Terbit online pada laman web jurnal: **http://journal.isas.or.id/index.php/JACOST**

JOURNAL OF APPLIED COMPUTER SCIENCE AND TECHNOLOGY (JACOST)

Vol. 4 No. 1 (2023) 19 – 26 | ISSN: 2723-1453 (Media Online)

Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI

M. Arief Algiffary[1], M. Izman Herdiansyah[2], Yesi Novaria Kunang[3]
[1,2,3]Program Studi Magister Teknik Informatika Universitas Bina Darma
[1]ariefalgiffary@gmail.com, [2]muhammad_izman_herdiansyah@binadarma.ac.id, [3]yesinovariakunang@binadarma.ac.id

Abstract

This study examines the implementation of information system at RSUD Palembang BARI with the aim of enhancing information system security. In this context, a security audit is conducted using the COBIT 2019 framework. The COBIT 2019 domains and processes utilizing include EDM03, APO12, APO13, APO14, and DSS05. The research involves the identification and evaluation of information security risks, determination of necessary security controls, and ensuring compliance with the information security standards established by COBIT 2019. The findings indicate that the level of information system security at RSUD Palembang BARI is at level 3 (Defined), with a gap analysis difference of 1 level below the expected target. Based on the above results, efforts to improve and enhance the information system security at RSUD Palembang BARI are still needed. The use of information system security techniques such as vulnerability scanning, penetration testing, WAF, IDS and IPS, and data encryption, as well as improving security in terms of server physical aspects such as installing CCTV and restricting user access with access cards or fingerprints, can be implemented to ensure compliance with relevant information security standards. Consideration for obtaining security certifications, like ISO 27001, should also be taken. Additionally, the quality of human resources in terms of policy-making and the ability of employees to address threats and attacks on information system security should be improved through training and strengthening coordination among employees.

Keywords: Security Audit, Information System, Hospital Management Information System, Information System Security, COBIT 2019, RSUD Palembang BARI

Abstrak

Penelitian ini mengkaji implementasi sistem informasi pada RSUD Palembang BARI dengan tujuan untuk meningkatkan keamanan sistem informasi. Dalam konteks ini, audit keamanan dilakukan menggunakan kerangka kerja *COBIT 2019*. Domain dan proses *COBIT 2019* yang digunakan meliputi *EDM03*, *APO12*, *APO13*, *APO14*, dan *DSS05*. Penelitian ini melibatkan identifikasi dan evaluasi risiko keamanan informasi, penentuan kontrol keamanan yang diperlukan, serta memastikan kepatuhan terhadap standar keamanan informasi yang ditetapkan oleh *COBIT 2019*. Hasil penelitian menunjukkan bahwa tingkat keamanan sistem informasi RSUD Palembang BARI berada pada tingkat 3 *(Defined)*, dengan selisih gap analysis sebesar 1 tingkat di bawah tingkat yang diharapkan. Berdasarkan hasil di atas, masih diperlukan upaya perbaikan dan peningkatan keamanan sistem informasi yang harus dilakukan oleh RSUD Palembang BARI. Penggunaan teknik keamanan sistem informasi, semacam *vulnerability scanning*, *penetration testing*, *WAF, IDS* dan *IPS*, dan enkripsi data, serta peningkatan keamanan dalam segi fisik server, seperti pemasangan CCTV dan pembatasan akses pengguna dengan a*ccess card* atau *fingerprint* dapat dilakukan untuk memastikan kepatuhan terhadap standar keamanan informasi yang relevan terjaga. Pertimbangan untuk mendapatkan sertifikasi keamanan, seperti *ISO 27001*, juga perlu dilakukan. Selain itu, peningkatan kualitas SDM mengenai kebijakan yang diambil serta kemampuan pegawai dalam menghadapi ancaman dan serangan terhadap keamanan sistemn informasi juga perlu ditingkatkan dengan pelatihan-pelatihan dan mempererat koordinasi antar pegawai.

Kata kunci: Audit Keamanan, Sistem Informasi, SIM-RS, Keamanan Sistem Informasi, *COBIT 2019*, RSUD Palembang BARI

1. Pendahuluan

Rumah sakit adalah institusi yang menyediakan pelayanan perawatan kesehatan dengan menggunakan berbagai fasilitas, teknologi, dan sumber daya manusia yang terlatih [1]. Sebagai aset penting, rumah sakit harus mengikuti perkembangan zaman. Penggunaan teknologi informasi merupakan indikator suatu institusi mengikuti perkembangan zaman.

Penggunaan teknologi informasi pada rumah sakit menjadi semakin penting dalam menghadapi tantangan dan perubahan dalam industri kesehatan. Teknologi informasi memainkan peran penting dalam membantu rumah sakit meningkatkan efisiensi, mengurangi biaya, dan meningkatkan kualitas pelayanan untuk pasien [2].

Salah satu contoh penggunaan teknologi informasi pada rumah sakit adalah Sistem Informasi Manajemen Rumah

Sakit (SIM-RS). SIM-RS adalah sistem yang dirancang untuk mengelola, menyimpan, mengambil, dan menganalisis data kesehatan pasien. Sistem ini memungkinkan penggunaannya di seluruh departemen dan memfasilitasi pengambilan keputusan klinis dan manajerial [3]. SIM-RS meliputi aplikasi medis, sistem informasi laboratorium, sistem informasi radiologi, sistem informasi farmasi, dan lain sebagainya.

RSUD Palembang BARI, sebagai salah satu rumah sakit terbesar di Kota Palembang, telah mengimplementasikan SIM-RS sebagai bagian penting dalam upaya mereka untuk mempercepat pertumbuhan serta meningkatkan daya saing. Sebagai institusi yang berfokus pada pemberian pelayanan optimal kepada masyarakat, ketersediaan sistem informasi yang dapat mempermudah proses pelayanan sangatlah penting. Berdasarkan tujuan tersebut, RSUD Palembang BARI membangun SIM-RS yang bertujuan untuk memenuhi, meningkatkan, dan mempermudah segala proses administratif terkait pelayanan pasien, manajemen informasi, akuntansi, dan pengadaan barang [4].

Namun, penggunaan teknologi informasi juga mengakibatkan meningkatnya risiko keamanan informasi, seperti ancaman peretasan, pencurian data, dan penyebaran malware. Untuk meminimalisir hal tersebut, sebuah audit keamanan perlu diterapkan. Audit keamanan sistem informasi rumah sakit adalah proses pengecekan dan evaluasi sistem informasi dan praktik keamanan yang digunakan oleh rumah sakit untuk memastikan bahwa keamanan data pasien terjaga dan sistem tersebut terlindungi dari ancaman luar atau dalam [5]. Oleh karena itu, audit keamanan sistem informasi menjadi sangat penting untuk memastikan bahwa SIM-RS terlindungi dari ancaman keamanan terhadap keberlangsungan operasi rumah sakit.

Control Objectives for Information and Related Technology (COBIT) 2019 adalah kerangka kerja pengelolaan teknologi informasi yang luas dan terpadu yang membantu organisasi mencapai tujuan bisnis mereka dengan menggunakan teknologi informasi. Dengan *COBIT 2019*, rumah sakit dapat melakukan audit dengan mengidentifikasi dan mengevaluasi risiko keamanan informasi, menentukan kontrol keamanan yang diperlukan, dan memastikan bahwa kontrol keamanan tersebut sesuai dengan standar keamanan informasi yang ditetapkan oleh *COBIT 2019* [6]. Dengan demikian, audit keamanan dengan *COBIT 2019* dapat membantu rumah sakit meningkatkan keamanan informasi dan memenuhi standar keamanan informasi yang ditetapkan oleh organisasi dan regulasi yang relevan.

1.1. Sistem Informasi Manajemen Rumah Sakit

Menurut [7], Sistem Informasi Manajemen Rumah Sakit (SIM-RS) adalah sistem yang terdiri dari perangkat keras dan lunak yang mengintegrasikan data kesehatan pasien, termasuk data administratif, klinis, dan keuangan. Sistem ini memberikan dukungan untuk keputusan klinis dan manajerial, serta memungkinkan kolaborasi antara departemen dan profesional kesehatan. Sedangkan [8] berpendapat, SIM-RS adalah sebuah sistem yang mengumpulkan, memproses, menyimpan, dan membagikan informasi kesehatan pasien secara terstruktur dan terpadu, dengan tujuan meningkatkan efisiensi dan efektivitas pelayanan kesehatan.

Dari kutipan jurnal-jurnal di atas, dapat disimpulkan bahwa SIM-RS adalah sistem yang dirancang untuk mengumpulkan, mengelola, dan menyimpan data kesehatan pasien secara terstruktur dan terintegrasi. Sistem ini terdiri dari perangkat keras dan lunak yang memungkinkan penggunaannya di seluruh departemen, dan memfasilitasi pengambilan keputusan klinis dan manajerial. Sistem ini juga dapat digunakan untuk memperbaiki efisiensi, efektivitas, dan kualitas pelayanan kesehatan, serta meningkatkan keselamatan pasien.

1.2. Keamanan Sistem Informasi

Keamanan sistem informasi adalah perlindungan terhadap akses, penggunaan, pengungkapan, modifikasi, atau kerusakan data secara tidak sah, dan juga perlindungan terhadap ancaman yang datang dari pengguna internal maupun eksternal [9]. Keamanan sistem informasi memiliki kaitan erat dengan keamanan informasi yang berfokus pada beberapa hal [10], seperti *Confidentiality* (Kerahasiaan), informasi hanya boleh diakses oleh pihak berwenang, sehingga dapat terhindar dari pihak yang tidak berhak, *Integrity* (Integritas), informasi harus tetap utuh dan tidak berubah, baik itu dari segi isi maupun dari segi asal usulnya, *Availability* (Ketersediaan), informasi harus dapat diakses oleh pihak yang berhak setiap saat dan dimana saja, *Authenticity* (Keaslian), informasi harus dapat dipercaya keasliannya dan tidak dimanipulasi, *Non-repudiation* (Ketiadaan Penyangkalan), pihak yang terlibat dalam pertukaran informasi tidak dapat menyangkal atau membantah kebenaran dari transaksi atau pertukaran informasi tersebut, dan *Accountability* (Pertanggungjawaban), setiap pihak yang mengakses informasi atau terlibat dalam transaksi atau pertukaran informasi harus dapat dipertanggungjawabkan atas tindakan yang dilakukannya terhadap informasi tersebut.

1.3. Audit Keamanan Sistem Informasi

Menurut [11], audit keamanan sistem informasi adalah proses pengumpulan bukti untuk mengevaluasi keamanan sistem informasi secara keseluruhan, termasuk kebijakan, prosedur, kontrol, dan infrastruktur teknologi informasi. Audit ini bertujuan untuk memastikan bahwa sistem informasi memenuhi kebutuhan keamanan organisasi dan meminimalkan risiko keamanan informasi.

Terdapat beberapa kerangka kerja dan metode audit keamanan sistem informasi, serta standar dan regulasi terkait keamanan sistem informasi yang dapat digunakan,

DOI : https://doi.org/10.52158/jacost.505

seperti *COBIT*, *ISO 27001*, *HIPAA*, dan lainnya. Alat dan teknik yang digunakan dalam audit keamanan sistem informasi, seperti *vulnerability scanner*, *penetration testing*, dan *social engineering*. Hasil dan temuan audit keamanan sistem informasi yang umumnya meliputi kelemahan keamanan, risiko, dan rekomendasi perbaikan.

1.4. *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. Menurut [12], *COBIT 2019* berfokus kepada dua hal, yaitu sistem tata kelola dan kerangka tata kelola. *COBIT 2019* memiliki 6 komponen tata kelola, yaitu proses, struktur organisasi, prinsip, informasi, budaya organisasi, SDM, dan layanan infrastruktur serta aplikasinya.

COBIT 2019 memiliki domain yang dilambangkan dengan kata kerja yang mengungkapkan tujuan utama dan area aktifitas yang terkandung di dalamnya, di dalam domain terdapat proses yang merupakan kumpulan aktivitas untuk mencapai tujuan TI secara keseluruhan. Daftar domain pada *COBIT 2019 adalah sebagai berikut: Evaluate, Direct and Monitor (EDM)*, bertujuan untuk mengelompokkan tujuan tata kelola perusahaan, *Align, Plan and Organize (APO)*, membahas organisasi secara keseluruhan, strategi, dan aktivitas yang mendukung teknologi dan informasi perusahaan, *Build, Acquire and Implement (BAI)*, membahas perancangan,akuisisi dan implementasi solusi TI termasuk integrasi proses bisnis, *Deliver, Service and Support (DSS)*, domain ini membahas tentang dukungan operasional dan dukungan layanan TI, dan *Monitoring, Evaluate, and Assess (MEA)*, membahas tentang pemantauan kinerja dan kesesuaian TI dengan target kinerja serta tujuan pengendalian internal dan eksternal.

Kemudian, dari proses tersebut dilakukan penilaian kapabilitas pada *COBIT 2019* yang dibagi menjadi 6 tingkatan, yaitu *Level 0 (Incomplete)*, *Level 1 (Initial)*, *Level 2 (Managed)*, *Level 3 (Defined)*, *Level 4 (Quantitative)*, dan *Level 5 (Optimising)*.

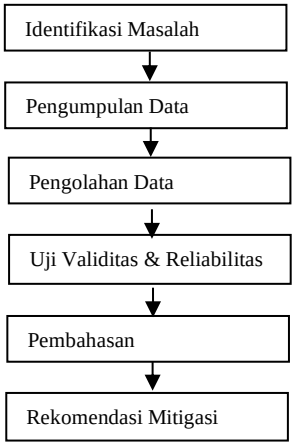
Penilaian kapabilitas pada *COBIT 2019* juga dapat dibantu dengan melakukan pemeringkatan pada aktivitas-aktivitas proses dengan pemeringkatan seperti *Fully (F)*, penilaian kapabilitas pada nilai 85-100, *Largely (L)*, penilaian kapabilitas pada nilai 50-85, *Partially (P)*, penilaian kapabilitas pada nilai 15-50, dan *Not (N)*, penilaian kapabilitas kurang dari 15 persen

1.5. Penelitian Terkait

Sejumlah penelitian telah dilakukan untuk mengevaluasi keamanan sistem informasi rumah sakit menggunakan *COBIT 2019* sebagai kerangka kerja audit. Salah satu hasil penelitian menunjukkan bahwa penggunaan *COBIT 2019* sebagai kerangka kerja audit keamanan apat membantu rumah sakit dalam mengidentifikasi kelemahan pada sistem informasi dan menetapkan rekomendasi untuk meningkatkan keamanan. Selain itu, penggunaan *COBIT 2019* juga dapat membantu meningkatkan efisiensi dan efektivitas penggunaan sumber daya teknologi informasi pada rumah sakit [13]. Penelitian tersebut dipertegas oleh penelitian [14], yang mengatakan bahwa audit keamanan sistem informasi di rumah sakit dan peran *COBIT 2019* sebagai kerangka kerja dapat membantu rumah sakit dalam meningkatkan keamanan informasi pasien dan meminimalkan risiko pelanggaran data kesehatan. Hasil yang sama juga didapatkan dari penelitian [15].

2. Metode Penelitian

Penelitian bersifat kuantitatif ini dilakukan di Unit Instalasi IT RSUD Palembang BARI. Penelitian menggunakan *COBIT 2019* sebagai variabel dependen dan Keamanan SIM-RS sebagai variabel independen dengan domain serta proses *EDM03 (Ensuring Information Security Risk Management)*, *APO12 (Risk Management)*, *APO13 (Security Management)*, *APO14 (Continuity Management)*, and *DSS05 (IT Knowledge Management)*. Identifikasi masalah dilakukan dengan mengadakan wawancara kepada pegawai-pegawai terkait keamanan sistem informasi di RSUD Palembang BARI. Pengukuran variabel dilakukan menggunakan kuesioner dengan skala likert 5 poin yang akan disebar kepada sampel yang ditentukan berdasarkan *RACI (Responsible, Accountable, Consulted, and Informed) Analysis*. Hasil respon dari kuesioner diuji dengan uji validitas dan uji reliabilitas. Setelah kedua pengujian selesai, dilakukan *rating process activities* untuk mengetahui tingkat kapabilitas Unit Instalasi IT Rumah Sakit RSUD Palembang BARI dalam mengelola keamanan sistem informasi. Dari hasil *rating process activities*, selanjutnya dilakukan *gap analysis* untuk mengetahui selisih gap yang dihasilkan pada keadaan sekarang *(as is)* dan yang diharapkan *(to be)*. Berdasarkan hasil dari gap analysis tersebut dapat disimpulkan beberapa rekomendasi mitigasi risiko untuk memperkecil selisih gap yang ada pada saat ini.



Gambar 1. Kerangka Kerja Penelitian

DOI : https://doi.org/10.52158/jacost.505

3. Hasil dan Pembahasan

3.1. *RACI Analysis*

RACI analysis adalah sebuah alat manajemen proyek yang digunakan untuk memperjelas tanggung jawab dan keterlibatan setiap individu dalam sebuah tim atau organisasi. *RACI Analysis (Responsible, Accountable, Consulted, and Informed)* pada domain *EDM (Evaluate, Direct, and Monitor)*, *APO (Align, Plan, and Organize)*, dan *DSS (Deliver, Service and Support)* dijelaskan pada Tabel 1.

Tabel 1. Hasil *RACI Analysis*

Key Management Practices	Direktur Rumah Sakit	Ka. Unit Instalasi IT	Unit Instalasi IT	Staff Admin.	Staff Lain
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*	*R*	*A*	*I*
APO13.02	*C*	*C*	*R*	*A*	*I*
APO13.03	*C*	*C*	*R*	*A*	*I*
APO14.01	*R*	*R*	*I*	*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*

Dari *RACI Analysis* di atas, dapat disimpulkan bahwa Unit Instalasi IT RSUD Palembang BARI memegang tanggung jawab terbesar dalam menjaga keamanan sistem informasi di RSUD Palembang BARI. Hal ini dapat dilihat dari banyaknya peran *responsible* (tanggung jawab) dari RACI Analysis yang dilakukan.

3.2. Uji Validitas

Uji validitas adalah pengujian untuk mengukur valid atau tidaknya suatu instrumen. Sebuah instrumen dikatakan valid jika pernyataan pada instrumen mampu mengungkapkan sesuatu yang akan diukur oleh instrumen tersebut. Tabel 2 menunjukkan hasil uji validitas terhadap pernyataan-pernyataan yang digunakan.

Tabel 2. Hasil Uji Validitas

Proses	rHitung	rTabel	*Sig.*	Keterangan
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

Berdasarkan data pada Tabel 2 dapat disimpulkan bahwa semua pernyataan pada kuesioner valid dengan *level significant* 5%, dikarenakan rHitung > rTabel.

3.3. Uji Reliabilitas

Uji reliabilitas adalah pengujian untuk mengukur konsistensi hasil pengukuran dari instrumen dalam penggunaan yang berulang. Jawaban responden terhadap pernyataan dikatakan reliabel jika masing-masing pernyataan dijawab secara konsisten atau jawaban tidak boleh acak. Tabel 3 menunjukkan hasil uji reliabilitas terhadap pernyataan-pernyataan yang digunakan.

Tabel 3. Hasil Uji Reliabilitas

Proses	*Cronbach's Alpha*	Cut off	Keterangan
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 uji reliabilitas di atas menunjukkan bahwa semua variabel memiliki nilai koefisien *cronchbach's alpha* > 0,60 sehingga dapat dikatakan semua pernyataan yang digunakan reliabel.

3.4. *Rating Process Activities*

Perhitungan tingkat kapabilitas didasarkan pada hasil *rating process activities* dari data kuesioner yang dihasilkan dari responden. *Rating process activities* berguna untuk mengukur sejauh mana proses dalam kerangka kerja *COBIT 2019* yang dianalisa tersebut telah memenuhi tujuan dan kontrol yang ditetapkan. Tabel 4-8 berikut menyajikan hasil analisis kapabilitas pada proses *COBIT 2019*.

Tabel 4. Hasil *Rating Process Activities EDM03*

Proses	Level 1	Level 2	Level 3	Level 4	Level 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%)

Berdasarkan Tabel 4, proses *EDM03 (Ensuring Information Security Risk Management)* telah mencapai tingkat 3 *(Defined)* dengan pencapaian aktivitas sebesar 71,2%. Namun, masih terdapat beberapa hambatan dalam pelaksanaan aktivitas proses tersebut, antara lain kurangnya pemantauan dan perbaruan profil risiko, serta

DOI : https://doi.org/10.52158/jacost.505

evaluasi sistem yang belum optimal, seperti belum adanya penggunaan analisis risiko, belum mendapatkan sertifikasi keamanan, serta belum melakukan metode atau teknik dalam memantau keamanan sistem.

Tabel 5. Hasil *Rating Process Activities APO12*

Proses	Level 1	Level 2	Level 3	Level 4	Level 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%)

Tabel 5 menunjukkan bahwa proses *APO12 (Risk Management)* telah mencapai tingkat 3 *(Defined)*, dengan pencapaian aktivitas sebesar 72,5%. Berdasarkan tabel di atas, masih terdapat beberapa kendala, seperti belum adanya dokumentasi mengenai pencatatan riwayat kejadian risiko (jika pun ada, belum dilakukan pengelompokkan kejadian secara mendalam dan juga belum mengikuti standar industri yang ditetapkan), serta belum diperbaruinya skenario risiko TI secara teratur.

Tabel 6. Hasil *Rating Process Activities APO13*

Proses	Level 1	Level 2	Level 3	Level 4	Level 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%)

Tabel 6 menunjukkan bahwa proses *APO13 (Security Management)* telah mencapai tingkat 3 *(Defined)*, dengan pencapaian aktivitas sebesar 70,3%. Namun, masih terdapat beberapa kendala yang perlu diperhatikan, seperti pelatihan pegawai terkait keamanan informasi jarang dilaksanakan.

Tabel 7. Hasil *Rating Process Activities APO14*

Proses	Level 1	Level 2	Level 3	Level 4	Level 5
Nilai		94%	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%)

Tabel 7 menunjukkan bahwa proses *APO14 (Continuity Management)* telah mencapai tingkat 3 *(Defined)*, dengan pencapaian aktivitas sebesar 73,2%. Berdasarkan tabel di atas, masih terdapat beberapa kendala yang perlu diperhatikan. Salah satunya adalah penilaian kualitas data dilakukan secara jarang dan belum terjadwal secara berkala. Hal ini dapat dikarenakan oleh sinergi antara manajemen dan pegawai dalam mengembangkan kualitas data masih sangat kurang.

Tabel 8. Hasil *Rating Process Activities DSS05*

Proses	Level 1	Level 2	Level 3	Level 4	Level 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%)

Tabel 8 menunjukkan bahwa proses *DSS05 (IT Knowledge Management)* telah mencapai tingkat 3 *(Defined)*, dengan pencapaian aktivitas sebesar 70,5%. Namun, berdasarkan tabel di atas, masih terdapat beberapa kendala yang perlu diperhatikan seperti tingkat keamanan secara fisik yang masih terbilang rendah. Belum maksimalnya penggunaan *firewall* dan *antivirus* atau ala-alat keamanan di sekitar fisik server perlu diperhatikan, juga mengenai kebijakan di sekitar itu.

Dari tabel 4-8 di atas, dapat dihitung tingkat kapabilitas berdasarkan hasil dari kuesioner sebagai berikut:

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

Hasil dari penghitungan menunjukkan tingkat kapabilitas yang dicapai oleh RSUD Palembang BARI adalah tingkat 3 *(Defined)*, dimana pada tingkatan ini proses sudah dilaksanakan, tetapi masih belum dilakukan pengukuran.

3.5. *Gap Analysis*

Gap analysis adalah proses perbandingan antara kondisi saat ini *(as-is)* dengan kondisi yang diinginkan *(to-be)* dalam kerangka kerja *COBIT 2019*. Hal ini dilakukan untuk mengidentifikasi gap atau kesenjangan antara kondisi yang ada dengan standar atau tujuan yang ditetapkan dalam *COBIT 2019*. Berikut ini adalah *gap analysis* yang didapat dari hasil *rating process analysis*:

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

Selisih gap ini menunjukkan keamanan pada Sistem Informasi Manajemen Rumah Sakit di RSUD Palembang BARI masih berada pada tingkat 3 *(Defined)*, dan belum mencapai tingkat kapabilitas yang diharapkan pada tingkat 4 *(Quantitative)*. Selisih gap pada penelitian ini adalah 1 tingkat di bawah kondisi yang diharapkan.

3.6. Rekomendasi Mitigasi

Dari hasil *gap analysis* di atas, peneliti menyimpulkan beberapa rekomendasi mitigasi untuk dipertimbangkan sebagai bahan evaluasi RSUD Palembang BARI dalam memperbaiki keamanan sistem informasi. Berikut dijelaskan rekomendasi mitigasi berdasarkan setiap proses.

DOI : https://doi.org/10.52158/jacost.505

Pada *EDM03 Ensuring Information Security Risk Management*, RSUD Palembang BARI perlu melakukan dan meningkatkan penilaian tingkat resiko secara berkala agar rumah sakit dapat mengidentifikasi dan mengelola risiko-risiko yang dapat mengancam keamanan sistem informasi dengan lebih baik, serta mengambil tindakan yang tepat untuk melindungi data, menjaga kerahasiaan, integritas, dan ketersediaan informasi yang vital bagi operasional rumah sakit. RSUD Palembang BARI juga perlu melakukan pembaruan terhadap profil risiko saat ini agar tetap relevan dengan risiko-risiko yang ada. Beberapa hal dapat dilakukan dalam hal ini, seperti melakukan analisis risiko dengan analisis *SWOT (Strengths, Weaknesses, Opportunities, and Threats)*, melakukan pemindaian keamanan sistem dengan *vulnerability scanner*, mempertimbangkan untuk mendapatkan sertifikasi keamanan seperti *ISO 27001* atau *HIPAA*, melakukan *penetration testing* yang akan membantu mengidentifikasi celah keamanan yang dapat dimanfaatkan oleh penyerang, menerapkan prinsip keamanan dalam lapisan yang berbeda dengan teknik *Web Application Firewall (WAF)* atau *database firewall*, melakukan implementasi *Intrusion Detection System (IDS)* atau *Intrusion Prevention System (IPS)*, dan melakukan enkripsi data dengan menggunakan protokol enkripsi seperti *SSL/TLS (Secure Sockets Layer/Transport Layer Security)* untuk melindungi komunikasi data dan enkripsi penyimpanan data. Dengan melakukan peningkatan ini, organisasi dapat lebih efektif dalam mengelola risiko dan menjaga keamanan sistem informasi mereka.

Pada *APO12 Risk Management,* RSUD Palembang BARI perlu melakukan pencatatan dan peninjauan rutin terhadap insiden keamanan yang terjadi serta melakukan pengelompokkan setiap insiden tersebut secara lebih komprehensif untuk memastikan keberlanjutan keamanan sistem dan mencegah gangguan baik dari dalam sistem maupun lingkungan sekitar. Hal ini dilakukan untuk memantau dan mengidentifikasi potensi celah atau gangguan keamanan yang dapat mempengaruhi sistem. Ini melibatkan pencatatan riwayat insiden keamanan, pelaporan kejadian yang mencurigakan, pengelompokkan jenis-jenis insiden, serta melakukan audit keamanan secara rutin. Beberapa hal dapat dilakukan dalam hal ini, seperti melakukan implementasi *Information Security Management System (ISMS)* yang mengikuti standar industri seperti *ISO 27001*, menggunakan sistem pelaporan insiden yang terpusat dan terotomatisasi untuk mencatat setiap insiden keamanan yang terjadi, menggunakan metode *machine learning* dengan algoritma klasifikasi atau sistem kategori yang sesuai untuk mengelompokkan insiden keamanan berdasarkan jenisnya, dan melakukan pemantauan keamanan dengan *Security Information and Event Management (SIEM)*. Dengan melakukan pencatatan dan peninjauan ini, dapat dilakukan tindakan preventif yang tepat untuk menjaga keberlanjutan keamanan sistem.

Pada *APO13 Security Management,* RSUD Palembang BARI perlu meningkatkan secara kuantitas dan kualitas mengenai pelatihan kepada pegawai terkait penggunaan sistem yang aman. Pegawai harus diberikan pelatihan, seperti bagaimana cara menggunakan sistem dengan aman, mengenali serangan phishing, memilih kata sandi yang kuat, dan menghindari tindakan yang dapat membahayakan keamanan sistem. Pelatihan ini membantu meningkatkan kesadaran dan pemahaman pegawai tentang pentingnya keamanan sistem informasi. Beberapa hal dapat dilakukan dalam hal ini, seperti mengikutsertakan pegawai dalam sertifikasi keamanan informasi, seperti *CISSP*, *CISM*, atau *CompTIA Security+*. Pelatihan ini berfokus pada pemahaman mendalam tentang praktik keamanan informasi dan persyaratan keamanan yang relevan, mengikuti pelatihan perlindungan data dan kepatuhan regulasi, semisalnya *GDPR*, pelatihan yang berfokus pada pemahaman tentang perlindungan data pribadi, mengikuti pelatihan sertifikasi *ISO 27001*, standar internasional untuk manajemen keamanan informasi, dan pelatihan keamanan jaringan dan infrastruktur, pelatihan yang akan memperkenalkan pegawai pada konsep dan praktik keamanan jaringan dan infrastruktur, termasuk proteksi firewall, deteksi intrusi, enkripsi, dan keamanan jaringan nirkabel.

Pada *APO14 Continuity Management,* RSUD Palembang BARI perlu meningkatkan komunikasi dan kolaborasi antara manajemen dan pegawai dalam mengembangkan kualitas data untuk memastikan bahwa data tetap berkualitas tinggi sepanjang waktu. Beberapa hal dapat dilakukan dalam hal ini, seperti membentuk tim khusus yang terdiri dari anggota manajemen dan pegawai yang bertanggung jawab untuk memantau dan meningkatkan kualitas data di rumah sakit. Tim ini harus memiliki representasi dari berbagai departemen yang terkait dengan pengelolaan data, seperti IT, medis, keperawatan, dan administrasi, menyeelenggarakan rapat rutin antara manajemen dan pegawai untuk membahas isu-isu terkait pengelolaan data dan keamanan informasi, dan menetapkan metrik dan indikator kualitas data yang relevan, seperti akurasi, kelengkapan, kekonsistenan, dan kebaruan. Lakukan pemantauan rutin terhadap data yang dikumpulkan dan identifikasi masalah atau ketidaksesuaian. Dengan mengatasi kendala ini, organisasi dapat memastikan bahwa data yang mereka kelola dapat diandalkan, akurat, dan berkualitas tinggi, yang pada gilirannya akan mendukung pengambilan keputusan yang lebih baik dan operasional yang efisien.

Dan pada *DSS05 IT Knowledge Management,* RSUD Palembang BARI perlu melakukan peningkatan tingkat keamanan fisik server untuk mencegah akses yang tidak sah dan mengurangi risiko pencurian dan mengimplementasikan prosedur ketat dalam mengawasi

DOI : https://doi.org/10.52158/jacost.505

tamu dan pegawai yang masuk ke dalam area server. Pemindaian data secara rutin pada komputer juga perlu dilakukan secara berkala untuk mencegah infeksi virus dan malware yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan data. Aktifitas *backup data* penting juga perlu dilakukan secara berkala. Aktifitas ini merupakan langkah yang sangat penting dalam melindungi sistem informasi dari serangan malware dan memastikan kelangsungan bisnis. Hal ini memungkinkan pemulihan cepat, melindungi integritas data, dan memberikan perlindungan dalam situasi darurat atau serangan yang tidak terduga. Beberapa hal dapat dilakukan dalam hal ini, seperti pemasangan kamera CCTV yang memantau ruangan server dan area sekitarnya untuk memantau aktivitas yang mencurigakan, memberi batas akses fisik ke ruangan server hanya kepada personal yang membutuhkannya dan terapkan sistem kontrol akses seperti *access card* atau *fingerprint*, mengaktifkan dan mengatur pengumpulan log aktivitas server yang mencakup informasi seperti login, akses file, dan perubahan konfigurasi, memasang dan memperbarui *firewall* dan perangkat lunak antivirus yang handal untuk melindungi server dari ancaman malware dan serangan jaringan, menggunakan *VPN* untuk mengamankan koneksi jarak jauh ke server, sehingga data yang dikirimkan melalui jaringan tidak dapat dibaca oleh pihak yang tidak berwenang, dan melakukan pencadangan data secara teratur dan simpan salinan cadangan di tempat yang aman untuk memastikan ketersediaan data jika terjadi kejadian tak terduga atau bencana.

4. Kesimpulan

Berdasarkan hasil pembahasan di atas maka dapat ditarik kesimpulan bahwa Sistem Informasi Manajemen Rumah Sakit (SIM-RS) RSUD Palembang BARI telah mencapai tingkat keamanan *level* 3 *(Defined)* berdasarkan audit yang dilakukan menggunakan kerangka kerja *COBIT 2019* dengan proses-proses seperti *EDM03*, *APO12*, *APO13*, *APO14*, dan *DSS05.* Untuk memastikan kepatuhan terhadap standar keamanan informasi dan memitigasi risiko potensial, diperlukan upaya perbaikan berkala dan peningkatan sistem secara bertahap pada sistem informasi rumah sakit RSUD Palembang BARI. Rekomendasi mitigasi yang telah dibahas pada bab sebelumnya harus diimplementasikan.

Sebagai kesimpulan, audit keamanan sistem informasi dengan menggunakan kerangka kerja *COBIT 2019* menunjukkan bahwa RSUD Palembang BARI telah mencapai tingkat keamanan yang memadai. Namun, perlu dilakukan upaya berkelanjutan untuk meningkatkan kualitas sistem dan mengatasi kerentanan yang teridentifikasi guna memastikan kepatuhan yang berkelanjutan terhadap standar keamanan informasi serta memitigasi risiko potensial.

Saran

Terdapat beberapa saran yang dapat diberikan untuk penyempurnaan dan pengembangan pada penelitian selanjutnya, seperti melibatkan aspek yang lebih luas, seperti manajemen risiko sistem informasi manajemen rumah sakit atau manajemen pelayanan sistem informasi manajemen rumah sakit. Hal ini dapat melibatkan identifikasi dan penilaian risiko yang lebih komprehensif, pengembangan kebijakan keamanan yang holistik, atau peningkatan kesadaran keamanan bagi pengguna sistem informasi. Penelitian selanjutnya juga dapat memperluas cakupan domain dan proses yang digunakan. Domain dan proses lain yang dapat dipertimbangkan dari kerangka kerja *COBIT 2019*, berupa domain *DSS (Delivery, Support, and Monitoring)* atau domain *MEA (Monitor, Evaluate, and Assess)*. Penelitian selanjutnya dapat menjelajahi kerangka kerja lain, seperti *ITIL (Information Technology Infrastructure Library)* untuk mengkaji aspek manajemen layanan TI dalam konteks rumah sakit, *ISO/IEC 27001* untuk mengidentifikasi dan mengimplementasikan kontrol keamanan informasi yang tepat, *NIST Cybersecurity Framework* untuk meningkatkan keamanan sistem informasi dari perspektif keamanan *cyber*, atau *Balanced Scorecard* untuk mengukur kinerja dan kesesuaian strategi keamanan informasi rumah sakit.

Dengan mempertimbangkan saran-saran ini, penelitian selanjutnya dapat menghasilkan wawasan yang lebih mendalam dan komprehensif tentang keamanan sistem informasi manajemen rumah sakit serta memberikan kontribusi yang lebih besar pada pengembangan praktik terbaik dalam keamanan informasi di bidang kesehatan.

Daftar Rujukan

[1] World Health Organization. (2018). Hospitals. https://www.who.int/health-topics/hospitals#tab=tab_1.
[2] Koumaditis, G. G., & Themistocleous, M. (2019). The Role of Information Technology in Modern Hospital Operations: A Case Study. Health Informatics Journal, 25(1), 71-81.
[3] Abdekhoda, M., Ahmadi, M., & Dehnad, A. (2014). Hospital information systems user needs analysis: A vendor-agnostic approach. Health Information Management Journal, 43(2), 20-27.
[4] Pribadi, M. R. (2015). Penerapan tata kelola teknologi informasi dengan menggunakan COBIT Framework 4.1 (studi kasus pada RSUD Bari Palembang). Jurnal Eksplora Informatika, 4(2), 115-124.
[5] Wibowo, A. P., & Anwar, M. Z. (2021). Audit Keamanan Sistem Informasi Rumah Sakit: Studi Kasus di Rumah Sakit Swasta di Surabaya. Jurnal Sistem Informasi, 16(1), 1-10.
[6] ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology.
[7] Afshari M, Ahmadi M, B. D. (2014). A study of Hospital Information System in Iran: Applying the Consolidated Framework for Implementation Research. Journal of Hospital Administration, 3(2), 1-7.
[8] Kumar, S., & Aldosari, B. (2017). Hospital information systems in Saudi Arabia: A qualitative analysis. International Journal of Health Policy and Management, 6(7), 403-408.
[9] Chang, V., Ramachandran, M., & Li, X. (2012). Towards a framework for managing the security of cloud computing. Journal of Organizational and End User Computing, 24(4), 1-20.

DOI : https://doi.org/10.52158/jacost.505

[10] Alhassan, M. M., & Adjei-Quaye, A. (2017). Information security in an organization. International Journal of Computer (IJC), 24(1), 100-116.
[11] Riyanarto, S. (2009). Audit Sistem dan Teknologi Informasi.
[12] Lainhart, J. W., Conboy, M., & Saull, R. COBIT 2019 Framework Introduction and methodology, Schaumburg: ISACA, 2019.
[13] Sari, R. P. (2021). Audit Keamanan Sistem Informasi Rumah Sakit Menggunakan COBIT 2019. Jurnal Sistem Informasi, 13(1), 51-58.
[14] Yulianti, E. (2020). Penggunaan COBIT 2019 untuk Audit Keamanan Sistem Informasi Rumah Sakit. Jurnal Ilmiah Teknologi Informasi Asia, 14(2), 47-55.
[15] Wulandari, R. (2020). Evaluasi Keamanan Sistem Informasi Rumah Sakit Menggunakan COBIT 2019. Jurnal Sistem Informasi, 12(2), 68-75.

DOI : https://doi.org/10.52158/jacost.505