BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini akan diuraikan tentang hasil analisis dan pembahasan tahap audit yang dilakukan, antara lain tahap perencanaan audit, tahap persiapan audit, tahap pelaksanaan audit dan tahap pelaporan audit.

4.1. Hasil Perencanaan Audit Sistem Informasi

Hasil dari tahapan perencanaan audit sistem informasi ini adalah identifikasi proses bisnis dan TI, Penentuan ruang lingkup, obyek dan tujuan audit, selain itu menentukan klausul, obyektif kontrol dan kontrol serta membuat surat perjanjian atau yang biasa disebut *Engagement Letter*.

4.1.1. Identifikasi Proses Bisnis dan TI

Pada tahap perencanaan audit ini, identifikasi proses bisnis dan TI merupakan hal pertama yang harus dilakukan untuk mengetahui informasi mengenai perusahaan, sebelum dilakukannya audit yaitu dengan cara memahami dokumen perusahaan antara lain profil perusahaan, visi misi perusahaan dan struktur organisasi perusahaan.

1. Profil Perusahaan

Parahita Diagnostic Center (PDC) adalah perusahaan yang bergerak pada bidang jasa pelayanan kesehatan masyarakat, khususnya pada bidang laboratorium. PDC ini didirikan pada tahun 1987 dengan nama Laboratorium Klinik Pramita. Pada tanggan 1 April 2007 laboratorium ini berubah nama menjadi “Pramita Utama Diagnostic Center” denga berkantor pusat di Jl. Dharmawangsa 66 & 70 Surabaya. Tetapi pada tanggal 1 Juni 2010 perusahaan ini beruba nama menjadi “Parahita

Diagnostic Center". Seiring perkembangannya PDC kini telah memiliki 50 cabang yang tersebar di 11 kota besar di Indonesia, seperti Surabaya, Gresik, Jember, Solo, Yogyakarta, Bandung, Bekasi, Tangerang, Jakarta, dan Makassar.

2. Visi Misi Perusahaan

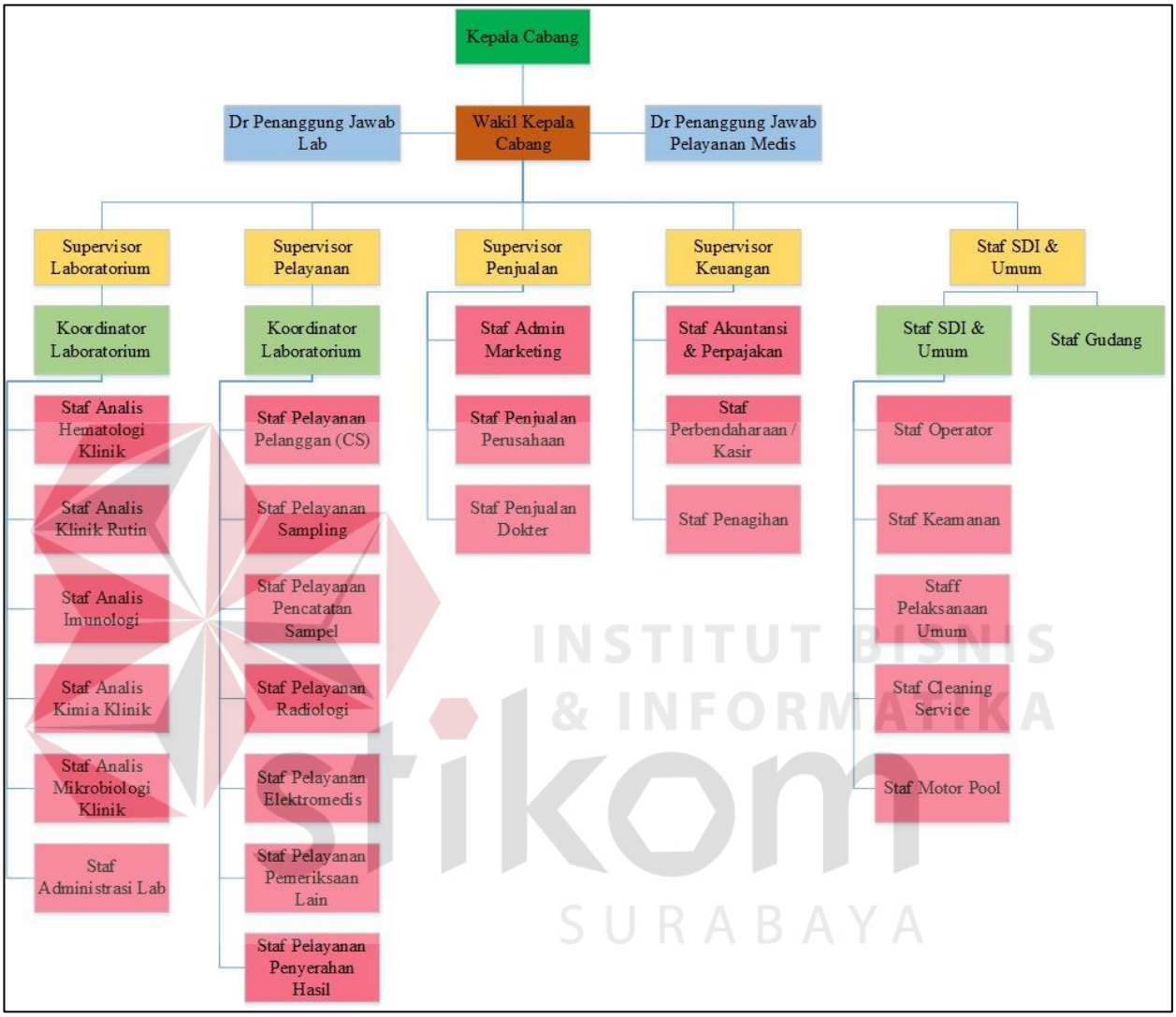
Parahita Diagnostic Center memilik visi "Menjadi Diagnostic Center terlengkap, terintegrasi, dan terpercaya dengan pelayanan sepenuh hati". Misi dari Parahita Diagnostic Center adalah sebagai berikut :

a. Menyediakan layanan diagnostic yang didukung oleh teknologi dan terintegrasi.
b. Menyediakan informasi layanan kesehatan yang berbasis kesehatan kerja / *occupational health*.
c. Membangun *integrase management diagnostic* dengan berbasis managemen spiritual.
d. Meraih kepercayaan masyarakat dengan memdasarkan pada keakuratan dan kejujuran.
e. Mengedukasi masyarakat tentang pentingnya tindakan preventif.
f. Membina SDM yang berdedikasi, smart, dan bertanggung jawab.
g. Mengingkatkan kesejahteraan keluarga besar Parahita Diagnostic Center.

3. Struktur Organisasi perusahaan

PDC merupakan perusahaan yang bergerak dibidang jasa kesehatan masyarakat. Perusahaan ini telah memiliki beberapa cabang di 11 kota besar di Indonesia seperti Surabaya, Gresik, Jember, Solo, Yogyakarta, Bandung, Bekasi, Tangerang, Jakarta, dan Makassar. Seperti perusahaan pada umumnya, PDC memiliki struktur organsisasi yang berguna untuk menentukan pembagian tugas

dan tanggung jawab masing-masing bagian pada perusahaan. Struktur organisasi yang dimiliki oleh PDC dapat dilihat pada Gambar 4.1



Gambar 4. 1 Struktur Organisasi Parahita *Diagnostic Center*

4. Proses Bisnis dan TI Perusahaan

PDC memiliki peran penting dalam mengelola sistem informasi bagi seluruh kantor cabang yang ada. PDC memiliki visi untuk menjadi diagnostic center terlengkap, terintegrasi, dan terpercaya dengan layanan sepenuh hati. Dalam mencapai visi tersebut perusahaan memiliki beberapa misi, salah satunya yaitu menyediakan layanan diagnostic yang didukung oleh teknologi dan terintegrasi.

Oleh karena itu perusahaan ini menerapkan teknologi yang terintegrasi dan terpusat untuk menangani seluruh proses bisnisnya. Teknologi tersebut adalah Sistem Informasi Parahita (PARIS).

PARIS digunakan untuk menunjang proses bisnis PDC secara keseluruhan meliputi proses keuangan, proses marketing, proses SDM, proses pendaftaran pasien, proses pemerikasaan hingga proses keluarnya hasil laboratorium. SIP menyediakan berbagai informasi penting, antara lain: informasi data pasien, data hasil pemeriksaan, data dokter, data keuangan, data karyawan serta data perusahaan yang bekerjasama dengan Parahita. PARIS digunakan oleh berbagai bagian yang terkait di PDC, yaitu bagian laboratorium, bagian pelayanan, bagian penjualan, bagian keuangan, bagian sumber daya insani (SDI) dan umum, bagian penanggung jawab lab dan penanggung jawab medis.

Seiring berkembangnya perusahaan yang semakin maju, maka PDC terus berupaya dalam melakukan pengembangan sistem informasi yang mereka miliki. hal ini dapat dilihat dari migrasi PARIS yang awalnya berbasis desktop menjadi berbasis web. Dengan adanya pengembangan ini tidak dapat dipungkiri PDC menemui beberapa permasalahan yang dapat mengancam keamanan informasi perusahaan.

4.1.2. Menentukan Ruang Lingkup, Objek dan Tujuan Audit

Setelah identifikasi proses bisnis dan TI dilakukan maka dapat disimpulkan tentang proses bisnis yang ada pada perusahaan saat ini. Penentuan ruang lingkup dilakukan dengan cara observasi dan wawancara pada bagian TI serta kepala cabang PDC Surabaya. Adapun hasil dari penentuan ruang lingkup yang akan di audit yaitu mengenai Sistem Informasi Parahita (PARIS). Objek audit adalah

bagian yang bertanggung jawab terhadap PARIS yaitu bagian TI dan kepada cabang PDC Surabaya. Tujuan dari audit ini agar dapat menghitung hasil uji kematangan atau *maturity level* dengan standar yang digunakan yaitu standar ISO/IEC 27002:2005. Selain itu juga menghasilkan temuan dan rekomendasi untuk diberikan kepada perusahan. Penentuan ruang lingkup, obyek dan tujuan audit dapat dilihat pada Table 4.1

Tabel 4. 1 Ruang Lingkup, Obyek, dan Tujuan Audit

Ruang Lingkup, Obyek, dan Tujuan Audit digunakan dalam Audit Kemanan Sistem Informasi Parahita Pada Parahita Diagnostic Center Surabaya		
Ruang Lingkup	**Obyek**	**Tujuan Audit**
Sistem Informasi Parahita (PARIS)	Kepala Cabang PDC Surabaya dan Bagian TI	- Perhitungan Hasil uji kemantangan atau maturity level. - Temuan dan Rekomendais

4.1.3. Menentukan Klausul, Obyektif Kontrol dan Kontrol

Setelah hasil ruang lingkup, obyek dan tujuan audit ditentukan maka dapat digunakan untuk menentukan klausul, obyektif kontrol dan kontrol yang digunakan dalam proses audit. Hal ini disesuaikan dengan kondisi perusahaan saat ini dan kesepakatan antara kedua belah pihak yaitu auditor dengan *auditee*. Penentuan klausul, obyektif kontrol dan kontrol ini menggunakan acuan standar keamanan yaitu ISO 27002:2005. Hasil dari penentuan klausul, obyektif kontrol dan kontrol dapat dilihat pada Tabel 4.2 untuk selengkapnya dapat dilihat pada lampiran 2.

Tabel 4. 2 Klausul, Obyektif Kontrol dan Kontrol yang digunakan

Klausul yang digunakan dalam Audit Kemanan Sistem Informasi Parahita Pada Parahita Diagnostic Center Surabaya			
No	Klausul	Obyektif Kontrol	Kontrol
1	Klausul 10 (Komunikasi dan Manajemen Operasional)	Untuk memastikan keamanan operasidn tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi	10.1.1 Pendokumentasian Prosedur Operasi
			10.1.2 Manajemen Pertukaran
			10.1.3 Pemisahan Tugas
			10.1.4 Pemisahan, Pengembangan, Pengujian dan Operasioanal Informasi

4.1.4. Membuat Engagement Letter

Setelah menetukan klausul, obyektif kontrol dan kontrol, langkah selanjutnya adalah membuat surat perjanjian atau *Engagement Letter*. Pembuatan *Engagement Letter* ini bertujuan untuk bukti bahwa pelaksanaan audit yang dilakukan oleh auditor telah disetujui oleh auditee. *Engagement Letter* berisikan tentang *role*, tanggung jawab, lingkup audit, pelaksanaan audit dan ketentuan perjanjian audit. Pada langkah ini akan menghasilkan perjanjian yang harus dipatuhi oleh kedua belah pihak yaitu auditor dan *auditee*. Lebih jelas *Engagement Letter* dapat dilihat pada lampiran 3.

4.2. Tahap Persiapan Audit

Hasil dari tahapan pesrsiapan audit ini adalah penyusunan Audit *Working Plan* (AWP), penyampaian kebutuhan data, membuat pernyataan, melakukan pembobotan dan membuat pertanyaan. Audit *Working Plan* digunakan sebagai acuan jadwal dalam melaksanakan audit. Sedangkan dalam pembuatan pernyataan dan pertanyaan dilakukan berdasarkan standar keamanan ISO 27002:2005.

4.2.1. Penyusunan Audit Working Plan (AWP)

Hasil pada langkah penyusunan *Audit Working Plan* (AWP) ini berupa tabel jadwal kerja yang berisikan susunan aktifitas apa saja yang akan dilakukan selama kegiatan audit berlangsung. Jadwal dilakukan secara bertahap, mulai dari awal kegiatan hingga akhir kegiatan. Untuk lebih jelas dapat dilihat pada Tabel 4.3

Tabel 4. 3 Audit Working Plan

No	Kegiatan	Maret				April				Mei			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Pembuatan dan Pengajuan Proposal TA												
2	Perencanaan Audit												
	a. Identifikasi proses bisnis dan TI												
	b. Menentukan Ruang Lingkup, Obyek dan tujuan audit												
	c. Membuat Klausul, Objektif Kontrol dan Kontrol												
	d. Membuat *Engagement Letter*												
3	Persiapan Audit												
	a. Penyusunan Audit Working Plan												
	b. Penyampaian Kebutuhan Dana												
	c. Membuat Pernyataan												
	d. Melakukan Pembobotan												
	e. Membuat Pertanyaan												
4	Pelaksanaan Audit												
	a. Pertemuan Pendahuluan												
	b. Menentukan Auditee												
	c. Wawancara dan Observasi												
	c.1. Klausul 10 (Manajemen Komunikasi dan Operasi)												
	c.2. Klausul 12 (Akuisi Sistem Informasi, Pembangunan dan Pemeliharaan)												
	c.3. Klausul 13 (Manajemen kejadian Keamanan Informasi)												
	c.4. Klausul 14 (Manajemen Kelangsungan Bisnis)												
	c.5. Klausul 15 (Kepatuhan)												
	d. Pemeriksaan Data dan Bukti												
	e. Penyusunan Temuan dan Rekomendasi Audit												
	f. Konfirmasi Temuan dan Rekomendasi												
5	Pelaporan Audit												
	a. Permintaan Tanggapan atas temuan												
	b. Penyusunanan Draf Laporan Audit												
	c. Persetujuan Draf Laporan Audit												
	d. Exit Meeting												

4.2.2. Penyampaian Kebutuhan Data

Setelah menyusun Audit Working Plan, langkah selanjutnya adalah penyampaian kebutuhan data kepada *auditee* yang digunakan untuk menunjang kegiatan audit yang dilakukan oleh auditor. Untuk lebih jelasnya penyampaian kebutuhan data dapat dilihat pada Lampiran 4.

4.2.3 Membuat Pernyataan

Langkah selanjutnya setelah penyampaian kebutuhan data adalah membuat pernyataan yang mengacu pada kontrol keamanan berdasarkan standard ISO 27002:2005. Lebih jelasnya pertanyaan yang telah dibuat dapat dilihat pada Tabel 4.4 dan selanjutnya dapat dilihat pada lampiran 5.

Tabel 4. 4 Pernyataan

Klausul 10 Manajemen Komunikasi Operasi	
10.1 Tanggung Jawab dan Prosedur Operasional	
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**	
10.1.1 Pendokumentasian Prosedur Operasi	
No	Pernyataan
1	Terdapat dokumentasi terhadap prosedur operasi
2	Terdapat pemeliharaan terhadap prosedur operasi

4.2.4 Melakukan Pembobotan

Langkah selanjutnya setelah membuat pernyataan adalah melakukan pembobotan. Setiap pernyataan yang sudah dibuat akan diberikan pembobotan. Pemberian pembobotan disesuaikan dengan seberapa besar resiko yang akan terjadi untuk perusahaan dan juga disesuaikan dengan acuan audit yang digunakan. Apabila tidak beresiko sedikitpun maka nilai dari pembobotan adalah nol. Sedangkan apabila diindikasikan risiko yang berpengaruh besar untuk organisasi, akan diberi nilai pembobotan adalah 1. Pembobotan yang telah dilakukan dapat dilihat pada Tabel 4.5 dan selanjutnya dapat dilihat pada lampiran 6.

Tabel 4. 5 Pembobotan yang dilakukan

Klausul 10 Manajemen Komunikasi Operasi		
10.1 Tanggung Jawab dan Prosedur Operasional		
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**		
10.1.1 Pendokumentasian Prosedur Operasi		
No	**Pernyataan**	**Pembobotan**
1	Terdapat dokumentasi terhadap prosedur operasi	1
2	Terdapat pemeliharaan terhadap prosedur operasi	0.8

4.2.5 Membuat Pertanyaan

Setelah melakukan pembobotan maka langkah selanjutnya adalah membuat pertanyaan. Pertanyaan dibuat berdasarkan pada pernyataanyang telah dibuat sebelumnya. Pertanyaan disesuaikan berdasarkan pelaksanaan kontrol yang ada pada standar keamanan ISO 27002:2005. Berikut adalah pertanyaan yang dibuat pada klausul 10 mengenai Komunikasi dan Manajemen Operasional pada Tabel 4.6 dan untuk lebih lengkapnya dapat dilihat pada Lampiran 7.

Tabel 4. 6 Pertanyaan yang dibuat

Klausul 10 Manajemen Komunikasi Operasi		
10.1 Tanggung Jawab dan Prosedur Operasional		
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**		
10.1.1 Pendokumentasian Prosedur Operasi		
No	**Pernyataan**	**Pertanyaan**
1	Terdapat dokumentasi terhadap prosedur operasi	1. Apakah terdapat dokumentasi semua prosedur operasi yang ada saat ini ?
		2. Dokumentasi disimpan dalam format apa ?

Tabel 4.6 (Lanjutan)

Klausul 10 Manajemen Komunikasi Operasi		
10.1 Tanggung Jawab dan Prosedur Operasional		
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**		
10.1.1 Pendokumentasian Prosedur Operasi		
No	**Pernyataan**	**Pertanyaan**
		3. Sejak kapan dokumentasi prosedur operasi tersebut dilakukan ?
		4. Siapa yang membuat dokumentasi prosedur tersebut ?

4.3 Pelaksanaan Audit

Pada tahapan pelaksanaan audit ada beberapa langkah-langkah yaitu melakukan pertemuan pendahuluan audit, menentukan auditee, wawancara dan observasi, pemeriksaan data dan bukti, melakukan uji kematangan, menyusun temuan dan rekomendasi audit, dan konfirmasi temuan audit. Tahapan ini akan menghasilkan hasil pertemuan pendahuluan audit, hasil penentuan auditee, hasil wawancara, hasil temuan bukti, hasil uji kematangan, penyusunan daftar temuan dan rekomendasi, dan konfirmasi temuan audit.

4.3.1 Pertemuan Pendahuluan

Pada tahapan ini dilakukan pertemuan pendahuluan audit yang digunakan untuk mendapatkan kesepakatan bersama dan mendapatkan pemahaman yang sama sebelum dilakukannya proses pelaksanaan aduit dimulai. Pertemuan ini dilakukan oleh auditor dan *auditee.*

4.3.2 Menentukan Auditee

Pada tahapan menentukan *auditee*, langkah yang digunakan yaitu memilih *auditee* yang sesuai dengan klausul yang digunakan. Pemilihan *auditee* ini dilakukan berdasarkan RACI. RACI sendiri merupakan singkatan dari *Responsible, Accountable, Consulted,* dan *Informed. Output* yang dihasilkan pada tahapan ini yaitu hasil *auditee* yang akan diwawancari pada tahapan wawancara sebagai sumber informasi yang dibutuhkan pada audit keamanan sistem informasi. Untuk lebih jelasnya data dapat dilihat pada Lampiran 8.

4.3.3 Hasil wawancara dan Observasi

Pada tahap ini dilakukan wawancara dan observasi oleh auditor kepada auditee. Wawancara dilakukan berdasarkan pertanyaan yang telah dibuat pada tahap sebelumnya. Berikut salah satu contoh hasil wawancara yang dilakukan berdasarkan pertanyaan pada klausul 10 mengenai Komunikasi dan Manajemen Operasional yang dapat dilihat pada Tabel 4.7 dan untuk selangkapnya dapat dilihat pada Lampiran 9.

Tabel 4. 7 Hasil Wawancara

Klausul 10 Manajemen Komunikasi Operasi			
10.1 Tanggung Jawab dan Prosedur Operasional			
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**			
10.1.1 Pendokumentasian Prosedur Operasi			
No	**Pernyataan**	**Pertanyaan**	**Jawaban**
1	Terdapat dokumentasi terhadap prosedur operasi	1. Apakah terdapat dokumentasi semua prosedur operasi yang ada saat ini ?	Untuk prosedur operasi yang sudah didokumentasikan hanya beberapa saja, belum semuanya hanya dianggap penting saja

Tabel 4.7 (Lanjutan)

Klausul 10 Manajemen Komunikasi Operasi			
10.1 Tanggung Jawab dan Prosedur Operasional			
Objektif Kontrol : **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**			
10.1.1 Pendokumentasian Prosedur Operasi			
No	**Pernyataan**	**Pertanyaan**	**Jawaban**
			seperti prosedur yang bersangkuan langsung dengan bagian keuangan saja.
		2. Dokumentasi disimpan dalam format apa ?	Untuk penyimpanannya di simpan dalam bentuk softcopy
		3. Sejak kapan dokumentasi prosedur operasi tersebut dilakukan ?	Sejak beberapa bulan ini, karena akan dilakukannya audi eksternal
		4. Siapa yang membuat dokumentasi prosedur tersebut ?	Tentunya bagian TI dan ada tim khusus juga yang ditugaskan untuk membua dokumentasi prosedur tersebut.

4.3.4 Pemeriksaan Data dan Bukti

Pemeriksaan data dan bukti ini mengacu pada hasil wawancara dan observasi yang telah dilakukan. Didalam tahapan ini dilakukan *review* terhadap data atau bukti yang ditemukan dari hasil wawancara. Hasil pemeriksaan ini dapat dilihat pada Tabel 4.8 dan selengkapnya dapat dilihat pada lampiran 10 menjadi satu dengan tabel perhitungan *maturity level*.

Tabel 4. 8 Hasil Pemeriksaan Dan Penilaian

Klausul 10 Manajemen Komunikasi Operasi										
Objektif Kontrol : 10.1 Tanggung Jawab dan Prosedur Operasional										
Kontrol: 10.1.1 Pendokumentasian Prosedur Operasi				Penilaian						Nilai
NO	Pernyataan	Hasil Pemeriksaan	Bobot	0	1	2	3	4	5	
1	Terdapat pendokumentasian prosedur operasi	Perusahaan sudah melakukan pendokumentasian prosedur operasi, namun prosedur operasi yang sudah didokumentasikan hanya mengenai operasional yang tidak berkaitan dengan TI atau sistem informasi yang digunakan. Bukti : Prosedur yang sudah dibuat disimpan pada aplikasi bernama SMM (Foto 1)	1						√	5

4.3.5 Hasil Melakukan Uji Kematangan

Berdasarkan wawancara dan observasi dengan *auditee* meliputi pemeriksaan serta pengumpulan bukti yang telah dilakukan, maka diperoleh hasil uji kepatutan dari tingkat kematangan atau *maturity level* untuk masing-masing kontrol. Oleh karena itu uji kematangan didapatkan dari masing-masing analisa yang telah dilakukan pada tiap klausul dan dapat dilihat pada tabel perhitungan *maturity level* yang terdapat pada Lampiran 10. Hasil dari perhitungan tingkat kematangan atau *maturity level* hasil audit keamanan sistem informasi adalah sebagai berikut :

a. Hasil *Maturity level* Klausul 10 Manajemen Komunikasi dan Operasi.

Bedasarkan hasil dari proses perhitungan *maturity level* pada klausul 10 tentang manajemen komunikasi dan operasi adalah 3.4 yaitu *defined*. Hasil tersebut menunjukkan bahwa proses manajemen komunikasi dan operasi sudah dilengkapi aturan dan prosedur mengenai manajemen komunikasi dan operasi. Aturan tersebut meliputi proses kontrol pemisahan tugas, layanan yang diberikan oleh pihak ketiga, *back-up* data, keamanan dalam layanan jaringan, aturan mengenai perjanjian pertukaran informasi hingga aturan mengenai rekaman audit yang telah dilakukan. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur karena belum adanya aturan dan prosedur secara resmi yang dibuat oleh perusahaan hal ini dikarenakan kurangnya sumber daya TI yang dapat fokus pada pembuatan dokumentasi mengenai TI, misalnya mengenai pengelolaan dalam pertukaran informasi yang dilakukan oleh perusahaan, kurangnya kontrol terhadap kode berbahaya (*malicious code*), kurangnya keamanan dokumentasi sistem informasi, kurangnya kontrol yang dilakukan terhadap *email* perusahaan yang ada, hingga belum adanya catatan *log* mengenai administrator dari sistem yang digunakan oleh perusahaan. Hal lain adalah belum adanya kebijakan dan prosedur mengenai pertukaran informasi yang dilakukan oleh perusahaan. Hasil perhitungan *maturity level* dapat dilihat pada Tabel 4.9. Selain itu hasil perhitungan *maturity level* klausul 10 tentang manajemen konuikasi dan operasi juga dapat ditunjukan dalam bentuk jaring laba-laba. Presentasi dalam jaring laba-laba dapat dilihat pada Gambar 4.2.

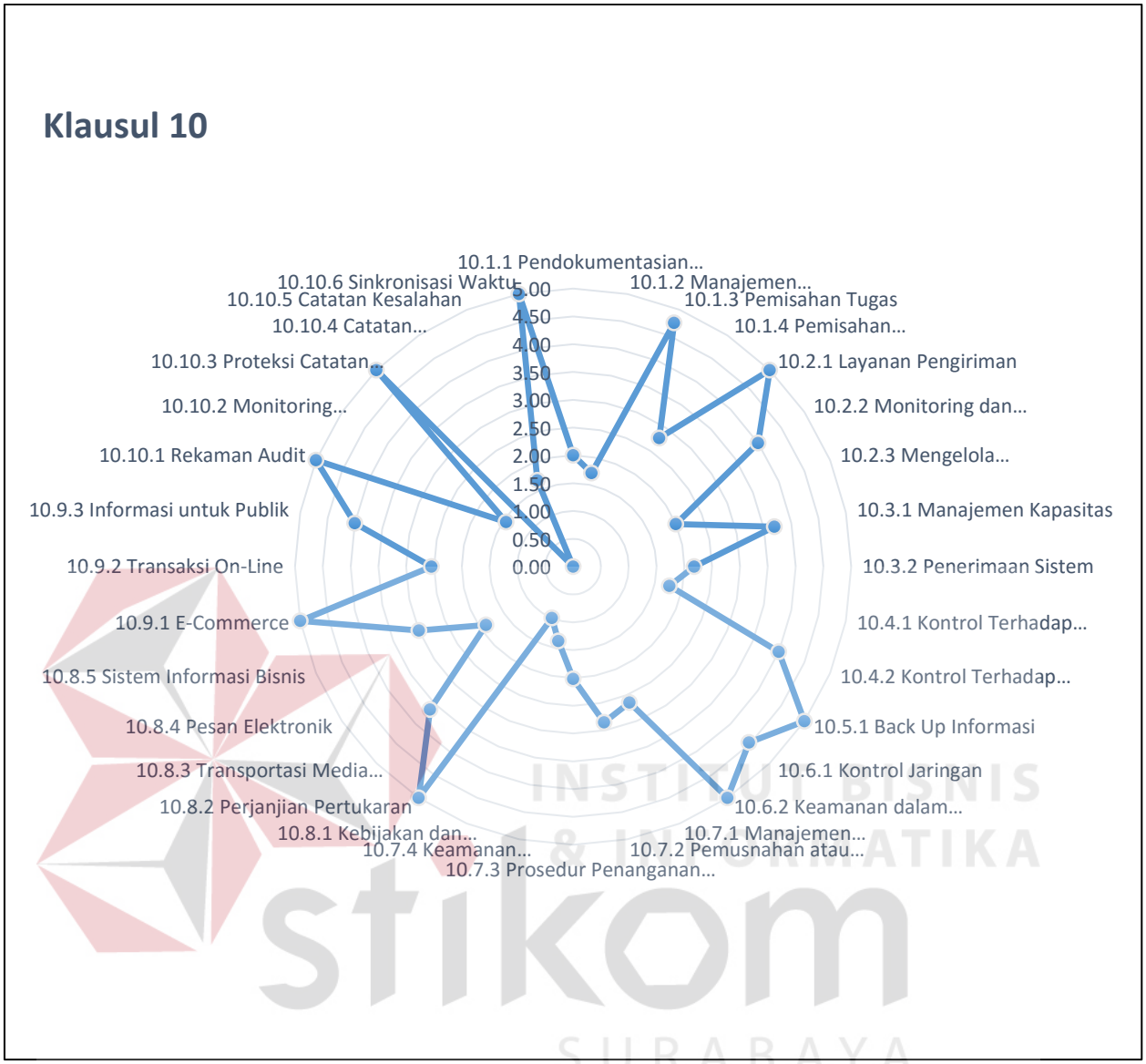
Tabel 4. 9 Hasil *Maturity Level* Klausul 10 Manajemen Komunikasi dan Operasi

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
Klausul 10 Manajemen Komunikasi Operasi	10.1 Tanggung Jawab dan Prosedur Operasional	10.1.1 Pendokumentasian Prosedur Operasi	2.00	2.81
		10.1.2 Manajemen Pertukaran	1.71	
		10.1.3 Pemisahan Tugas	4.74	
		10.1.4 Pemisahan Pengembangan, Pengujian dan Fasilitas Operasional	2.78	
	10.2 Manajemen Layanan Pengiriman Oleh Pihak Ketiga	10.2.1 Layanan Pengiriman	5.00	3.67
		10.2.2 Monitoring dan Peninjauan Layanan Pihak Ketiga	4.00	
		10.2.3 Mengelola Perubahan Pada Layanan Pihak Ketiga	2.00	
	10.3 Perencanaan Sistem dan Penerimaan	10.3.1 Manajemen Kapasitas	3.69	2.93
		10.3.2 Penerimaan Sistem	2.18	
	10.4 Perlindungan terhadap malicious dan mobile code	10.4.1 Kontrol Terhadap Kode Berbahaya (malicious code)	1.76	2.88
		10.4.2 Kontrol Terhadap mobile code	4.00	
	10.5 Back-Up	10.5.1 Back Up Informasi	5.00	5.00

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
Klausul 10 Manajemen Komunikasi Operasi	10.6 Manajemen Keamanan Jaringan	10.6.1 Kontrol Jaringan	4.47	4.74
		10.6.2 Keamanan dalam Layanan Jaringan	5.00	
	10.7 Penanganan Media	10.7.1 Manajemen Pemindahan Media	2.65	2.22
		10.7.2 Pemusnahan atau pembuangan media	2.85	
		10.7.3 Prosedur Penanganan Informasi	2.02	
		10.7.4 Keamanan Dokumentasi Informasi	1.36	
	10.8 Pertukaran Informasi	10.8.1 Kebijakan dan Prosedur Pertukaran Informasi	1.00	2.90
		10.8.2 Perjanjian Pertukaran	5.00	
		10.8.3 Transportasi Media Fisik	3.64	
		10.8.4 Pesan Elektronik	1.88	
		10.8.5 Sistem Informasi Bisnis	3.00	
	10.9 Layanan E-Commerce	10.9.1 E-Commerce	5.00	3.85
		10.9.2 Transaksi On-Line	2.55	
		10.9.3 Informasi untuk Publik	4.00	
	10.10 Monitoring	10.10.1 Rekaman Audit	5.00	3.02

Tabel 4.9 (Lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
Klausul 10 Manajemen Komunikasi Operasi		10.10.2 Monitoring Penggunaan Sistem	1.44	
		10.10.3 Proteksi Catatan Informasi	5.00	
		10.10.4 Catatan Administrator dari Operator	0.00	
		10.10.5 Catatan Kesalahan	1.68	
		10.10.6 Sinkronisasi Waktu	5.00	
Rata-rata				3.40



Gambar 4. 2 Jaring Laba-laba Nilai *Maturity Level* Klausul 10

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

Bedasarkan hasil dari proses perhitungan *maturity level* pada klausul 12 tentang akuisisi sistem informasi, pembangunan dan pemeliharaan adalah 3.04 yaitu *defined*. Hasil tersebut menunjukkan bahwa proses akuisisi sistem informasi, pembangunan dan pemeliharaan sudah dilengkapi aturan dan prosedur mengenai

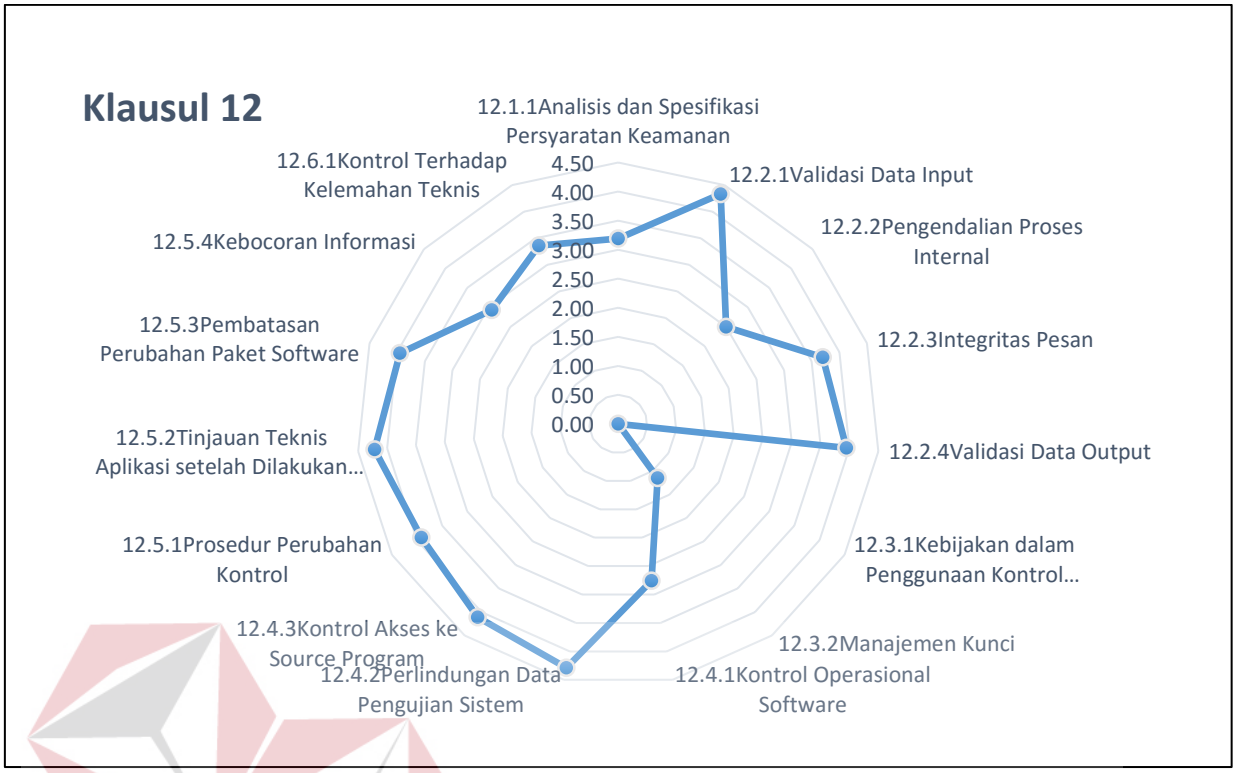
akuisisi sistem informasi, pembangunan dan pemeliharaan. Aturan tersebut meliputi proses validasi data *input*, validasi data *output*, perlindungan terhadap data yang digunakan dalam proses pengujian sistem, kontrol akses terhadap *source program*, batasan dalam perubahan sistem, kontrol terhadap kelemahan sistem hingga tinjauan yang dilakukan setelah perubahan sistem. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur karena belum adanya aturan dan prosedur secara resmi yang dibuat oleh perusahaan hal ini dikarenakan kurangnya sumber daya TI yang dapat fokus pada pembuatan dokumentasi mengenai TI, misalnya mengenai kontrol operasional *software* perusahaan, pengendalian proses internal yang dilakukan seperti belum adanya pemeriksaan validasi mengenai kerusakan data. Hal lain adalah belum adanya kebijakan dalam penggunaan kontrol kriptografi serta manajemen kunci kriptografi dikarenakan sampai saat ini hanya berupa wacana saja dan belum diimplementasikan. Hasil perhitungan *maturity level* dapat dilihat pada Tabel 4.10. Selain itu hasil perhitungan *maturity level* klausul 12 tentang akuisisi sistem informasi, pembangunan dan pemeliharaan juga dapat ditunjukan dalam bentuk jarring laba-laba. Presentasi dalam jaring laba-laba dapat dilihat pada Gambar 4.3.

Tabel 4. 10 Hasil *Maturity Level* Klausul 12 Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
Klausul 12 Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	12.1 Persyaratan Keamanan Untuk Sistem Informasi	12.1.1Analisis dan Spesifikasi Persyaratan Keamanan	3.19	3.19
	12.2 Pemrosesan yang Benar dalam Aplikasi	12.2.1 Validasi Data Input	4.33	3.62
		12.2.2 Pengendalian Proses Internal	2.50	
		12.2.3 Integritas Pesan	3.70	
		12.2.4 Validasi Data Output	3.95	
	12.3 Kontrol Kriptografi	12.3.1 Kebijakan dalam Penggunaan Kontrol Kriptografi	0.00	0.58
		12.3.2 Manajemen Kunci	1.15	
	12.4 Keamanan File sistem	12.4.1 Kontrol Operasional Software	2.76	3.72
		12.4.2 Perlindungan Data Pengujian Sistem	4.29	
		12.4.3 Kontrol Akses ke Source Program	4.11	
	12.5 Keamanan dalam pembanguna n dan proses-	12.5.1 Prosedur Perubahan Kontrol	3.91	3.75
		12.5.2 Tinjauan Teknis Aplikasi	4.22	

Tabel 4.10 (Lanjutan)

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
	proses pendukung	setelah Dilakukan Perubahan Sistem Operasi		
		12.5.3 Pembatasan Perubahan Paket Software	3.95	
		12.5.4 Kebocoran Informasi	2.93	
	12.6 Manajemen Teknik Kelemahan	12.6.1 Kontrol Terhadap Kelemahan Teknis	3.36	3.36
Maturity Level Klausul 12				**3.04**



Gambar 4. 3 Jaring Laba-laba Nilai *Maturity Level* Klausul 12

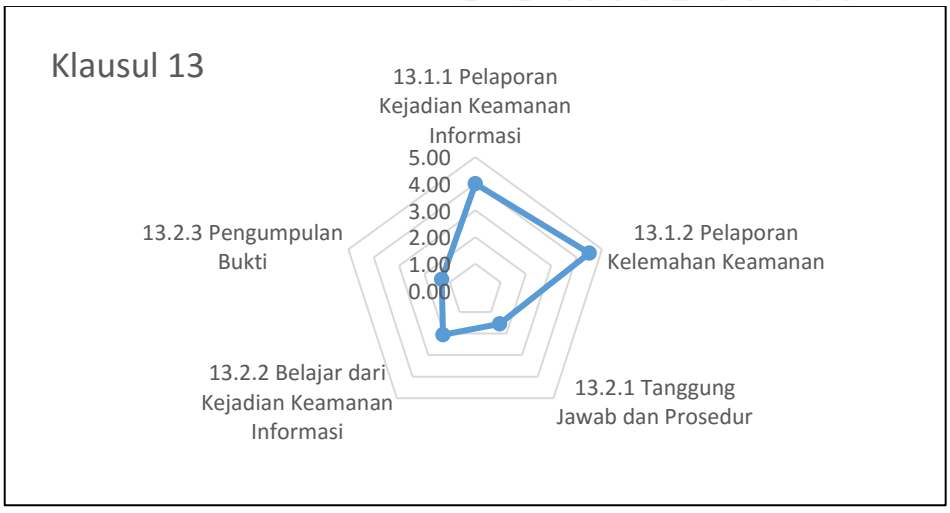
c. Hasil *Maturity Level* Klausul 13 Manajemen Kejadian Keamanan Informasi

Bedasarkan hasil dari proses perhitungan *maturity level* pada klausul 13 tentang manajemen kejadian keamanan informasi adalah 2.95 yaitu *limited/repeatable*. Hal tersebut menunjukan bahwa kontrol keamanan pada proses manajemen kejadian keamanan informasi masih dalam pengembangan serta dokumentasi yang digunakan untuk mendukung kebutuhan masih sangat terbatas. Hal ini dapat ditunjukkan dengan belum adanya prosedur pendukung keamanan informasi yang dibuat secara resmi oleh perusahaan dan belum ada mekanisme yang digunakan untuk memperlihatkan informasi kejadian keamanan informasi secara rinci. Hal lain adalah belum dilakukan pengumpulan terhadap bukti kejadian keamanan informasi yang telah terjadi karena perusahaan kekurangan sumber daya TI untuk dapat fokus ke hal tersebut. Hasil perhitungan *maturity level* dapat dilihat

pada Tabel 4.11. Selain itu hasil perhitungan *maturity level* klausul 13 tentang manajemen kejadian keamanan informasi juga dapat ditunjukan dalam bentuk jarring laba-laba. Presentasi dalam jaring laba-laba dapat dilihat pada Gambar 4.4.

Tabel 4. 11 Hasil *Maturity Level* Klausul 13 Manajemen Kejadian Keamanan Informasi

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
Klausul 13 Manajemen Kejadian Keamanan Informasi	13.1 Pelaporan Kejadian dan Kelemahan Keamanan Informasi	13.1.1 Pelaporan Kejadian Keamanan Informasi	4.00	4.25
		13.1.2 Pelaporan Kelemahan Keamanan	4.50	
	13.2 Manajemen Kejadian Keamanan Infromasi dan Pengembangannya	13.2.1 Tanggung Jawab dan Prosedur	1.55	1.64
		13.2.2 Belajar dari Kejadian Keamanan Informasi	2.06	
		13.2.3 Pengumpulan Bukti	1.32	
Maturity Level Klausul 13				**2.95**



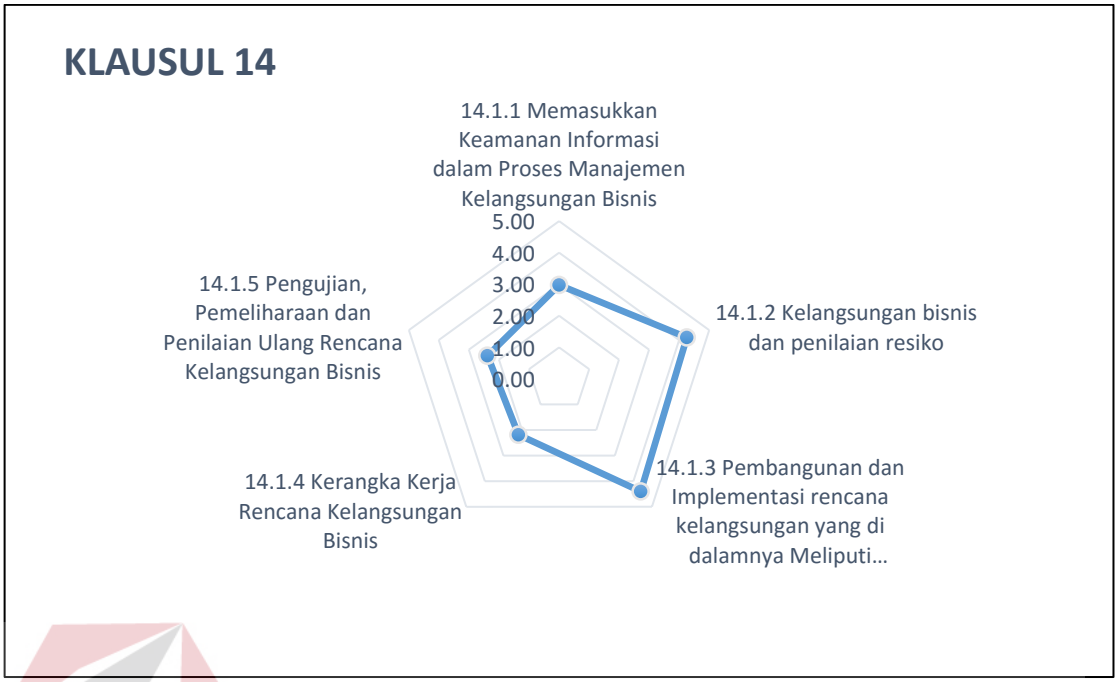
Gambar 4. 4 Jaring Laba-laba Nilai *Maturity Level* Klausul 13

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

Bedasarkan hasil dari proses perhitungan *maturity level* pada klausul 14 tentang manajemen kelangsungan bisnis adalah 3.24 yaitu *defined*. Hasil tersebut menunjukkan bahwa proses manajemen kelangsungan bisnis sudah dilengkapi aturan dan prosedur mengenai manajemen kelangsungan bisnis. Aturan tersebut meliputi proses memasukkan keamanan informasi dalam proses manajemen kelangsungan bisnis, proses kelangsungan bisnis dan penilaian resiko yang ada, serta pembangunan dan implementasi rencana kelangsungan yang didalamnya meliputi keamanan informasi. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur karena belum adanya aturan dan prosedur secara resmi yang dibuat oleh perusahaan hal ini dikarenakan kurangnya sumber daya TI yang dapat fokus pada pembuatan dokumentasi mengenai TI, misalnya mengenai kerangka kerja rencanan kelangsungan bisnis seperti belum adanya kerangka kerja yang dipertahankan kekonsistenannya. Selain itu adalah pengujian, pemeliharaan dan penilaian ulang rencanan kelangsungan bisnis yang belum maksimal dilakukan oleh perusahaan seperti belum ada teknik yang digunakan oleh perusahaan untuk menggambarkan rencana pemulihan secara spesifik dan belum adanya pengujian terhadap penjadwalan rencana kelangsungan bisnis yang telah ditetapkan. Hasil perhitungan *maturity level* dapat dilihat pada Tabel 4.12. Selain itu hasil perhitungan *maturity level* klausul 14 tentang manajemen kelangsungan bisnis juga dapat ditunjukan dalam bentuk jarring laba-laba. Presentasi dalam jaring laba-laba dapat dilihat pada Gambar 4.5.

Tabel 4. 12 Hasil Maturity Level Klausul 14 Manajemen Kelangsungan Bisnis

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
Klausul 14 Manajemen Kelangsungan Bisnis	14.1 Aspek Keamanan dalam Manajemen Kelangsungan Bisnis	14.1.1 Memasukkan Keamanan Informasi dalam Proses Manajemen Kelangsungan Bisnis	3.24	3.24
		14.1.2 Kelangsungan bisnis dan penilaian resiko	4.26	
		14.1.3 Pembangunan dan Implementasi rencana kelangsungan yang di dalamnya Meliputi Keamanan Informasi	4.40	
		14.1.4 Kerangka Kerja Rencana Kelangsungan Bisnis	2.18	
		14.1.5 Pengujian, Pemeliharaan dan Penilaian Ulang Rencana Kelangsungan Bisnis	2.38	
Maturity Level Klausul 14				**3.24**



Gambar 4. 5 Jaring Laba-laba Nilai *Maturity Level* Klausul 14

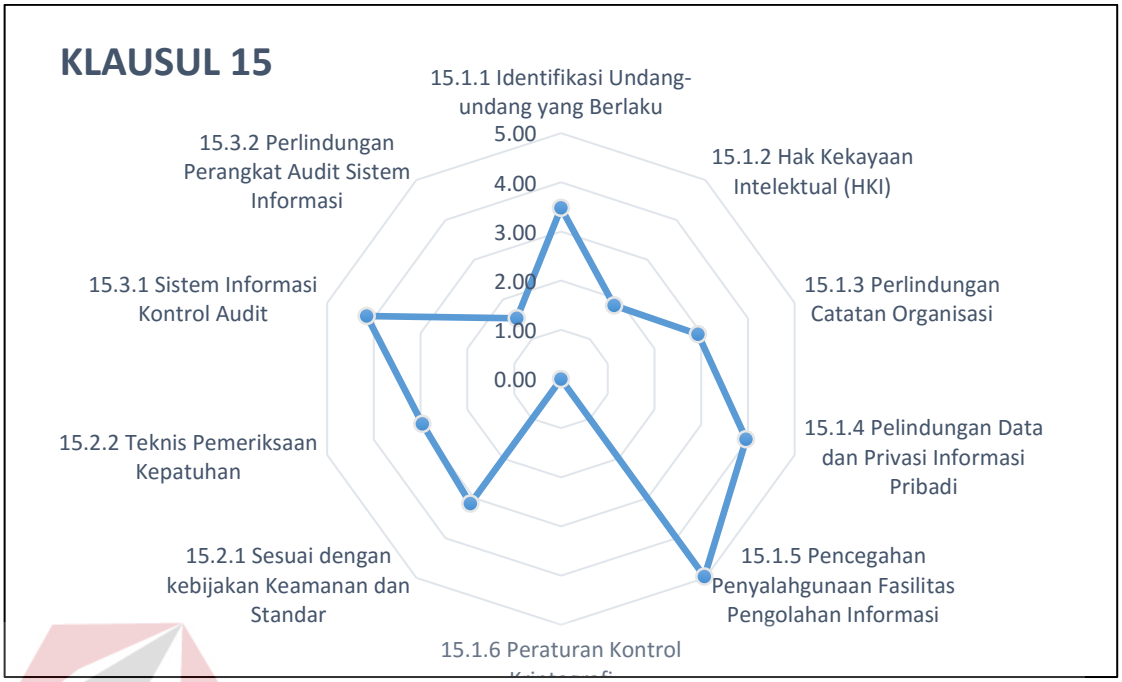
e. Hasil *Maturity Level* Klausul 15 Kepatuhan

Bedasarkan hasil dari proses perhitungan *maturity level* pada klausul 15 tentang kepatuhan adalah 2.92 yaitu *limited/repeatable*. Hal tersebut menunjukan bahwa kontrol keamanan pada proses manajemen kejadian keamanan informasi masih dalam pengembangan serta dokumentasi yang digunakan untuk mendukung kebutuhan masih sangat terbatas. Hal ini dapat ditunjukkan dengan banyaknya prosedur, panduan, kebijakan maupun peraturan yang belum didokumentasikan secara resmi namun ada beberapa yang dicatat pada catatan pribadi bagian TI maupun direktur. Hal lain adalah belum adanya peraturan mengenai kontrol kriptografi karena hal ini masih berupa wacana yang belum diimplementasikan oleh perusahaan. Hasil dari perhitungan *maturity level* Klausul 15 Kepatuhan dapat dilihat pada Tabel 4.13. Selain itu hasil perhitungan *maturity level* pada Klausul 15

Kepatuhan juga dapat ditunjukan dalam bentuk jaring laba-laba. Jaring laba-laba tersebut dapat dilihat pada Gambar 4.6

Tabel 4. 13 Hasil *Maturity Level* Klausul 15 Kepatuhan

Klausul	Objektif Kontrol	Kontrol keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
Klausul 15 Kepatuhan	15.1 Kepatuhan dengan Persyaratan Hukum	15.1.1 Identifikasi Undang-undang yang Berlaku	3.48	2.87
		15.1.2 Hak Kekayaan Intelektual (HKI)	1.84	
		15.1.3 Perlindungan Catatan Organisasi	2.94	
		15.1.4 Pelindungan Data dan Privasi Informasi Pribadi	3.96	
		15.1.5 Pencegahan Penyalahgunaan Fasilitas Pengolahan Informasi	4.97	
		15.1.6 Peraturan Kontrol Kriptografi	0.00	
	15.2 Sesuai dengan Kebijakan Keamanan dan Standard Kepatuhan Teknis	15.2.1 Sesuai dengan kebijakan Keamanan dan Standar	3.14	3.05
		15.2.2 Teknis Pemeriksaan Kepatuhan	2.96	
	15.3 Sistem Informasi Pertimbangan Audit	15.3.1 Sistem Informasi Kontrol Audit	4.15	2.84
		15.3.2 Perlindungan Perangkat Audit Sistem Informasi	1.53	
Maturity Level Klausul 15				**2.92**



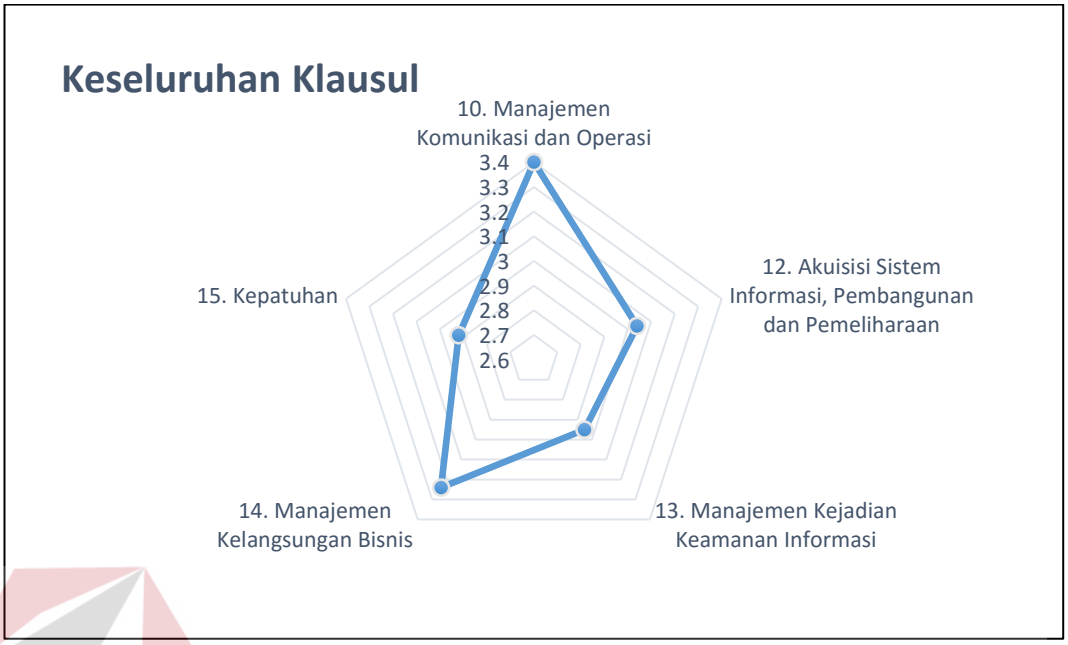
Gambar 4. 6 Jaring Laba-laba Nilai *Maturity Level* Klausul 15

f. Hasil *Maturity Level* Keseluruhan Klausul yang digunakan

Hasil dari proses perhitungan *maturity level* pada keseluruhan klausul yang digunakan adalah 3.11 yaitu *defined*. Hal tersebut menunjukkan bahwa sebagian besar proses keamanan sistem informasi sudah mempunyai aturan dan dilakukan secara rutin. Hal tersebut dapat dilihat pada Tabel 4.14 dan representasi semua klausul yang digunakan dapat dilihat pada jaring laba-laba pada Gambar 4.7.

Tabel 4. 14 Hasil *Maturity Level* Keseluruhan Klausul

klausul	Tingkat Kematangan
10. Manajemen Komunikasi dan Operasi	3.4
12. Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	3.04
13. Manajemen Kejadian Keamanan Informasi	2.95
14. *Manajemen Kelangsungan Bisnis*	3.24
15. Kepatuhan	2.92
Jumlah Tingkat Kematangan	15.55
Rata-rata	3.11



Gambar 4. 7 Jaring Laba-laba Nilai *Maturity Level* Keseluruhan Klausul

Hasil pengukuran *maturity level* klausul 10 tentang manajemen komunikasi dan operasi yaitu 3.4 sedangkan *maturity level* klausul 12 tentang akuisisi sistem, pembangunan dan pemeliharaan yaitu 3.04 dan untuk pengukuran *maturity level* klausul 14 tentang manajemen kelangsungan bisnis yaitu 3.24. Ketiga klausul tersebut yaitu berada pada level 3 (*defined*) yang berarti manajemen sudah mempunyai dasar tentang aturan, prosedur dan kebijakan pada proses manajemen komunikasi dan operasi, proses akuisisi sistem, pembangunan dan pemeliharaan, serta proses manajemen kelangsungan bisnis. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur karena belum adanya aturan dan prosedur secara resmi yang dibuat oleh perusahaan hal ini dikarenakan kurangnya sumber daya TI yang dapat fokus pada pembuatan dokumentasi mengenai TI. Hasil pengukuran *maturity level* klausul 13 tentang manajemen kejadian keamanan informasi yaitu 2.95 dan klausul 15 tentang kepatuhan yaitu 2.92. Kedua klausul

tersebut yaitu berada pada level 2 (*limited/repeatable*) yang berarti manajemen sedang melakukan pengembangan pada proses manajemen kejadian keamanan informasi serta pada proses kepatuhan dan kedua proses ini masih belum mempunyai sebagian besar aturan maupun prosedur yang dijadikan acuan atau dasar dalam proses tersebut.

Berdasarkan hasil audit keamanan sistem informaasi yang telah dilakukan, permasalahan yang terjadi merupakan akibat banyaknya proses yang masih belum memiliki aturan maupun prosedur yang digunakan sebagai acuan atau dasar dalam menjalankan proses tersebut. Hal ini dikarenakan kurangnya sumber daya TI pada perusahaan yang dapat fokus pada hal tersebut. Selain itu perusahaan sendiri terkesan kurang menanggapi serius hal tersebut. Hal ini dibuktikan dengan masih banyaknya proses yang dibiarkan dan dijalankan tanpa adanya aturan maupun prosedur yang resmi. Seperti pada proses manajemen pertukaran (kontrol keamanan 10.1.2) yang memiliki nilai 1.71. Hal tersebut juga diperparah dengan belum adanya kebijakan mengenai pertukaran informasi (kontrol keamanan 10.8.1) yang memiliki nilai 1.00. Selain itu pada proses keamanan dokumen informasi (kontrol keamanan 10.7.4) memiliki nilai 1.36. Hal ini menunjukan perusahaan masih kurang peduli mengenai keamanan dokumen informasi perusahaan. Proses monitoring perusahaan juga masih sangat kurang, terbukti tidak adanya catatan administrator dari operator (kontrol keamanan 10.10.4) yang bernilai sangat rendah yaitu 0.00.

Selain itu tidak adanya standar keamanan khusus untuk *password* yang digunkan oleh perusahaan. hal ini terbukti dengan hasil nilai *maturity* level kebijakaan mengenai penggunaan kontrol kriptografi (kontrol keamanan 12.3.1)

dan peraturan kontrol kriptografi (kontrol keamanan 15.1.6) yang bernilai sangat rendah yaitu 0.00.

Hal lain yang ditemukan pada proses audit adalah belum adanya prosedur pendukung yang digunakan sebagai acuan dalam keamanan informasi. Hal ini dapat dibuktikan dengan hasil *maturity level* tanggung jawab dan prosedur (kontrol keamanan 13.2.1) yang bernilai 1.55. Selain itu perusahaan juga belum memiliki kerangka kerja yang dapat dipertahankan dalam penggunaanya. Hal ini dapat dibuktikan dengan hasil *maturity level* kerangka kerja rencana kelangsungan bisnis (kontrol keamanan 14.1.4) yang bernilai 2.18.

4.3.6 Penyusunan Temuan dan Rekomendasi Audit

Pada tahap penyusuan temuan dan rekomendasi ini merupakan hasil dari evaluasi yang muncul setelah dilakukan pembandingan antara apa yang ada dan terjadi serta hal apa yang harus dilakukan dengan proses yang sedang berlangsung di perusahaan. Setelah mendapatkan hasil temuan maka akan diberikan rekomendasi yang bertuuan untuk dilakukan perbaikan di kemudian hari. Perbaikan ini dilakukan untuk meningkatkan keamanan pada sistem yang digunakan oleh perusahaan. Salat satu contoh temuan dan rekomendasi pada klausul 12 tentang Akuisi Sistem Informasi, Pengembangan, dan Pemeliharaan dengan kontrol 12.1.1 Analisis dan Spesifikasi Persyaratan Keamanan dapat dilihat pada Tabel 4.15 dan selengkapnya dapat dilihat pada Lampiran 11

Tabel 4. 15 Temuan dan Rekomendasi

Klausul 10 Manajemen Komunikasi dan Operasi					
10.1 Tanggung Jawab dan Prosedur Operasional					
Objektif Kontrol: **Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.**					
10.1.1 Pendokumentasian Prosedur Operasi					
No	Pernyataan	Temuan	Bukti	Rekomendasi	Tanggapan
1	Terdapat pendokumentasian prosedur operasi	- Banyak prosedur operasi yang masih belum terdokumentasikan, yaitu khususnya prosedur operasi yang menyangkut IT. - Prosedur operasi hanya ditinjau ulang jika terjadi masalah.	Bukti : Prosedur yang sudah dibuat disimpan pada aplikasi bernama SMM (Foto 1)	- Perusahaan harus membuat prosedur yang belum ada saat ini. Khususnya prosedur yang berhubungan dengan TI. Karena prosedur merupakan hal penting yang digunakan sebagai acuan atau pedoman baku dalam melaksanakan aktivitas tertentu. (Ref : Peraturan Menteri Badan Usaha Milik Negara Republik Indonesia. Nomor : PER-02/MBU/2013)	- Manajeman terkendala dengan kurangnya SDM bagian TI. - Manajemen mempertimbangkan rekomendasi tersebut.

4.3.7 Konfirmasi dan tanggapan Temuan Rekomendasi

Sebelum dilaporan secara formal kepada *auditee* temuan harus dikonfirmasikan terlebih dahulu agar memperoleh tanggapan perusahaan mengenai rekomendasi yang diberikan oleh auditor. Konfirmasi ini dilakukan untuk mengklarifikasi temuan yang ada. Sedangkan tanggapan ini dilakukan untuk mengetahui bagaimana tanggapan perusahaan mengenai rekomendasi yang telah diberikan. Konfirmasi dan tanggapan temuan rekomendasi dapat dilihat pada L**a**mpiran 10 menjadi satu dengan tabel temuan rekomendasi.

4.4 Tahap Pelaporan Audit

Tahap pelaporan yaitu: memberikan laporan audit (*audit report*) sebagai pertanggungjawaban atas penugasan proses audit keamanan sistem informasi yang dilaksanakan. Laporan audit ditunjukkan kepada pihak yang manajemen yang memiliki hak saja, karena laporan audit keamanan sistem informasi merupakan dokumen yang bersifat rahasia.

4.5 Pembahasan Tugas Akhir

Proses audit keamanan sistem informasi pada Parahita *Diagnostic Center* telah selesai dilakukan. Audit keamanan ini dimulai pada bulan Maret sampai pada bulan Juni 2016. Dalam melakukan audit keamanan sistem informasi ini, auditor melakukan wawancara tahap awal dengan manajer dan bagian TI pada perusahaan. Hal ini dimaksudkan untuk mengetahui masalah apa yang ada pada Parahita *Diagnostic Center*. Dari hasil wawancara ini, auditor melakukan diskusi dengan manajer dan bagian TI untuk menggunakan standar ISO 27002:2005 sebagai standar keamanan dalam proses audit ini dengan menggunakan lima klausul. Klausul yang digunakan adalah Klausul 10 tentang Manajemen komunikasi dan operasi, klausul 12 tentang Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan, klausul 13 tentang Manajemen Kejadian Keamanan Informasi, klausul 14 tentang Manajemen Kelangsungan Bisnis, dan klausul 15 tentang Kepatuhan.

Setelah itu auditor melakukan persiapan audit dengan melakukan pemetaan dari kontrol yang ada pada tiap-tiap klausul yang digunakan. Pemetaan kontrol ini mencakup pembuatan pernyataan, pembobotan hingga membuat pertanyaan untuk wawancara dari pernyataan yang sudah dibuat sebelumnya. Setelah tahap persiapan audit ini selesai dilakukan, auditor melakukan pelaksanaan audit.

Tahap pelaksanaan audit ini dilakukan dengan melakukan wawancara dan observasi. Sebelum melakukan wawancara, auditor menentukan *auditee* terlebih dahulu. Selanjutnya wawancara dilakukan terhadap *auditee* yang telah ditentukan yaitu bagian TI dan manajer Parahita *Diagnostic Center*. Selain melakukan

wawancara, auditor juga melakukan observasi. Dalam melakukan observasi, auditor menemukan beberapa temuan.

Menghasilkan nilai rata-rata *maturity level* hasil audit keamanan sistem informasi pada Parahita *Diagnostic Center* adalah 3,11 dengan menggunakan perhitungan CMMI. Nilai *maturity level* 3,11 yaitu berada pada level 3 (*defined*). Hal tersebut menunjukkan bahwa sebagian besar proses keamanan sistem informasi sudah mempunyai aturan dan dilakukan secara rutin. Sedangkan nilai dari masing-masing klausul adalah klausul 10 tentang manajemen komunikasi dan operasi yaitu 3.4 yaitu *defined*, klausul 12 tentang akuisisi sistem informasi, pembangunan dan pemeliharaan yaitu 3.04 yaitu *defined*, klausul 13 tentang manajemen kejadian keamanan informasi yaitu 2.95 yaitu *limited/repeatable*, klausul 14 tentang manajemen kelangsungan bisnis yaitu 3.24 yaitu *defined,* dan klausul 15 tentang kpatuhan yaitu 2.92 yaitu *limited/repeatable*.

Hasil pengukuran *maturity level* klausul 10 tentang manajemen komunikasi dan operasi yaitu 3.4 yaitu *defined*. Hasil tersebut menunjukkan bahwa proses manajemen komunikasi dan operasi sudah dilengkapi aturan dan prosedur mengenai manajemen komunikasi dan operasi. Aturan tersebut meliputi proses kontrol pemisahan tugas, layanan yang diberikan oleh pihak ketiga, *back-up* data, keamanan dalam layanan jaringan, aturan mengenai perjanjian pertukaran informasi hingga aturan mengenai rekaman audit yang telah dilakukan. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur karena belum adanya aturan dan prosedur secara resmi yang dibuat oleh perusahaan hal ini dikarenakan kurangnya sumber daya TI yang dapat fokus pada pembuatan dokumentasi mengenai TI, misalnya mengenai pengelolaan dalam pertukaran

informasi yang dilakukan oleh perusahaan, kurangnya kontrol terhadap kode berbahaya (*malicious code*), kurangnya keamanan dokumentasi sistem informasi, kurangnya kontrol yang dilakukan terhadap *email* perusahaan yang ada, hingga belum adanya catatan *log* mengenai administrator dari sistem yang digunakan oleh perusahaan. Hal lain adalah belum adanya kebijakan dan prosedur mengenai pertukaran informasi yang dilakukan oleh perusahaan. Dari hasil temuan tersebut, auditor memberikan rekomendasi yaitu perusahaan menambahkan sumber daya TI, perusahaan harus membuat aturan maupun prosedur secara resmi mengenai pertukaran informasi, melakukan kontrol terhadap kode berbahaya (*malicious code*), membuat dokumentasi sistem informasi dan memeliharanya, meningkatkan kontrol terhadap email perusahaan, dan membuat catatan log untuk administrator sistem.

Hasil pengukuran *maturity level* klausul 12 tentang akuisisi sistem informasi, pembangunan dan pemeliharaan yaitu 3.04 yaitu *defined*. Hasil tersebut menunjukkan bahwa proses akuisisi sistem informasi, pembangunan dan pemeliharaan sudah dilengkapi aturan dan prosedur mengenai akuisisi sistem informasi, pembangunan dan pemeliharaan. Aturan tersebut meliputi proses validasi data input, validasi data output, perlindungan terhadap data yang digunakan dalam proses pengujian sistem, kontrol akses terhadap *source program*, batasan dalam perubahan sistem, kontrol terhadap kelemahan sistem hingga tinjauan yang dilakukan setelah perubahan sistem. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur karena belum adanya aturan dan prosedur secara resmi yang dibuat oleh perusahaan hal ini dikarenakan kurangnya sumber daya TI yang dapat fokus pada pembuatan dokumentasi mengenai TI, misalnya mengenai kontrol

operasional *software* perusahaan, pengendalian proses internal yang dilakukan seperti belum adanya pemeriksaan validasi mengenai kerusakan data. Hal lain adalah belum adanya kebijakan dalam penggunaan kontrol kriptografi serta manajemen kunci kriptografi dikarenakan sampai saat ini hanya berupa wacana saja dan belum diimplementasikan. Dari hasil temuan tersebut, auditor memberikan rekomendasi yaitu perusahaan menambahkan sumber daya TI, perusahaan harus membuar aturan maupun prosedur secara resmi mengenai kontrol operasional *software* perusahaan, pemeriksaan validasi serta kebijakan mengenai penggunaan kontrol kriptografi. Serta perusahaan harus segera menentukan *framework* yang digunakan untuk perencanaan dalam pembuatan sistem baru.

Hasil pengukuran *maturity level* klausul 13 tentang manajemen kejadian keamanan informasi yaitu 2.95 yaitu *limited/repeatable*. Hal tersebut menunjukan bahwa kontrol keamanan pada proses manajemen kejadian keamanan informasi masih dalam pengembangan serta dokumentasi yang digunakan untuk mendukung kebutuhan masih sangat terbatas. Hal ini dapat ditunjukkan dengan belum adanya prosedur pendukung keamanan informasi yang dibuat secara resmi oleh perusahaan dan belum ada mekanisme yang digunakan untuk memperlihatkan informasi kejadian keamanan informasi secara rinci. Hal lain adalah belum dilakukan pengumpulan terhadap bukti kejadian keamanan informasi yang telah terjadi karena perusahaan kekurangan sumber daya TI untuk dapat fokus ke hal tersebut. Dari hasil temuan tersebut, auditor memberikan rekomendasi yaitu perusahaan menambahkan sumber daya TI, perusahaan harus membuat prosedur pendukung keamanan informasi secara resmi, memikirkan dan membuat mekanisme untuk memperlihatkan informasi kejadian keamanan informasi secara rinci serta

melakukan pengumpulan terhadap bukti kejadian keamanan informasi yang telah ditemukan.

Hasil pengukuran *maturity level* klausul 14 tentang manajemen kelangsungan bisnis yaitu 3.24 yaitu *defined*. Hasil tersebut menunjukkan bahwa proses manajemen kelangsungan bisnis sudah dilengkapi aturan dan prosedur mengenai manajemen kelangsungan bisnis. Aturan tersebut meliputi proses memasukkan keamanan informasi dalam proses manajemen kelangsungan bisnis, proses kelangsungan bisnis dan penilaian resiko yang ada, serta pembangunan dan implementasi rencana kelangsungan yang didalamnya meliputi keamanan informasi. Tetapi ada proses yang belum dilakukan sesuai dengan aturan dan prosedur karena belum adanya aturan dan prosedur secara resmi yang dibuat oleh perusahaan hal ini dikarenakan kurangnya sumber daya TI yang dapat fokus pada pembuatan dokumentasi mengenai TI, misalnya mengenai kerangka kerja rencanan kelangsungan bisnis seperti belum adanya kerangka kerja yang dipertahankan kekonsistenannya. Selain itu adalah pengujian, pemeliharaan dan penilaian ulang rencanan kelangsungan bisnis yang belum maksimal dilakukan oleh perusahaan seperti belum ada teknik yang digunakan oleh perusahaan untuk menggambarkan rencana pemulihan secara spesifik dan belum adanya pengujian terhadap penjadwalan rencana kelangsungan bisnis yang telah ditetapkan. Dari hasil temuan tersebut, auditor memberikan rekomendasi yaitu perusahaan harus memulai menggunakan kerangka kerja yang sesuai sehingga dapat dipertahankan kekonsistenannya, perusahaan harus memikirkan dan menggunakan teknik untuk menggambarkan rencana pemulihan secara spesifik serta perusahaan harus

melakukan pengujian terhadap penjadwalan rencana kelangsungan bisnis yang telah ditetapkan.

Hasil pengukuran *maturity level* klausul 15 tentang kpatuhan yaitu 2.92 yaitu *limited/repeatable*. Hal tersebut menunjukan bahwa kontrol keamanan pada proses manajemen kejadian keamanan informasi masih dalam pengembangan serta dokumentasi yang digunakan untuk mendukung kebutuhan masih sangat terbatas. Hal ini dapat ditunjukkan dengan banyaknya prosedur, panduan, kebijakan maupun peraturan yang belum didokumentasikan secara resmi namun ada beberapa yang dicatat pada catatan pribadi bagian TI maupun direktur. Hal lain adalah belum adanya peraturan mengenai kontrol kriptografi karena hal ini masih berupa wacana yang belum diimplementasikan oleh perusahaan. Dari hasil temuan tersebut, auditor memberikan rekomendasi yaitu perusahaan harus membuat dan memdokumentasikan prosedur, panduan, kebijakan maupun peraturan yang belum ada saat ini.

Secara keseluruhan rekomendasi yang diberikan auditor mengarah pada sumber daya TI perusahaan harus ditambah dan pembuatan aturan, prosedur maupun kebijakan yang lebih detil dengan tujuan agar menjamin keamanan PARIS yang digunakan oleh perusahaan.