e-ISBN 978-623-93343-4-5
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 15 September 2021

Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019

Rizqi Satria Andhika Gusni[1], Kraugusteeliana [2], I Wayan Widi Pradnyana[3]
S1 Sistem Informasi / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Jawa Barat
rizqi.sa@upnvj.ac.id[1], kraugusteeliana@upnvj.ac.id[2], wayan.widi@upnvj.ac.id[3]

Abstrak. Rumah sakit merupakan fasilitas pelayanan kesehatan yang perlu didukung oleh sistem informasi rumah sakit (SIM-RS) yang aman. Permasalahan yang terjadi pada Rumah Sakit Bhayangkara Sespima Polri Jakarta adalah kurang maksimalnya tata kelola keamanan sistem informasi. Penelitian ini menggunakan COBIT 2019 sebagai framework penilaian karena COBIT 2019 merupakan sekumpulan *best practices* tata kelola di sebuah perusahaan. Penilaian pada penelitian ini mengacu kepada proses EDM03, APO12, APO13, APO14, dan DSS05. Hasil dari penelitian ini menunjukkan level kapabilitas tata kelola di RS Bhayangkara Sespima Polri Jakarta ini berada ditingkat 3 (*Defined*), permasalahan utama terdapat pada proses pengelolaan layanan keamanan (DSS05) serta selisih *gap analysis* dari semua proses adalah 1 tingkat di bawah dari tingkat yang diharapkan. Hasil dari penelitian ini diharapkan menjadi usulan perbaikan untuk pihak RS Bhayangkara Sespima Polri Jakarta pada tata kelola keamanan SIM-RS.

Kata Kunci: Tata Kelola TI, Rumah Sakit, SIM-RS, Keamanan Sistem, COBIT 2019.

1 Pendahuluan

Sistem Informasi Rumah Sakit (SIM-RS) adalah komponen yang wajib pada setiap rumah sakit untuk mendukung pelayanan dan operasional rumah sakit, Faktor-faktor yang tidak dapat dipisahkan dari SIM-RS adalah kualitas sistem, yang meliputi kualitas data dan informasi. Sistem informasi rumah sakit yang berkualitas juga perlu didukung oleh kualitas keamanan sistem yang baik, karena keamanan informasi dasarnya adalah kerahasiaan, integritas, ketersediaan [1]. Apabila sistem informasi rumah sakit mengabaikan keamanan informasi maka hal ini akan mengakibatkan kualitas informasi, data, dan keamanan menjadi buruk dan akan menghasilkan kerugian [2].

Di Rumah Sakit Bhayangkara Sespima Polri Jakarta, beberapa permasalahan keamanan yang muncul pada sistem informasi rumah sakit adalah ketidaksesuaian data, keamanan sistem yang masih lemah, SOP penggunaan sistem yang kurang diterapkan oleh pegawai, belum ada pembagian tugas dan penanggung jawab yang jelas pada bagian TI, pihak rumah sakit jarang melakukan audit internal, dan sistem yang sering mengalami *error* atau *down*. Kondisi ini jelas berbanding terbalik dengan tujuan SIM-RS dan tata kelola sistem yang baik. Apabila hal ini dibiarkan dapat merugikan pasien dan rumah sakit yang akhirnya berpengaruh kepada kualitas pelayanan di Rumah Sakit Bhayangkara Sespima Polri Jakarta

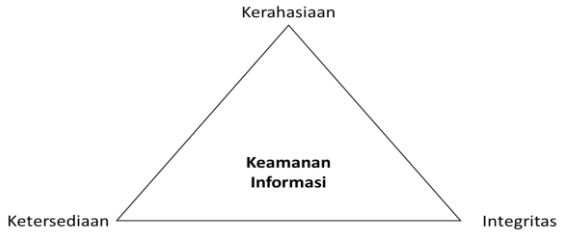
Dari permasalahan diatas, peneliti akan merumuskan bagaimana cara *framework* COBIT 2019 dapat mengukur nilai kapabilitas keamanan sistem informasi di RS Bhayangkara Sespima Polri Jakarta, dan bagaimana rekomendasi mitigasi dari risiko yang ditimbulkan dalam kinerja SIM-RS. Ruang lingkup pada penelitian ini hanya membatasi seputar penilaian tata kelola keamanan sistem informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta dan hanya menggunakan *framework* COBIT 2019 dengan domain yang dinilai berupa domain EDM (Evaluate, Direct, and Monitor), domain APO (*Align, Plan, and Organize*), dan domain DSS (*Deliver, Service and Support)*. Tujuan dari penelitian ini adalah untuk memberikan bahan evaluasi tentang tata kelola keamanan sistem informasi rumah sakit Bhayangkara Sespima Polri Jakarta serta mengetahui kelebihan dan kekurangan sistem informasi rumah sakit Bhayangkara Sespima Polri Jakarta.

2 Dasar Teori

Landasan teori pada penelitian ini adalah keamanan informasi dan Cobit 2019, yang selengkapnya akan dijelaskan pada sub-bagian 2.1 dan 2.2 berikut ini.

2.1 Keamanan Informasi

Konsep keamanan informasi berfokus pada 3 hal yaitu: *Confidentiallity* (Kerahasiaan), I*ntegrity* (Integritas), dan *Availibility* (Ketersediaan) [1], ketiganya ini membentuk susunan berupa segitiga yang disebut CIA Triad.

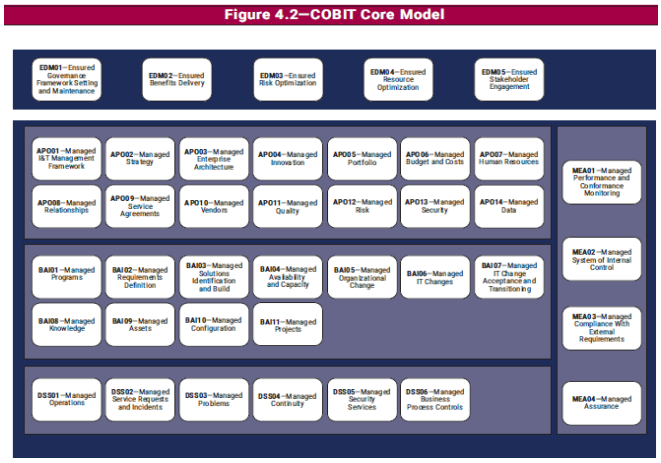


Gambar. 3. Segitiga keamanan informasi.

Kerahasiaan adalah bagaimana menjaga sebuah informasi dari kebocoran atau penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab, integritas bertujuan untuk menjaga data dan/atau informasi yang ada bersifat sebagaimana mestinya informasi tersebut disampaikan dan ketersediaan merupakan konsep di mana data tersedia dan keadaannya utuh.

2.2 COBIT 2019

COBIT adalah kerangka kerja untuk tata kelola pengelolaan informasi dan teknologi perusahaan yang bertujuan untuk mengatur tata kelola perusahaan. COBIT 2019 merupakan penyempurnaan dari COBIT 5.0 yang diluncurkan pada tahun 2012 yang mempunyai dua prinsip utama, yaitu *Governance System Principles* (Prinsip tata kelola) dan *Governance Framework Principles* (Kerangka Tata Kelola). [3]
COBIT 2019 memiliki 6 komponen tata kelola yaitu: proses, struktur organisasi, prinsip, informasi, budaya organisasi, SDM, dan layanan infrastruktur serta apilkasinya [3]. Sama seperti COBIT 5 sebelumnya, domain pada COBIT 2019 dibagi menjadi 5 domain, dengan tujuan tata kelola dan manajemen di COBIT dikelompokkan menjadi lima domain
.



Gambar. 4. Domain dan proses pada COBIT 2019.

Domain pada COBIT 2019 dikelompokkan menjadi 5 yaitu:

- EDM (*Evaluate, Direct and Monitoring*), domain ini menjelaskan bagaimana perusahaan mengevaluasi, menngarahkan dan menilai rencana strategis, domain ini memiliki total 5 proses.
- APO (*Align, Plan and Organize*), domain ini membahas organisasi secara keseluruhan, strategi, dan aktivitas yang mendukung teknologi dan informasi perusahaan, domain ini memiliki 14 proses.
- BAI (*Build, Acquire, and Implement*), domain ini membahas tentang perancangan, akuisisi dan implementasi solusi TI, domain ini memiliki 11 proses.
- DSS (*Deliver, Service and Support*), domain ini membahas tentang dukungan operasional dan dukungan layanan T&I, domain ini memiliki 6 proses.
- MEA (*Monitor, Evaluate and Assess)*, domain ini membahas tentang pemantauan kinerja dan kesesuaian T&I dengan target kinerja serta tujuan pengendalian internal dan eksternal, domain ini memiliki 4 proses.

Kemudian, dari proses tersebut dilakukan penilaian kapabilitas pada COBIT 2019 ini dibagi menjadi 6 tingkatan yaitu:

a. Level 0 *(Incomplete*/Tidak Lengkap)
b. Level 1 (*Initial*/Tahap Awal)
c. Level 2 (*Managed*/Dikelola)
d. Level 3 (Defined/Ditetapkan)
e. Level 4 (Quantitative/Kuantitatif)
f. Level 5 (Optimising/Mengoptimalkan)

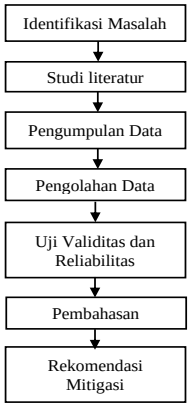
Penilaian kapabilitas pada COBIT 2019 juga dapat dibantu dengan melakukan pemeringkatan pada aktivitas-aktivitas proses dengan pemeringkatan sebagai berikut.:

a. *Fully* (F), penilaian kapabilitas berada pada rentang nilai 85-10*0*
b. *Largely* (L), penilaian kapabilitas berada pada rentang 50-85
c. *Partially* (P), penilaian kapabilitas berada pada rentang 15-50
d. *Not* (N), penilaian kapabilitas kurang dari 15 persen
e.

Untuk mengukur pencapaian tingkat kapabilitas setiap proses di COBIT 2019, diperlukan pengukuran aktivitas-aktivitas pada sub proses di setiap proses yang ada.[4][5]

3 Metode Penelitian

Penelitian ini menggunakan metode deskriptif kuantitatif, yang menggambarkan hasil penelitian sebagaimana yang didapatkan berdasarkan hasil dari analisis RACI *(Responsible, Accountable, Consulted, and Informed*), penghitungan *rating process activities* dan kuisioner.



Gambar. 5. Kerangka penelitian.

Identifikasi masalah dilakukan dengan melakukan observasi dan wawancara terlebih dahulu kepada bagian-bagian terkait tata kelola keamanan sistem di RS Bhayangkara Sespima Polri Jakarta, setelah melakukan wawancara terhadap pihak-pihak terkait, peneliti melakukan studi literatur terkait COBIT 2019 dan analisis RACI.
Penelitian ini menggunakan COBIT 2019 sebagai variabel dependen dan tata kelola keamanan SIM-RS Bhayangkara Sespima Polri Jakarta. Peneliti melakukan analisis RACI untuk mengetahui siapa saja pihak yang bertanggung jawab dalam tata kelola keamanan sistem informasi rumah sakit Bhayangkara Sespima Polri Jakarta. Hasil dari analisis RACI [5] akan dijadikan sebagai acuan untuk membuat kuisioner dan penilaian *rating process activities.*

Penelitian ini dilaksanakan pada bulan Maret – Juni 2021. Peneliti melakukan penyebaran kuesioner secara *hybrid* menggunakan Google Forms dan penyebaran kuesioner cetak untuk melakukan pengumpulan data. Peneliti juga melakukan penilaian *rating process activities* untuk mengetahui seberapa maksimal penerapan aktivitas proses COBIT 2019 [5] pada tata kelola keamanan sistem informasi RS Bhayangkara Sespima Polri Jakarta. Rumus yang digunakan peneliti dalam menentukan penilaian aktivitas *rating process activities* adalah sebagai berikut [6]

Σnap = Jumlah aktivitas terpenuhi / Jumlah aktivitas keseluruhan x 100%. (**3**)

Pengukuran variabel dilakukan dengan metode kuantitatif dengan menggunakan kuisioner berdasarkan skala Likert, yang akan disebarkan kepada 108 responden dari populasi sebanyak 168 orang. Hasil respon yang didapatkan dari kuisioner diuji dengan uji validitas pada penelitian ini memiliki nilai minimum R = 0,158 untuk menentukan apakah pernyataan pada kuisioner tersebut valid atau tidak, dan uji reliabilitas dengan nilai Cronbach's *Alpha* minimal 0,8 supaya pernyataan dapat dikatakan handal atau reliabel. Apabila kuesioner valid dan reliabel, maka akan dilakukan rekapitulasi kuesioner. Hasil dari rkapitulasi kuesioner akan dilakukan penghitungan pencapaian aktivitas proses dengan rumus sebagai berikut:

ΣNak = Nilai rata-rata pernyataan/5 x 100% (**4**)

Hasil dari penilaian *rating process activities* dan kuisioner yang didapatkan dari rumus 1 dan rumus 2 selanjutnya dilakukan penjumlahan total rating dan pemeringkatan tingkat kapabilitas.dengan rumus berikut:

Kap= ΣNap + ΣNak / 2 (**5**)

Apabila rating total dari pernyataan di bawah 51% maka proses dianggap tidak lulus atau nilai K dihitung 0, selanjutnya hasil dari rating yang didapatkan dari kuesioner dan pengamatan tersebut akan dilakukan penghitungan kapabilitas dengan rumus sebagai berikut [7]:

ΣNk = (*level* kapabilitas x Jumlah Kap) / jumlah proses (**6**)

Hasil berupa rata-rata tingkat kapabilitas yang didapatkan dari rumus 4 ini dapat bervariasi mulai dari Level 0 (*Incomplete*/Tidak Lengkap); Tingkat 1 (*Initial*/Tahap Awal); Tingkat 2 (*Managed*/Dikelola); Tingkat 3 (*Defined/*Ditetapkan); Tingkat 4 (*Quantitative*/Kuantitatif); dan Tingkat 5 (*Optimising*/Mengoptimalkan). Semakin tinggi tingkatan yang didapatkan, semakin baik performa tata kelolanya.

4 Pembahasan

Pada sub-bagian 4.1 – 4.5 berikut ini berisikan pembahasan dan hasil dari penelitian yang telah dilaksanakan.

4.1 Analisis RACI

Analisis RACI (*Responsible, Accountable, Consulted, and Informed*) pada domain EDM (Evaluate, Direct, and Monitor), domain APO (*Align, Plan, and Organize*), dan domain DSS (*Deliver, Service and Support)* dijabarkan pada tabel 1 dibawah ini:

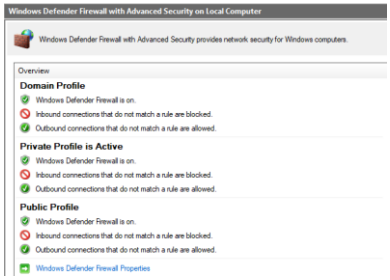
Tabel 2. Hasil analisis RACI.

Key Management	Karumkit	K3RS	SIM-RM	Kemin	Divisi IT	Staff
EDM03.01	C	R	R	R	R	I
EDM03.02	A	A	R	R	R	I
EDM03.03	A	R	R	R	R	I
APO12.01	I	A	R	R	R	R
APO12.02	A	R	C	C	C	C
APO12.04	C	A	R	R	R	R
APO12.05.	A	A	R	R	R	R
APO12.06.	C	A	R	R	R	R
APO13.01	C	C	A	C	R	I
APO13.02	C	C	A	C	R	I
APO13.03	C	C	A	C	R	I
APO14.01	R	R	R	I	I	I
APO14.04	A	C	R	R	R	R
APO14.06	C	A	R	R	R	R
APO14.07	C	C	R	R	R	I
APO14.09	C	C	A	R	R	I
APO14.10	C	C	A	C	R	R
DSS05.01	R	R	R	R	R	R
DSS05.02	C	C	A	I	R	R
DSS05.03	C	C	A	I	R	R

Dari analisis RACI pada tabel 1 diatas, didapatkan hasil bahwa bagian divisi IT memegang tanggung jawab paling besar dalam keberlangsungan tata kelola sistem informasi rumah sakit Bhayangkara Sespima Polri Jakarta, hal ini dilihat dari banyaknya peran *responsible* (tanggung jawab) dari analisis RACI yang dilakukan.

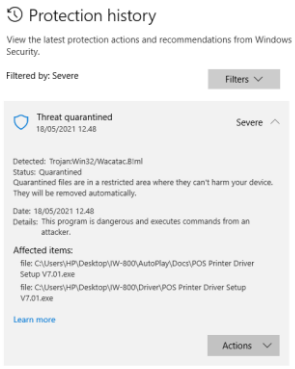
4.2 Analisis Tata Kelola Keamanan Sistem

Tata kelola keamanan pada sistem informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta yang menggunakan Khanza HMS saat ini telah didukung menggunakan infrastruktur TI dan keamanan sistem yang handal.



Gambar. 6. Windows Defender *Firewall* yang sudah diaktifkan.

Pengamanan sistem pada sistem informasi rumah sakit Bhayangkara Sespima Polri Jakarta yang sudah mutakhir yang didukung dengan *firewall*, enkripsi basis data menggunakan BASE64, enkripsi sistem dengan hak akses masing-masing *user*, dan anti virus standar bawaan Windows 10, serta didukung dengan SOP yang diberlakukan di RS Bhayangkara Sespima Polri Jakarta.



Gambar. 7. Ancaman virus Wacatac yang bersumber dari salah satu file *installer driver printer*.

Akan tetapi masih ada kelemahan dalam pengamanan sistem informasinya yaitu masih adanya program yang mengandung virus trojan dan *hacktools* yang bersumber program bajakan, apabila permasalahan ini tidak segera ditangani maka hal ini membahayakan kerahasiaan dan integritas data maupun sistem informasi yang dapat berakibat fatal bagi kelangsungan SIM-RS Bhayangkara Sespima Polri Jakarta kedepannya.

4.3 Rekapitulasi, uji validasi, dan reliabilitas data

Kuesioner yang disebar berupa tautan google forms dan kuesioner cetak yang menargetkan partisipasi responden sebanyak 110 sampel, tetapi dalam rekapitulasi didapatkan dua kuisioner yang tidak lengkap isiannya, kuesioner yang tidak lengkap isiannya tersebut selanjutnya diabaikan, total keseluruhan kuesioner setelah dilakukan penghitungan ulang menjadi 108 sampel. Uji validasi mendapatkan hasil hasil bahwa seluruh pernyataan pada kuesioner yang disebar valid, tingkat validitasnya berkisar antara 0,560-0,802. Hasil uji reliabilitas didapat hasil bahwa Cronbach's Alpha dari 108 kuisioner tersebut memiliki keandalan yang sangat tinggi dengan nilai 0,955.

4.4 Hasil analisis proses COBIT 2019

Penghitungan kapabilitas didasarkan pada hasil penilaian aktivitas proses dan data kuesioner yang didapat dari responden, tabel 2-6 berikut ini menyajikan hasil analisis kapabilitas pada proses COBIT 2019.

Tabel 3. Hasil analisis kapabilitas proses EDM03

Proses EDM03	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Jumlah Aktivitas Terpenuhi (*as is/to be*)			11/11 (100%)	2/3 (60%)	0/2 (0%)	0/1 (0%)
Rating berdasarkan kriteria	*True*	*True*	100%	79,7%		
Pencapaian Rating Berdasarkan Kriteria				69,85 *(Largely)*		
Pencapaian Level Kapabilitas				**3 *(Defined)***		

Tabel 2 menunjukkan bahwa proses EDM03 (Optimasi kontrol risiko) telah mencapai tingkat **3 (*Defined*),** dengan pencapaian aktivitas sebesar **69,85%.** tetapi masih terdapat kendala dalam pelaksanaan aktivitas prosesnya seperti belum maksimalnya evaluasi pada sistem, monitoring terhadap profil risiko masih kurang, serta belum adanya pembaharuan profil risiko saat ini.

Tabel 4. Hasil analisis kapabilitas proses APO12

Proses APO12	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Jumlah Aktivitas Terpenuhi (*as is/to be*)			3/3 (100%)	10/16 (62,5%)	2/8 (25%)	0/2 (0%)
Rating berdasarkan kriteria	*True*	*True*	100%	79,1%		
Pencapaian Rating Berdasarkan Kriteria				70,8 *(Largely)*		
Pencapaian Level Kapabilitas				**3 *(Defined)***		

Tabel 3 menunjukkan bahwa proses APO12 (mengelola risiko) telah mencapai tingkat **3 (*Defined*)**, dengan pencapaian aktivitas sebesar **70,8%.** tetapi masih terdapat kendala seperti pencatatan riwayat kejadian risiko yang belum didokumentasikan, belum diperbaharui skenario risiko TI (terakhir tahun 2019), dan pengkategorian insiden hanya sebatas insiden yang umum terjadi pada SIM-RS.

Tabel 5. Hasil analisis kapabilitas proses APO13.

Proses APO13	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Jumlah Aktivitas Terpenuhi (*as is/to be*)			11/11 (100%)	2/3 (66%)	1/5	0/1
Rating berdasarkan kriteria	True	True	100%	79,2%	20%	-
Pencapaian Rating Berdasarkan Kriteria				72,6% *(Largely)*		
Pencapaian Level Kapabilitas				**3 *(defined)***		

Tabel 4 menunjukkan bahwa proses APO13 (Mengelola keamanan) telah mencapai tingkat **3 (Defined**), dengan pencapaian aktivitas sebesar **72,6%.** Sayangnya, beberapa aktivitas seperti pelatihan terkait keamanan informasi jarang dilakukan, pengukuran keefektifan dan audit keamanan informasi jarang dilaksanakan.

Tabel 6. Hasil analisis kapabilitas proses APO14.

Proses APO14	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Jumlah Aktivitas Terpenuhi (*as is/to be*)			9/9 (100%)	7/8 (87,5)	5/11 (45%)	-
Rating berdasarkan kriteria	*True*	*True*	*True*	79	-	-
Pencapaian Rating Berdasarkan Kriteria				83,25 *(Largely)*		
Pencapaian Level Kapabilitas				**3 *(defined*)**		

Tabel 5 menunjukkan bahwa proses **APO14** (Mengelola data) telah mencapai tingkat **3 (*Defined*)**, dengan pencapaian aktivitas sebesar **83,25%.** tetapi masih terdapat kendala seperti kurangnya sinergi antara manajemen dan pegawai untuk mengembangkan kualitas data dan jarangnya penilaian kualitas data secara berkala

Tabel 7. Hasil analisis kapabilitas proses DSS05.

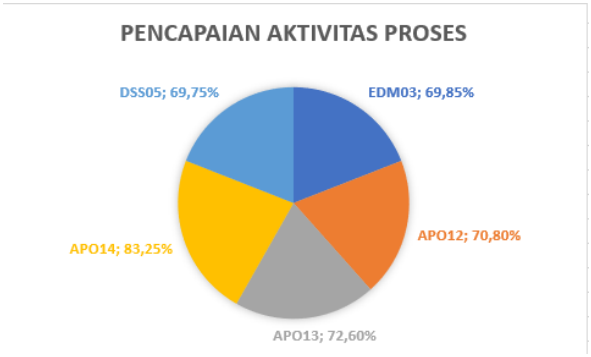
Proses DSS05	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Jumlah Aktivitas Terpenuhi (*as is/to be*)			22/26 (84,6)	11/18 (61,1)	0/5	-
Rating berdasarkan kriteria	*True*	*True*	*True*	L 78%	-	-
Pencapaian Rating Berdasarkan Kriteria				69,75% *(Largely)*		
Pencapaian Level Kapabilitas				**3 *(defined*)**		

Tabel 6 menunjukkan bahwa proses DSS05 (Mengelola layanan keamanan) telah mencapai tingkat 3 ***(Defined),*** dengan pencapaian aktivitas sebesar **69,75%.** tetapi masih terdapat aktivitas yang belum dilakukan seperti kurangnya sosialisasi terkait kewaspadaan ancaman siber, belum adanya kebijakan keamanan jaringan dan penggunaan komputer secara aman, dan keamanan fisik yang masih terbilang lemah (tidak adanya pengamanan akses fingerprint, CCTV).

Dari tabel 2-6 diatas, dapat dihitung kapabilitas berdasarkan hasil dari kuesioner sebagai berikut:

$$\Sigma Nk = \frac{(1 \times 0) + (2 \times 0) + (3 \times 5) + (4 \times 0) + (5 \times 0)}{5} = 3$$

Hasil dari penghitungan Nk menunjukkan tingkat kapabilitas yang dicapai oleh RS Bhayangkara Sespima Polri adalah tingkat 3 (*Defined*), dimana pada tingkatan ini proses sudah dilaksanakan, tetapi masih belum dilakukan pengukuran. Dan, berikut ini adalah diagram pencapaian aktivitas proses pada kinerja tata kelola keamanan SIM-RS



Gambar. 8. Persentase pencapaian aktivitas proses

Dari diagram aktivitas proses diatas, standar tata kelola keamanan berada pada **tingkat 3 (*Defined)*** dengan tingkat implementasi **73,25%**. Selanjutnya, hasil dari ***Gap analysis*** yang didapatkan berdasarkan analisis kapabilitas diatas adalah sebagai berikut:

Tabel 8 Hasil *Gap Analysis*

Proses	*As Is*	*To Be*	*Gap*
EDM03	3	4	1
APO12	3	4	1
APO13	3	4	1
APO14	3	4	1
DSS05	3	4	1

Selisih gap ini menunjukkan tata kelola keamanan yang ada di RS Bhayangkara Sespima Polri Jakarta ini masih berada pada tingkat 3 (**Defined),** dan belum mencapai tingkat kapabilitas yang diharapkan pada tingkat **4 (Quantitative**).

4.5 Saran Mitigasi

Dari hasil gap analysis diatas, peneliti mempertimbangkan saran mitigasi untuk dijadikan bahan evaluasi manajemen RS Bhayangkara Sespima Polri dalam memperbaiki kinerja tata kelola keamanan sistem informasi rumah sakit, berikut adalah saran mitigasi oleh peneliti:

1. Melakukan *scanning* komputer secara berkala untuk mencegah adanya infeksi virus maupun *malware* dalam komputer maupun sistem informasi yang dapat membahayakan kerahasiaan, integritas dan ketersediaan data.
2. Membuat prosedur preventif dalam pencegahan malware dengan melakukan pelatihan personil, pengecekan keamanan pada sistem, *backup* data penting untuk menjaga ketersediaan data, dan evaluasi berkala terkait ancaman keamanan.

3. Memperbaiki keamanan fisik pada situs untuk mencegah adanya akses orang yang tidak bertanggungjawab dan meminimalkan risiko pencurian, seperti dengan menambah CCTV, *fingerprint authentication*, retina scanner, dan melakukan prosedur pengetatan pengawasan tamu atau pegawai yang memasuki ruangan situs.
4. Melakukan pencatatan dan peninjauan terkait masalah keamanan secara rutin untuk memastikan sistem selalu aman dan tidak terdapat gangguan terkait keamanan baik dari dalam komputer maupun keamanan lingkungan sekitar.
5. Meninjau dan memperbarui profil risiko TI untuk memastikan bahwa profil risiko yang ada saat ini sudah siap dalam menghadapi risiko-risiko baru yang kemungkinan terjadi pada sistem.

5 Kesimpulan dan Saran

Rumah sakit sebagai fasilitas pelayanan kesehatan dituntut untuk memberikan pelayanan yang cepat dan tepat, yang didukung oleh SIM-RS yang aman, handal dan cepat. Apabila kualitas tata kelola keamanan sistem SIM-RS baik maka kualitas sistem yang baik akan tercapai,. Hasil penelitian menunjukkan manajemen SIM-RS telah melakukan pengamanan pada sistem, kemudian hasil penilaian kapabilitas COBIT 2019 menunjukkan manajemen RS Sespima Bhayangkara Polri Jakarta sudah menetapkan proses-proses COBIT 2019 pada tata kelola keamanan informasinya sebesar **73,25%** pada tingkat **3 (Defined**), serta penelitian ini menemukan perlunya perbaikan pada keamanan akses, keamanan komputer dan pembaruan profil risiko.

Referensi

[1] M. M. Alhassan and A. Adjei-Quaye, “Information Security in an Organization,” *Int. J. Comput.*, vol. 24, no. 1, pp. 100–116, 2017, [Online]. Available: http://ijcjournal.org/.

[2] K. Aswar and M. H. R. Hafizh, “Empirical study on organizational performance: the moderating effect of organizational culture,” *Pressacademia*, vol. 7, no. 3, pp. 287–297, 2020, doi: 10.17261/pressacademia.2020.1295.

[3] J. W. Lainhart, M. Conboy, and R. Saull, *COBIT 2019 Framework Introduction and Methodology*. Schaumburg: ISACA, 2019.

[4] T. Huygh, S. De Haes, A. Joshi, and W. Van Grembergen, “Answering Key Global IT Management Concerns Through IT Governance and Management Processes: A COBIT 5 View,” *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, vol. 9, 2018, doi: 10.24251/hicss.2018.665.

[5] J. W. Lainhart, M. Conboy, and R. Saull, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg: ISACA, 2019.

[6] L. H. Atrinawati *et al.*, “Assessment of Process Capability Level in University XYZ Based on COBIT 2019,” *J. Phys. Conf. Ser.*, vol. 1803, no. 1, pp. 0–11, 2021, doi: 10.1088/1742-6596/1803/1/012033.

[7] R. Umar, I. Riadi, and E. Handoyo, “Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI),” *J. Sist. Inf. Bisnis*, vol. 9, no. 1, p. 47, 2019, doi: 10.21456/vol9iss1pp47-54