AUDIT KEAMANAN SISTEM INFORMASI PADA RS MATA DR.YAP YOGYAKARTA MENGGUNAKAN *FRAMEWORK COBIT 5*

Oleh:
Rifki Dimas Krisdiyawan, RB.Hendri Kuswantoro
Sekolah Tinggi Multi Media Yogyakarta
rifkidimas11@gmail.com, rbhendrikuswantoro@gmail.com

ABSTRAK

Rumah Sakit Mata "Dr.YAP" Yogyakarta merupakan instansi yang memanfaatkan sistem informasi manajemen rumah sakit sangat memerlukan perlindungan keamanan terhadap data pasien yang ada dalam sistem informasi. Penelitian ini bertujuan untuk mengukur tingkat keamanan sistem informasi berdasarkan penerapan *Framework* COBIT 5 pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta. Metode penelitian deskriptif kualitatif digunakan dalam penelitian ini dengan pengambilan data melalui wawancara, observasi, dan kuesioner serta teknik analisis data menggunakan *capability level* pada COBIT 5 Framework pada domain *Align, Plan, Organize* (APO13) dan *Delivery, Service, Support* (DSS 05). Hasil penelitian menunjukkan bahwa pengelolaan keamanan pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta sudah hampir memenuhi keseluruhan aspek dalam domain APO 13 (*Manage Security)* dan DSS 05 (*Manage Security Services)* COBIT 5 *Framework* dibuktikan dengan tingkat kapabilitas yang dicapai pada domain APO 13 yaitu 2,59 berada pada level 3 *(Esteblished Process)* yang menunjukan bahwa pengelolaan keamanan sistem informasi telah dikelola dengan baik dan masih terus dikembangkan agar semakin mapan. Sedangkan pada domain DSS 05 mencapai angka 3,09 berada pada level 3 *(Established Process)*. Pengelolaan layanan keamanan sistem informasi telah dikelola dengan baik dan masih terus dikembangkan agar semakin mapan.

Kata Kunci : Audit Keamanan, Sistem Informasi, COBIT 5

ABSTRACT

"Dr. YAP" Yogyakarta Eye Hospital is an institution that utilizes hospital management information system therefore it needs security protection of the patients' data in the information system. This study aims to measure the level of information system security based on the application of Framework COBIT 5 on the Management Information System of "Dr. YAP" Yogyakarta Eye Hospital. Qualitative descriptive research method used in this research by taking data through interview, observation, and questionnaires and data analysis techniques using capability level on COBIT 5 Framework in Align, Plan, Organize (APO13) and Delivery, Service, Support (DSS 05) domains. The results shows that the management of security in the "Dr.YAP" Yogyakarta Eye Hospital Management Information System has almost fulfilled all aspects in the domain of APO 13 (Manage Security) and DSS 05 (Manage Security Services) COBIT 5 Framework evidenced by the level of capability achieved on APO 13 domain is 2.59 is at level 3 (Established Process) which shows that the management of information system security has been well managed and is still being developed to be more established. While the domain DSS 05 reaches the number 3.09 is at level 3 (Established Process). Management of information system security services in "Dr. YAP" Yogyakarta Eye Hospital has been well managed and is still being developed to be more established.

Keywords: *Security Audit, Information System, COBIT 5*

PENDAHULUAN

Perkembangan teknologi dan sistem informasi yang semakin pesat berdampak pada risiko keamanan yang melekat pada informasi juga semakin besar. Seperti yang terjadi pada kasus serangan *malware Ransomware Wannacrypt* yang mengunci data dalam sistem informasi rumah sakit kanker Dharmais di Jakarta sehingga tidak dapat diakses oleh pihak rumah sakit. Rumah Sakit Mata "Dr. YAP" Yogyakarta yang merupakan rumah sakit khusus mata memanfaatkan sistem informasi rumah sakit guna memberikan kemudahan dalam pelayanan informasi di bidang kesehatan.

Upaya pencegahan diperlukan oleh Rumah Sakit Mata "Dr.YAP" Yogyakarta untuk melindungi aset informasi seperti data pasien yang ada di dalam sistem informasi sebagai mana diatur dalam pasal 32 Undang-Undang Nomor 44 Tahun 2009 Tentang Rumah Sakit. Oleh karena itu perlu adanya audit untuk mengetahui tingkat keamanan dari sistem informasi tersebut. Diperlukan suatu *framework* yang digunakan untuk membantu mengetahui tingkat keamanan sistem informasi manajemen RS Mata "Dr.YAP" Yogyakarta seperti COBIT 5 yang direkomendasikan dalam Permenkes Nomor 82 Tahun 2013.

COBIT merupakan Kerangka Kerja TI yang mendukung proses audit dan tata kelola TI untuk menjembatani kesenjangan antara resiko TI, sumber daya TI dan masalah masalah teknik TI di suatu organisasi atau lembaga dan juga merupakan standar international yang digunakan dalam melakukan Audit Sistem Informasi yang dikeluarkan oleh ISACA (*Information System Control and Audit*). Cobit versi terbaru adalah COBIT 5, dikeluarkan oleh ISACA pada tahun 2012, dan menyediakan kerangka kerja yang lengkap. Penelitian ini bertujuan untuk mengetahui tingkat keamanan sistem informasi berdasarkan penerapan *Framework* COBIT 5 pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr. YAP" Yogyakarta melalui level kapabilitas keamanan sistem informasi serta terbatas dalam lingkup domain APO13 dan DSS05 *Framework* Cobit 5.

TINJAUAN PUSTAKA

1. Audit Keamanan Sistem Informasi

a. Audit

Kegiatan mengumpulkan informasi secara sistematis, obyektif dan terdokumentasi untuk mendapatkan kesimpulan yang berasaskan nilai dan manfaat adalah kegiatan audit." Susilo (2003: 80).

b. Audit Sistem Informasi

c. Audit Sistem infromasi adalah Proses pengumpulan dan evaluasi sebuah sistem informasi dan teknologi informasi untuk mengetahui apakah sudah sejalan dengan tujuan dari ognasisasi dan digunakan secara efektif dn efisien (Weber, 2000).

Langkah – langkah dalam audit sistem informasi (Rochaety, 2013: 188) terdiri dari :

1) Perencanaan pemeriksaan
2) Pemeriksaan Rinci
3) Pengujian Kesesuaian
4) Pengujian Kebenaran Bukti
5) Penilaian Secara Umum Atas Hasil Pengujian

d. Keamanan Sistem Informasi

Keamanan sistem informasi berkaitan erat dengan aspek keamanan informasi yaitu *confidentiality, integrity, dan availability* (ISO/IEC 27002, 2005). "Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi suatu organisasi baik berupa organisasi komersial (perusahaan), perguruan tinggi, maupun lembaga

pemerintahan dan individual" (Riyanarto Sarno & Irsyat Iffano, 2009;35).

2. COBIT 5 *Framework*

COBIT 5 adalah panduan terbaru yang dikeluarkan oleh ISACA untuk membantu pengelola teknologi informasi mengaudit teknologi informasi yang sudah diimplementasikan. Di dalam COBIT 5 terdapat kerangka kerja sebagai alat ukur untuk memantau kinerja teknologi informasi. melalui 5 domain di dalamnya (ISACA,2012) yakni EDM (*Evaluate, Direct and Monitor*), APO (*Align, Plan and Organize*), BAI (*Build, Acquire and Implement*), MEA (*Monitor, Evaluate and Assess*), dan DSS (*Deliver, Service and Support*).

***Process Capability* Level COBIT 5**

Menurut ISACA (2012) ada enam tingkat kemampuan yang dapat dicapai oleh masing-masing proses, yaitu :

Tabel . *Capability Level* COBIT 5 *Framework*

Level	Indeks Kemdangan	Keterangan
0 : Incomplete Process	0 - 0,49	Pada level ini, proses tidak lengkap dan menunjukan tidak tercapainya tujuan yang diinginkan.
1 : Performed Process	0,50 – 1,49	Pada level ini, proses telah dijalankan untuk mencapai tujuan
2 : Managed Process	1,50 – 2,49	Pada level ini, proses yang telah dijalankan, ditetapkan untuk dikelola dengan baik
3 : Established Process	2,50 – 3,49	Pada level ini, proses yang telah dikelola, dibangun menjadi semakin mapan
4 : Predictable Process	3,50 – 4,49	Pada level ini, proses yang telah mapan, kemudian dioperasikan untuk mencapai hasil akhir sesuai dengan yang diprediksi
5 : Optimizing Process	4,50 – 5,00	Pada level ini, dilakukan optimasi pada proses yang sudah ada agar menjadi lengkap dan sempurna

KERANGKA PIKIR

Gambar 1. Kerangka Pikir

Kerangka pikir pada Gambar 1 menunjukkan bahwa audit keamanan sistem informasi dilakukan memenuhi aspek keamanan informasi yaitu *Confidentiality, Integrity, Availability* pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta menggunakan *framework* COBIT 5 berdasarkan pada domain APO 13 *Manage security* dan DSS 05 *Manage Security Services*. Audit dilakukan dengan menganalisis dan mengukur proses pada domain APO 13 dan DSS 05 melalui tingkat kapabilitas COBIT 5 yang dicapai sehingga mendapatkan sebuah kesimpulan dan rekomendasi.

METODE PENELITIAN

Penelitian ini dilakukan di Rumah Sakit Mata "Dr.YAP" Yogyakarta pada unit Instalasi Pemeliharaan Sarana dan Prasarana dengan menggunakan domain APO13 (*Manage Security)* dan DSS05 (*Manage Security Services*) COBIT 5. Penelitian ini menggunakan penelitian kualitatif yang bertujuan untuk memahami situasi melalui interaksi melalui Interview secara mendalam. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah wawancara, observasi, dan kuesioner.

Wawancara dilakukan untuk memperoleh informasi atau penjelasan yang terkait dengan Keamanan Sistem Informasi RS Mata "Dr.YAP" Yogyakarta melalui Informan yaitu Penanggung Jawab Teknologi Informasi pada Unit Instalasi Pemeliharaan Sarana dan Prasarana RS Mata "Dr.YAP" Yogyakarta. Informasi-informasi tersebut akan diukur menggunakan domain APO13 dan DSS05 Framework Cobit 5. Pengisian kuesioner dilakukan dengan cara memberikan sekumpulan pertanyaan kepada responden guna mendapatkan data tambahan untuk mengetahui tingkat kapabilitas pada *Framework COBIT 5* menggunakan metode statistika deskriptif. Proses analisis data menggunakan metode analisis data model Miles dan Huberman dalam Sugiyono (2011:246) yakni reduksi data, penyajian data dan penarikan kesimpulan. Agar data yang diperoleh dapat diyakini kebenarannya maka teknik triangulasi dilakukan melalui pengecekan data kepada sumber yang sama dengan teknik yang berbeda" (Sugiyono, 2011).

HASIL PENELITIAN

1. *Align, Plan, Organize* (APO 13)

Tabel 1. Hasil Observasi Domain APO 13

APO 013	*Manage Security* (Mengelola Keamanan)	Ada	Tidak
APO 013.01	Mengelola Sistem Manajemen Keamanan Informasi.	✓	
APO 013.02	Mengelola Manajemen resiko keamanan Informasi		✓
APO 013.03	Memantau dan meninjau kembali Sistem Manajemen Keamanan Informasi	✓	

Pengelolaan Sistem Manajemen Keamanan Informasi pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta dilakukan menggunakan pedoman dalam standar akreditasi rumah sakit pada kelompok kerja Manajemen Komunikasi Informasi (MKI) yang terdiri dari beberapa aspek pengelolaan kelompok komunikasi dan Informasi. MKI terdiri dari beberpa elemen penilaian standar berupa dokumen yang harus dipenuhi oleh pihak pengelola IT dalam mengelola keamanan data pasien pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta.

Manajemen Resiko dilakukan untuk mengelola resiko terhadap keamanan data dan Informasi dalam Sistem Informasi Manajemen Rumah Sakit. Namun pihak pengelola belum menerapkan manajemen resiko untuk meminimalisir kejadian yang dapat mengancam keamanan data dan informasi pada Sistem Informasi Manajemen Rumah Sakit. Manajemen Resiko yang diterapkan oleh pengelola Sistem Informasi Manajemen Rumah Sakit meliputi resiko keselamatan kerja seperti melakukan register terhadap resiko kerja unit IT yang kemudian akan di monitor dan dianalisis tindak lanjut dari resiko IT tersebut serta pedoman ICRA (*Infection Control Risk Assesment*) saat akan membangun perangkat IT baru. Peninjauan kembali terhadap sistem manajemen keamanan informasi dilakukan oleh pengelola Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" secara berkala setiap 1 kali dalam 1 bulan terhadap pedoman dalam MKI. Pihak pengelola juga melakukan peninjauan kembali terhadap kebijakan Teknologi Informasi secara periodik yaitu setiap sekali dalam 1 tahun.

2. *Delivery Service Support* (DSS 05)

Tabel 3. Hasil Observasi Domain DSS 05

DSS 05	Manage security services (Mengelola pelayanan keamanan)	Ada	Tidak
DSS 05. 01	Melindungi Terhadap Malware	✓	
DSS 05. 02	Mengelola Jaringan dan Keamanan Konektivitas	✓	
DSS 05. 03	Mengelola Keamanan End point	✓	
DSS 05. 04	Mengelola Identitas Pengguna dan Akses Logis	✓	
DSS 05. 05	Mengelola Akses Fisik ke Aset TI	✓	
DSS 05. 06	Mengelola Dokumen Sensitif dan Perangkat Output	✓	
DSS 05. 07	Memantau infrastruktur untuk keamanan	✓	

Menjaga keamanan informasi merupakan hal yang sangat penting dalam membangun dan mengelola sebuah sistem informasi rumah sakit karena dalam sebuah sistem informasi rumah sakit terdapat aset informasi yang sangat sensitif seperti data pasien yang wajib untuk diamankan melalui pengelolaan pelayanan keamanan dalam Sistem Informasi Manajemen Rumah Sakit. Perlindungan terhadap malware dilakukan pada tingkat server melalui jaringan router (mikrotik) yang secara otomatis akan memblok *malware* yang mungkin menyerang server. Pada level perangkat komputer dilakukan perlindungan terhadap virus melalui SOP pemasangan antivirus pada setiap perangkat komputer baik yang sudah terpasang aplikasi Sistem Informasi Manajemen Rumah Sakit maupun belum.

Pengelolaan jaringan konektivitas dilakukan dengan sangat baik melalui melalui *firewall* dalam hal sharing data dan melalui *router* (mikrotik) yang dapat memblok otomatis serangan terhadap jaringan koneksi yang dipantau secara periodik 1 bulan sekali untuk 1 komputer. Pengelolaan keamanan *end point* pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta dilakukan melalui antisipasi virus menggunakan antivirus pada setiap perangkat yang mengakses aplikasi Sistem Informasi Manajemen Rumah Sakit dan pemakaian *firewall* guna *sharing* data antar komputer.

Pengelolaan identitas pengguna dan akses logis dilakukan dengan membagi akses pengguna menjadi 2 level yaitu *Administrator* yang dipegang oleh pengelola IT dan *user* untuk pengguna aplikasi Sistem Informasi Manajemen Rumah Sakit. Setiap orang memiliki akun yang berbeda sesuai bidang tugas sehingga hanya dapat menggunakan fasilitas dalam aplikasi Sistem Informasi Manajemen Rumah Sakit yang terkait bidang tugas yang dikerjakan. Pengelolaan akses fisik ke aset TI dilakukan melalui perlindungan aset fisik TI dari pengunjung dilakukan dengan menempatkan aset TI di tempat yang tidak terjangkau oleh pengunjung seperti prosedur instalasi kabel jaringan yang dilakukan dengan instalasi tertutup di dalam plafon serta pengamanan ruang server yang diamankan oleh kunci dan terdapat prosedur untuk memasuki ruang server.

Pengelolaan dokumen sensitif dibagi menjadi 2 bagian yaitu pengelolaan data yang dilakukan oleh unit Teknologi Informasi dan pengelolaan file yang dilakukan oleh Sie. Tata Usaha. Pengelolaan data sensitif seperti data rekam medis pasien, kebutuhan gizi pasien, logistik hingga data keuangan rumah sakit pada Sistem Informasi Manajemen Rumah sakit dilakukan menggunakan sistem database yang dienkripsi dengan password dan hanya dapat diakses oleh aplikasi Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta dengan adanya konektivitas jaringan. Pengelolaan *file storage* dipusatkan di Sie. Tata Usaha. File dokumen di kelola dan disimpan di komputer pada Sie. Tata Usaha dengan prosedur pengaksesan keseluruhan file dokumen dilakukan melalui TU dan harus diketahui oleh direksi. Pemantauan infrastruktur terkait keamanan dilakukan dengan pemasangan CCTV yang dipasang di area server dan dimonitor langsung oleh satpam. Pihak pengelola juga melakukan pemantauan jaringan komputer secara fisik secara periodik selama 1 bulan sekali.

Analisis *Capability Level* COBIT 5

Setelah dilakukan pengambilan data dengan menggunakan metode wawancara dan observasi, selanjutnya di bagikan kuesioner untuk mengambil data terkait pencapaian tingkat kapabilitas COBIT 5 dan diperoleh hasil sebagai berikut:

Tabel 4. *Capability Level* Domain APO 13

Aktivitas	Indeks Kematangan	Capability Level
APO 13.01 (Mengelola Sistem Manajemen Keamanan Informasi)	3,25	3 : Established Process
APO 13.02 (Mengelola Manajemen resiko keamanan informasi)	0,75	1 : Performed Process
APO 13.03 (Memantau dan meninjau kembali Sistem Manajemen Keamanan Informasi)	3,75	4 : Predictable Process
Rata-Rata	2,59	3 : Established Process

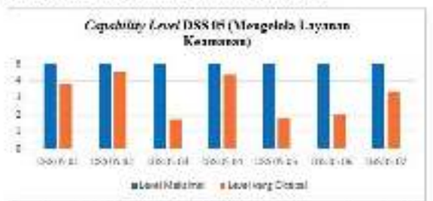
Berdasarkan data diatas, rata-rata indeks kematangan keseluruhan domain APO 13 ada adalah 2,59 ada pada level 3 (*Estoblished Process*). Hal ini menunjukan bahwa pengelolaan keamanan Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta telah dikelola dengan baik dan masih terus dikembangkan agar Sistem Informasi Manajemen Rumah Sakit menjadi sebuah sistem yang semakin mapan. Pencapaian tingkat kapabilitas dalam pengelolaan proses yang ada pada domain APO 13 (Mengelola Keamanan) COBIT 5 masih belum mencapai level maksimal yaitu pada level *5 : Optimized Process*. Hal tersebut dapat dilihat pada Gambar 2.

Gambar 2. Grafik *Capability Level* Domain APO 13

Tabel 5. *Capability level Domain DSS 05*

Aktivitas	Indeks Kematangan	Capability Level
DSS 05.01 (Melindungi Terhadap Malware)	3.8	*4 : Predictable Process*
DSS 05.02 (Mengelola Jaringan dan Keamanan Konektivitas)	4.5	*5 : Optimizing Process*
DSS 05.03 (Mengelola Keamanan *End point*)	1,75	*2 : Managed Process*
DSS 05.04 (Mengelola Identitas Pengguna dan Akses Logis)	4,35	*4 : Predictable Process*
DSS 05.05 (Mengelola Akses Fisik ke Aset TI)	1,85	*2 : Managed Process*
DSS 05.06 (Mengelola Dokumen Sensitif dan	2.0	*2 : Managed Process*
DSS 05.07 (Memantau infrastruktur untuk keamanan)	3,39	*3 : Established Process*
Rata-Rata	3,09	*3 : Established Process*

Berdasarkan data diatas, rata-rata indeks kematangan keseluruhan domain DSS 05 ada adalah 3,09 ada pada level 3 (Established Process). Hal ini menunjukan bahwa pelayanan keamanan yang dilakukan pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta telah dikelola dengan baik dan masih terus dikembangkan agar Sistem Informasi Manajemen Rumah Sakit menjadi sebuah sistem yang semakin mapan. Pencapaian tingkat kapabilitas dalam pengelolaan proses yang ada pada domain DSS 05 (Mengelola Layanan Keamanan) COBIT 5 masih belum mencapai level maksimal yaitu pada level 5 : Optimized Process. Hal tersebut dapat dilihat pada Gambar 3.



Gambar 3. Grafik *Capability Level* Domain DSS 05

Analisis Aspek Keamanan Informasi

Keamanan sistem informasi berkaitan erat dengan aspek keamanan informasi. Perlindungan pada aset informasi yang terdapat dalam sistem informasi diperlukan untuk memenuhi aspek keamanan informasi yaitu *Confidentiality*, *Integrity*, dan *Availability*. Berdasarkan hasil penelitian, kita dapat mengetahui hasil dari audit keamanan sistem informasi pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta dengan menggunakan COBIT 5 sebagai alat ukur meliputi :

1. ***Confidentiality***

   Berdasarkan hasil penelitian menggunakan domain APO 13 dan DSS 05 Framework COBIT 5, pengelola Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta menjamin kerahasiaan informasi melalui pengelolaan hak akses. Disamping itu, kedudukan Sistem Informasi Manajemen Rumah Sakit sebagai data *storage* menggunakan sistem *database* yang dienkripsi dengan password yang hanya dapat diakses oleh aplikasi Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta. Pengelolaan database

2. ***Integrity***

   Hasil menggunakan domain APO 13 dan DSS 05 Framework COBIT 5, penjaminan kelengkapan informasi pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta dilakukan melalui perlindungan terhadap *malware* dan virus yang mengancam pada server, perlindungan terhadap jaringan konektivitas serta melalui prosedur permintaan dan pelepasan data dalam kebijakan Teknologi Informasi.

3. ***Availability***

   Hasil menggunakan domain APO 13 dan DSS 05 Framework COBIT 5, penjaminan aspek *availability* dikelola melalui pengelolaan akses fisik ke aset TI pengamanan ruang server yang diamankan menggunakan kunci dan terdapat prosedur untuk memasuki ruang server serta dipantau melalui CCTV langsung oleh petugas keamanan rumah sakit.

REKOMENDASI

Dari hasil pengukuran audit keamanan sistem informasi manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta diberikan beberapa rekomendasi. Instansi diharapkan untuk mengembangkan pengelolaan keamanan informasi yang baik terhadap SIM Rumah Sakit yang dikelola khusus oleh divisi TI Rumah Sakit Mata "Dr.YAP" Yogyakarta. Instansi perlu menerapkan suatu kerangka kerja (*framework*) TI terintegrasi seperti COBIT dalam mengelola tata kelola TI rumah sakit. Instansi diharapkan menerapkan pendekatan Sistem Manajemen Keamanan Informasi melalui standarisasi seperti ISO/IEC 27001 dan Indeks KAMI. Pengelola diharapkan meningkatkan manajemen resiko khusus terkait keamanan informasi menggunakan standar manajemen resiko pada Sistem Manajemen Keamanan Informasi. Pengelola diharapkan untuk menerapkan penggunaan pengamanan sistem sidik jari maupun *password* pada ruangan *server* untuk lebih menjaga keamanan *server.* Instansi perlu merekrut sumber daya manusia yang kompeten dalam bidang TI untuk menunjang pengelolaan layanan keamanan sistem informasi. Pengelola diharapkan mengembangkan pengaturan internet protokol menggunakan IP Publik agar dapat diakses melalui jaringan internet oleh pasien guna meningkatkan pelayanan informasi kesehatan serta perwujudan keterbukaan informasi pada pelayanan publik. Pengelola perlu mengembangkan keamanan *endpoint* terhadap pihak eksternal yaitu pada perangkat pasien atau pengunjung seiring pengembangan pengaturan IP Publik.

SIMPULAN

Pengelolaan keamanan pada Sistem Informasi Manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta sudah hampir memenuhi keseluruhan aspek dalam domain APO 13 (*Manage Security)* dan DSS 05 (*Manage Security Services)* COBIT 5 *Framework* yang dibuktikan dengan tingkat kapabilitas yang dicapai pada masing-masing domain yaitu mencapai angka 2,59 berada pada level 3 (*Established Process*) pada domain APO 13 (Mengelola Keamanan) dan 3,09 berada pada level 3 *(Established Process)* pada domain DSS 05 COBIT 5. Proses yang dilakukan pada kedua domain telah mencapai level 3 *(Established Process)* yang dapat diartikan bahwa pengelolaan keamanan Sistem Informasi Manajemen rumah Sakit Mata "Dr.YAP" Yogyakarta telah dikelola dengan baik dan masih terus dikembangkan agar Sistem Informasi Manajemen Rumah Sakit menjadi sebuah sistem yang semakin mapan. Dari hasil audit keamanan sistem informasi manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta juga dapat diketahui juga bahwa aspek keamanan informasi yang erat kaitannya dengan keamanan sistem informasi dikelola dengan baik oleh pengelola sistem informasi manajemen Rumah Sakit Mata "Dr.YAP" Yogyakarta.

SARAN

Kuantitas sumber daya manusia yang dimiliki Rumah Sakit Mata "Dr.YAP" Yogyakarta perlu ditingkatkan guna mengelola keamanan sistem informasi manajemen. Instansi perlu melakukan pengelolaan yang lebih maksimal terhadap masing-masing proses yang terdapat pada domain APO 13 dan DSS 05 agar keamanan sistem informasi menjadi lebih baik. Untuk penelitian selanjutnya dapat digunakan domain yang lebih menyeluruh yang erat kaitannya dengan keamanan sistem informasi.

DAFTAR PUSTAKA

Gondodiyoto, S. (2007). *Audit Sistem Informasi + Pendekatan CobIT (Edisi Revisi)*. Jakarta : Mitra Wacana Media.

ISACA. (2012) . *Cobit 5 Enabling Processess ISACA*. USA : ISACA.

ISACA. (2012). *Cobit 5 A business Framework for the Governance and Management of Enterprise IT*. USA : ISACA.

Mohammad Nazir. 2005. *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Rochaety, E., Ridwan, F., & Setyowati, T. (2013). *Sistem Manajemen Informasi (Edisi 2)*. Jakarta : Mitra Wacana Media.

Sarno, Riyanarto & Irsyat Iffano. (2009). *Sistem Manajemen Keamanan Informasi*. Surabaya : ITSPress.

Sugiyono. 2011. *Metode penelitian kuantitatif kualitatif dan R & D*. Bandung: Alfabeta.

Sugiyono. 2005. *Metode penelitian kualitatif*. Bandung: Alfabeta.

Undang - Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Weber, R. 2000. *Information System Audit and Control Audit*. New Jersey : Prenctice Hall, Inc.