P-ISSN : 2338-2899
E-ISSN: 2807-1271

Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit XYZ Menggunakan Cobit 2019 (Studi Kasus pada Rumah Sakit XYZ)

Rizqi Satria Andhika Gusni[1], Kraugusteeliana[2], dan I Wayan Widi Pradnyana*[3]*

[1,2,3] Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta

Email Correspondent Author : rizqi.sa@upnvj.ac.id

***Abstract* — Hospital is a health service facility that needs to be supported by a hospital information system (HIS) and information security. The problem in this study is how information security influences the governance on risk management of hospital information systems. System security governance is regulated by COBIT 2019. The domains used in this study are EDM, APO, and DSS with the EDM03, APO11, APO12, APO13, and DSS05 processes. The results of this study indicate that the level of governance capability at XYZ Hospital is at level 3 (Defined), the difference in gap analysis is 1 level below the expected level. Therefore, the governance of system security in XYZ Hospital must be improved.**

***Keyword* — Hospital Information System, Information Security, COBIT 2019, IT Governance.**

Abstrak — Rumah sakit merupakan fasilitas pelayanan kesehatan yang perlu didukung oleh sistem informasi rumah sakit (SIM-RS) dan kualitas keamanan informasi yang aman. Permasalahan pada penelitian ini adalah bagaimana pengaruh tata kelola keamanan informasi terhadap pengelolaan risiko sistem informasi rumah sakit. Tata kelola keamanan sistem diatur dalam COBIT 2019. Domain yang digunakan pada penelitian ini adalah EDM, APO, dan DSS dengan proses EDM03, APO11, APO12, APO13, dan DSS05. Hasil dari penelitian ini menunjukkan level kapabilitas tata kelola di RS XYZ ini berada di tingkat 3 (*Defined*), selisih *gap analysis* adalah 1 tingkat dibawah dari tingkat yang diharapkan, oleh karenanya perlu ada perbaikan yang dilakukan oleh pihak RS XYZ pada tata kelola keamanan sistem informasinya.

.*Kata kunci* — SIM-RS, keamanan informasi, COBIT 2019, tata kelola TI.

I. PENDAHULUAN

A. Latar Belakang Masalah

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[1] dan kepatuhan SDM terhadap prosedur [2]. Keamanan informasi pada sistem informasi rumah sakit sangat penting karena melibatkan data pasien.[3] Apabila rumah sakit mengabaikan keamanan informasi pada sistem informasinya, maka dapat meningkatkan risiko keamanan yang disebabkan baik oleh faktor eksternal maupun internal [4]. Di RS XYZ, beberapa permasalahan keamanan yang muncul pada sistem informasi rumah sakit adalah ketidaksesuaian data, kesalahan memasukkan nama obat, kesalahan pada pencatatan diagnosa medis, kesalahan penghitungan data, 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, pihak rumah sakit jarang mengimplementasikan rencana tindak lanjut untuk melakukan perbaikan secara cepat, 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 XYZ itu sendiri.

B. Sistem Informasi Manajemen Rumah Sakit

Sistem Informasi Manajemen Rumah Sakit yaitu seperangkat sistem teknologi informasi dan komunikasi yang berfungsi untuk memproses dan mengintegrasikan seluruh layanan di rumah sakit secara cepat dan tepat [4]

C. Keamanan Informasi

Konsep keamanan informasi berfokus pada 3 hal, yaitu: *Confidentiallity* (Kerahasiaan), *Integrity* (Integritas), dan Availibility (Ketersediaan), selain ketiga hal tersebut, keamanan informasi juga perlu didukung oleh *autenthication* (otentikasi), *authorization* (otorisasi), *auditing*, dan *non-repudiation* [1]

D. Audit Sistem Informasi

Audit sistem informasi adalah pengumpulan bukti-bukti yang digunakan untuk menilai apakah sebuah sistem informasi dapat melindungi aset perusahaan, menjaga integritas data yang disimpan dan dikomunikasikan, mendukung tujuan perusahaan dengan efektif, dan bekerja secara efisien [5].

E. 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. COBIT 2019 berfokus kepada dua hal yaitu sistem tata kelola dan kerangka tata kelola [6]. COBIT 2019 memiliki 6 komponen tata kelola yaitu: proses, struktur organisasi, prinsip, informasi, budaya organisasi, SDM, dan layanan infrastruktur serta apilkasinya.

COBIT 2019 memiliki domain yang dilambangkan dengan kata kerja yang mengungkapkan tujuan utama dan area

aktivitas yang terkandung di dalamnya, di dalam domain terdapat proses yang merupakan kumpulan aktivitas untuk mencapai tujuan TI secara keseluruhan. Domain pada COBIT 2019 ini tidak jauh berbeda dengan domain COBIT 5 yang diluncurkan pada 2012. [6], tetapi ada penambahan beberapa proses di COBIT 2019 [7]. Berikut ini adalah daftar dari domain dan proses pada COBIT 2019:

- *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 T&I.
- *Monitoring, Evaluate, and Assess* (MEA) membahas tentang pemantauan kinerja dan kesesuaian T&I dengan target kinerja serta tujuan pengendalian internal dan eksternal.

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

- Level 0 (Incomplete/Tidak Lengkap)
- Level 1 (Initial/Tahap Awal)
- Level 2 (Managed/Dikelola)
- Level 3 (Defined/Ditetapkan)
- Level 4 (Quantitative/Kuantitatif)
- Level 5 (Optimising/Mengoptimalkan)

Penilaian kapabilitas pada COBIT 2019 juga dapat dibantu dengan melakukan pemeringkatan pada aktivitas-aktivitas proses [7] dengan pemeringkatan sebagai berikut.:

- Fully (F), penilaian kapabilitas berada pada rentang nilai 85-100
- Largely (L), penilaian kapabilitas berada pada rentang 50-85
- Partially (P), penilaian kapabilitas berada pada rentang 15-50
- Not (N), penilaian kapabilitas kurang dari 15 persen

F. Analisis dan Mitigasi Risiko

Risiko pada TI adalah akibat yang ditimbulkan dari tindakan dan kejadian pada sistem, apabila risiko tidak ditangani secara tepat maka kerugiannya akan berdampak negatif pada kemampuan organisasi untuk menjalankan bisnis [8]. Oleh karenanya dibutuhkan analisis risiko yang merupakan proses sistematis untuk memahami dan mengungkapkan sifat dari risiko [9].

G. Uji Validitas dan Reliabilitas

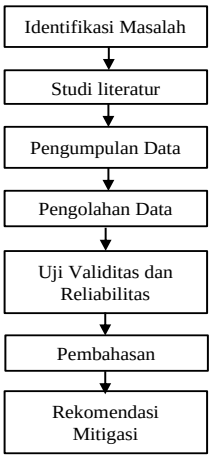
Uji validitas bertujuan untuk mengetahui sejauh mana ketepatan dari sebuah pengukuran dalam mengukur pernyataan dalam sebuah penelitian [10]. Sedangkan, uji reliabilitas digunakan untuk mengukur dan mengetahui tingkat kehandalan dan dari sebuah pengukuran pernyataan.[10]

H. Penelitian Terkait

Penelitian ini dilakukan dengan melihat dan membandingkan metode dan hasil dengan penelitian-penelitian sebelumnya, penelitian sebelumnya menunjukkan bahwa keamanan informasi di sebuah rumah sakit perlu ditingkatkan karena ada beberapa kelemahan pada proses APO13 [11], kemudian aspek keamanan sangat penting pada penyelarasan manajemen TI pada COBIT 5 [12]. dan hasil dari penilaian *rating process activities* dapat dijadikan sebagai bahan pertimbangan perbaikan tata kelola [13].

II. METODE PENELITIAN

Penelitian ini dilakukan dengan metode deskriptif kuantitatif yang menggambarkan hasil penelitian sebagaimana yang didapatkan berdasarkan hasil dari penyebaran kuisioner kepada 72 responden, penelitian ini menggunakan COBIT 2019 sebagai variabel dependen dan tata kelola keamanan sistem informasi rumah sakit XYZ sebagai variabel independen, dan dilakukan dengan tahapan penelitian sebagai berikut



Gambar 1. Tahapan penelitian.

Pengukuran variabel dilakukan dengan metode kuantitatif dengan menggunakan kuisioner berdasarkan skala Likert, yang akan disebarkan kepada 72 responden dari populasi sebanyak 168 orang.

Hasil respon yang didapatkan dari kuisioner diuji dengan uji validitas pada penelitian ini memiliki nilai minimum R = 0,72 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.

Setelah uji validitas dan reliabilitas selesai, dilakukan *rating process activities* untuk mengetahui sejauh mana tingkat kapabilitas yang dicapai oleh manajemen rumah sakit XYZ dalam mengelola keamanan sistem informasi.

Dari hasil rating process activities, selanjutnya dilakukan analisis gap yang bertujuan untuk mengetahui seberapa besar selisih gap yang didapat pada keadaan *as is* (sekarang) dan *to be* (yang diharapkan), dari *gap analysis* tersebut dapat dibuat beberapa rekomendasi mitigasi risiko untuk memperkecil selisih *gap* yang ada saat ini.

III. HASIL DAN PEMBAHASAN

A. Hasil Uji Validitas dan Reliabilitas

Hasil dari uji validitas dapat dilihat pada tabel 1 berikut:

TABEL 1
HASIL UJI VALIDITAS

Pernyataan	R Hitung > R Tabel		Level *Significant*	Keterangan
EDM03.01	0,653	0,229	5%	Valid
EDM03.02	0,839	0,252	5%	Valid
EDM03.03	0,801	0,252	5%	Valid
APO12.01	0,806	0,252	5%	Valid
APO12.02	0,845	0,252	5%	Valid
APO12.04	0,778	0,252	5%	Valid
APO12.05	0,741	0,252	5%	Valid
APO12.06	0,825	0,252	5%	Valid
APO13.01	0,862	0,252	5%	Valid
APO13.02	0,885	0,252	5%	Valid
APO13.03	0,867	0,252	5%	Valid
APO14.01	0,833	0,252	5%	Valid
APO14.04	0,851	0,252	5%	Valid
APO14.06	0,856	0,252	5%	Valid
APO14.07	0,881	0,252	5%	Valid
APO14.09	0,822	0,252	5%	Valid
APO14.10	0,882	0,252	5%	Valid
DSS05.01	0,807	0,252	5%	Valid
DSS05.02	0,864	0,252	5%	Valid
DSS05.03	0,898	0,252	5%	Valid
DSS05.04	0,903	0,252	5%	Valid
DSS05.05	0,867	0,252	5%	Valid
DSS05.06	0,865	0,252	5%	Valid
DSS05.07	0,896	0,252	5%	Valid

Dari tabel diatas dapat dipastikan bahwa seluruh pernyataan pada kuisioner valid dengan level signifikan sebesar 5%, berikutnya pada tabel 2 dapat dilihat hasil dari uji reliabilitas.

TABEL 2
HASIL UJI RELIABILITAS

Pernyataan	Cronbach Alpha *Variable* > Cronbach Alpha		Keterangan Kehandalan
EDM03	0,883	0,8	Sangat Tinggi
APO12	0,925	0,8	Sangat Tinggi
APO13	0,930	0,8	Sangat Tinggi
APO14	0,954	0,8	Sangat Tinggi
DSS05	0,968	0,8	Sangat Tinggi

Dari tabel 2 diatas, dapat dinyatakan bahwa seluruh proses yang ada memiliki nilai reliabilitas yang sangat tinggi.

B. Penilaian Aktivitas Proses

Pada penelitian ini, penilaian aktivitas proses dilakukan dengan menghitung hasil kuisioner yang didapat kemudian dari hasil kuisioner yang didapat akan dilakukan pemeringkatan berdasarkan persen aktivitas. Berikut adalah hasil dari penilaian aktivitas proses:

TABEL 3
PENILAIAN AKTIVITAS PROSES EDM03

	LEVEL			
	2	3	4	5
JUMLAH AKTIVITAS	8	5	2	1
TERPENUHI	8	3	0	0
PERSENTASE	100%	60%	0%	0%
KETERANGAN	*FULLY*	*LARGELY*	*NOT*	*NOT*
LEVEL		3		

TABEL 4
PENILAIAN AKTIVITAS PROSES APO12

	LEVEL			
	2	3	4	5
JUMLAH AKTIVITAS	3	16	8	2
TERPENUHI	3	10	2	0
PERSENTASE	100%	62,5%	25%	0%
KETERANGAN	*FULLY*	*LARGELY*	*PARTIALLY*	*NOT*
LEVEL		3		

TABEL 5
PENILAIAN AKTIVITAS PROSES APO13

	LEVEL			
	2	3	4	5
JUMLAH AKTIVITAS	11	3	5	1
TERPENUHI	11	2	1	0
PERSENTASE	100%	66%	20%	0%
KETERANGAN	*FULLY*	*LARGELY*	*PARTIALLY*	*NOT*
LEVEL		3		

TABEL 6
PENILAIAN AKTIVITAS PROSES APO14

	LEVEL			
	2	3	4	5
JUMLAH AKTIVITAS	9	8	11	-
TERPENUHI	9	7	7	-
PERSENTASE	100%	87,5%	45%	-
KETERANGAN	*FULLY*	*FULLY*	*PARTIALLY*	-
LEVEL		3		

TABEL 7
PENILAIAN AKTIVITAS PROSES DSS05

	LEVEL			
	2	3	4	5
JUMLAH AKTIVITAS	26	18	5	-
TERPENUHI	23	12	0	-
PERSENTASE	84,6%	61,1%	0%	-
KETERANGAN	*FULLY*	*LARGELY*	*NOT*	-
LEVEL		3		

Hasil dari penjumlahan penilaian aktivitas proses ini dapat dilihat pada penjumlahan dibawah ini

$$\big((0 \times 0) + (1 \times 0) + (2 \times 0) + (3 \times 5) + (4 \times 0) + (5 \times 0)\big) \div 5 = 3 \quad (1)$$

Pada tabel 3 sampai tabel 7 diatas menunjukkan bahwa tingkat kapabilitas pada penelitian ini berada pada level 3, dimana tata kelola keamanan informasi pada RS XYZ ini sudah mencapai tingkat *defined*, yaitu tingkatan dimana seluruh proses telah dilaksanakan, tetapi belum ada pengukuran yang dilakukan.

C. Gap Analysis

Berikut ini adalah analisis gap (kesenjangan) dari hasil penilaian aktivitas proses yang dapat dilihat pada tabel 8

TABEL 8
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 pada penelitian ini adalah 1 level dibawah kondisi yang diharapkan (to be).

D. Saran Mitigasi

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

- Memperbaiki pengamanan fisik pada ruangan server dengan alat sidik jari atau kartu akses
- Melakukan *testing* penetrasi pada sistem.
- Melakukan penilaian tingkat resiko secara berkala.
- Melakukan *training* kepada SDM di RS XYZ terkait dengan penggunaan sistem yang aman.

IV. KESIMPULAN

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, dan perlu didukung oleh beberapa prosedur tetap. Hasil dari penelitian ini menunjukkan bahwa tingkat kapabilitas tata kelola sistem informasi di RS XYZ ini sudah mencapai tingkat defined, namun perlu dilakukan peningkatan kualitas secara berkala dan perbaikan secara bertahap, pengukuran terkait resiko juga perlu dilakukan supaya SIM-RS di RS XYZ dapat menyesuaikan dengan profil resiko terbaru.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada Tuhan Yang Maha Esa, Kedua orang tua peneliti, Kepala Rumah Sakit XYZ, Kepala Divisi TI RS XYZ, Ibu Kraugusteeliana, dan Bapak I Wayan Widi Pradnyana selaku pembimbing dalam menyusun penelitian ini.

DAFTAR ACUAN

[1] Alhassan, M. M., & Adjei-Quaye, "A. Information Security in an Organization," *International Journal of Computer (IJC)*, vol *24* no.1, pp. 100–116. 2017. Available: http://ijcjournal.org/

[2] Peikari, H. R., Ramayah, T., Shah, M. H., & Lo, M. C, "Patient's perception of the information security management in health centers: The role of organizational and human factors,". *BMC Medical Informatics and Decision Making*, vol *18* no.102, pp 1–13. November 2018. Available: https://doi.org/10.1186/s12911-018-0681-z

[3] Mbonihankuye, S., Nkunzimana, A., Ndagijimana, A., & García-Magariño, "Healthcare Data Security Technology: HIPAA Compliance," *Wireless Communications and Mobile Computing*, vol *2019 no.* 1927495. October 2019. Available: https://doi.org/10.1155/2019/1927495

[4] Peraturan Menteri Kesehatan RI Nomor 82 Tahun 2013 tentang Sistem Manajemen Rumah Sakit, Kementerian Kesehatan RI. Available: https://www.kemhan.go.id/itjen/wp-content/uploads/2017/03/bn87-2014.pdf

[5] Enyclopedia Brittanica. *Information Systems Audit.* Available: https://www.britannica.com/topic/information-system/Information-systems-audit

[6] Lainhart, J. W., Conboy, M., & Saull, R. *COBIT 2019 Framework Introduction and methodology*, Schaumburg: ISACA, 2019. Available: https://www.isaca.org/resources/cobit

[7] Lainhart, J. W., Conboy, M., & Saull, R. *COBIT 2019 Framework: Governance and Management Objectives*, Schaumburg: ISACA, 2019. Available: https://www.isaca.org/resources/cobit

[8] Aven, T., & Ben-Haim, Y. "Society for Risk Analysis Glossary", *Encyclopedia of Science and Technology Communication* Vol. August, pp. 1–9. April 2020. Available: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

[9] Fernando, M. S. "IT disaster recovery system to ensure the business continuity of an organization". *2017 National Information Technology Conference, 2017-September*, pp. 46–48. September 2017. Available: https://doi.org/10.1109/NITC.2017.8285648

[10] Yusup, F. "Uji Validitas dan Reliabilitas Instrumen Penelitian Kuantitatif," *Jurnal Tarbiyah : Jurnal Ilmiah Kependidikan*, vol. *7* no.1, pp. 17–23. 2018. Available: https://doi.org/10.18592/tarbiyah.v7i1.2100

[11] Nistrina, K., & Bin Bon, H. A. T. (2019). "Information security for hospital information system using COBIT 5 framework," *Proceedings of the International Conference on Industrial Engineering and Operations Management*, *2019*, pp. 3369–3374. March 2019. Available: http://ieomsociety.org/ieom2019/papers/767.pdf

[12] Huygh, T., De Haes, S., Joshi, A., & Van Grembergen, W. Answering Key Global IT Management Concerns Through IT Governance and Management Processes: A COBIT 5 View. *Proceedings of the 51st Hawaii International Conference on System Sciences*, Vol. *9*. January 2018

https://doi.org/10.24251/hicss.2018.665

[13] Atrinawati, L. H., Ramadhani, E., Fiqar, T. P., Wiranti, Y. T., Abdullah, A. I. N. F., Saputra, H. M. J., & Tandirau, D. B. (2021). Assessment of Process Capability Level in University XYZ Based on COBIT 2019. *Journal of Physics: Conference Series*, Vol *.1803* No.1, pp 1–11. https://doi.org/10.1088/1742-6596/1803/1/012033