.10 Hasil *Maturity Level* Klausul 9 Wilayah Aman

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
9 Keamanan Fisik dan Lingkungan	9.1 Wilayah aman	9.1.1 Pembatas keamanan fisik	3.00	3.18
		9.1.2 Kontrol masuk fisik	1.22	
		9.1.3 Keamanan kantor, ruang dan fasilitasnya	2.94	
		9.1.4 Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar	3.56	
		9.1.5 Bekerja di wilayah aman	3.33	
		9.1.6 Akses publik, area pengiriman dan penurunan barang	5.00	
	9.2 Keamanan peralatan	9.2.1 Penempatan peralatan dan perlindunganya	5.00	2.38
		9.2.2 Utilitas pendukung	2.22	
		9.2.3 Keamanan pengkabelan	0.71	
		9.2.4 Pemeliharaan peralatan	1.00	
		9.2.5 Keamanan peralatan di luar tempat kerja yang tidak diisyaratkan	5.00	
		9.2.6 Keamanan pembuangan atau pemanfaatan kembali peralatan	1.50	
		9.2.7 Hak pemindahan peralatan	1.25	
***Marturity level* Klausul 9**				**2.78**



Gambar 4.4 Representasi Nilai *Maturity Level* Klausul 9 Wilayah Aman

c. Hasil *Maturity Level* Klausul 10 Manajemen Komunikasi dan Operasi

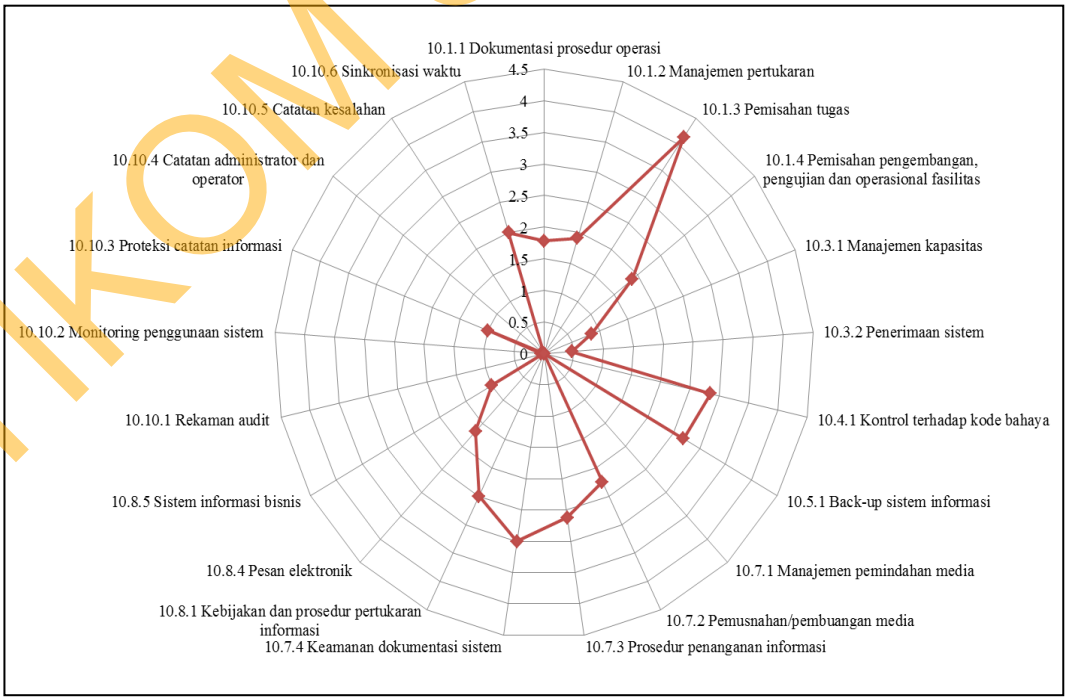
Hasil dari proses perhitungan *maturity level* pada klausul 10 manajemen komunikasi dan operasi adalah 1.46 yaitu *initial*. Hasil tersebut menunjukkan bahwa proses manajemen komunikasi dan operasi dilakukan secara tidak konsisten dan informal. Hal tersebut dapat dilihat dengan adanya beberapa prosedur yang belum terdokumentasi dan masih banyak kontrol yang belum dilakukan misalnya pemisahan pengujian sistem, *back-up* di luar lokasi organisasi, pencatatan informasi, kontrol audit *trail*, dll. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.11 di halaman 63. Hasil perhitungan *maturity level* pada klausul 10 manajemen komunikasi dan operasi dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 10 manajemen komunikasi dan operasi dapat dilihat pada Gambar 4.5 di halaman 64.

Tabel 4.11 Hasil *Maturity Level* Klausul 10 Manajemen Komunikasi dan Operasi

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
10 Manajemen Komunikasi dan Operasi	10.1 Prosedur dan tanggung jawab operasional	10.1.1 Dokumentasi prosedur operasi	1.78	2.43
		10.1.2 Manajemen pertukaran	1.91	
		10.1.3 Pemisahan tugas	4.14	
		10.1.4 Pemisahan pengembangan, pengujian dan operasional fasilitas	1.89	
	10.3 Perencanaan dan penerimaan sistem	10.3.1 Manajemen kapasitas	0.86	0.59
		10.3.2 Penerimaan sistem	0.47	
	10.4 Perlindungan terhadap malicious dan *mobile code*	10.4.1 Kontrol terhadap kode bahaya	2.85	2.85
	10.5 *Back-up*	10.5.1 *Back-up* sistem informasi	2.69	2.69
	10.7 Penanganan media	10.7.1 Manajemen pemindahan media	0.00	1.97
		10.7.2 Pemusnahan atau pembuangan media	2.25	
		10.7.3 Prosedur penanganan informasi	2.62	
		10.7.4 Keamanan dokumentasi sistem	3.00	
	10.8 Pertukaran informasi	10.8.1 Kebijakan dan prosedur pertukaran informasi	2.50	1.72
		10.8.4 Pesan elektronik	1.67	
		10.8.5 Sistem informasi bisnis	1.00	

Tabel 4.11 Hasil *Maturity Level* Klausul 10 Manajemen Komunikasi dan Operasi (Lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
10 Manajemen Komunikasi dan Operasi (Lanjutan)	10.10 Monitoring	10.10.1 Rekaman audit	0.00	0.51
		10.10.2 Monitoring penggunaan sistem	0.05	
		10.10.3 Proteksi catatan informasi	1.00	
		10.10.4 Catatan administrator dan operator	0.00	
		10.10.5 Catatan kesalahan	0.00	
		10.10.6 Sinkronisasi waktu	2.00	
***Marturity level* Klausul 10**				**1.46**



Gambar 4.5 Representasi Nilai *Maturity Level* Klausul 10 Manajemen Komunikasi dan Operasi

d. Hasil *Maturity Level* Klausul 11 Persyaratan Bisnis untuk Kontrol Akses

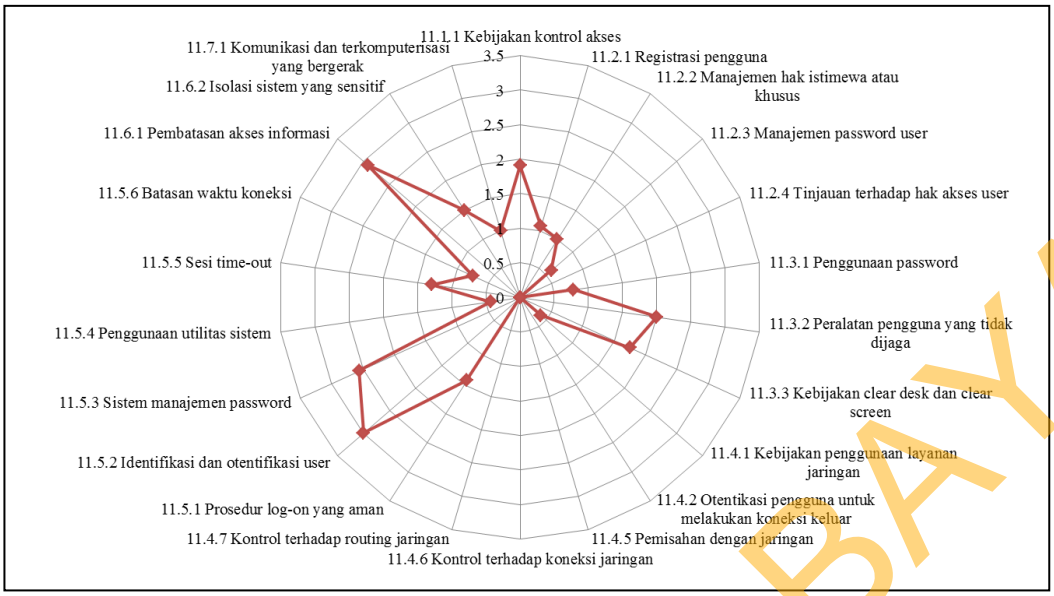
Hasil dari proses perhitungan *maturity level* pada klausul 11 persyaratan bisnis untuk kontrol akses adalah 1.28 yaitu *initial*. Hasil tersebut menunjukkan bahwa proses persyaratan bisnis untuk kontrol akses dilakukan secara tidak konsisten dan informal. Hal tersebut dapat dilihat tidak adanya pernyataan resmi yang ditandatangani untuk menjaga *password*, tidak adanya tinjauan terhadap hak akses *user*, dan terdapat kebijakan yang masih dilakukan secara informal misalnya kebijakan dan otorisasi terhadap keamanan informasi, persyaratan bisnis kontrol akses, persyaratan keamanan, dan lain-lain. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.12. Hasil perhitungan *maturity level* pada klausul 11 persyaratan bisnis untuk kontrol akses dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 11 persyaratan bisnis untuk kontrol akses dapat dilihat pada Gambar 4.6 di halaman 67.

Tabel 4.12 Hasil *Maturity Level* Klausul 11 Kontrol Akses

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
11 Kontrol Akses	11.1 Persyaratan bisnis untuk kontrol akses	11.1.1 Kebijakan kontrol akses	1.91	1.91
	11.2 Manajemen akses user	11.2.1 Registrasi pengguna	1.07	0.67
		11.2.2 Manajemen hak istimewa atau khusus	1.00	
		11.2.3 Manajemen *password user*	0.60	
		11.2.4 Tinjauan terhadap hak akses *user*	0.00	

Tabel 4.12 Hasil *Maturity Level* Klausul 11 Kontrol Akses (Lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
11 Kontrol Akses (Lanjutan)	11.3 Tanggung jawab pengguna	11.3.1 Penggunaan *password*	0.78	1.51
		11.3.2 Peralatan pengguna yang tidak dijaga	2.00	
		11.3.3 Kebijakan *clear desk* dan *clear screen*	1.75	
	11.4 Kontrol akses jaringan	11.4.1 Kebijakan penggunaan layanan jaringan	0.40	0.08
		11.4.2 Otentikasi pengguna untuk melakukan koneksi keluar	0.00	
		11.4.5 Pemisahan dengan jaringan	0.00	
		11.4.6 Kontrol terhadap koneksi jaringan	0.00	
		11.4.7 Kontrol terhadap *routing* jaringan	0.00	
	11.5 Kontrol akses sistem operasi	11.5.1 Prosedur log-on yang aman	1.43	1.58
		11.5.2 Identifikasi dan otentifikasi *user*	3.00	
		11.5.3 Sistem manajemen *password*	2.56	
		11.5.4 Penggunaan utilitas sistem	0.43	
		11.5.5 Sesi *time-out*	1.29	
		11.5.6 Batasan waktu koneksi	0.75	
	11.6 Kontrol akses informasi dan aplikasi	11.6.1 Pembatasan akses informasi	2.92	2.21
		11.6.2 Isolasi sistem yang sensitif	1.50	
	11.7 Komputasi bergerak dan bekerja dari lain tempat/*teleworking*	11.7.1 Komunikasi dan terkomputerisasi yang bergerak	1.00	1.00
***Marturity level* Klausul 11**				**1.28**



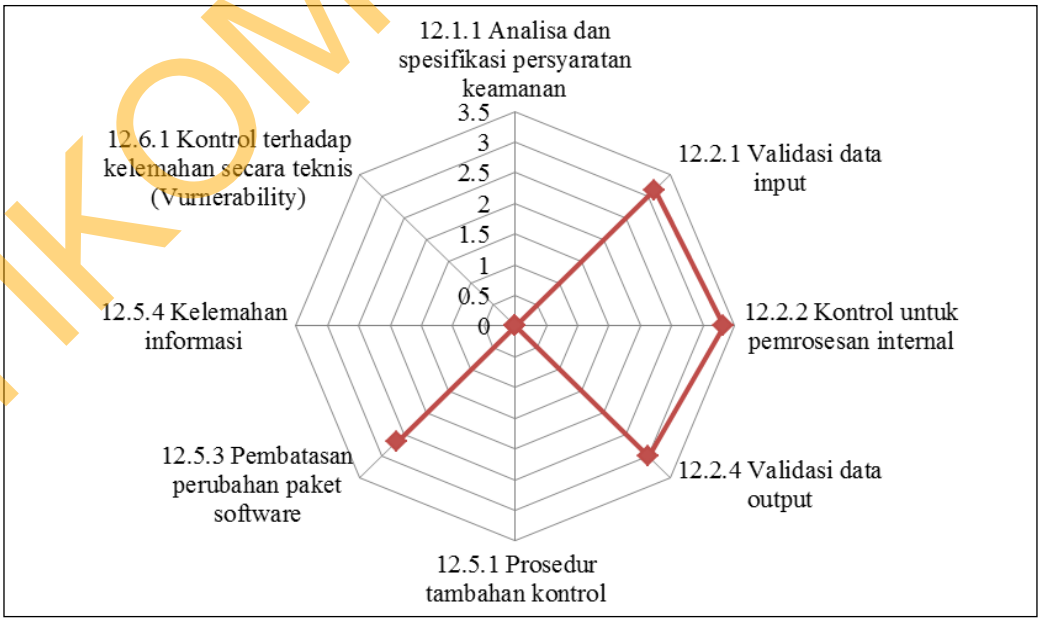
Gambar 4.6 Representasi Nilai *Maturity Level* Klausul 11 Kontrol Akses

e. Hasil *Maturity Level* Klausul 12 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan

Hasil dari proses perhitungan *maturity level* pada 13 manajemen kejadian keamanan informasi adalah 1.01 yaitu *initial*. Hasil tersebut menunjukkan bahwa proses akuisisi sistem informasi, pembangunan, dan pemeliharaan yang ada pada PT. AJBS dilakukan secara tidak konsisten dan informal. Hal tersebut dapat dilihat dengan adanya modifikasi pada *software* telah diuji, hanya saja belum dilakukan pada suatu badan yang independen. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.13 di halaman 68. Hasil perhitungan *maturity level* pada klausul 12 akuisisi sistem informasi, pembangunan, dan pemeliharaan dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 12 akuisisi sistem informasi, pembangunan, dan pemeliharaan dapat dilihat pada Gambar 4.7 di halaman 68.

Tabel 4.13 Hasil *Maturity Level* Klausul 12 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
12 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	12.1 Persyaratan keamanan untuk sistem informasi	12.1.1 Analisa dan spesifikasi persyaratan keamanan	0.00	0.00
	12.2 Pemrosesan yang benar dalam aplikasi	12.2.1 Validasi data *input*	3.00	3.16
		12.2.2 Kontrol untuk pemrosesan internal	3.33	
		12.2.4 Validasi data *output*	2.83	
	12.5 Keamanan dalam pembangunan dan proses-proses pendukung	12.5.1 Prosedur tambahan kontrol	0.00	0.89
		12.5.3 Pembatasan perubahan paket *software*	2.67	
		12.5.4 Kelemahan informasi	0.00	
	12.6 Manajemen teknik kelemahan (*Vurnerability*)	12.6.1 Kontrol terhadap kelemahan secara teknis (*Vurnerability*)	0.00	0.00
***Marturity level* Klausul 12**				**1.01**



Gambar 4.7 Representasi Nilai *Maturity Level* Klausul 12 Akuisisi Sistem Informasi,Pembangunan, dan Pemeliharaan

f. Hasil *Maturity Level* Klausul 13 Manajemen Kejadian Keamanan Informasi

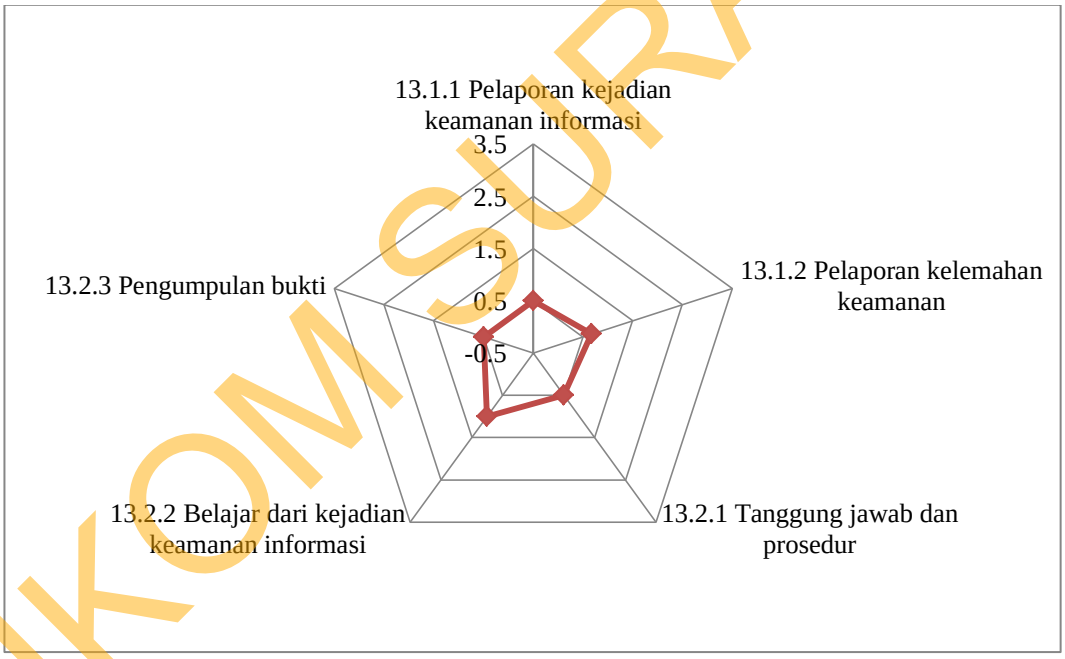
Hasil dari proses perhitungan *maturity level* pada 13 manajemen kejadian keamanan informasi adalah 0.63 yaitu *non-existent*. Hasil tersebut menunjukkan bahwa proses manajemen kejadian keamanan informasi yang ada pada PT. AJBS tidak memiliki kontrol sama sekali. Hal tersebut dapat dilihat dengan banyaknya kontrol yang belum dilakukan misalnya belum ada isyarat untuk mencatat temuan atau dugaan apapun dari kelemahan keamanan dalam sistem atau layanan, tidak ada pengukuran yang dilakukan untuk mengetahui resiko yang terkait, tidak ada prosedur khusus yang dibuat untuk memastikan kecepatan dan keefektivitasan dalam penanganan kejadian keamanan sistem informasi, bukti kejadian keamanan informasi belum dicatat dan dipelihara. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.14. Hasil perhitungan *maturity level* pada klausul 13 manajemen kejadian keamanan informasi dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 13 manajemen kejadian keamanan informasi dapat dilihat pada Gambar 4.8 di halaman 70.

Tabel 4.14 Hasil *Maturity Level* Klausul 13 Manajemen Kejadian Keamanan Informasi

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
13 Manajemen Kejadian Keamanan Informasi	13.1 Pelaporan kejadian dan kelemahan keamanan informasi	13.1.1 Pelaporan kejadian keamanan informasi	0.50	0.59
		13.1.2 Pelaporan kelemahan keamanan	0.67	

Tabel 4.14 Hasil *Maturity Level* Klausul 13 Manajemen Kejadian Keamanan Informasi (Lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
13 Manajemen Kejadian Keamanan Informasi (Lanjutan)	13.2 Manajemen kejadian keamanan informasi dan pengembanganya	13.2.1 Tanggung jawab dan prosedur	0.50	0.67
		13.2.2 Belajar dari kejadian keamanan informasi	1.00	
		13.2.3 Pengumpulan bukti	0.50	
***Marturity level* Klausul 13**				**0.63**



Gambar 4.8 Representasi Nilai *Maturity Level* Klausul 13 Manajemen Kejadian Keamanan Informasi

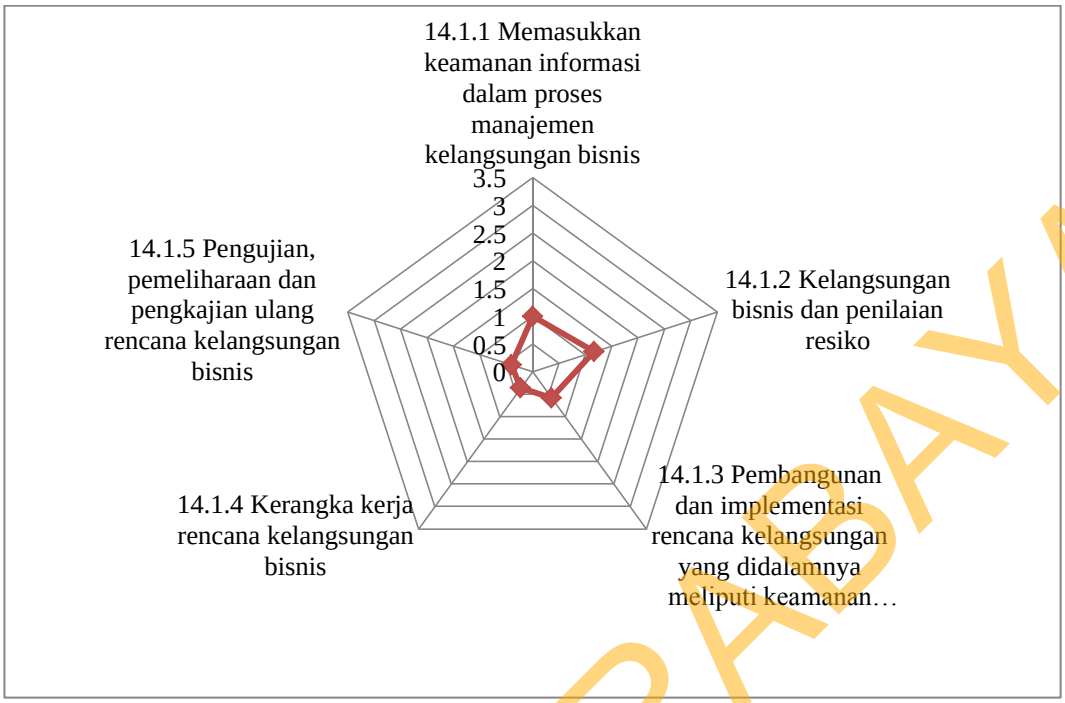
g. Hasil *Maturity Level* Klausul 14 Manajemen Kelangsungan Bisnis

Hasil dari proses perhitungan *maturity level* pada klausul 14 manajemen kelangsungan adalah 0.70 yaitu *non-existent*. Hasil tersebut menunjukkan bahwa proses manajemen kelangsungan bisnis yang ada pada PT. AJBS tidak

memiliki kontrol sama sekali. Hal tersebut dapat dilihat dengan banyaknya kontrol yang belum dilakukan misalnya tidak adanya dokumen rencana kelangsungan bisnis, perhitungan resiko, identifikasi prosedur darurat, penanggung jawab khusus, kontrol perubahan, tidak ada pendidikan atau pelatihan tentang manajemen kelangsungan bisnis, dan lain-lain. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.15. Hasil perhitungan *maturity level* pada klausul 14 manajemen kelangsungan dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 14 manajemen kelangsungan dapat dilihat pada Gambar 4.9 di halaman 72.

Tabel 4.15 Hasil *Maturity Level* Klausul 14 Manajemen Kelangsungan Bisnis

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-rata Objektif Kontrol**
14 Manajemen Kelangsungan Bisnis	14.1 Aspek keamanan informasi dalam manajemen kelangsungan bisnis.	14.1.1 Memasukkan keamanna informasi dalam proses manajemen kelangsungan bisnis	1.00	0.70
		14.1.2 Kelangsungan bisnis dan penilaian resiko	1.17	
		14.1.3 Pembangunan dan implementasi rencana kelangsungan yang didalamnya meliputi keamanan informasi	0.58	
		14.1.4 Kerangka kerja rencana kelangsungan bisnis	0.36	
		14.1.5 Pengujian, pemeliharaan dan pengkajian ulang rencana kelangsungan bisnis	0.40	
***Marturity level* Klausul 14**				**0.70**



Gambar 4.9 Representasi Nilai *Maturity Level* Klausul 14 Manajemen Kelangsungan Bisnis

h. Hasil Pembahasan Audit Keamanan Sistem Informasi PT.AJBS

Berdasarkan audit keamanan sistem informasi yang telah dilakukan, kebocoran informasi yang terjadi merupakan akibat dari adanya penyalahgunaan *password* yang terjadi. Berdasarkan temuan-temuan hasil audit penyalahgunaan *password* yang terjadi disebabkan karena peraturan perusahaan yang kurang tegas dan kurang spesifik untuk kerahasiaan *password*, belum adanya perjanjian atau pernyataan tertulis yang ditandatangani untuk benar-benar menjaga kerahasiaan *password* masing-masing, penerapan manajemen *password* yang tidak sesuai standar, tidak ada tinjauan terhadap hak akses *user*, dan kurangnya kesadaran serta pengetahuan karyawan terhadap pentingnya merahasiakan *password*. Hal tersebut dapat dilihat pada hasil *maturity level* kontrol keamanan 8.2.2 pendidikan dan pelatihan keamanan informasi bernilai 0 (nol), kontrol keamanan 11.2.3

manajemen *password user* yang hanya memiliki nilai 0.60, kontrol keamanan 11.2.4 tinjauan terhadap akses *user* yang bernilai 0 (nol), dan kontrol keamanan 11.3.1 penggunaan *password* yang hanya memiliki nilai 0.78.

Kerusakan-kerusakan peralatan sistem informasi yang terjadi dan sistem yang sering *hang* merupakan salah satu akibat dari kurangnya pemeliharaan yang dilakukan oleh perusahaaan, kurangnya manajemen kapasitas yang dilakukan, dan pemindahan peralatan yang kurang dimanajemen. Hal tersebut dapat dilihat pada hasil *maturity level* kontrol keamanan 9.2.4 pemeliharaan peralatan yang memiliki nilai 1 (satu), kontrol keamanan 9.2.7 hak pemindahan peralatan yang bernilai 1.25, kontrol keamanan 10.3.1 manajemen kapasitas yang memiliki nilai 0.86.

Gangguan-gangguan sistem yang terjadi merupakan akibat dari serangan virus yang mengacau keberlangsungan operasional perusahaan. Berdasarkan temuan-temuan hasil audit permasalahan virus yang terjadi disebabkan oleh tidak ada pelatihan penggunaan perlindungan virus, tidak dilakukan penyelidikan secara formal tentang keberadaan kelompok data tanpa persetujuan, tidak dilakukan penyelidikan secara formal tentang perubahan tanpa otorisasi, dan kurangnya pengetahuan karyawan tentang virus. Hal tersebut dapat dilihat pada hasil *maturity level* kontrol keamanan 10.4.1 kontrol terhadap kode bahaya dengan nilai 2.85. Selain itu juga ditemukan kelemahan-kelemahan perusahaan dalam hal pendokumentasian prosedur-prosedur yang ada, pencatatan insiden keamanan informasi, dan rencana kelangsungan bisnis.

4.2.5 Hasil Penyusunan Daftar Temuan dan Rekomendasi

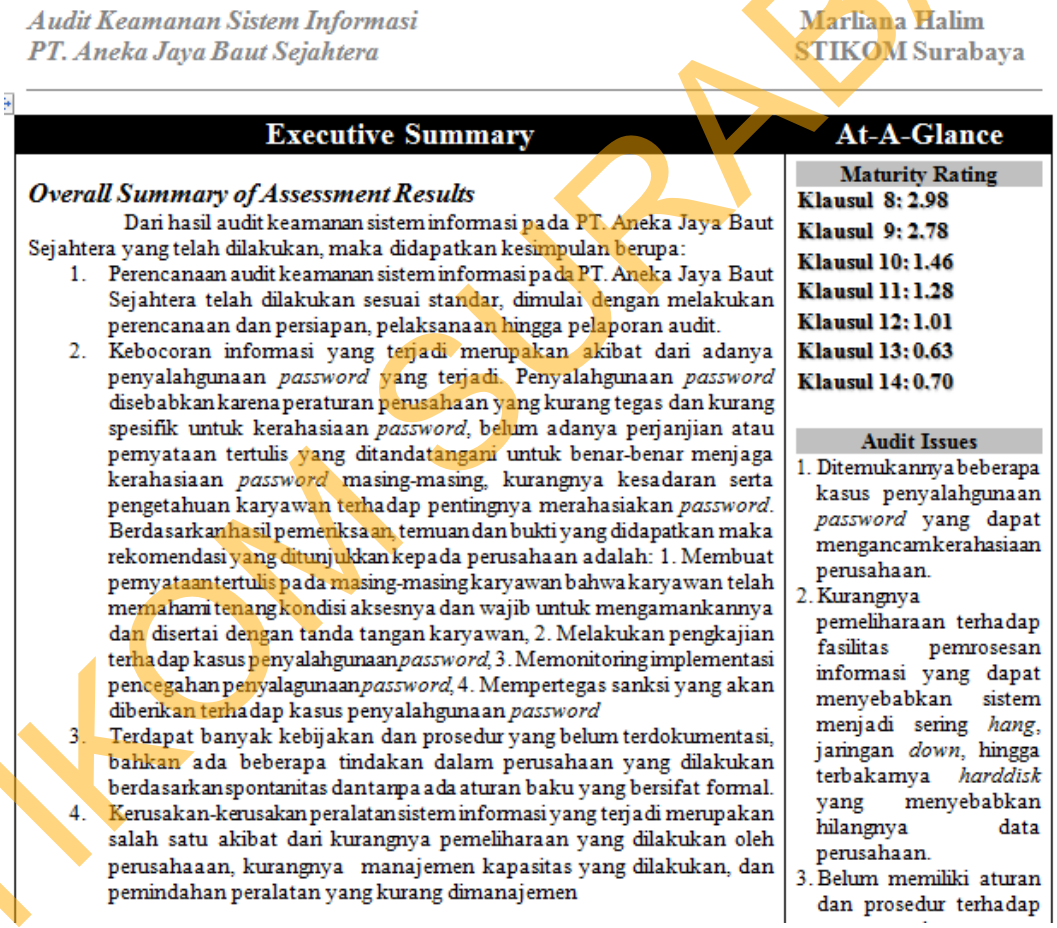
Penyusunan temuan dan rekomendasi sebagai hasil evaluasi dari pelaksanaan audit keamanan sistem informasi ini muncul setelah dilakukan pembandingan antara apa yang seharusnya dilakukan dengan proses yang sedang berlangsung pada perusahaan. Dari hasil temuan tersebut kemudian diberikan rekomendasi yang dapat digunakan untuk perbaikan proses sistem informasi di kemudian hari. Salah satu contoh hasil temuan dan rekomendasi pada klausul 9 keamanan fisik dan lingkungan dengan kontrol keamanan 9.1.2 kontrol masuk fisik dapat dilihat pada Tabel 4.16 dan untuk selengkapnya dapat dilihat pada Lampiran 11.

Tabel 4.16 Hasil Temuan Dan Rekomendasi

No	Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
10	9 Keamanan Fisik dan Lingkungan	9.1 Wilayah aman	9.1.2 Kontrol masuk fisik	Tidak ada pencatatan waktu kunjungan kedatangan maupun kepergian untuk pengunjung. (Bukti: Hasil pemeriksaan pada Lampiran 4 Klausul 9.1.2 no. 1 dan no. 2)	- Membuat buku tamu untuk mencatat kegiatan dan waktu berkunjung - Mengajukan ke direksi untuk penambahan peralatan kontrol otentikasi seperti kartu gesek atau peralatan biometrik lainnya seperti *finger print*. (Ref: Pedoman Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum).

4.3 Hasil Pelaporan Audit Sistem Informasi

Tahap pelaporan yaitu: memberikan laporan audit (*audit report*) sebagai pertanggung jawaban atas penugasan proses audit SI yang dilaksanakan. Laporan audit ditunjukkan kepada pihak yang berhak saja karena laporan audit SI merupakan dokumen yang bersifat rahasia. Hasil laporan audit dapat dilihat Gambar 4.10 dan selengkapnya dapat dilihat pada Lampiran 12.



Audit Keamanan Sistem Informasi
PT. Aneka Jaya Baut Sejahtera

Marliana Halim
STIKOM Surabaya

Executive Summary

Overall Summary of Assessment Results

Dari hasil audit keamanan sistem informasi pada PT. Aneka Jaya Baut Sejahtera yang telah dilakukan, maka didapatkan kesimpulan berupa:

1. Perencanaan audit keamanan sistem informasi pada PT. Aneka Jaya Baut Sejahtera telah dilakukan sesuai standar, dimulai dengan melakukan perencanaan dan persiapan, pelaksanaan hingga pelaporan audit.
2. Kebocoran informasi yang terjadi merupakan akibat dari adanya penyalahgunaan *password* yang terjadi. Penyalahgunaan *password* disebabkan karena peraturan perusahaan yang kurang tegas dan kurang spesifik untuk kerahasiaan *password*, belum adanya perjanjian atau pernyataan tertulis yang ditandatangani untuk benar-benar menjaga kerahasiaan *password* masing-masing, kurangnya kesadaran serta pengetahuan karyawan terhadap pentingnya merahasiakan *password*. Berdasarkan hasil pemeriksaan, temuan dan bukti yang didapatkan maka rekomendasi yang ditunjukkan kepada perusahaan adalah: 1. Membuat pernyataan tertulis pada masing-masing karyawan bahwa karyawan telah memahami tenang kondisi aksesnya dan wajib untuk mengamankannya dan disertai dengan tanda tangan karyawan, 2. Melakukan pengkajian terhadap kasus penyalahgunaan *password*, 3. Memonitoring implementasi pencegahan penyalagunaan *password*, 4. Mempertegas sanksi yang akan diberikan terhadap kasus penyalahgunaan *password*
3. Terdapat banyak kebijakan dan prosedur yang belum terdokumentasi, bahkan ada beberapa tindakan dalam perusahaan yang dilakukan berdasarkan spontanitas dan tanpa ada aturan baku yang bersifat formal.
4. Kerusakan-kerusakan peralatan sistem informasi yang terjadi merupakan salah satu akibat dari kurangnya pemeliharaan yang dilakukan oleh perusahaaan, kurangnya manajemen kapasitas yang dilakukan, dan pemindahan peralatan yang kurang dimanajemen

At-A-Glance

Maturity Rating

Klausul 8: 2.98
Klausul 9: 2.78
Klausul 10: 1.46
Klausul 11: 1.28
Klausul 12: 1.01
Klausul 13: 0.63
Klausul 14: 0.70

Audit Issues

1. Ditemukannya beberapa kasus penyalahgunaan *password* yang dapat mengancam kerahasiaan perusahaan.
2. Kurangnya pemeliharaan terhadap fasilitas pemrosesan informasi yang dapat menyebabkan sistem menjadi sering *hang*, jaringan *down*, hingga terbakarnya *harddisk* yang menyebabkan hilangnya data perusahaan.
3. Belum memiliki aturan dan prosedur terhadap

Gambar 4.10 Laporan Audit Sistem Informasi