Gudang Jurnal Multidisiplin Ilmu
Volume 3 ; Nomor 6 ; Juni 2025 ; Page 12-18
https://doi.org/10.59435/gjmi.v3i6.1615
Website : https://gudangjurnal.com/index.php/gjmi

E-ISSN : 2988-5760

Audit Keamanan SIMRS Dengan COBIT 2019: Studi Kasus RS XYZ

Gilis Fadhil Hisyam[1*], Muhammad Afdan Rojabi[2]

[1] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Mercu Buana
[2]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Sains Indonesia
[1*]gilissaliti@gmail.com@email.com, [2]muhammad.afdan@lecturer.sains.ac.id

Abstrak

Tujuan dilaksanakannya penelitian ini bertujuan untuk mengevaluasi tingkat keamanan dari Sistem Informasi Manajemen Rumah Sakit (SIMRS) di RS XYZ serta mengidentifikasi langkah-langkah yang diperlukan untuk meningkatkan keandalan dan kepatuhan sistem terhadap standar keamanan informasi. Salah satu langkah untuk menilai tingkat keamanan dilakukan dengan menerapkan kerangka kerja COBIT 2019, yang mencakup beberapa domain utama, yaitu Menetapkan dan Memastikan Manajemen Risiko atau EDM03, Mengelola Risiko atau APO12, Mengelola Keamanan atau APO13, Mengelola Data atau APO14, dan Mengelola Keamanan Layanan atau DSS05. Proses audit ini mencakup identifikasi potensi ancaman terhadap keamanan informasi, penilaian risiko, serta evaluasi efektivitas kontrol yang telah diterapkan. Hasil dari penelitian menunjukkan tingkatan kematangan keamanan SIMRS di RS XYZ berada di level 3 (*Defined*), yang berarti sistem telah memiliki prosedur keamanan yang terdokumentasi, tetapi implementasinya masih perlu diperkuat untuk mencapai tingkat yang lebih optimal. Berdasarkan *gap analysis*, terdapat selisih satu tingkat dari target yang diharapkan, sehingga perbaikan perlu dilakukan guna meningkatkan ketahanan sistem terhadap ancaman siber. Beberapa langkah strategis yang direkomendasikan meliputi penerapan teknik keamanan lanjutan, seperti *vulnerability scanning, penetration testing, Web Application Firewall* (WAF), serta sistem deteksi dan pencegahan intrusi (IDS/IPS). Selain itu, peningkatan keamanan fisik dengan pemasangan CCTV, pembatasan akses menggunakan kartu akses atau sidik jari, serta penerapan enkripsi data menjadi aspek penting dalam melindungi informasi pasien. Sertifikasi keamanan, seperti ISO 27001, juga dapat dipertimbangkan untuk memastikan kepatuhan terhadap standar global. Selain itu, peningkatan kompetensi SDM melalui pelatihan berkala terkait keamanan siber dan peningkatan koordinasi internal akan berkontribusi signifikan dalam memperkuat ketahanan sistem informasi di RS XYZ.

Kata Kunci: Audit Keamanan, Sistem Informasi Manajemen Rumah Sakit, COBIT 2019, Manajemen Risiko, Manajemen Keamanan.

PENDAHULUAN

Rumah sakit adalah instansi yang memberikan fasilitas layanan kesehatan dengan memanfaatkan berbagai macam aspek, beberapa diantaranya meliputi teknologi, dan tenaga medis yang kompeten (Rambe et al., 2025). Sebagai institusi yang memiliki peran krusial dalam pelayanan kesehatan masyarakat, rumah sakit dituntut agar terus berproses seiring dengan berkembangnya teknologi agar meningkatkan efisiensi serta kualitas dari layanan yang diberikan. Pemanfaatan teknologi informasi menjadi salah satu indikator utama dalam menentukan kesiapan sebuah rumah sakit dalam menghadapi tantangan serta perubahan di sektor kesehatan (Ndraha et al., 2024). Teknologi informasi berperan penting dalam meningkatkan efisiensi operasional, menekan biaya, serta memperbaiki kualitas pelayanan terhadap pasien (Effendy et al., 2024). Salah satu bentuk implementasi teknologi informasi yang umum digunakan dalam rumah sakit adalah Sistem Informasi Manajemen Rumah Sakit (SIMRS). SIMRS dirancang untuk pengelolaan, menyimpan, mengakses, serta menganalisis data pasien secara terintegrasi, sehingga dapat meningkatkan pengambilan keputusan baik secara klinis maupun manajerial. Sistem ini memiliki cakupan berbagai aplikasi, diantaranya sistem informasi laboratorium, sistem informasi radiologi, sistem informasi farmasi, serta berbagai sistem pendukung operasional lainnya (Algiffary et al., 2024). Implementasi SIMRS memungkinkan peningkatan akurasi data, percepatan layanan, serta optimalisasi koordinasi antar unit di dalam rumah sakit (Siregar et al., 2024).

Sebagai salah satu dari banyaknya rumah sakit besar di Jakarta yang berkomitmen untuk terus meningkatkan layanan kesehatan, RS XYZ di Jakarta telah mengadopsi SIMRS guna mempercepat pertumbuhan institusi serta meningkatkan daya saing. Dalam upayanya untuk memberikan pelayanan yang optimal kepada pasien, keberadaan sistem informasi yang mampu mempercepat dan mempermudah berbagai proses operasional menjadi kebutuhan utama. Oleh karena itu, RS XYZ di Jakarta menerapkan SIMRS dengan tujuan meningkatkan efisiensi pelayanan, mempermudah administrasi, mengoptimalkan pengelolaan informasi, serta memperkuat sistem keuangan dan logistik rumah sakit (Nugroho & Ali, 2022). Namun, meskipun SIMRS memberikan berbagai manfaat, sistem ini juga menghadapi berbagai risiko keamanan. Ancaman seperti serangan siber, pencurian data pasien, serta penyebaran malware menjadi tantangan yang harus diantisipasi oleh rumah sakit (Setiorini et al., 2021). Oleh sebab itu, penerapan audit dalam lingkup Sistem Manajemen Keamanan Informasi merupakan suatu langkah yang sangat penting untuk memastikan bahwa SIMRS tetap

terjaga dari berbagai risiko, baik dari dalam maupun luar organisasi. Audit keamanan sistem informasi merupakan suatu proses evaluasi yang bertujuan untuk mengidentifikasi celah keamanan, menilai tingkat proteksi yang telah diterapkan, serta memastikan bahwa data pasien tetap aman dan terjaga (Binta, 2025).

Control Objectives for Information and Related Technology 2019 atau yang lebih dikenal sebagai (COBIT) 2019 adalah salah satu kerangka kerja yang dapat digunakan dalam melakukan audit Sistem Manajemen Keamanan Informasi di rumah sakit (Sodik & Nugraheni, 2022). COBIT 2019 menyediakan langkah-langkah serta panduan bagi organisasi atau perusahaan dalam mengidentifikasi, mengevaluasi, serta mengklasifikasikan berbagai risiko-risiko terkait keamanan informasi, lalu menentukan kontrol-kontrol keamanan apa saja yang yang diperlukan, dan sekaligus memastikan agar pengelolaan teknologi informasi telah sesuai dengan standar yang berlaku (Kuncoro et al., 2024). Dengan menerapkan COBIT 2019, rumah sakit dapat meningkatkan efektivitas serta efisiensi dalam pengelolaan keamanan informasi, sekaligus memenuhi regulasi dan standar keamanan yang telah ditetapkan. Dalam konteks SIMRS, perlindungan sistem informasi menjadi faktor utama yang harus diperhatikan demi menjaga kelangsungan operasional rumah sakit. Beberapa metode yang dapat diterapkan dalam audit keamanan sistem informasi meliputi tes kerentanan atau *vulnerability scanning*, tes penetrasi atau *penetration testing*, serta simulasi serangan siber melalui *social engineering*. Hasil dari audit ini akan memberikan gambaran mengenai kelemahan sistem, potensi ancaman, serta rekomendasi perbaikan yang dapat diterapkan untuk meningkatkan keamanan sistem informasi rumah sakit. Sejumlah penelitian sebelumnya menunjukkan bahwa penerapan COBIT 2019 dalam proses audit Sistem Manajemen Keamanan Informasi di rumah sakit dapat membantu dalam mengidentifikasi kelemahan sistem serta memberikan rekomendasi yang sesuai untuk peningkatan keamanan (Novriyanto et al., 2024). Dengan menerapkan audit keamanan berbasis COBIT 2019, RS XYZ dapat memperkuat ketahanan sistem informasi, meminimalkan risiko kebocoran data, serta memastikan bahwa SIMRS dapat berjalan secara optimal sesuai dengan standar Sistem Manajemen Keamanan Informasi yang telah ditetapkan.

METODE

Tahapan Penelitian

Penelitian ini menggunakan metode pendekatan secara kuantitatif dan berfokus pada Unit Instalasi Teknologi Informasi (IT) di PT XYZ. Dalam studi ini, COBIT 2019 dijadikan sebagai variabel dependen, sementara Keamanan Sistem Informasi Manajemen Rumah Sakit (SIMRS) berperan sebagai variabel independen. Fokus penelitian mencakup beberapa lingkup domain dan juga proses dalam penerapan COBIT 2019, yaitu EDM03 (Manajemen Risiko Keamanan Informasi), APO12 (Manajemen Risiko), APO13 (Manajemen Keamanan), APO14 (Manajemen Keberlanjutan), dan DSS05 (Manajemen Pengetahuan IT). Tahapan awal penelitian ini diawali dengan identifikasi permasalahan yang dilakukan melalui wawancara mendalam dengan staf yang bertanggung jawab atas keamanan sistem informasi di PT XYZ. Wawancara ini bertujuan untuk menggali informasi mengenai praktik keamanan yang sedang diterapkan serta tantangan yang dihadapi oleh unit IT dalam menjaga dan meningkatkan keamanan SIMRS.

Langkah yang dilakukan untuk melakukan pengukuran variabel adalah dengan melalui penyebaran kuesioner berbasis skala Likert dengan nilai 5 poin kepada responden yang dipilih berdasarkan analisis RACI yaitu prinsip (*Responsible, Accountable, Consulted, and Informed*). Kuesioner ini dirancang untuk mengumpulkan data mengenai persepsi dan evaluasi pegawai terhadap penerapan serta efektivitas pengelolaan keamanan sistem informasi di PT XYZ. Setelah data terkumpul, langkah berikutnya adalah melakukan uji validitas dan reliabilitas untuk memastikan bahwa instrumen yang digunakan menghasilkan data yang akurat dan konsisten. Setelah melalui tahapan uji validitas dan reliabilitas, dilakukan penilaian aktivitas proses (rating process activities) guna mengukur seberapa jauh tingkatan kapabilitas Unit Instalasi IT PT XYZ dalam mengelola keamanan sistem informasi berdasarkan standar COBIT 2019. Penilaian ini bertujuan untuk mengetahui sejauh mana unit IT perusahaan telah memenuhi standar keamanan yang telah ditetapkan.

Hasil dari penilaian tersebut dianalisis menggunakan gap analysis untuk mengidentifikasi perbedaan antara kondisi saat ini (*as is*) dan kondisi yang diharapkan (*to be*). Analisis ini memberikan wawasan mengenai aspek yang perlu ditingkatkan dalam pengelolaan keamanan SIMRS di PT XYZ. Berdasarkan hasil *gap analysis*, dirancang rekomendasi mitigasi risiko guna mengurangi kesenjangan antara kondisi eksisting dan kondisi ideal, sehingga tingkat keamanan sistem informasi perusahaan dapat ditingkatkan secara lebih optimal. Melalui pendekatan ini, penelitian ini diharapkan dapat memberikan kontribusi yang berarti dalam upaya peningkatan manajemen keamanan informasi di PT XYZ.

HASIL DAN PEMBAHASAN

Analisa RACI

RACI atau yang lebih dikenal sebagai prinsip (*Responsible, Accountable, Consulted, and Informed*) dalam domain (*Evaluate, Direct, and Monitor*) atau disingkat EDM, (*Align, Plan, and Organize*) atau disingkat APO, serta (*Deliver, Service, and Support*) atau disingkat DSS dapat diuraikan secara lebih mendetail dalam Tabel 1.

Tabel 1. Hasil RACI *Analysis*

Key Management Practices	Director RS	Head of IT Unit Installation	IT Unit Instalation	Administration Staff	Staff etc
EDM03.01	C	R	R	R	I
EDM03.02	A	A	R	R	I
EDM03.03	A	R	R	R	I
APO12.01	I	A	R	R	R
APO12.02	A	R	C	C	C
APO12.04	C	A	R	R	R
APO12.05	A	A	R	R	R
APO12.06	C	A	R	R	R
APO13.01	C	C	I	A	I
APO13.02	C	C	R	A	I
APO13.03	C	C	R	A	I
APO14.01	R	R	R	R	I
APO14.04	A	C	R	R	R
APO14.06	C	A	R	R	R
APO14.07	C	C	R	R	I
APO14.09	C	C	R	A	I
APO14.10	C	C	R	A	R
DSS05.01	R	R	R	R	R
DSS05.02	C	C	R	A	R
DSS05.03	C	C	R	A	R

Berdasarkan hasil analisis RACI, dapat ditarik kesimpulan bahwa Unit Instalasi IT PT XYZ memiliki peran yang paling signifikan dalam memastikan keamanan sistem informasi di perusahaan. Hal ini ditunjukkan oleh banyaknya tanggung jawab *(responsible)* yang dipegang oleh unit tersebut dalam analisis RACI yang telah dilakukan.

Uji Validitas

Teknik pengujian validitas dilaksanakan guna memastikan instrumen-instrumen yang digunakan secara akurat mampu mengukur aspek yang ingin diteliti. Hasil pengujian validitas terhadap pernyataan-pernyataan dalam instrumen dapat dilihat pada Tabel 2.

Tabel 2. Hasil dari Uji Validitas

Process	rCount	rTable	*Sig.*	Description
EDM03.01	0,870	0,229	5%	Valid
EDM03.02	0,648	0,229	5%	Valid
EDM03.03	0,988	0,229	5%	Valid
APO12.01	0,828	0,229	5%	Valid
APO12.02	0,818	0,229	5%	Valid
APO12.04	0,685	0,229	5%	Valid
APO12.05	0,815	0,229	5%	Valid
APO12.06	0,833	0,229	5%	Valid
APO13.01	0,678	0,229	5%	Valid
APO13.02	0,968	0,229	5%	Valid
APO13.03	0,865	0,229	5%	Valid
APO14.01	0,860	0,229	5%	Valid
APO14.04	0,854	0,229	5%	Valid
APO14.06	0,787	0,229	5%	Valid
APO14.07	0,741	0,229	5%	Valid
APO14.09	0,582	0,229	5%	Valid
APO14.10	0,822	0,229	5%	Valid
DSS05.01	0,810	0,229	5%	Valid
DSS05.02	0,938	0,229	5%	Valid
DSS05.03	0,635	0,229	5%	Valid

Merujuk pada data yang dipaparkan pada Table 2, disimpulkan bahwa seluruh pernyataan yang ada dalam kuesioner dinyatakan valid pada tingkat signifikansi 5%, karena nilai rCount melebihi rTable.

Uji Reliabilitas

Pengujian reliabilitas dilakukan untuk memastikan bahwa jawaban responden terhadap setiap pernyataan bersifat konsisten dan tidak acak. Hasil dari uji reliabilitas yang telah dilakukan terhadap pernyataan-pernyataan yang digunakan dapat dilihat pada Tabel 3.

Tabel 3. Hasil dari Uji Reliabilitas

Process	*Cronbach's Alpha*	*Cut off*	Description
EDM03	0,838	0,60	Reliabel
APO12	0,952	0,60	Reliabel
APO13	0,903	0,60	Reliabel
APO14	0,945	0,60	Reliabel
DSS05	0,869	0,60	Reliabel

Hasil dari uji reliabilitas di atas menunjukkan bahwa semua variabel memiliki nilai koefisien *Cronbach's Alpha* lebih dari 0,60, yang berarti semua pernyataan yang digunakan dapat dianggap reliabel.

Rating Process Activities

Pengukuran suatu tingkatan kapabilitas dilakukan berdasarkan dari hasil yang didapat dari evaluasi aktivitas proses yang diperoleh melalui data kuesioner yang diisi oleh responden. Evaluasi ini bertujuan untuk menilai sampai sejauh mana proses-proses dalam implementasi *Framework* COBIT 2019 yang dianalisis telah mencapai tujuan serta memenuhi kontrol-kontrol yang telah ditetapkan. Tabel 4-8 berikut ini memaparkan hasil dari analisis kapabilitas untuk tiap proses dalam penerapan *Framework* COBIT 2019.

Tabel 4. Hasil dari *Rating Process Activities* EDM03

Process	Level				
	1	2	3	4	5
Nilai		92	71,2		
Skala Penilaian		F	L		
Kapabilitas			Level 3		
Keterangan: N (Not Achieved, 0 – 15), P (Partially Achieved, > 15 - 50), L (Largely Achieved, > 50 - 85), F (Fully Achieved, > 85 - 100)					

Mengacu pada Tabel 4, yaitu proses dari *Ensuring Information Security Risk Management* atau EDM03 sudah berada di tingkat 3 (Defined) dimana capaian aktivitasnya sebesar 71,2. Meskipun demikian, masih adanya beberapa kendala pada proses pelaksanaannya, seperti kurangnya pemantauan serta pembaruan profil risiko, dan evaluasi sistem yang belum berjalan secara optimal. Beberapa permasalahan yang ditemukan mencakup belum adanya penerapan *Risk Assessment*, belum diperolehnya sertifikasi keamanan, dan belum digunakannya teknik atau cara yang efektif untuk memonitoring keamanan sistem yang dimiliki.

Tabel 5. Hasil dari *Rating Process Activities* APO12

Process	Level				
	1	2	3	4	5
Nilai		100	72,5		
Skala Penilaian		F	L		
Kapabilitas			Level 3		
Keterangan: N (Not Achieved, 0 – 15), P (Partially Achieved, > 15 - 50), L (Largely Achieved, > 50 - 85), F (Fully Achieved, > 85 - 100)					

Berdasarkan Tabel 5, pada proses *Risk Management* atau APO 12 sudah berada di tingkat 3 (*Defined*) dimana tingkat aktivitas yang tercapai sebesar 72,5. Namun, terdapat beberapa tantangan yang masih dihadapi, seperti belum tersedianya dokumentasi lengkap terkait pencatatan riwayat terjadinya risiko (dan apabila sudah ada, pengelompokkan terjadinya risiko tersebut masih belum dilakukan secara mendalam serta belum selaras dengan standar industri yang berlaku). Selain itu, skenario risiko pada TI belum diperbarui secara berkala.

Tabel 6. Hasil dari *Rating Process Activities* APO13

Process	Level				
	1	2	3	4	5
Nilai		100	70,3		
Skala Penilaian		F	L		
Kapabilitas			Level 3		
Keterangan: N (Not Achieved, 0 – 15), P (Partially Achieved, > 15 - 50), L (Largely Achieved, > 50 - 85), F (Fully Achieved, > 85 - 100)					

Mengacu pada Tabel 6, proses dari *Security Management* atau APO13 telah mencapai tingkat 3 (*Defined*) dimana tingkat aktivitas yang tercapai sebesar 70,3. Namun, terdapat adanya beberapa isu yang perlu diperhatikan, salah satunya adalah kurangnya frekuensi pelatihan bagi pegawai yakni terkait dengan keamanan informasi.

Tabel 7. Hasil dari *Rating Process Activities* APO14

Process	Level				
	1	2	3	4	5
Nilai		100	73,2		
Skala Penilaian		F	L		
Kapabilitas			Level 3		
Keterangan: N (Not Achieved, 0 – 15), P (Partially Achieved, > 15% - 50), L (Largely Achieved, > 50% - 85%), F (Fully Achieved, > 85% - 100%)					

Berdasarkan Tabel 7, proses *Continuity Management* atau APO 14 telah mencapai tingkat 3 (*Defined*) dengan tingkat pencapaian aktivitas sebesar 73,2%. Namun, masih terdapat beberapa hambatan yang perlu diperhatikan, salah satunya adalah evaluasi kualitas data yang belum dilakukan secara rutin dan tidak memiliki jadwal yang terstruktur. Faktor utama yang kemungkinan mempengaruhi kondisi ini adalah kurangnya koordinasi antara manajemen dan pegawai dalam upaya meningkatkan kualitas data.

Tabel 8. Hasil *Rating Process Activities* DSS05

Process	Level				
	1	2	3	4	5
Nilai		100%	70,5%		
Skala Penilaian		F	L		
Kapabilitas			Level 3		
Keterangan: N (Not Achieved, 0% – 15%), P (Partially Achieved, > 15% - 50%), L (Largely Achieved, > 50% - 85%), F (Fully Achieved, > 85% - 100%)					

Mengacu pada Tabel 8, proses *IT Knowledge Management* atau DSS05 telah mencapai tingkat 3 (*Defined*) dengan tingkat pencapaian aktivitas sebesar 70,5%. Meskipun demikian, masih terdapatnya beberapa tantangan yang perlu diperhatikan, seperti rendahnya tingkat keamanan fisik. Penerapan firewall, antivirus, serta perangkat keamanan lainnya di sekitar server fisik masih belum maksimal dan memerlukan perhatian lebih lanjut, termasuk dalam aspek kebijakan yang mendukungnya. Berdasarkan Tabel 4-8, tingkat kapabilitas dapat dihitung menggunakan hasil kuesioner sebagai berikut:

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

Hasil analisis menunjukkan bahwa PT XYZ telah mencapai tingkat kapabilitas 3 (*Defined*). Pada level ini, proses sudah diterapkan, tetapi masih belum dilengkapi dengan mekanisme pengukuran yang optimal.

Gap Analysis

Analisis kesenjangan ini bertujuan untuk mengidentifikasi perbedaan antara kondisi saat ini dengan standar atau target yang ditetapkan dalam COBIT 2019. Berikut merupakan hasil *gap analysis* berdasarkan penilaian aktivitas proses.

Tabel 9. 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

Hasil analisis kesenjangan mengindikasikan bahwa keamanan Sistem Informasi Manajemen Rumah Sakit di PT XYZ masih berada pada level 3 (*Defined*) dan belum mencapai tingkat kapabilitas yang ditargetkan, yaitu level 4 (*Quantitative*). Hal ini menandakan bahwa kondisi saat ini masih berada satu tingkat di bawah standar yang diharapkan.

Rekomendasi Mitigasi

Berdasarkan hasil analisis kesenjangan yang telah dilakukan, terdapat beberapa langkah mitigasi yang dapat diterapkan oleh PT XYZ guna meningkatkan keamanan sistem informasi mereka. Pada proses EDM03 (*Ensuring Information Security Risk Management*), PT XYZ disarankan untuk meningkatkan efektivitas identifikasi dan pengelolaan risiko keamanan informasi melalui evaluasi berkala dengan metode yang lebih sistematis. Profil risiko perlu diperbarui secara rutin agar tetap relevan dengan ancaman yang berkembang. Langkah-langkah yang dapat diterapkan meliputi penggunaan analisis SWOT untuk mengidentifikasi risiko, implementasi *vulnerability scanner* untuk mendeteksi celah keamanan, serta mempertimbangkan sertifikasi keamanan seperti ISO 27001 atau HIPAA. Selain itu, pengujian penetrasi (*penetration testing*) perlu dilakukan untuk mengidentifikasi kelemahan dalam sistem, serta penerapan *Web Application Firewall* (WAF), database firewall, sistem deteksi dan pencegahan intrusi (IDS/IPS), dan enkripsi data menggunakan SSL/TLS guna memastikan keamanan komunikasi dan penyimpanan data.

Pada proses APO12 (*Risk Management*), PT XYZ perlu memastikan pencatatan dan analisis insiden keamanan dilakukan secara menyeluruh dan berkelanjutan, dengan pengelompokan insiden yang lebih sistematis agar evaluasi dan tindakan mitigasi dapat dilakukan dengan lebih efektif. Beberapa strategi yang dapat diterapkan meliputi implementasi *Information Security Management System* (ISMS) berbasis standar industri seperti ISO 27001, pengembangan sistem pencatatan insiden otomatis, serta penggunaan algoritma machine learning untuk mengklasifikasikan insiden berdasarkan pola yang teridentifikasi. Selain itu, penerapan *Security Information and Event Management* (SIEM) dapat membantu dalam pemantauan dan analisis ancaman secara *real-time*. Pada proses APO13 (Security Management), peningkatan kesadaran pegawai terhadap keamanan informasi menjadi salah satu aspek penting dalam menjaga keamanan sistem. Oleh karena itu, PT XYZ disarankan untuk lebih aktif dalam menyelenggarakan pelatihan dan sertifikasi bagi pegawai yang berkaitan dengan keamanan informasi. Materi pelatihan dapat mencakup aspek keamanan seperti cara mendeteksi serangan phishing, pentingnya penggunaan kata sandi yang kuat, serta langkah-langkah dalam menjaga keamanan data. Selain itu, pegawai juga dapat diberikan kesempatan untuk memperoleh sertifikasi keamanan seperti CISSP, CISM, atau CompTIA Security+. Penerapan kebijakan yang lebih ketat dalam penggunaan perangkat dan jaringan internal juga dapat membantu mengurangi risiko kebocoran informasi.

Pada proses APO14 (*Continuity Management*), PT XYZ perlu meningkatkan koordinasi antara manajemen dan pegawai dalam pengelolaan dan peningkatan kualitas data. Salah satu cara yang dapat dilakukan adalah dengan membentuk tim khusus yang bertanggung jawab terhadap pemantauan dan evaluasi kualitas data. Tim ini perlu menetapkan metrik kualitas data yang relevan, seperti tingkat akurasi, konsistensi, dan kelengkapan data. Selain itu, penyelenggaraan pertemuan rutin antara manajemen dan pegawai dapat membantu mengidentifikasi serta mengatasi permasalahan yang muncul dalam pengelolaan data. Pada proses DSS05 (*IT Knowledge Management*), keamanan fisik server perlu ditingkatkan untuk mengurangi potensi akses tidak sah dan risiko pencurian data. PT XYZ disarankan untuk menerapkan sistem pengawasan ketat terhadap area server, seperti pemasangan kamera pengawas (CCTV), pembatasan akses hanya untuk pihak yang berwenang dengan kartu akses atau fingerprint, serta penerapan sistem pemantauan aktivitas server secara berkala. Selain itu, firewall dan antivirus perlu diperbarui secara rutin untuk melindungi infrastruktur TI dari ancaman eksternal. Penggunaan *Virtual Private Network* (VPN) untuk akses jarak jauh ke server juga dapat meningkatkan keamanan koneksi. Langkah mitigasi tambahan yang disarankan meliputi pencadangan data secara berkala dan penyimpanan salinan cadangan di lokasi yang aman untuk memastikan data tetap tersedia saat terjadi gangguan atau insiden tak terduga. Dengan menerapkan langkah-langkah mitigasi ini, PT XYZ diharapkan dapat meningkatkan keamanan sistem informasi mereka, menjaga stabilitas operasional, serta memenuhi standar keamanan yang sesuai dengan kebutuhan industri.

KESIMPULAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa tingkat keamanan Sistem Informasi Manajemen Rumah Sakit (SIMRS) di RS XYZ telah mencapai level 3 (*Defined*) sesuai dengan audit menggunakan kerangka kerja COBIT 2019. Evaluasi terhadap proses-proses seperti EDM03, APO12, APO13, APO14, dan DSS05 menunjukkan bahwa sebagian besar aspek keamanan sistem telah diterapkan sesuai standar yang berlaku. Meskipun demikian, agar kepatuhan terhadap standar keamanan informasi tetap terjaga serta untuk mengurangi potensi risiko, diperlukan perbaikan yang berkelanjutan dan peningkatan sistem secara bertahap di lingkungan rumah sakit. Rekomendasi mitigasi yang telah diusulkan sebelumnya perlu segera diterapkan guna meningkatkan efektivitas serta kapabilitas sistem informasi di RS XYZ. Walaupun sistem ini telah mencapai tingkat keamanan yang cukup baik, perbaikan dan pengembangan yang berkelanjutan tetap diperlukan guna mengatasi kelemahan yang telah diidentifikasi serta mengoptimalkan strategi mitigasi risiko di masa mendatang. Hasil audit menunjukkan bahwa RS XYZ telah berhasil memenuhi tingkat keamanan yang layak berdasarkan kerangka kerja COBIT 2019. Namun, upaya peningkatan harus

terus dilakukan agar rumah sakit tetap memenuhi standar keamanan informasi yang berlaku serta mampu mengantisipasi ancaman dan risiko yang mungkin terjadi di masa depan.

Untuk penelitian selanjutnya, terdapat beberapa saran yang dapat dipertimbangkan guna memperluas cakupan analisis dan meningkatkan efektivitas penelitian. Salah satunya adalah memperdalam kajian mengenai manajemen risiko dalam sistem informasi rumah sakit atau strategi pengelolaan layanan sistem informasi rumah sakit. Studi lanjutan juga dapat mencakup identifikasi serta evaluasi risiko yang lebih menyeluruh, penyusunan kebijakan keamanan yang lebih komprehensif, serta peningkatan kesadaran pengguna terhadap pentingnya keamanan informasi dalam operasional rumah sakit.

DAFTAR PUSTAKA

Abror, N., Delvika, B., Rahayu, D. S., Zikri, M. H., Putra, H. D., & Megawati, M. (2024). Tata Kelola Audit Sistem Informasi Pada BMKG Stasiun Meteorologi SSK II Pekanbaru Menggunakan COBIT 2019. *Jurnal Testing dan Implementasi Sistem Informasi*, *2*(1), 28-38. https://doi.org/10.57152/malcom.v4i3.1320.

Algiffary, A., M. Izman Herdiansyah, & Yesi Novaria Kunang. (2023). Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI. *Journal of Applied Computer Science and Technology*, *4*(1), 19 - 26. https://doi.org/10.52158/jacost.v4i1.505.

Binta, A. P. (2025). Peran Manajemen Risiko Dalam Meningkatkan Keselamatan Pasien di Fasilitas Kesehatan. *Jurnal Riset Multidisiplin Edukasi*, *2*(2), 107-122. https://doi.org/10.71282/jurmie.v2i2.130.

Effendy, C. A. ., Paramarta, V. ., & Purwanda, E. . (2024). Peran Teknologi Informasi, Pengelolaan Sumber Daya Manusia, Dan Sistem Informasi Rumah Sakit Dalam Meningkatkan Kinerja Rumah Sakit (Kajian Literatur). *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *7*(4), 13479–13489. https://doi.org/10.31004/jrpp.v7i4.34703.

Kuncoro, D., Mairani, M., & Putri, N. Y. (2024). Analisa Audit Sistem Informasi Barang Atau Jasa PT. Jaya Karya Menggunakan COBIT 5.0. *Bridge: Jurnal publikasi Sistem Informasi dan Telekomunikasi*, *2*(3), 24-32. https://doi.org/10.62951/bridge.v2i3.96.

Ndraha, A. B., Waruwu, E., & Zega, A. (2024). Dinamika pelayanan publik di BKPSDM Kota Gunungsitoli: Analisis terhadap prosedur kendala dan rapat evaluatif. *Jurnal Ilmu Ekonomi, Pendidikan Dan Teknik*, *1*(2), 32-39. https://doi.org/10.70134/identik.v1i2.38.

Nugroho, F., & Ali, H. (2022). Determinasi SIMRS: Hardware, Software Dan Brainware (Literature Review Executive Support Sistem (ESS) For Business). *Jurnal Manajemen Pendidikan Dan Ilmu Sosial*, *3*(1), 254-265. https://doi.org/10.38035/jmpis.v3i1.871.

Rambe, D. H., Lubis, M., Ritonga, N., & Purba, S. H. (2025). Solusi Teknologi SIMRS dalam Meningkatkan Kualitas Layanan Kesehatan Publik di Indonesia. *Jurnal Riset Ilmu Kesehatan Umum dan Farmasi (JRIKUF)*, *3*(1), 33-43. https://doi.org/10.57213/jrikuf.v3i1.488.

Setiorini, A., Natasia, S. R., Wiranti, Y. T., & Ramadhan, D. A. (2021). Evaluation of the application of hospital management information system (SIMRS) in RSUD Dr. Kanujoso Djatiwibowo using the HOT-Fit method. *Journal of Physics: Conference Series, 1726*(1), 012011. https://doi.org/10.1088/1742-6596/1726/1/012011.

Siregar, H., Fitriani, A., Fitria, A., Efendy, I., & Nuraini, N. (2024). Analisis Implementasi Sistem Informasi Rumah Sakit Terhadap Pelayanan Administrasi Rumah Sakit Haji Syaiful Anwar. *urnal romotif reventif*, *7*(5), 1011-1021. https://doi.org/10.47650/jpp.v7i5.1513

Sodik, I. A., & Nugraheni, D. M. K. (2022). Implementation Cobit 2019 For Evaluation Of Health Clinic Information System Governance In Central Java. *Jurnal Teknik Informatika (Jutif)*, *3*(6), 1549-1556. https://doi.org/10.20884/1.jutif.2022.3.6.361.