AUDIT KEAMANAN SISTEM INFORMASI PARAHITA BERDASARKAN ISO 27002:2005 PADA PARAHITA DIAGNOSTIC CENTER SURABAY

Meita Eny Kusumaning Diah. [1] Haryanto Tanuwijaya [2] Erwin Sutomo [3]
Fakultas Teknik Informatika
Program Studi S1 Sistem Informasi
Institut Bisnis dan Informatika Stikom Surabaya
Jl. Kedung Baruk 98 Surabaya, 60298
Email : 1) meitaeny@gmail.com, 2) haryanto@stikom.edu, 3) sutomo@stikom.edu

Abstract: *Parahita Diagnostic Center (PDC) is a company engaged in the field of public health service, particularly in the field of laboratory. PDC using technology that is integrated and centralized called Parahita Information System (PARIS) for running and supporting existing business processes. Implementation of the (PARIS) has some problems: frequent occurrence of malicious code attacks, misuse by unauthorized parties, and lack of maintenance on the system. Existing obstacles which lead to some risk of data loss, misuse of data and information, failures in data processing and the performance of the system becomes impaired. In order to determine the cause of problems that may occur, PDC need to conduct a Information System Security Audit using the standard ISO 27002: 2005 as the best security. This audit process using ISACA developed stage and calculations of maturity model using CMMI. The scope used is clause 10, clause 12, clause 13, clause 14 and clause 15 which is adapted to the problem. The results obtained from the information system security audit is the level of maturity of 3,11 that is defined. It shows that most of the information systems security process already have rules and conducted on a regular basis. This research also produced recommendations which are used to improve the process of information systems owned by the PDC.*

Kata Kunci : *Information System Security Audit, ISO 27002, Laboratorium*

Parahita *Diagnostic Center* (PDC) adalah perusahaan yang bergerak pada bidang jasa pelayanan kesehatan masyarakat, khususnya pada bidan laboratorium. 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 pemeriksaan hingga proses keluarnya hasil laboratorium. PARIS 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 laboratorium 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 PARIS ini tidak dapat dipungkiri PDC menemui beberapa permasalahan. yaitu menyangkut backup recovery, serangan malicious code

yang mengancam keutuhan data perusahaan, modifikasi tanpa hak yang mengancam kerahasian perusahaan, sulitnya dalam mengidentifikasi kelemahan keamanan sistem informasi serta pemeriksaan sistem yang tidak sesuai dengan standar keamanan yang ada. Berdasarkan kendala tersebut PDC perlu melakukan audit keamanan sistem informasi untuk mengetahui terjadinya permasalahan yang sering terjadi, agar perusahaan dapat menjaga keamanan sistem informasi yang dimiliki. Audit keamanan sistem informasi ini digunakan sebagai evaluasi keamanan sistem informasi (Asmuni & Firdaus, 2005). Tiga aspek keamanan informasi yang harus dijaga adalah aspek kerahasiaan (Confidentiality), Keutuhan (Integrity) dan ketersediaan (Availability) dari informasi (ISO/IEC 27002, 2005). Menurut Tanuwijaya & Sarno (June 2010), diperlukan standar untuk melakukan audit tersebut agar audit keamanan sistem informasi dapat berjalan dengan baik. Oleh karena itu, dalam penelitian tugas akhir ini standar yang digunakan mengacu pada *Information Systems Audit and Control Association* (ISACA) dengan standar *International Standard Organization* ISO 27002:2005 sebagai *best practice* penerapan keamanan informasi dengan menggunakan bentuk kontrol agar dapat mencapai sasaran yang diterapkan.

Klausul yang digunakan dalam audit keamanan sistem informasi ini adalah Komunikasi dan Manajeman Operasional (Klausul 10), Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan (Klausul 12), Manajemen Insiden Keamanan Informasi (Klausul 13), Manajemen Kelangsungan Bisnis (Klausul 14), dan Kesesuaian (Klausul 15).

Dengan dilakukannya audit keamanan informasi pada PDC diharapkan dapat mengetahui tingkat keamanan sistem informasi yang ada, sehingga dapat mengetahui permasalahan yang terjadi selama ini. Hasil audit ini berupa temuan dan diharapkan menjadi rekomendasi yang dapat digunakan untuk meningkatkan keamanan sistem informasi yang ada pada PDC serta menjadi acuan untuk mendapatkan ISMS *certification* dengan standar ISO 27002:2005.

LANDASAN TEORI

Audit Keamanan Informasi

Menurut Ahmad (2012) audit keamanan sistem informasi merupakan suatu kejadian atau proses yang berbasis pada standar maupun kebijakan keamanan yang bertujuan untuk menentukan perlindungan terhadap kejadian keamanan yang terjadi dan untuk melakukan pemeriksaan terhadap perlindungan yang dilakukan. Tujuan utama dari audit keamanan informasi ini yaitu melakukan perlindungan yang sesuai dengan standar maupun kebijakan keamanan yang ada. Implementasi dari audit keamanan sistem informasi ini agar dapat mengatasi permasalahan atau kendala keamanan sistem informasi secara teknis maupun non teknis.

ISO/IEC 27002:2005

Standar keamanan ISO 27002:2005 ini merupakan standar yang berisikan pedoman mengenai penerapan keamanan sistem informasi. ISO 27002:2005 ini memiliki beberapa kontrol yang telah ditetapkan, yaitu 12 klausul, 41 objektif kontrol, dan 133 kontrol. Standar ini memberikan kebebasan kepada pengguna untuk memilih dan menerapkan kontrol yang sesuai dengan kebutuhannya, dengan mempertimbangkan hasil kajian risiko yang telah dilakukannya (Direktorat Keamanan Informasi, 2011).

Tingkat Kedewasaan (*Maturity Level*)

Menurut IT Governance Institute (2007: 17), model kedewasaan (*maturity level*) merupakan model yang digunakan dalam mengendalikan suatu proses TI yang terdiri dari pengembangan suatu metode penilaian sehingga suatu organisasi dapat melakukan pengukuran dirinya sendiri. Menurut DISC Infosec (2009) salah satu cara untuk dapat mencapai kontrol keamanan informasi yang optimal adalah menilai keamanan informasi organisasi berdasarkan ISO 27002 dan pemetaan setiap

kontrol keamanan menggunakan *Capability Maturity Model Integration* (CMMI).

Gambar 1 Tingkat Kematangan CMMI
(Sumber: DISC Infosec, 2009)

CMMI memiliki lima tingkatan kematangan proses yaitu :

a. Level 0 *(non-existent)*: Tidak ada kontrol sama sekali.
b. Level 1 *(initial)*: Pada level ini, organisasi memiliki pendekatan yang tidak konsisten, kontrol keamanan dilakukan secara informal. Informal berarti tidak ada dokumentasi, tidak ada standar.
c. Level 2 *(limited/repeatable)*: Pada level ini, kontrol keamanan masih dalam pengembangan dan/atau ada dokumentasi terbatas untuk mendukung kebutuhan.
d. Level 3 *(defined)*: Pada level ini, kontrol keamanan telah didokumentasikan rinci dan dikomunikasikan melalui pelatihan, tetapi tidak ada pengukuran kepatuhan.
e. Level 4 *(managed)*: Pada level ini, terdapat pengukuran efektivitas kontrol keamanan, tetapi tidak ada bukti dari setiap ulasan kepatuhan dan/atau kontrol memerlukan perbaikan lebih lanjut untuk mencapai tingkat kepatuhan yang diperlukan.
f. Level 5 *(optimized)*: Pada level ini, kontrol keamanan telah disempurnakan hingga sesuai dengan ISO 27002 berdasarkan pada kepemimpinan yang efektif, manajemen perubahan, perbaikan berkelanjutan, dan komunikasi internal.

METODE

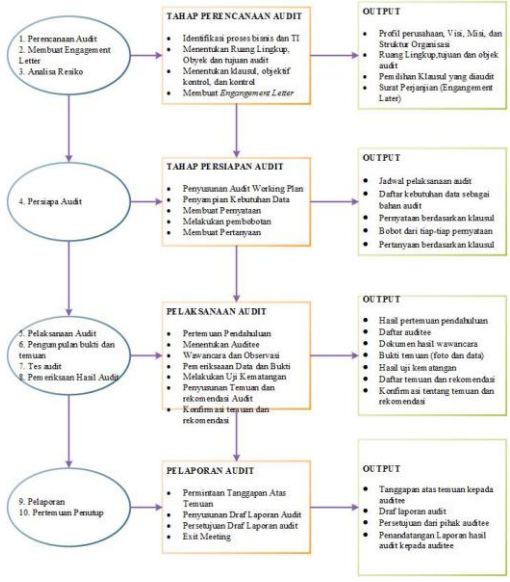
Terdapat 10 tahapan audit menurut Canon (2011), yang digunakan sebagai acuan dalam mengembangkan metode yang digunakan. saya membagi menjadi empat langkah dapat dilihat pada Gambar 2, yaitu :

1. Tahap perencanaan audit yang menghasilkan *output* berupa dokumen mengenai perusahaan, ruang lingkup, klausul yang digunakan pada proses audit, serta surat perjanjian atau *engagement letter*.

2. Tahap persiapan audit yang menghasilkan *output* berupa jadwal pelaksanaan audit, daftar kebutuhan data, pernyataan berdasarkan klausul, bobot dari tiap klausul, serta pertanyaan berdasarkan klausul.

3. Tahap Pelaksanaan audit yang menghasilkan *output* berupa hasil pertemuan pendahuluan, daftar *auditee*, dokumen hasil wawancara, bukti temuan, hasil uji kematangan serta daftar temuan dan rekomendasi.

4. Tahap pelaporan audit yang menghasilkan *output* berupa tanggapan atas temuan, draf laporan audit, persetujuan dari *auditee*, serta penandatanganan laporan hasil audit kepada *auditee* yang dilakukan pada *exit meeting*.



Gambar 2 Tahapan audit yang digunakan

IMPLEMENTASI DAN HASIL

Identifikasi Proses Bisnis

Identifikasi proses bisnis ini dilakukan dengan cara melakukan wawancara dengan *branch manager* PDC. Selain itu juga dilakukan observasi langsung ke perusahaan. Hal ini menghasilkan profil perusahaan, visi, misi perusahaan, struktur organisasi, serta proses bisnis dan TI perusahaan.

Menentukan Ruang Lingkup, Objek dan Tujuan Audit

Wawancara dan observasi merupakan cara yang digunakan untuk menentukan ruang lingkup Sehingga 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.

Menentukan Klausul, Obyektif Kontrol dan Kontrol

Penentuan klausul dalam audit keamanan PARIS berdasarkan permasalahan yang terjadi pada PDC. Rincian permasalahan yang terjadi adalah menyangkut backup recovery, serangan malicious code yang mengancam keutuhan data perusahaan, modifikasi tanpa hak yang mengancam kerahasian perusahaan, sulitnya dalam mengidentifikasi kelemahan keamanan sistem informasi serta pemeriksaan sistem yang dilakukan tidak sesuai dengan standar keamanan yang ada. Oleh karena itu klausul yang dipilih dalam audit keamanan sistem informasi ini yaitu :

1. Komunikasi dan Manajeman Operasional (Klausul 10)
2. Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan (Klausul 12)
3. Manajemen Insiden Keamanan Informasi (Klausul 13)
4. Manajemen Kelangsungan Bisnis (Klausul 14)
5. Kepatuhan (Klausul 15

Membuat 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.

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 Gambar 3.

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												

Gambar 3 Audit Working Plan

Penyampaian Kebutuhan Data

Penyampaian kebutuhan data kepada *auditee* yang digunakan untuk menunjang kegiatan audit yang dilakukan oleh auditor. Pada proses ini auditor memberikan list kebutuhan data-data yang dibutuhkan dalam proses audit. *List* penyampaian kebutuhan data dapat dilihat pada Tabel 1.

Tabel 1 Permintaan Penyampaian Data

NO	Kebutuhan Data	Ketersediaan Data		Keterangan
		Ada	Tudak	

1	Profil Perusahaan	√		

Membuat Pernyataan

Membuat pernyataan yang mengacu pada kontrol keamanan berdasarkan standar ISO 27002:2005. Contoh pernyataan dapat dilihat pada Tabel 2.

Tabel 2 Pernyataan

Klausul 10 Manajemen Komunikasi Operasi	
10.1 Tanggung Jawab dan Prosedur	
10.1.1 Pendokumentasia Prosedur Operasi	
NO.	Pernyataan
1.	Terdapat dokumentasi terhadap prosedur Operasi
2.	Terdapat pemeliharaan terhadap prosedur operasi

Melakukan Pembobotan

Setiap pernyataan yang sudah dibuat akan diberikan pembobotan. Pemberian Nilai bobot ini sesuai dengan besar kecilnya resiko yang dapat terjadi pada PDC dan juga sesuai dengan pedoman audit yang digunakan. Apabila tidak terdapat resiko sedikitpun maka nilai bobot yang diberikan adalah nol. Contoh pemberian nilai bobot ada pada Tabel 3

Tabel 3 Pembobotan

Klausul 10 Manajemen Komunikasi Operasi		
10.1 Tanggung Jawab dan Prosedur		
10.1.1 Pendokumentasia Prosedur Operasi		
No.	**Pernyataan**	**Pembobotan**
1.	Terdapat dokumentasi terhadap prosedur Operasi	1
2.	Terdapat pemeliharaan terhadap prosedur operasi	0.8

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.

Tabel 4 Pertanyaan

Klausul 10 Manajemen Komunikasi Operasi		
10.1 Tanggung Jawab dan Prosedur		
10.1.1 Pendokumentasia 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 ?

Menentukan Auditee

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 menjadi narasumber pada tahapan wawancara sebagai sumber informasi yang dibutuhkan pada audit keamanan sistem informasi. Contoh menentukan auditee dapat dilihat pada Tabel 5.

Tabel 5 Penentuan Auditee

Klausul	Bagian TI	Bagian Laboratorium	Bagian keuangan	Bagian Pelayanan	Bagian SDM	Manajer	Direktur
10	R/A	C	C	C	C	C/I	R/A/I
12	R/A	C	C	C	C	C/I	R/A/I
13	R/A/C	C	C	C	C	C/I	R/A/C/I
14	R/A	C	C	C	C	C/I	R/A/I
15	R	C	C	C	C	C/I	R/A

Hasil wawancara dan Observasi

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 6.

Tabel 6 Hasil Wawancara

Klausul 10 Manajemen Komunikasi Operasi			
10.1 Tanggung Jawab dan Prosedur			
10.1.1 Pendokumentasia 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 seperti prosedur yang bersangkuan langsung dengan bagian keuangan saja.

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. Contoh hasil pemeriksaan dapat dilihat pada tabel 7 pada tabel ini juga terdapat penilaian yang dilakukan.

Tabel 7 Hasil pemeriksaan dan penilaian

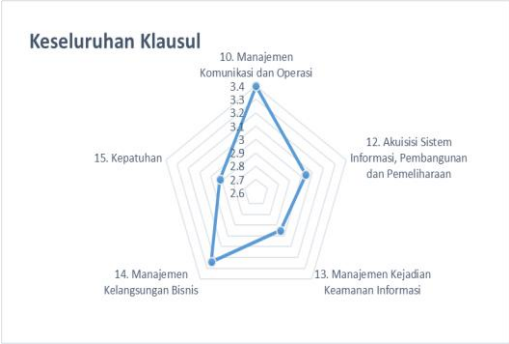
Klausul 10 Manajemen Komunikasi Operasi										
Objektif Kontrol : 10.1 Tanggung Jawab dan Prosedur Operasional										
Kontrol: 10.1.1 Pendokumentasian Prosedur Operasi				Penilaian						Nilai
NO	Pernyataan	Hasil Pemeriksaan	Bobot	0	1	2	3	4	5	
1	Terdapat pendokumentasian prosedur operasi	Perusahaan 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

Melakukan Uji Kematangan

Sebelum melakukan penghitungan *maturity level* harus dilakukan penilaian terlebih dahulu. Contoh penilaian dapat dilihat pada Tabel 7 diatas. Dari hasil proses perhitungan *maturity level* semua 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. Lebih detailnya dapat dilihat pada Tabel 8 dan juga dapat ditunjukan dalam bentuk jaring laba-laba. Jaring laba-laba tersebut dapat dilihat pada Gambar 4

Tabel 8 Hasil Perhitungan Tingkat Keamanan Seluruh 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
Rata-rata	3.11



Gambar 4 Jaring Laba-laba Nilai Maturty Level Keseluruhan klausul

Penyusunan Temuan dan Rekomendasi Audit

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 bertujuan untuk dilakukan perbaikan di kemudian hari. Perbaikan ini dilakukan untuk meningkatkan keamanan pada sistem yang digunakan oleh perusahaan. Salah satu contoh temuan dan rekomendasi pada klausul 10 tentang Manajemen Komunikasi dan Operasi dengan kontrol 10.1.1 Pendokumentasian prosedur operasi dapat dilihat pada Tabel 9

KESIMPULAN

1. Perencanaan audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center telah berhasil dilakukan dengan menghasilkan ruang lingkup audit, mengumpulkan data, dan menentukan klausul yang digunakan yaitu klausul 10, 12, 13, 14, dan 15.

Tabel 9 Temuan dan Rekomendasi

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	Temuan	Bukti	Rekomendasi	Tanggapan
1	Terdapat persyaratan kebutuhan bisnis untuk sistem informasi yang baru	- 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 persyaratan atau prosedur khusus kebutuhan bisnis untuk sistem informasi yang baru. (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.

2. Persiapan audit audit keamanan sistem informasi parahita berdasarkan standar ISO 27002:2005 pada Parahita Diagnostic Center telah berhasil dilakukan dengan menghasilkan semua-dokumen yang dibutuhkan yaitu daftar pernyataan, daftar pembobotan, daftar pertanyaan, daftar hasil pemeriksaan, perhitungan *maturity level* hingga daftar temuan dan rekomendasi yang nantinya akan digunakan sebagai acuan perusahaan untuk memperbaiki kontrol keamanan sistem informasi.
3. Dari hasil audit keamanan sistem informasi ini didapatkan perhitungan rata-rata *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.

SARAN

1. Untuk kedepannya diharapkan Parahita *Diagnostic Center* segera melakukan perbaikan mulai dari aturan, panduan, prosedur keamanan sistem informasi, kebijakan dan persyaratan yang digunakan untuk keamanan sistem informasi hingga manajemen keamanan sistem informasi.
2. Perusahaan diharapkan untuk melakukan audit keamanan sistem informasi kembali setelah dilakukan perbaikan karena audit keamanan sistem informasi yang telah dilakukan ini belum menerapkan keseluruhan kontrol keamanan yang ada. Hal ini dilakukan agar perusahaan dapat mengetahui dan mengukur bagaimana keberhasilan dalam menerapkan hasil rekomendasi yang telah diberikan sebelumnya.

DAFTAR PUSTAKA

Ahmad, A. (2012). *Bakuan Audit Keamanan Informasi Kemenpora*. Indonesia: Kementerian Pemuda dan Olahraga.

Asmuni, L., dan Firdaus, R. (2005). Peranan Pengendalian Berbasis Audit Sistem Informasi untuk Pengembangan Strategi Perusahaan Berbasis Komputer (Suatu Bahasan Teoritis Atas Faktor Penentu Keberhasilan dan Penyimpangan Penerapan Sistem Informasi dalam Suatu Organisasi Usaha). *Seminar Nasional Aplikasi Teknologi Informasi 2005*, E21-E26.

Canon, D. (2011). *CISA (Certified Information SYstem Auditor) Study Guide (Vol. 3rd edition).* Indriana Polis: Wiley Publising.

Direktorat Keamanan Informasi. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik.* Jakarta: Kementrian Keamanan Informasi dan Informatika RI.

Institute, i. T. (2007). *COBIT 4.10: Control Objective, Management Guidelines, Maturity Models.* United States of America: IT Governance institute.

ISO/IEC 27002. (2005). *Information Technology - Security techniques - Code of practice for information security management International* . ISO.

Tanuwijaya, H., dan Sarno, R. (June 2010). Comparation of CObit Maturity Level and Structural Equation Model for Measuring the Alignment between University of Computer Science and Network Security. *International Journal of Computer Science and Network Security, VOL.10 No.6*.