ISSN:2442-5567 | E-ISSN:2443-289X

AUDIT KEMANAN INFORMASI MENGGUNAKAN ISO 27002 PADA DATA CENTER PT.GIGIPATRA MULTIMEDIA

Herman Afandi[1] Abdi Darmawan[2]

[1]Gigapatra Multimedia PT [2]M.TI Institut Informatika dan Bisnis Darmajaya
Email: [1]hermanafandi1516@gmail.com [2]abdi@darmajaya.ac.id

ABSTRAK

Perseroan PT.Giga Patra Multimedia adalah sebuah perusahaan swasta nasional yang berkonsentrasi pada internet service provider, penjualan hosting dan pengadaan perlengkapan dan peralatan pendukung teknologi. Mengingat pentingnya informasi perusahaan, maka informasi harus dilindungi atau diamankan oleh seluruh personil perusahaan. Seluruh informasi perusahaan yang ada harus memiliki backup dan recovery yang berjalan dengan baik.Sementara itu, selama perusahaan PT.Giga Patra Multimedia ini berdiri telah terjadi beberapa permasalahan antara lain sering ditemukan terjadinya kebocoran informasi dan hacking terhadapa website pelanggan yang berda di web server. Selain itu, dikhawatirkan dapat merambat pada terjadinya penyalahgunaan informasi.Maka di perlukanya audit internal di dalam perusahaan PT.Giga Patra Multimedia. Jenis audit yang di gunakan dalam penelitian ini yaitu audit internal menggunakan standar kemanan informasi Iso 27002:2013. Dan beberapa klausal yitu Keamanan Sumber Daya Manusia (Klausul 7), Kontrol Akses (Klausul 9), Keamanan Fisisk Dan Lingkungan (Klausul 11), Managemen Komunikasi Dan Oprasi 12).Dengan adanya audit keamanan informasi pada PT. Giga Patra Multimedia dapat mengetahui kelemahan-kelemahan sistem yang menjadi penyebab permasalahan keamanan informasi yang selama ini terjadi. Selain itu audit ini dapat mengukur tingkat keamanan dimiliki PT. Giga Patra Multimedia. Dari hasil audit keamanan sistem informasi yang telah dilakukan, maka didapatkan kesimpulan yaitu pada bidang Keamanan Sumber Daya Manusia (Klausul 7) menghasilkan nilai maturity level 2.71 dan pada bidang Kontrol Akses (Klausul 9) memiliki nilai maturity level 2,75 dan bidang Keamanan Fisik dan Lingkungan (Klausul 11) kemanan sumber daya manuia menghasilkan nilai maturity level 2.75 yaitu berada pada level 2 (limited/repeatable) yang berarti kontrol keamanan sedang dalam pengembangan, sudah ada dokumentasi terbatas tetapi belum ada pelatihan dan pengukuran efektifitas kontrol keamanan, dan bidang oprasional (Klausul 12) menghasilkan nilai maturity level 1,33 yaitu berada pada level Level 2 (limited/repeatable) Pada level ini, kontrol keamanan masih dalam pengembangan dan/atau ada dokumentasi terbatas untuk mendukung kebutuhan. Diharapkan PT. GIGA PATRA MULTIMEDIA dapat melakukan perbaikan manajemen keamanan sistem informasi, aturan, dan prosedur keamanan sistem informasi agar ancaman-ancaman terkait keamanan informasi dapat diminimalisir.

Kata Kunci : Audit, ISO 27002, audit kemanan data center,kemanan informasi

ISSN:2442-5567 | E-ISSN:2443-289X

ABSTRACT

PT. Giga Patra Multimedia Company is a private company which concentrates on Internet service providers, hosting sales and procurement of supplies and support equipment technology. Given the importance of enterprise information, then the information must be protected or secured by the entire personnel of the company. All information company that there must have backup and recovery baik.Sementara that goes with it, as long as the company PT.Giga Multimedia Patra stands have been some problems, among others, are often found to leak information and hacking websites terhadapa customers arriving at the web server. In addition, it is feared may propagate in the abuse informasi.Maka in perlukanya internal audit in the company PT.Giga Patra Multimedia. Types of audits are used in this research that uses an internal audit of security standards Iso 27002: 2013. And some clauses yitu Security Human Resources (Clause 7), Access Control (Clause 9), elderly physic Safety and Environment (Clause 11), Management Communication and Oprasi 12) .With the security audit information on PT. Giga Multimedia Patra can find out the weaknesses of the system is the cause of information security problems which have occurred. Besides this audit can measure the level of security by PT. Giga Patra Multimedia. From the results of a security audit of information systems that have been done, it was concluded that in the field of Human Resource Security (Clause 7) yielded values 2.71 and maturity level in the field of Access Control (Clause 9) has a value of 2.75 and a maturity level and field of Physical Security Environment (Clause 11) security resources Manuia generate value maturity level of 2.75 is located on level 2 (limited / repeatable) which means that security controls are under development, there have been limited documentation but no training and measuring the effectiveness of security controls, and field operational (Clause 12) yielded values of 1.33 maturity level that is at the level of Level 2 (limited / repeatable) At this level, security controls are still in development and / or there is limited documentation to support the need. Expected PT. GIGA PATRA MULTIMEDIA can do the repair information system security management, rules, and procedures that the information system security threats related to information security can be minimized.

***Keywords* :** *Audit, ISO 27002, audit kemanan data center,kemanan informasi*

1. PENDAHULUAN

Perseroan PT. Giga Patra Multimedia adalah sebuah perusahaan swasta nasional yang berkonsentrasi pada internet service provider, penjualan hosting dan pengadaan perlengkapan dan peralatan pendukung teknologi. PT.Giga Patra Multimedia terus berupaya untuk meningkatkan pelayanan, sejak pendiriannya pada tahun 2010. Sejalan dengan peningkatan volume usaha dan semakin luasnya wilayah usaha, PT.Giga Patra Multimedia mengembangkan sebuah pola manajemen menuju ke arah pengelolaan usaha memperhatikan ketepatan dan kelengkapan pelayanan terhadap pelanggan.

Sebagai perusahaan yang berskala nasional, PT.Giga Patra Multimedia memiliki sentral usaha di RT. 04 RW. 02 Desa Nabang Baru Kec Margatiga Kabupaten Lampung Timur Propinsi Lampung. PT.Giga Patra Multimedia sangat berperan penting dalam mengelola keamanan informasi, karena seluruh informasi perusahaan yang merupakan aset berharga bagi perusahaan berada di sana. PT.Giga Patra Multimedia memiliki 2 (dua) *server* yang beroperasi, yaitu 1 (satu) *server* untuk data aplikasi web server dan mail server, 1 (satu) *server* untuk *router* dan *proxy*. Seiring perkembangan bisnis yang semakin maju, maka pengembangan informasi yang dilakukan juga semakin besar. Hal ini dapat dilihat dari banyaknya jumlah *server* yang dimiliki yaitu sebanyak 2 (server) *server*. Mengingat pentingnya informasi perusahaan, maka informasi harus dilindungi atau

ISSN:2442-5567 | E-ISSN:2443-289X

diamankan oleh seluruh personil perusahaan. Seluruh informasi perusahaan yang ada harus memiliki *backup* dan *recovery* yang berjalan dengan baik. Rahardjo (2005: 1) menyatakan bahwa masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Terjadinya masalah keamanan dapat menimbulkan kerugian bagi perusahaan misalnya kerugian apabila sistem informasi tidak bekerja selama kurun waktu tertentu, kerugian apabila ada kesalahan data atau informasi dan kehilangan data. Sementara itu, selama perusahaan PT.Giga Patra Multimedia ini berdiri telah terjadi beberapa permasalahan antara lain sering ditemukan terjadinya kebocoran informasi dan hacking terhadapa website pelanggan yang berda di web server. Selain itu, dikhawatirkan dapat merambat pada terjadinya penyalahgunaan informasi yang merugikan PT. Giga Patra Multimedia dalam persaingan dengan para kompetitor. Kendala lain yang ditemukan adalah kerusakan peralatan sistem informasi yang dapat menyebabkan hilangnya data perusahaan dan sistem yang sering *hang*. Di samping itu, terjadi gangguan-gangguan yang menyebabkan kekacauan antara lain kerusakan data.

Selama ini PT. Giga Patra Multimedia belum pernah melakukan analisa penyebab terjadinya permasalahan tersebut dan PT. Giga Patra Multimedia tidak mengetahui sampai di mana tingkat keamanan informasi yang di milikinya. Oleh karena itu PT. Giga Patra Multimedia membutuhkan evaluasi keamanan informasiuntuk menjaga keamanan informasiyang berda di data center tempat menyimpan semua data informasi pelanggan. Evaluasi keamanan informasi dapat dilakukan dengan audit keamanan informasi(Asmuni dan Firdaus, 2005: 23). Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*Availability*) dari Informasi (ISO/IEC 27002, 2005: 1).

Agar audit keamanan informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukan audit tersebut (Tanuwijaya dan Sarno, 2010: 80). Menurut Sarno dan Iffano (2009: 59) tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh perusahaan untuk melaksanakan audit keamanan sistem informasi. Pemilihan standar ditentukan oleh bersama sama dengan pipmpinan perusahaan itu sendiri. PT. Giga Patra Multimedia memilih menggunakan standar ISO 27002. Salah satu alasan PT. Giga Patra Multimedia memilih menggunakan ISO 27002 ini karena PT. Giga Patra Multimedia juga telah menggunakan standarisasi ISO tetang sistem manajemen mutu yaitu ISO 9001: 2008. Standar ISO 27002 dipilih dengan pertimbangan bahwa standar ini sangat fleksibel dikembangkan tergantung pada kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai dan ukuran struktur organisasi. Selain itu, pertimbangan lainnya adalah ISO 27002 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara internasional yang disebut *Information Security Management Sistem* (ISMS) *certification* (Sarno dan Iffano, 2009: 59-60).

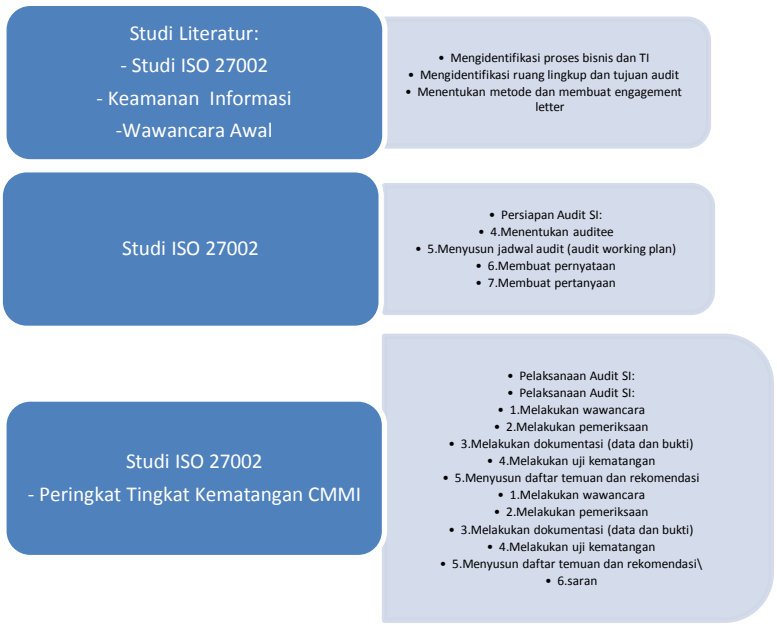
Mengingat permasalahan yang dihadapi PT. Giga Patra Multimedia menyangkut antara lain: masalah sumber daya manusia, keamanan fisik dan lingkungan, operasional sistem informasi, kontrol akses, dan kejadian-kejadian yang menyangkut keamanan informasipada data center, maka klausul yang dipilih dalam audit keamanan informasia dalah Keamanan Sumber Daya Manusia (Klausul 7), Kontrol Akses (Klausul 9), Keamanan Fisisk Dan Lingkungan (Klausul 11), Managemen Komunikasi Dan Oprasi 12).Dengan adanya audit keamanan informasi pada PT. Giga Patra Multimedia dapat mengetahui kelemahan-kelemahan sistem yang menjadi penyebab permasalahan keamanan informasi yang selama

ISSN:2442-5567 | E-ISSN:2443-289X

ini terjadi. Selain itu audit ini dapat mengukur tingkat keamanan dimiliki PT. Giga Patra Multimedia. Audit ini juga menghasilkan rekomendasi tentang perbaikan yang harus dilakukan untuk meningkatkan keamanan informasi pada perusahaan, serta menjadi pertimbangan untuk memperoleh ISMS *certification* dengan standar ISO 27002 pada masa mendatang, sehingga menambah nilai tambah akan kepercayaan pelanggan terhadap PT. Giga Patra Multimedia.

2. METODOLOGI PENELITIAN

Perencanaan dalam melaksanakan audit keamanan informasi mencakup semua aktivitas auditor dari awal kegiatan hingga hasil akhir audit yang didapat.merupakan alur dari serangkaian kegiatan audit.



Penomoran digunakan untuk menunjukkan langkah-langkah kegiatan inti, sedangkan aktivitas lain merupakan inputan yang digunakan untuk kegiatan inti tersebut. Untuk penjabaran dari aktivitas kegiatan yang lebih detail akan dijelaskan pada sub bab metode penelitian ini.

2.1 Perencanaan dan Persiapan Audit kemanan 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. Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Melakukan identifikasi proses bisnis dan TI, 2. Mengidentifikasi ruang lingkup dan tujuan audit, 3. Menentukan metode dan membuat *engagement letter*, 4. Menentukan *auditee*, 5. Menyusun jadwal audit (*audit working plan*), 6. Membuat pernyataan, dan 7. Membuat pertanyaan. Tahap ini akan menghasilkan pengetahuan tentang proses bisnis dan TI perusahaan, ruang lingkup dan tujuan yang telah ditentukan, klausul yang digunakan, tabel *auditee* dan *audit working plan*, pernyataan yang telah dibuat berdasarkan standar ISO 27002, dan pertanyaan yang telah dibuat berdasarkan pernyataan. Hasil dari tahap

ISSN:2442-5567 | E-ISSN:2443-289X

perencanaan dan persiapan audit sistem informasi ini akan dituangkan ke dalam surat perjanjian audit (*engagement letter*), lampiran perencanaan audit, dan kertas kerja audit.

2.1.1 Mengidentifikasi Proses Bisnis dan TI

Pada tahapan perencanaan audit, proses pertama yang dilakukan adalah melakukan pemahaman proses bisnis dan TI perusahaan yang diaudit (*auditee*). Pemahaman dilakukan dengan cara mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen tersebut berupa profil perusahaan, *standard operating procedure*, kebijakan, standar, prosedur, portopolio, arsitektur, infrastruktur, dan aplikasi sistem informasi. Langkah selanjutnya adalah mencari informasi apakah sebelumnya perusahaan telah melaksanakan proses audit. Apabila pernah dilakukan audit, maka auditor perlu mengetahui dan memeriksa laporan audit sebelumnya. Untuk menggali pengetahuan tentang *auditee* langkah yang dilakukan adalah dengan cara mengetahui dan memeriksa dokumen-dokumen yang terkait dengan proses audit, wawancara manajemen dan staff, serta melakukan observasi kegiatan operasional dan teknologi sistem informasi yang digunakan. *Output* yang dihasilkan pada proses ini adalah profil perusahaan, visi dan misi perusahaan, struktur organisasi, serta gambaran umum teknologi informasi yang selengkapnya akan dipaparkan pada Bab IV.

2.1.2 Menentukan *Auditee*

Pada proses menentukan *auditee*, langkah yang dilakukan yaitu memilih *auditee* berdasarkan klausul yang telah ditetapkan.

2.1.3 Menentukan Jadwal Audit (*Audit Working Plan*)

Pada proses membuat audit *working plan* langkah yang dilakukan adalah membuat daftar semua kegiatan yang akan dilakukan dalam melakukan proses audit mulai dari proses awal hingga proses pelaporan audit

2.1.4 Membuat Pernyataan

Proses selanjutnya pada tahapan persiapan audit ini dilakukan dengan membuat pernyataan berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah ditentukan. Kontrol keamanan dapat dilihat pada panduan implementasi ISO 27002. Pada tiap kontrol keamanan dapat ditemukan pernyataan yang mendeskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut. Salah satu contoh kontrol keamanan yaitu Pembatas Keamanan Fisik yang ada dalam Klausul 9 (sembilan)

2.1.5 Membuat Pertanyaan

Setelah dilakukan pembobotan pernyataan pada tiap proses TI, maka selanjutnya auditor membuat pertanyaan berdasarkan pernyataan tersebut. Pada tiap pernyataan tidak selalu menghasilkan satu pertanyaan bahkan mungkin menghasilkan lebih dari satu pertanyaan. Pertanyaan tersebut akan dijadikan acuan dalam melakukan wawancara kepada pihak yang telah ditentukan sebelumnya.

ISSN:2442-5567 | E-ISSN:2443-289X

2.2 Pelaksanaan Audit Keamanan Informasi

Pelaksanaan audit keamanan informasi ini menggunakan jenis audit kepatutan atau audit kesesuaian yang di lakukan dalam internal perusahaan. Menurut Sarno dan Iffano (2009: 172) audit kepatutan yang dilaksanakan untuk tujuan dalam menegaskan apakah kontrol-kontrol keamanan yang ditentukan telah diimplementasi, dipelihara, memenuhi syarat pada panduan implementasi dan berjalan sesuai dengan yang diharapkan. Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Melakukan wawancara, 2. Melakukan pemeriksaan, 3. Melakukan dokumentasi (data dan bukti), 4. Melakukan uji kematangan, dan 5. Menyusun daftar temuan dan rekomendasi. Tahap ini akan menghasilkan dokumen wawancara, temuan dan bukti, nilai kematangan, dan rekomendasi.

2.2.1 Melakukan Wawancara

Pada proses ini langkah yang dilakukan adalah melakukan wawancara berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan terhadap pihak-pihak yang terlibat dalam eksekusi. Salah satu contoh dokumen wawancara dengan kontrol keamanan yaitu Pembatas Keamanan Fisik yang ada dalam Klausul 9 (sembilan) Keamanan Fisik dan Lingkungan

2.2.2 Melakukan Pemeriksaan

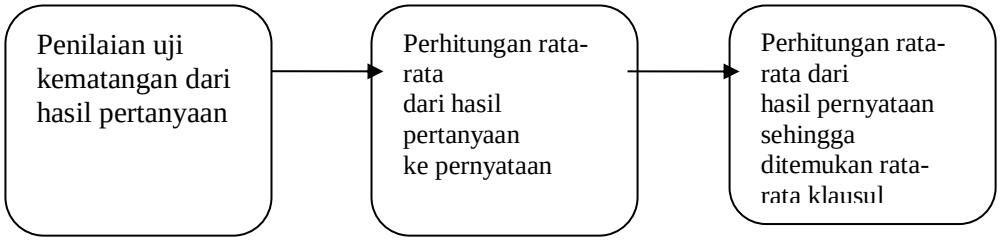
Pada proses ini langkah yang dilakukan adalah melakukan pemeriksaan. Pemeriksaan dilakukan dengan cara melakukan wawancara dan observasi kepada *auditee* sesuai dengan ruang lingkup serta klausul yang telah disepakati oleh PT.GPM. Wawancara dan observasi dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Pada saat observasi berlangsung untuk beberapa kasus dapat dilakukan pengujian baik secara *compliance test* maupun *substantive test*

2.2.3 Melakukan Dokumentasi (Data dan Bukti)

Pada tahap ini langkah yang dilakukan adalah melakukan dokumentasi baik berupa data maupun bukti-bukti atas temuan atau fakta yang ada. Bukti-bukti tersebut dapat berupa foto, rekaman, data atau video.

2.2.4 Melakukan Uji Kematangan

Setelah melakukan pemeriksaan dan mendokumentasikan bukti-bukti audit, maka langkah berikutnya yaitu melakukan perhitungan *maturity level*. Setiap pernyataan dinilai tingkat kepatutannya sesuai dengan hasil pemeriksaan yang ada menggunakan kriteria penilaian yang ada dalam standar penilaian *maturity level*. Tingkat kriteria yang digunakan meliputi non-eksisten yang memiliki nilai 0 (nol) hingga ke tingkat optimal yang memiliki nilai 5 (lima). Jumlah kriteria nilai yang ada dibagi dengan jumlah bobot seluruh pernyataan dalam satu kontrol keamanan untuk mendapatkan nilai maturity level pada kontrol keamanan tersebut.



2.2.5 Penyusunan Daftar Temuan dan Rekomendasi

Pada proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah memeriksa data profil perusahaan, kebijakan, standar, prosedur dan portopolio serta mengobservasi *standard operating procedure*, melakukan wawancara kepada *auditee* hingga melakukan pemeriksaan atau pengujian baik secara *compliance test* maupun *substantive test.* Seluruh aktivitas tersebut menghasilkan bukti *(evidence)* yang berarti terkait dengan sistem yang berlangsung diperusahaan. Masih dibutuhkannya banyak evaluasi dan perbaikan yang harus dijalankan untuk meningkatkan keamanan informasi pada perusahaan, serta menjadi acuan untuk memperoleh ISMS *certification* dengan standar ISO 27002. Ada proses yang telah dilakukan dengan baik, namun terdapat juga beberapa temuan yang masih perlu diperbaiki. Diadakan analisa sebab dan akibat untuk temuan tersebut, serta diberikan rekomendasi untuk perusahaan agar penerapan kontrol keamanan dapat diterapkan dengan lebih baik dan sesuai dengan standar ISO 27002.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Perencanaan dan Persiapan Audit Keamanan 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.

3.1.1 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. Klausul yang digunakan adalah Klausul 7 tentang Keamanan Sumber Daya Manusia, Klausul 9 tentang Akses Kontrol kecuali bagian *teleworking*.Klausul 11 tentang Keamanan Fisisk dan Lingkungan dan Kalusul 12 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. GPM, Klausul 11 kecuali bagian *teleworking*

3.1.2 Hasil Penentuan Metode dan Pembuatan *Engagement Letter*

Pada audit keamanan sistem informasi di PT. Giga Patra Multimedia 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*

ISSN:2442-5567 | E-ISSN:2443-289X

letter yang berisi kesepakatan antara auditor dengan pihak perusahaan dan mengajukan permintaan kebutuhan data. Lampiran *engagement letter* yang telah disetujui oleh PT. Giga Patra Multimedia.

3.1.3 Hasil Penentuan *Auditee*

Sebelum melakukan audit keamanan sistem informasi dilakukan terlebih dahulu menentukan bagian mana di perusahaan yang akan diaudit atau yang disebut *auditee*. Tabel 1. menunjukkan bagian yang akan diwawancara berdasarkan klausul yang telah ditentukan.*Audite*.

Tabel 1. Auditee

KLAUSUL	DESKRIPSI	BAGIAN
7	Sumberdaya manusisa	HRD
9	Kontrol akses	PROGRAMMING
11	Keamanan fisik dan lingkungan	NETWORKING
12	Manajemen Komunikasi dan Operasi	SISTEM INFORMASI

3.1.4 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 penyususnan jadwal audit.

Tabel 2. Penyusunan Jadwal Audit

No	Kegiatan	Bulan Agustus 2015			
		Minggu			
		1	2	3	4
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				

3.1.5 Hasil Pembuatan Pernyataan

Hasil dari proses membuat pernyataan dan pembobotan berupa tabel yangberisi rincian pernyataan yang sesuai dengan standar ISO 27002. Pernyataan yang telah dibuat dapat dilihat pada tabel 3. pernyataan.

Tabel 3. Pernyataan

KLAUSUL	BAGIAN	PERNYATAAN	BOBOT
12	operasi keamanan		
12.1	Prosedur dan tanggung jawab operasional		
12.1.1	Prosedur operasi didokumentasikan	didokumentasikan prosedur operasi untuk mendukung kegiatan operasional yang terkait dengan pengolahan informasi dan komunikasi fasilitas - misalnya komputer start up dan shut down, cadangan, pemeliharaan peralatan dll	0,3

3.1.6 Hasil Pembuatan Pertanyaan dan Pernyataan

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. Pertanyaan dan Tabel Pernyataan

Tabel 4. Pertanyaan dan Tabel Pernyataan

KLAUSUL	BAGIAN	PERNYATAAN	PERTANYAAN
12	operasi keamanan		
12.1	Prosedur dan tanggung jawab operasional		
12.1.1	Prosedur operasi didokumentasikan	dokumentasikan prosedur operasi untuk mendukung kegiatan operasional yang terkait dengan pengolahan informasi dan komunikasi fasilitas - misalnya komputer start up dan shut down, cadangan, pemeliharaan peralatan dll	Apakah ada didokumentasikan prosedur operasi untuk mendukung kegiatan operasional yang terkait dengan pengolahan informasi dan komunikasi fasilitas - misalnya komputer start up dan shut down, cadangan, pemeliharaan peralatan dll?

3.2 Hasil Pelaksanaan Audit Keamanan Sistem Informasi

ISSN:2442-5567 | E-ISSN:2443-289X

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 pada Lampiran4

3.2.1 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 3.5 Wawancara

Tabel 5. Wawancara

KLAUSUL	BAGIAN	PERTANYAAN	JAWABAN
7	Human resources security (Keamanan sumber daya manusia)		
7.1	Sebelum kerja		
7.1.1	Screening	Apakah pemeriksaan verifikasi latar belakang untuk semua calon pekerja, kontraktor, dan pengguna pihak ketiga dilakukan sesuai dengan peraturan yang relevan? Apakah pengecekan meliputi referensi karakter, konfirmasi atas kualifikasi akademik dan profesional	untuk kepala bagian semuanya di seleksi berdasrkan akademik dan prestasi serta pengalaman kerja seblumnya, untuk staff pembantu tidak di seleksi hanya di lihat apakkah mereka mengerti dan paham tentang pekerjaan yang akan mereka kerjakan menurut bidang nya masing masing untuk kontraktor tidak di seleksi berdasrkan akademik,hanya dilihat berdasrkan portofolio pekerjaan yang pernah di kerjakan sebelumnya.
7.1.2	Syarat dan kondisi pekerjaan	Apakah peran keamanan karyawan dan tanggung jawab karyawan, kontraktor dan pengguna pihak ketiga didefinisikan dan didokumentasikan sehubungan dengan kebijakan sekuritas informasi organisasi ? Apakah peran dan tanggung jawab didefinisikan dan dikomunikasikan dengan jelas kepada calon karyawan selama proses pra-kerja ?	Sema tanggung jawab yang menyakngkut keamanan dan tanggung jawab pekerjaan di jelaskan tapi tidak di dokumentasikan secara tertulis.

3.2.2 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. Hasil dari proses pemeriksaan adalah temuan beserta bukti yang dapat dilihat pada Tabel dan selanjutnya dapat dilihat pada Lampiran 4.

3.2.3 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 4 . Hasil perhitungan tingkat kematangan hasil audit keamanan informasi pada PT. Giga Patra Multimedia adalah sebagai berikut.

a. Hasil *Maturity Level* Klausul 7 Keamanan Sumber Daya Manusia

ISSN:2442-5567 | E-ISSN:2443-289X

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

Hasil dari proses perhitungan *maturity level* pada klausul 7 keamanan sumber daya manusia adalah 2,71 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 belum ada seleksi karywaan dengan akademik yang sesuai bidangnya.berikut adalah tabel 6. maturity level klausul 7.

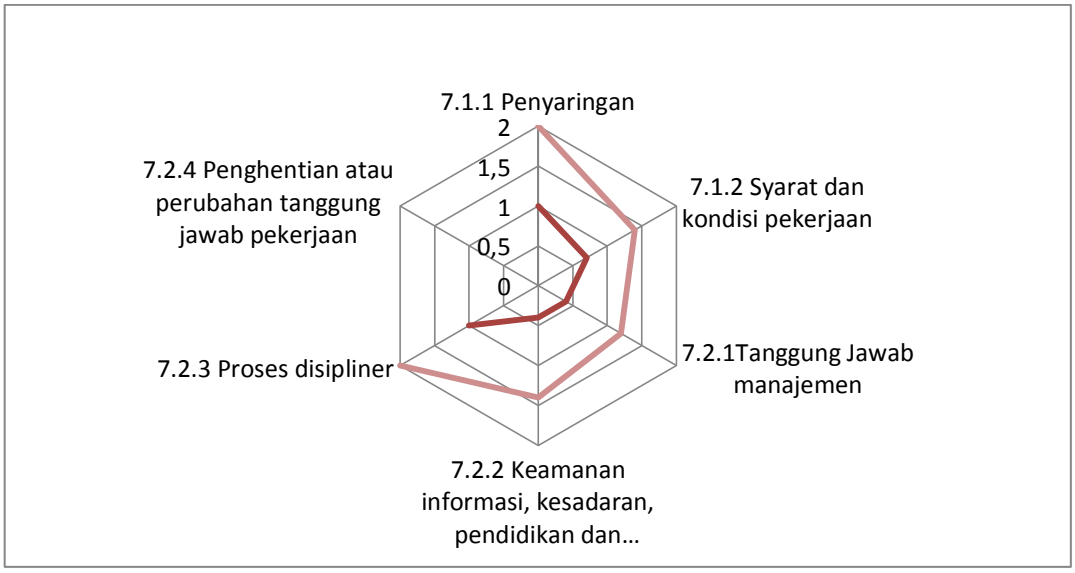
Tabel 6. Maturity Level Klausul 7

TABEL MATURITI LEVEL
KLAUSUL 7 SUMBER DAYA MANUSIA

KLAUSUL	OBJEKTIF KONTROL	KONTROL KEMANAN	BOBOT	NILAI	RATA-RATA OBJEKTIF KONTROL
7	7.1 Sebelum Bekerja	7.1.1 Penyaringan	1	2	
		7.1.2 Syarat dan kondisi pekerjaan	0,7	1,4	
		TOTAL	1,7	3,4	2
	7.2 Selama Bekerja	7.2.1Tanggung Jawab manajemen	0,4	1,2	
		7.2.2 Keamanan informasi, kesadaran, pendidikan dan pelatihan	0,4	1,4	
		7.2.3 Proses disipliner	1	2	
		7.2.4 Penghentian atau perubahan tanggung jawab pekerjaan	1	5	
		TOTAL	2,8	9,6	3,42
		Maturity Level Klausul 7			2,71

keamanan sumber daya manusia dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan *maturity level* klausul 7 keamanan sumber daya manusia dapat dilihat pada grafik *maturity level* klausul.

ISSN:2442-5567 | E-ISSN:2443-289X



b. Hasil *Maturity Level* Klausul 9 Persyaratan Bisnis untuk Kontrol Akses
Hasil dari proses perhitungan *maturity level* pada klausul 9 persyaratan bisnis untuk kontrol akses adalah 1.5 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.

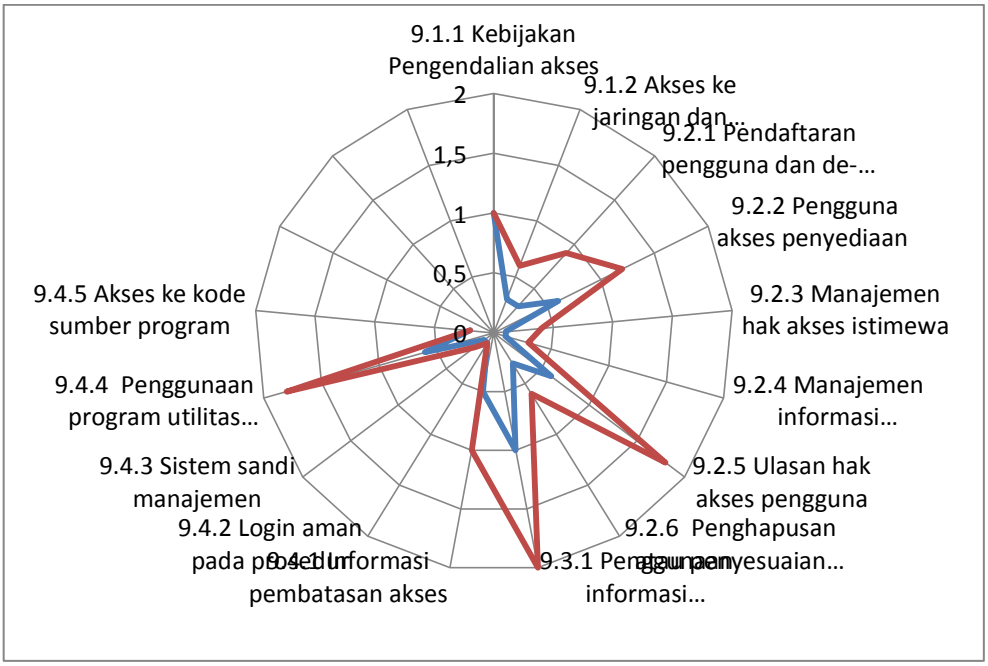
Tabel 7. Maturity Level Klausul 9

TABEL MATURYTI LEVE
KLAUSAL 9 KONTROL AKSES

KLAUSUL	OBJEKTIF KONTROL	KONTROL KEMANAN	Maturity ISO 27002	RATA-RATA OBJEKTIF KONTROL
9	9.1 Kebutuhan bisnis kontrol akses	9.1.1 Kebijakan Pengendalian akses	1	0,8
		9.1.2 Akses ke jaringan dan layanan jaringan	0,6	
	9.2 User access management	9.2.1 Pendaftaran pengguna dan de-registrasi	0,9	
		9.2.2 Pengguna akses penyediaan	1,2	
		9.2.3 Manajemen hak akses istimewa	0,4	
		9.2.4 Manajemen informasi otentikasi rahasia pengguna	0,3	
		9.2.5 Ulasan hak akses pengguna	1,8	
		9.2.6 Penghapusan atau penyesuaian hak akses	0,6	
	9.3 User responsibilities (tanggung jawab pengguna)	9.3.1 Penggunaan informasi otentikasi rahasia	3	3
	9.4 System and application access control	9.4.1 Informasi pembatasan akses	1	0,7
		9.4.2 Login aman pada prosedur	0,1	
		9.4.3 Sistem sandi manajemen	0,2	
		9.4.4 Penggunaan program utilitas istimewa	1,8	
		9.4.5 Akses ke kode sumber program	0,4	
		Maturity Level Klausul 9		**1,5**

Hasil perhitungan *maturity level* pada klausul 9 persyaratan bisnis untuk kontrol akses dapat direpresentasikan dalam bentuk grafik.

Hasil representasi perhitungan *maturity level* klausul 9 persyaratan bisnis untuk kontrol sebagai berikut



c. Hasil *Maturity Level* Klausul 11 Kemanan Fisisk Dan Lingkungan

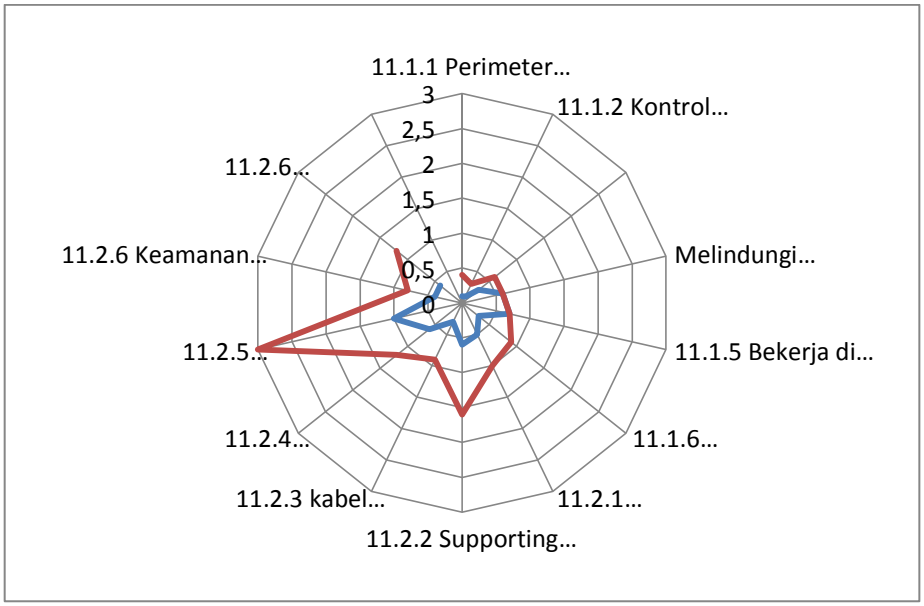
Hasil dari proses perhitungan *maturity level* pada klausul 11 Kemanan Fisisk Dan Lingkungan 2 yaitu *limited/repeatable*. Hasil tersebut menunjukkan proses keamanan wilayah yang ada masih dalam pengembangan dan ada dokumentasi terbatas. Hal tersebut dapat dilihat dengan adanya beberapa prosedur yang 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 8. *maturity* level klausul 11.

Tabel 8. Maturity level klausul 11

TABEL MATURYTI LEVE
KLAUSAL 11 KEAMANA FISIK DAN LINGKUNGAN

KLAUSUL	OBJEKTIF KONTROL	KONTROL KEMANAN	BOBOT	NILAI	RATA RATA OBJEKTIF KONTROL
11	11.1 Daerah aman	11.1.1 Perimeter keamanan fisik	0,1	0,4	
		11.1.2 Kontrol entri fisik	0,1	0,3	
		11.1.3 Tanggung Jawab manajemen Mengamankan kantor, dan fasilitas ruangan	0,3	0,6	
		11.1.4 Melindungi terhadap ancaman eksternal dan lingkungan	0,6	0,6	
		11.1.5 Bekerja di Daerah Aman	0,7	0,7	
		11.1.6 Pengiriman dan pemuatan daerah	0,3	0,9	
		TOTAL	2	3,5	1,75
	11.2 Peralatan	11.2.1 Pemeliharaan peralatan	0,5	1	
		11.2.2 Supporting utilities	0,6	1,2	
		11.2.3 kabel Keamanan	0,3	0,9	
		11.2.4 pemeliharaan peralatan	0,6	1,2	
		11.2.5 Penghapusan aset	1	3	
		11.2.6 Keamanan Peralatan dan Aset off-Tempat	0,4	0,8	
		11.2.6 Pembuangan aman atau penggunaan kembali peralatan	0,4	1,2	
		TOTAL	3,8	9,3	2,44
		Maturity Level Klausul 11			2

ISSN:2442-5567 | E-ISSN:2443-289X



1. Hasil *Maturity Level* Klausul 12 Manajemen Komunikasi dan Operasi

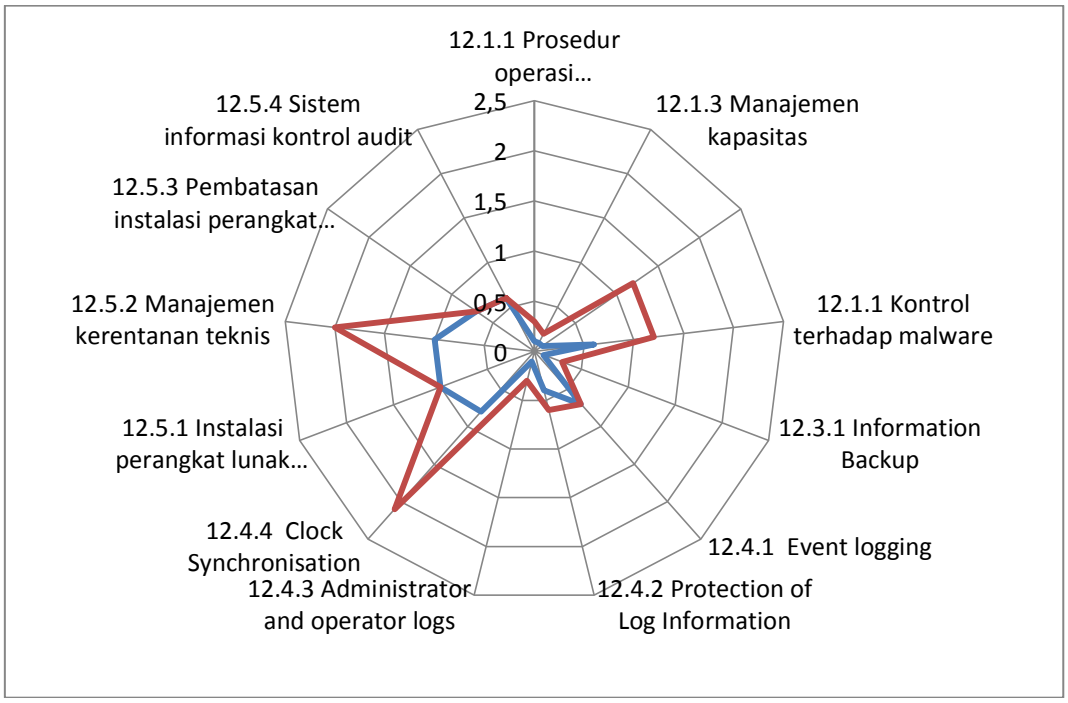
Hasil dari proses perhitungan *maturity level* pada klausul 12 manajemen komunikasi dan operasi adalah 2 (*limited/repeatable*): Pada level ini, kontrol keamanan masih dalam pengembangan dan/atau ada dokumentasi terbatas untuk mendukung kebutuhan. Hal tersebut dapat dilihat dengan adanya beberapa prosedur yang belum terdokumentasi dan masih banyak kontrol yang masih dalam pengembangan atau tahap penyusunan pemisahan sistem,contohnya seperti *back-up* di luar lokasi organisasi, pencatatan informasi, kontrol audit *trail*, dll.

Tabel 9. maturity level klausul 12

TABEL MATURITI LEVEL
KLAUSUL 12

KLAUSUL	OBJEKTIF KONTROL	KONTROL KEMANAN	BOBOT	NILAI	RATA-RATA OBJEKTIF KONTROL
12	12.1 perubahan manajemen	12.1.1 Prosedur operasi didokumentasikan	0,1	0,3	
		TOTAL	0,1	0,3	3
	12.1.4 Perubagan manajemen	12.1.3 Manajemen kapasitas	0,1	0,2	
		12.1.4 Pemisahan pengembangan, pengujian dan lingkungan	0,6	1,2	
		TOTAL	**0,7**	**1,4**	**2**
	12.2 Kontrol terhadap malware	12.1.1 Kontrol terhadap malware	0,6	1,2	
		TOTAL	**0,6**	**1,2**	**2**
	12.3 Bakup	12.3.1 Information Backup	0,1	0,3	
		TOTAL	**0,1**	**0,3**	**3**
	12.4 Logging and monitoring	12.4.1 Event logging	0,7	0,7	
		12.4.2 Protection of Log Information	0,4	0,6	
		12.4.3 Administrator and operator logs	0,1	0,3	
		12.4.4 Clock Synchronisation	0,8	2,1	
		TOTAL	**2**	**3,7**	**1,85**
	12.5 Control of operational software	12.5.1 Instalasi perangkat lunak pada sistem operasional	1	1	
		12.5.2 Manajemen kerentanan teknis	1	2	
		12.5.3 Pembatasan instalasi perangkat lunak	0,7	0,7	
		12.5.4 Sistem informasi kontrol audit	0,6	0,6	
		TOTAL	**3,3**	**4,3**	**1,33**
		Maturity Level Klausul 12			**2**

Hasil perhitungan *maturity level* pada klausul 12 manajemen komunikasi dan operasi dapat direpresentasikan dalam bentuk grafik.



4. KESIMPULAN DAN SARAN

4.1 KESIMPULAN

Dari hasil audit keamanan sistem informasi yang telah dilakukan, maka didapatkan kesimpulan sebagai berikut:

1. Perancangan audit keamanan sistem informasi pada PT. GIGA PATRA MULTIMEDIA berdasarkan standar ISO 27002 yang dilakukan pada Klausul 7 hingga Klausul 12, pengumpulan data, dam langkah-langkah pelaksanaan audit hingga pelaporan hasil audit keamanan sistem informasi telah berhasil dilakukan.
2. Hasil audit keamanan informasi pada PT. GIGA PATRA MULTIMEDIA pada bidang Keamanan Sumber Daya Manusia (Klausul 7) menghasilkan nilai *maturity level* 2.71 dan pada bidang Kontrol Akses (Klausul 9) memiliki nilai *maturity level* 2,75 dan bidang Keamanan Fisik dan Lingkungan (Klausul 11) kemanan sumber daya manuia menghasilkan nilai *maturity level* 2.75 yaitu berada pada level 2 (limited/*repeatable*) yang berarti kontrol keamanan sedang dalam pengembangan, sudah ada dokumentasi terbatas tetapi belum ada pelatihan dan pengukuran efektifitas kontrol keamanan, dan bidang oprasional (Klausul 12) menghasilkan nila*i maturity level* 1,33 yaitu berada pada level Level 2 (*limited/repeatable*) Pada level ini, kontrol keamanan masih dalam pengembangan dan/atau ada dokumentasi terbatas untuk mendukung kebutuhan.
3. Berdasarkan temuan-temuan dari hasil audit keamanan sistem informasi berdasarkan standar ISO 27002 pada PT. GIGA PATRA MULTIMEDIA terdapat beberapa kelemahan-kelemahan aturan dan prosedur keamanan sistem informasi mengakibatkan PT. GIGA PATRA MULTIMEDIA rentan terhadap ancaman keamaman informasi yang dapat menyebabkan timbulnya resiko-resiko, antara lain: penyalah gunaan informasi, kekacauan pada internal perusahaan, dan hilangnya data perusahaan yang akan merugikan PT. GIGA PATRA MULTIMEDIA sendiri.

ISSN:2442-5567 | E-ISSN:2443-289X

4. Belum adanya pencatatan mengenai insiden kelemahan keamanan informasi yang disebabkan karena tidak terdapat kebijakan, prosedur maupun aturan untuk menanggulangi insiden kelemahan sistem informasi

4.2 SARAN

Saran yang dapat diberikan bagi pengembangan yang berkaitan dengan pencapaian hasil yang optimal dari audit keamanan sistem sistem informasi ini sebagai berikut:

1. Diharapkan PT. GIGA PATRA MULTIMEDIA dapat melakukan perbaikan manajemen keamanan sistem informasi, aturan, dan prosedur keamanan sistem informasi agar ancaman-ancaman terkait keamanan informasi dapat diminimalisir.
2. Diharapkan bagi pengembang dapat melakukan tata kelola keamanan sistem informasi dan audit keamanan sistem informasi kembali dengan menggunakan keseluruhan klausul dan kontrol keamanan ISO 27002 setelah pihak perusahaan melakukan perbaikan keamanan informasinya.
3. PT. GIGA PATRA MULTIMEDIA dapat melakukan Audit Keamanan Sistem Informasi secara berkala selama 6 bulan atau 1 tahun sekali agar keamanan sistem informasi tetap terkontrol audit dapat dilakukan oleh penanggung jawab Instalasi PT. GIGA PATRA MULTIMEDIA demi meningkatkan keamanan sistem
4. Diharapkan pengembang dapat merancang tata kelola TI pada PT. GIGA PATRA MULTIMEDIA dengan berdasarkan laporan audit yang telah dihasilkan.

REFERENSI

[1] Direktorat Keamanan Informasi. 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*. Jakarta: Kominfo.

[2] Gondodiyoto, S. 2007. *Audit Sistem Informasi Pendekatan COBIT*. Jakarta: Mitra Wacana Media.

[3] Information Technology Governance Institute. 2007. *COBIT 4.10: Control Objective, Management Guidelines, Maturity Models*. United States of America: IT Governance Institute.

[4] ISACA. 2010. *Guide to the Audit of IT Application*. Switzerland : Felice Lutz.

[5] ISO/IEC. 2005. *Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005*. Switzerland.

[6] ISO/IEC. 2005. *Information Technology-Security Techniques-Information Security Management System ISO/IEC 27001:2005*. Switzerland.

[7] *Information technology – Security techniques – Information security management systems* – Requirement. BS ISO/ IEC 27001:2005 BS 7799-2:2005

[8] Ferdinand Aruan (2003), Tugas Keamanan Jaringan Informasi (Dosen. Dr. Budi Rahardjo) Tinjauan Terhadap ISO 17799 - Program Magister Teknik Elektro Bidang Khusus Teknologi Informasi ITB Indocommit (23 Desember 2005), Kepatuhan terhadap Sistem Keamanan Informasi http://www.indocommit.com/index.html?menu=29&idnews=1506&kid=0&PHPSESSID=ac0fa9bf4b764ea21e26b230102b4ecb,

[9] Jacquelin Bisson, CISSP (Analis Keamanan Informasi, Callio Technologies) & René Saint-Germain (Direktur Utama, Callio Technologies), Mengimplementasi kebijakan keamanan dengan standar BS7799 /ISO17799 untuk pendekatan terhadap

ISSN:2442-5567 | E-ISSN:2443-289X

informasi keamanan yang lebih baik, White Paper, http://202.57.1.181/~download/linux_ opensource/artikel+tutorial/ general_tutorials/wp_iso_id.pdf