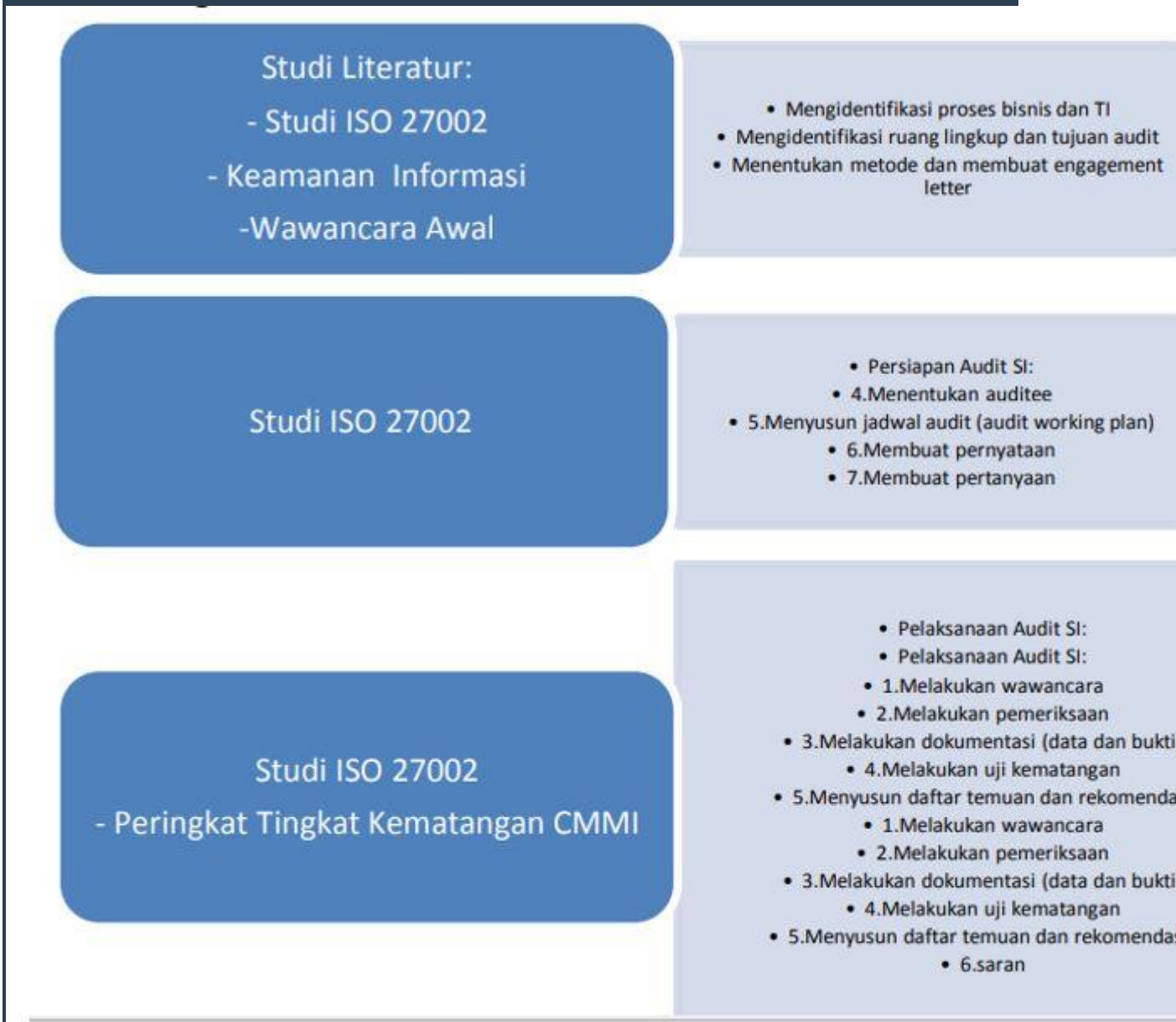
JURNAL: AUDIT KEMANAN INFORMASI MENGGUNAKAN ISO 27002 PADA DATA CENTER PT.GIGIPATRA MULTIMEDIA

PT. Giga Patra Multimedia yang merupakan perusahaan swasta yang beroperasi dalam lingkup internet service provider, penjualan hosting, dan pengadaan perlengkapan dan peralatan pendukung teknologi telah mengelami sejumlah masalah seperti ditemukannya kebocoran informasi dan hacking terhadap website pelanggan yang berada di web server. 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. Oleh karena itu diperlukan audit internal dengan menggunakan standar keamaan informasi ISO 27002:2013 untuk mengetahui kelemahan-kelemahan sistem yang menjadi penyebab permasalah keamaan informasi yang telah terjadi selama ini.

Metodologi Penelitian



Berdasarkan hasil observasi maka ditetapkan ruang lingkup audit keamaan sistem informasi dan standar yang digunakan adalah ISO 27002. Klausal 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
- Klausal 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).

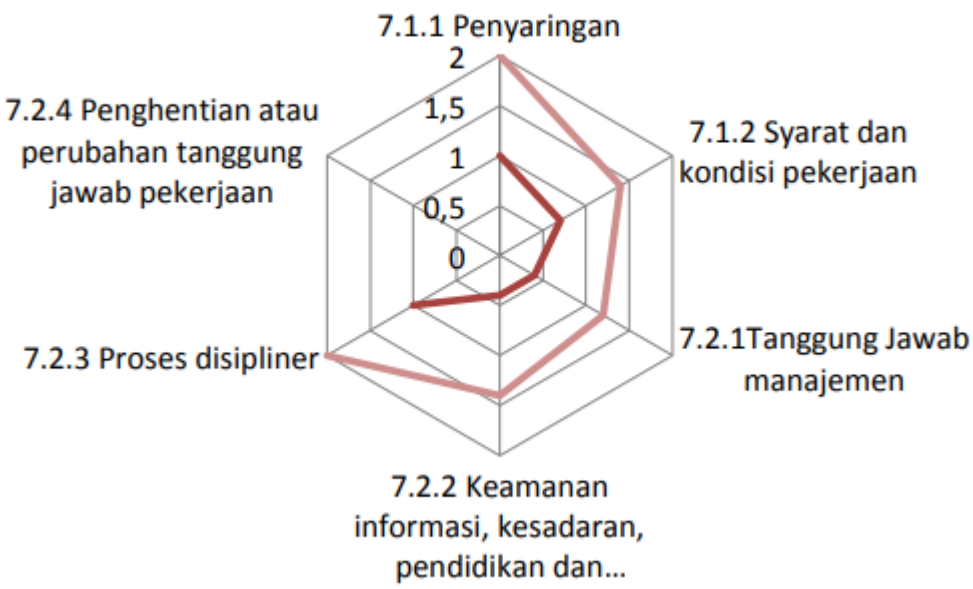
Tabel auditee yang menunjukkan bagian yang akan diwawancara berdasarkan klausal yang telah ditetapkan.

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

Hasil Uji Maturity Level

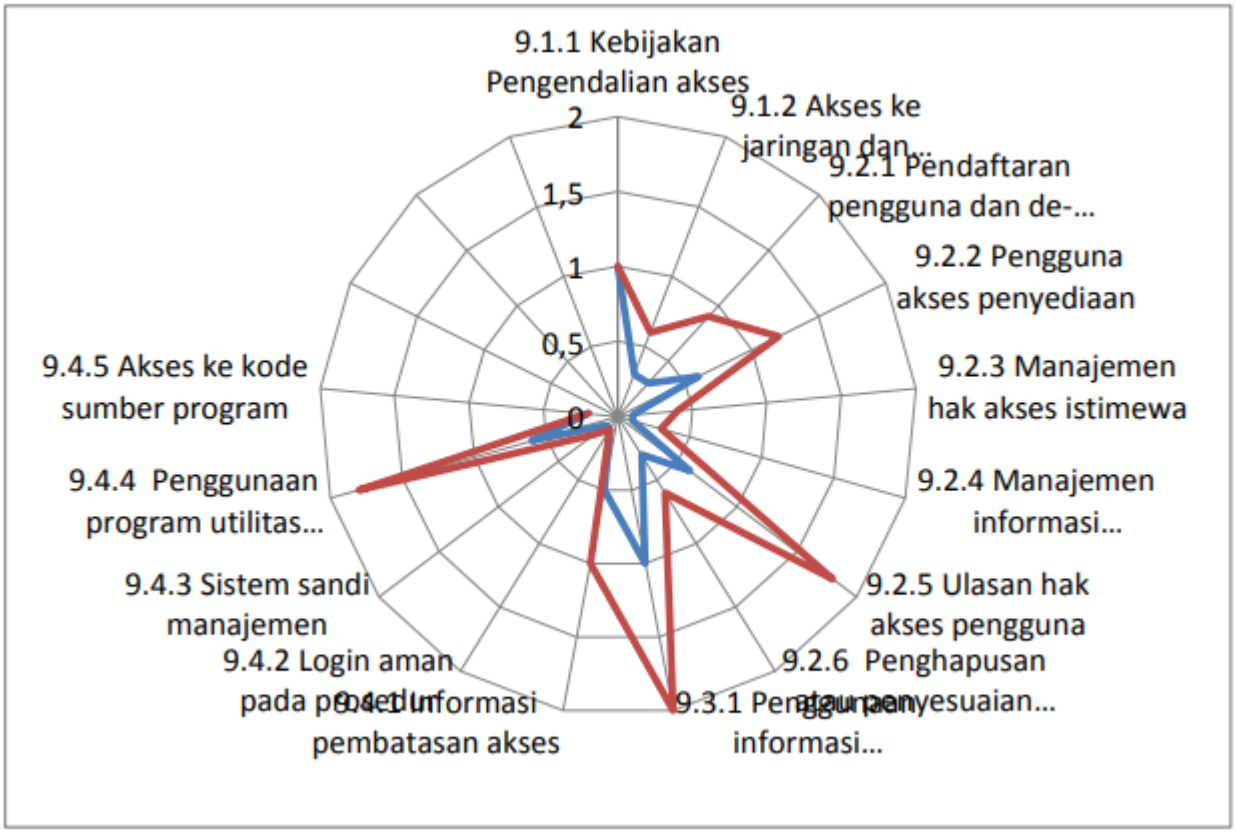
1. **Klausal 7: Keamanan Sumber Daya Manusia**

Nilai maturity level untuk klausal 7 adalah 2,71 (terbatas/dapat diulang). Oleh karena itu, level ini masih berada pada tahap pengembangan dan dokumentasi yang terbatas, yang berarti masih tedapat sejumlah prosedur yang belum didokumentasikan serta berbagai kontol yang belum dilakukan.



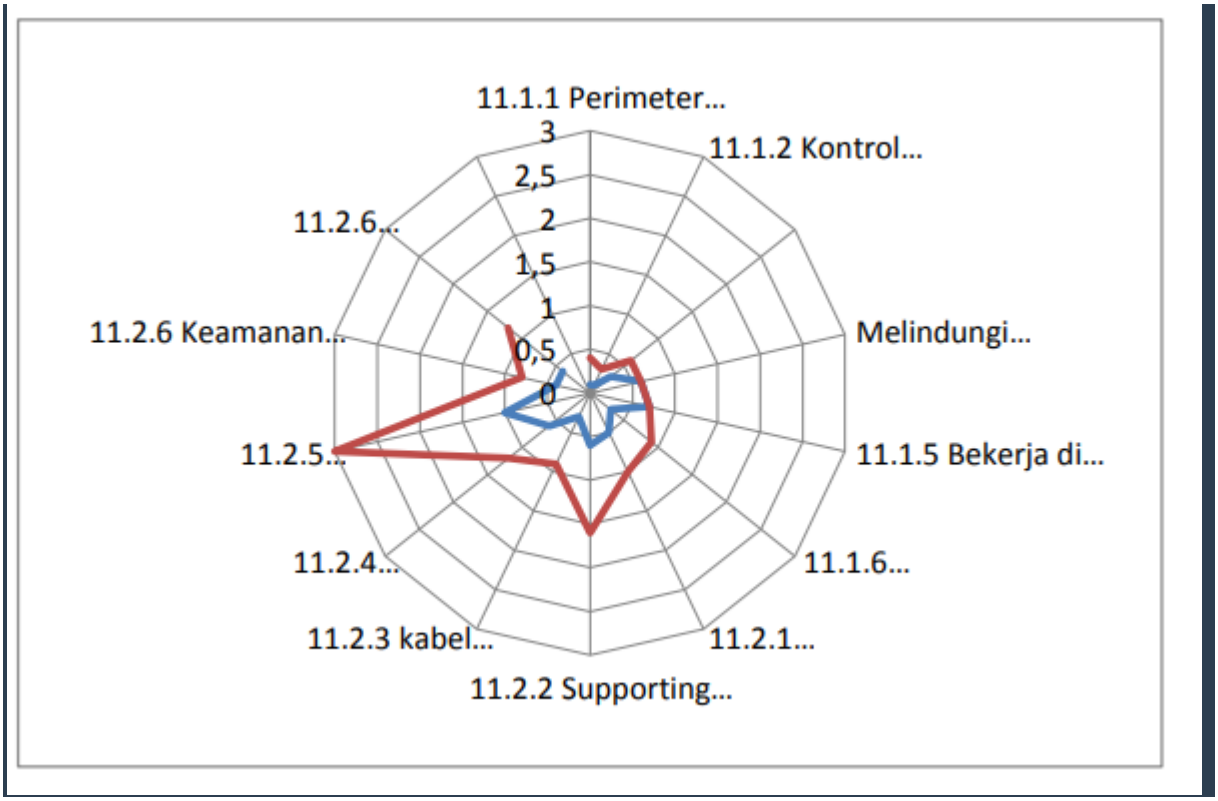
2. Klusal 9: Persyaratan Bisnis dan Kebijakan Pengendalian Akses

Nilai maturity level klausal 9 adalah 1.5 yaitu initial. Berarti bahwa persyaratan bisnis untuk kotrok akses dilakukan secara tidak konsisten dan informal karena tida terdapat pernyataan resmi dalam hal penjagaan password, tinjauan hak akses user, otorisasi keamanan informasi, dll.



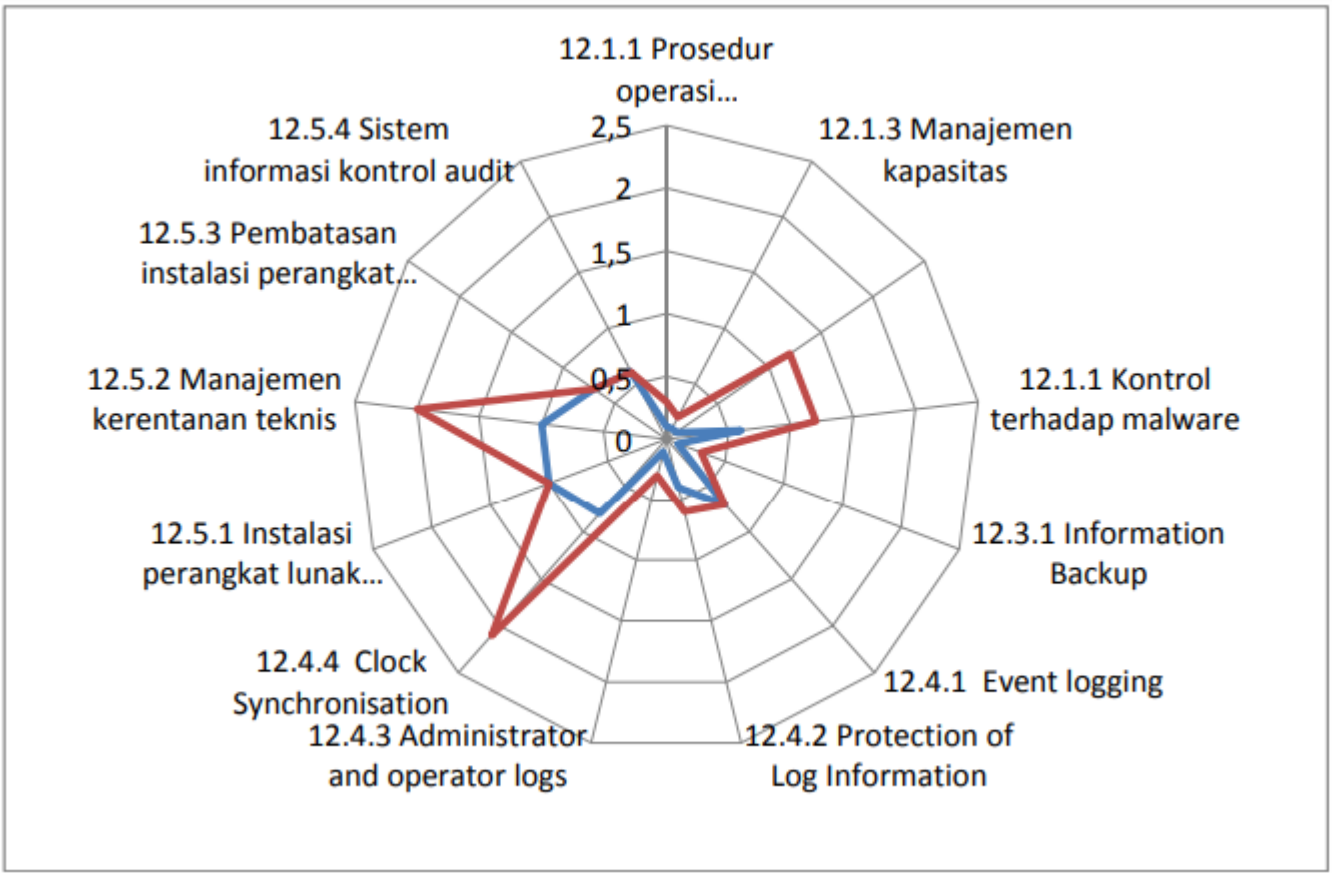
3. Klausal 11: Keamanan Fisik dan Lingkungan

Nilai maturity level untu klausal 11 adalah 2 (terbatas/dapat diulang), proses keamanan wilayah berada dalam tahap pengembangan dan dokumentasi yang terbatas. Hal ini disebabkan karena terdapat sejumlah prosedur yang belum terdokumentasikan, serta sejumlah kontrol yang belum dilakukan seperti pemasangan tanda bahaya, log pengunjung, catatan peminjaman peralatan, dan maintenance peralatan.



4. Klausal 12: Manajemen Komunikasi dan Operasi

Nilai dari maturity level pada klausal 12 adalah 2 (terbatas/dapat diulang), sehingga kontrol keamanan yang masih pada level pengembangan serta dokumntasi yang terbatas untuk mendukung kebutuhan. Hal ini sidebabkan oleh beberapa prosedur yang belum terdokumentasikan dan masih dalam tahap penyusunan pemisahan sistem seperti.



KESIMPULAN

Hasil audit keamanan informasi yang dilakukan pada PT. GIGA PATRA MULTIMEDIA karena banyak terjadinya masalah yang mennyangkut keamanan informasi selama perusahaan berdiri dengan menggunakan standar ISO 27002:2013. Niai maturity level dari klausal yang dipilih yaitu klausal 7 (sumber daya manusia) adalah 2.71, klausal 9 (kontrol akses) adalah 2.75, klausal 11 (keamanan fisik dan lingkungan) adalah 2.75, dan klausal 12 (manajemen komunikasi dan operasi) adalah 1.33. keseluruhan klausal berdiri pada level 2 yaitu (terbatas/dapat diulang) yang berarti kontrol keamanan masih terdapat pada tahapan pengembangan dan dibutuhkan dokumentasi untuk mendukung kebutuhan karena masih terbatas atau kurangnya peelatihan pengukuran efektifitas kontrol keamanan. Hal signifikan yang menyebabkan risiko-risiko seperti penyalahgunaan informasi, inkonsistensi internal perusahaan, ataupun kehilangan data adalah karena belum adanya kebijakan, prosedur dan aturan yang digunakan untuk menangani kelemahan sistem informasi secara tertulis.

REFERENSI:

Afandi, Herman dan Darmawan, Abdi. 2015. Audit Kemanan Informasi Menggunakan ISO 27002 Pada Data Center PT .Gigipatra Multimedia. Jurnal TIM Darmajaya. https://jurnal.darmajaya.ac.id/index.php/jtim/article/viewFile/638/422 (Diakses pada 20 November 2018)

https://en.wikipedia.org/wiki/ISO/IEC_27002 (Diakses pada 20 November 2018)

http://www.iso27001security.com/html/27002.html (Diakses pada 20 November 2018)

https://www.iso.org/standard/54533.html (Diakses pada 20 November 2018)

https://ostec.blog/en/general/iso-27002-best-practices-ism (Diakses pada 20 November 2018)