Jurnal Manajemen dan Teknologi Informasi (JMTI)
Volume 15, Issue 02, 2025, pp. 103-114
ISSN 2721-7604 (Online); ISSN 2087-5312 (Print)
DOI: 10.59819

AUDIT TATA KELOLA TEKNOLOGI INFORMASI DI RSUD X MENGGUNAKAN FRAMEWORK COBIT 2019

I Komang Satria Wibawa[1], Anak Agung Ngurah Hary Susila[2], Ni Made Ika Marini Mandenni[3]
[1]Universitas Udayana, Badung, Indonesia; *wibawasatria68@gmail.com
[2]Universitas Udayana, Badung, Indonesia; harysusila@unud.ac.id
[3]Universitas Udayana, Badung, Indonesia; made_ikamarini@unud.ac.id
*)Corresponding author; E-mail addresses: wibawasatria68@gmail.com

ARTICLE INFO
Article history
Received September 24, 2025
Revised October 14, 2025
Accepted October 27, 2025
Available online October 31,2025

Keyword: IT Governance, Governance Audit, RSUD X, COBIT 2019

Copyright ©2025 by Author. Published by Fakultas Teknik dan Informatika Universitas PGRI Mahadewa Indonesia

Abstract. An IT governance audit at X Hospital was conducted due to various issues affecting service quality and system performance. Critical points included an overloaded database that resulted in suboptimal website information updates, inadequate server specifications to run the website when users were active, poorly managed network cables that made the server vulnerable to disruptions, and an under-protected IT unit in website management. The study aimed to identify critical points, elicit IT process capabilities, and provide improvement recommendations based on the COBIT 2019 Framework. The methods used included interviews, observations, business goal mapping and alignment, and a capability level questionnaire. The audit results identified five main domains, namely APO12, BAI10, DSS02, DSS03, and DSS04, all at capability level 2. Recommendations included IT risk integration, asset management, accelerated incident handling, improved service and satisfaction, and rapid adaptation to increase capabilities to levels 3, 4, and 5.

PENDAHULUAN

Audit tata kelola teknologi informasi merupakan proses evaluasi yang bertujuan untuk memastikan bahwa penerapan dan pengelolaan TI dalam suatu organisasi berjalan secara efektif, efisien, dan sesuai dengan regulasi serta standar yang berlaku. Audit penting karena teknologi informasi berperan vital dalam mendukung operasional dan pengambilan keputusan strategis. Apabila audit dilakukan dengan baik, organisasi dapat memastikan bahwa sistem TI mereka aman, dapat diandalkan, serta mampu mendukung tujuan bisnis jangka panjang. Audit tata kelola teknologi informasi juga membantu organisasi mengidentifikasi risiko potensial, seperti ancaman keamanan siber, inefisiensi sistem, atau kegagalan dalam kepatuhan terhadap regulasi yang berlaku, seperti perlindungan data pribadi. Hasil audit memberikan wawasan tentang area yang memerlukan perbaikan dan peningkatan, serta memastikan bahwa pengelolaan TI selaras dengan kebutuhan organisasi.

Audit tata kelola TI di RSUD X dilatarbelakangi oleh sejumlah masalah yang mengganggu kualitas layanan dan kinerja sistem, antara lain: sistem gagal memperbarui data saat database

mengalami overload; spesifikasi server yang tidak memadai sehingga kinerja melambat atau terhenti pada lonjakan pengguna; jaringan kabel yang usang dan kurang terkelola menyebabkan koneksi tidak stabil; serta keterbatasan kompetensi unit IT yang berisiko menimbulkan kesalahan penginputan dan pengelolaan data. Karena itu diperlukan audit untuk mengidentifikasi akar masalah dan merekomendasikan perbaikan yang meningkatkan efisiensi, stabilitas, dan keamanan sistem informasi sehingga mendukung layanan yang lebih optimal. Audit ini menggunakan framework **COBIT 2019** karena pendekatannya yang fleksibel dan dapat disesuaikan dengan tujuan strategis organisasi serta kemampuannya mendukung transformasi digital, meningkatkan alignment antara TI dan bisnis, dan memberikan panduan pengelolaan risiko TI. [1]

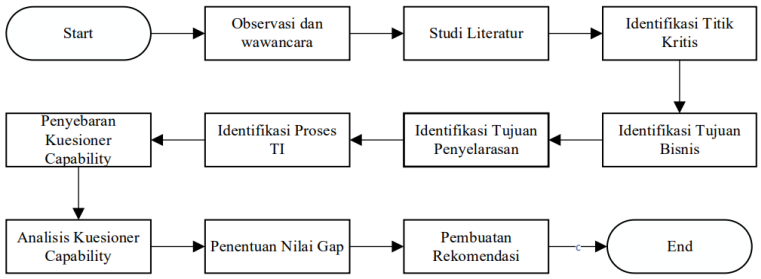
METODE

Tempat dan Waktu Penelitian

Penelitian mengenai Audit Tata Kelola Teknologi Informasi menggunakan *Framework* COBIT 2019 dilaksanakan di RSUD X dan di Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana, Kampus Jimbaran. Waktu pelaksanaan penelitian dimulai pada bulan September 2024 sampai bulan Desember 2024.

Metode Penelitian

Metode penelitian merupakan proses yang telah ditetapkan dalam melakukan penelitian agar lebih teratur dan terarah. Tahapan penelitian dirancang mengacu kepada *Framework* COBIT 2019. Alur dari tahap pelaksanaan penelitian audit untuk mengetahui tingkat kapabilitas pada RSUD X yang meliputi tahap observasi dan wawancara, studi literatur, identifikasi titik kritis, identifikasi tujuan bisnis, identifikasi tujuan penyelarasan, identifikasi proses TI, penyebaran kuesioner capability, analisis kuesioner capability, penentuan nilai gap dan pemberian saran serta perbaikan. Gambaran umum tahapan penelitian audit tata kelola pada RSUD X menggunakan COBIT 2019 dapat dilihat pada Gambar 1 di bawah ini.



Gambar 1. Metode Penelitian

Teknik Pengumpulan Data

Pengumpulan data merupakan tahapan lanjutan dalam proses audit. Proses ini memiliki peran penting dalam penelitian karena bertujuan untuk memperoleh informasi serta bukti pendukung. Pengumpulan data dilakukan dengan melibatkan pihak-pihak yang memiliki peran atau kepentingan dalam manajemen, khususnya yang terlibat langsung dalam pelaksanaan proses bisnis di RSUD X. Teknik yang digunakan dalam pengumpulan data meliputi observasi, wawancara, dan penyebaran kuesioner. Penjelasan mengenai masing-masing metode tersebut disajikan sebagai berikut.

1. Metode Observasi
   Observasi merupakan teknik pengumpulan data dengan cara mengamati secara langsung objek penelitian dari jarak dekat. Dalam observasi, dilakukan pencatatan secara sistematis

terhadap peristiwa, tingkah laku, objek yang diamati, serta aspek lain yang dibutuhkan untuk mendukung penelitian yang sedang berjalan.

2. Metode Wawancara
   Wawancara adalah metode pengumpulan data dengan cara bertatap muka secara langsung antara pengumpul data dan narasumber, dimana dilakukan sesi tanya jawab untuk mendapatkan informasi yang berguna sebagai bahan dalam penelitian. Hasil dari wawancara dapat menjadi bahan pertimbangan untuk titik kritis yang diangkat oleh RSUD X.
3. Kuesioner
   Kuesioner merupakan metode pengumpulan data yang menggunakan rangkaian pertanyaan tertulis untuk mengumpulkan informasi dari para responden. 19 Metode ini bertujuan memperoleh data yang sesuai dengan tujuan penelitian sekaligus menjamin validitas dan reliabilitas yang tinggi. Dalam penelitian, kuesioner yang digunakan adalah kuesioner untuk mengukur tingkat kapabilitas. Kuesioner tingkat kapabilitas yang disusun berdasarkan hasil pemetaan proses TI dengan mengacu pada buku COBIT 2019 yang berjudul Governance and Management Objectives. Penyebaran kuesioner tingkat kapabilitas dilakukan dengan menggunakan Google Form

HASIL DAN PEMBAHASAN

1. Identifikasi Titik Kritis dan Tujuan Bisnis
   Identifikasi titik kritis membahas isu-isu tata kelola dalam suatu institusi, yang berasal dari kerangka kerja COBIT 2019 dan wawancara dengan para pemimpin TI utama di RSUD X Proses ini mengidentifikasi titik-titik kritis berdasarkan kategori risiko TI rumah sakit. Setelah itu, tujuan bisnis ditentukan dengan mengacu pada tujuan yang diuraikan dalam kerangka kerja COBIT 2019, dan menyelaraskannya dengan titik-titik kritis yang telah diidentifikasi.

Tabel 1. Titik Kritis RSUD X dan Identifikasi Tujuan Bisnis

No	Titik Kritis	Tujuan Bisnis	
		Code	Description
1	Database yang mengalami overload menyebabkan pembaruan informasi pada website tidak optimal.	EG06	Keberlanjutan dan aksesibilitas layanan bisnis
		EG07	Kualitas informasi manajerial
		EG08	Peningkatan kinerja proses bisnis internal
2	Spesifikasi server yang kurang memadai untuk menjalankan website saat terjadi lonjakan pengguna	EG01	Portofolio produk dan layanan yang bersaing
		EG02	Manajemen risiko bisnis
		EG06	Keberlanjutan dan aksesibilitas layanan bisnis
		EG08	Peningkatan kinerja proses bisnis internal
3	Jaringan kabel yang kurang terkelola menyebabkan server rentan terhadap gangguan, seperti koneksi terputus	EG02	Manajemen risiko bisnis
		EG05	Budaya layanan yang fokus pada kepuasan pelanggan
		EG06	Keberlanjutan dan aksesibilitas layanan bisnis

		EG01	Portofolio produk dan layanan yang bersaing
		EG05	Budaya layanan yang fokus pada kepuasan pelanggan
4	Unit IT yang kurang terlatih dalam pengelolaan *website*.	EG10	Kemampuan staf, motivasi, dan produktivitas
		EG13	Inovasi dalam produk dan model bisnis

2. Identifikasi Tujuan Penyelarasan

Identifikasi tujuan penyelarasan dilakukan dengan melakukan pemetaan tujuan bisnis dengan tujuan penyelarasan. Proses dilakukan untuk mengetahui kebutuhan bisnis akan ketersediaan TI. Tabel 2 merupakan hasil dari pemetaan tujuan bisnis dengan tujuan penyelarasan.

Tabel 2. Identifikasi Tujuan Penyelarasan

Kode EG	Tujuan Bisnis	Kode AG	Tujuan Penyelarasan
EG01	Portofolio produk dan layanan yang kompetitif	AG05	Penyampaian layanan T&I sejalan dengan kebutuhan bisnis
		AG06	Kelincahan untuk mengubah persyaratan bisnis menjadi solusi operasional
		AG08	Mengaktifkan dan mendukung proses bisnis dengan mengintegrasikan aplikasi dan teknologi
		AG09	Penyampaian program tepat waktu sesuai dengan anggaran dan memenuhi persyaratan dan standar kualitas
			Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis
		AG13	Penyampaian program tepat waktu sesuai dengan anggaran dan memenuhi persyaratan dan standar kualitas
EG02	Risiko bisnis yang dikelola	AG02	Risiko terkait T&I yang dikelola
		AG07	Keamanan informasi, pemrosesan infrastruktur, dan aplikasi
EG05	Budaya pelayanan yang berorientasi pada pelanggan	AG08	Mengaktifkan dan mendukung proses bisnis dengan mengintegrasikan aplikasi dan teknologi
EG06	Kontinuitas dan ketersediaan layanan bisnis	AG07	Keamanan informasi, pemrosesan infrastruktur, dan aplikasi.
EG07	Kualitas informasi manajemen	AG04	Kualitas informasi keuangan terkait teknologi
		AG10	Kualitas informasi manajemen TI
EG08	Optimalisasi fungsi proses bisnis internal	-	
EG10	Keterampilan staf, motivasi, dan produktivitas	AG12	Personel TI yang kompeten serta memiliki motivasi.

EG13	Inovasi produk dan bisnis	AG13	Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis

3. Identifikasi Proses TI
   Identifikasi memuat pemetaan tujuan penyelarasan dengan proses TI sehingga menghasilkan domain dan proses TI yang sesuai dengan titik kritis. Tabel 3 merupakan proses TI yang sesuai dengan tujuan penyelarasan.

Tabel 3. Identifikasi Proses TI

No	Domain	Proses TI	Titik Kritis
1	APO12	Mengelola Resiko	Spesifikasi server yang kurang memadai untuk menjalankan website saat terjadi lonjakan pengguna.
2	BAI10	Mengelola Konfigurasi	Jaringan kabel yang kurang terkelola menyebabkan server rentan terhadap gangguan, seperti koneksi terputus.
3	DS002	Mengelola Permintaan dan Insiden Layanan Terkelola	Unit IT yang kurang terlatih dalam pengelolaan website.
4	DSS03	Mengelola Masalah	Unit IT yang kurang terlatih dalam pengelolaan website.
5	DSS04	Mengelola Kontinuitas	Spesifikasi server yang kurang memadai untuk menjalankan website saat terjadi lonjakan pengguna dan jaringan kabel yang kurang terkelola menyebabkan server rentan terhadap gangguan, seperti koneksi terputus.

4. Hasil Analisis Kuesioner COBIT 2019
   Hasil analisis kuesioner COBIT 2019 bertujuan untuk mengukur tingkat kapabilitas setiap domain yang diaudit. Tabel 4 merupakan hasil kuesioner COBIT 2019 yang telah dibagikan kepada 4 responden.

Tabel 4. Analisis Hasil Kuesioner Capability Level 3 Domain APO12

Sub Domain	Jumlah Pertanyaan	R1	R2	R3	R4	Jawaban		Total Aktivitas	Persentase
						Y	T		
APO12.01	2	2	1	0	2	5	3	8	62.5%
APO12.02	6	3	4	3	6	16	8	24	67%
APO12.03	2	1	2	1	2	6	2	8	75%
APO12.04	4	3	3	4	3	13	3	16	82%
APO12.05	2	1	2	2	2	7	1	8	88%
APO12.06	2	2	1	2	2	7	1	8	88%
								Capability Level 3	**77%**

Tabel 5. Analisis Hasil Kuesioner Capability Level 3 Domain BAI10

	R1	R2	R3	R4	Jawaban	Persentase

Sub Domain	Jumlah Pertanyaan					Y	N	Total Aktivitas	
BAI10.01	2	2	2	1	1	6	2	8	75%
BAI10.02	1	0	1	1	1	3	1	4	75%
BAI10.03	1	1	0	1	1	3	1	4	75%
BAI10.04	2	1	2	2	2	7	1	8	88%
								Capability Level 3	**79%**

Tabel 6. Analisis Hasil Kuesioner Capability Level 3 Domain DSS02

Sub Domain	Jumlah Pertanyaan	R1	R2	R3	R4	Jawaban		Total Aktivitas	Persentase
						Y	T		
DSS02.01	5	3	2	2	3	10	11	20	50%
DSS02.03	1	1	1	0	1	4	1	4	75%
DSS02.07	1	1	0	1	1	3	1	4	75%
								Capability Level 3	**67%**

Tabel 7. Analisis Hasil Kuesioner Capability Level 3 Domain DSS03

Sub Domain	Jumlah Pertanyaan	R1	R2	R3	R4	Jawaban		Total Aktivitas	Persentase
						Y	T		
DSS03.02	3	2	3	3	2	10	2	12	83%
DSS03.03	1	1	0	1	1	3	1	4	75%
DSS03.04	1	1	1	1	0	3	1	4	75%
DSS03.05	3	3	3	3	2	11	1	12	92%
								Capability Level 3	**82%**

Tabel 8. Analisis Hasil Kuesioner Capability Level 3 Domain DSS04

Sub Domain	Jumlah Pertanyaan	R1	R2	R3	R4	Jawaban		Total Aktivitas	Persentase
						Y	T		
DSS04.02	4	3	3	4	2	12	4	16	75%
DSS04.03	1	1	1	0	1	3	1	4	75%
DSS04.04	1	0	1	1	1	3	1	4	75%
DSS04.05	4	3	4	4	3	14	2	16	87.5%
DSS04.06	2	2	2	1	2	7	1	8	87.5%
								Capability Level 3	**80%**

Kapabilitas semua domain proses TI di RSUD X saat ini berada pada level 2, yang menunjukkan bahwa aktivitas yang diimplementasikan telah mencapai tujuannya melalui serangkaian praktik dasar yang lengkap dan dianggap

operasional. Namun, terdapat kesenjangan antara level kapabilitas saat ini dan level yang ditargetkan. Tabel 9 menyajikan diagram laba-laba yang secara visual menggambarkan perbandingan ini dan kesenjangan yang ada.

Tabel 9. Perbandingan Tingkat Kapabilitas.

No	Domain Proses TI	Kapabilitas Saat Ini	Kapabilitas yang Diharapkan	Gap
1.	APO12	2	5	3
2.	BAI10	2	5	3
3.	DSS02	2	5	3
4.	DSS03	2	5	3
5.	DSS04	2	5	3

Berdasarkan Tabel 9 tingkat kapabilitas proses TI di RSUD X saat ini berada pada level 2 yaitu aktivitas yang dilakukan telah mencapai tujuan melalui penerapan serangkaian kegiatan dasar yang lengkap dan dapat dikategorikan telah berjalan secara operasional. Namun, terdapat kesenjangan (*gap*) antara tingkat kapabilitas saat ini dan tingkat kapabilitas yang diharapkan. Gambar 2 merupakan *spider chart* yang menggambarkan secara visual perbandingan dan *gap capability level*.

Gambar 2. Spider Chart Perbandingan Tingkat Kapabilitas

Gambar 2 merupakan *spider chart* yang menunjukkan *gap capability level* dari hasil kuesioner yang diberikan kepada responden di RSUD X. Terlihat dua warna yang membedakan nilai pada proses TI. Warna biru menunjukkan nilai kapabilitas berdasarkan hasil kuesioner yang telah disebar kepada responden (*current capability*), sedangkan warna jingga menunjukkan nilai kapabilitas yang diharapkan (*expected capability*).

5. Rekomendasi

   Nilai kesenjangan (*gap*) yang diperoleh melalui proses penentuan capability level di RSUD X digunakan untuk menentukan langkah- langkah perubahan kondisi saat ini dengan kondisi yang diharapkan pimpinan RSUD X pada masa depan. Kesenjangan antara harapan terhadap kegiatan dengan capaian pada kenyataan dapat diatasi dengan pemberian saran dan rekomendasi dari panduan buku COBIT 2019 yang berjudul *Governance and Management Objectives*. Buku tersebut menawarkan langkah-langkah peningkatan yang dapat digunakan untuk meningkatkan nilai *capability level* di RSUD X. Berikut merupakan saran dan rekomendasi untuk proses TI di RSUD X.

Tabel 10. Rekomendasi Domain APO12

No	Rekomendasi Domain APO12	
1	Tujuan Proses TI Domain APO12	Mengintegrasikan pengelolaan risiko perusahaan terkait IT dengan manajemen risiko perusahaan secara keseluruhan, menyeimbangkan biaya, dan manfaat pengelolaan risiko perusahaan terkait IT.
2.	Titik Kritis	Titik kritis 2 : Spesifikasi server yang kurang memadai untuk menjalankan website saat terjadi lonjakan pengguna
3.	Rekomendasi untuk mencapai capability level 3	Disarankan agar RSUD X menerapkan taksonomi risiko COBIT 2019 untuk memastikan definisi skenario risiko, kategori dampak, dan kemungkinan yang konsisten. Hal ini selaras dengan klausul 6.1.2 ISO 27001:2022 dan kontrol A.5.12. Misalnya, CPU > 90% selama ≥15 menit diklasifikasikan sebagai dampak tinggi dan kemungkinan, yang memicu tiket Jira/ServiceNow otomatis melalui CloudWatch/Grafana. Insiden diprioritaskan berdasarkan tingkat risiko, dan taksonomi ditinjau setiap triwulan untuk memastikan konsistensi dan validitasnya.
4.	Rekomendasi untuk mencapai capability level 4	Disarankan agar RSUD X melakukan survei dan menganalisis data risiko TI masa lalu beserta insiden kerugian eksternal, sesuai COBIT 2019. Hal ini sejalan dengan ISO 27001:2022 (A.5.7, A.8.15, A.7.5.3). Hal ini mencakup ekspor log (misalnya, CPU > 90% ≥15 menit, kesalahan 503) dari Grafana/Loki ke CSV terenkripsi, menggabungkannya dengan laporan eksternal seperti DBIR dan SANS, mengarsipkannya dalam brankas aman yang dikontrol versinya, dan menganalisisnya setiap triwulan di PowerBI untuk mengidentifikasi tren pada Risk Register.
5.	Rekomendasi untuk mencapai capability level 5	Rekomendasi berdasarkan buku COBIT 2019 berjudul Governance and Management Objectives adalah menghitung keuntungan dan kerugian dari setiap opsi respons risiko, lalu memilih opsi terbaik. Prometheus/Grafana ditinjau setiap enam bulan dan dibahas dalam Tinjauan Manajemen untuk memilih opsi yang paling hemat biaya.

Tabel 11. Rekomendasi Domain BAI10

No	Rekomendasi Domain BAI10	
1	Tujuan Proses TI Domain BAI10	Memberikan informasi yang cukup tentang aset layanan, agar layanan dapat dikelola secara efektif. Menilai dampak perubahan dan menangani insiden layanan.
2	Titik Kritis	Titik kritis 3 : Kabel jaringan yang kurang terkelola menyebabkan server rentan terhadap gangguan, seperti koneksi terputus.

3	Rekomendasi untuk mencapai capability level 3	Rekomendasinya adalah menerapkan cakupan manajemen konfigurasi terperinci sesuai COBIT 2019 dan ISO 27001:2022, menggunakan CMDB untuk layanan, aset, dan konfigurasi dengan metadata utama. CMDB harus disinkronkan secara otomatis dengan Ansible Inventory, melacak perubahan dalam repositori IaC berbasis Git dan Jira, menyimpan dokumen terenkripsi di SharePoint dengan versi, dan menjalani tinjauan keamanan dan kepatuhan triwulanan.
4	Rekomendasi untuk mencapai capability level 4	Disarankan untuk melakukan validasi item konfigurasi secara rutin sesuai dengan COBIT 2019 dan ISO 27001:2022 dengan membandingkan konfigurasi fisik dan logis melalui penggunaan alat penemuan. RSUD X menggunakan Nmap dan Ansible-Discovery untuk memindai infrastruktur, mencocokkan hasil dengan CMDB, memperbarui repositori IaC yang didukung Git, mencatat ketidakcocokan di ServiceNow, dan menyimpan dokumentasi terenkripsi di SharePoint/Vault untuk memastikan konfigurasi dan data audit yang akurat dan aman.
5	Rekomendasi untuk mencapai capability level 5	Rekomendasinya adalah menilai kelengkapan dan akurasi repositori secara berkala terhadap target, dan mengambil tindakan korektif sesuai kebutuhan. Sesuai COBIT 2019 dan ISO 27001:2022 (A.8.3.1, A.8.3.3, A.7.5.3), RSUD X harus menjalankan pemindaian Nmap dan Ansible Discovery bulanan untuk server, switch, dan kabel, membandingkan hasilnya dengan CMDB, dan membuat tiket ServiceNow jika kelengkapannya di bawah 95%. Semua proses disimpan dalam repositori IaC terenkripsi yang didukung Git dan SharePoint dengan versi, yang ditinjau setiap tiga bulan untuk menjaga akurasi.

Tabel 12. Rekomendasi Domain DSS02

No	Rekomendasi Domain DSS02	
1	Tujuan Proses TI Domain DSS02	Meraih peningkatan produktivitas dan minimalkan gangguan melalui penyelesaian cepat atas permintaan dan insiden pengguna. Nilai dampak perubahan dan tangani insiden layanan. Selesaikan permintaan pengguna dan pulihkan layanan sebagai respons atas insiden.
2.	Titik Kritis	Titik kritis 4 : Unit IT yang kurang terlatih dalam pengelolaan *website.*
3.	Rekomendasi untuk mencapai capability level 3	Rekomendasi: Terapkan COBIT 2019 & ISO 27001:2022 dengan mengaktifkan klasifikasi/prioritas insiden berbasis ITSM, mengotomatiskan analisis akar penyebab, meningkatkan server (EPYC 7302P, RAM 32GB, NVMe 1TB), mengoptimalkan MySQL, dan menyelesaikan insiden berdasarkan prioritas bisnis.

4.	Rekomendasi untuk mencapai capability level 4	Rekomendasi: Terapkan COBIT 2019 & ISO 27001:2022 dengan mengaktifkan pemantauan waktu nyata (Zabbix/Prometheus + Grafana/Kibana), laporan insiden mingguan otomatis, pencadangan log terpusat, dan, jika perlu, peningkatan server dan MySQL untuk deteksi dan respons yang lebih baik.
5.	Rekomendasi untuk mencapai capability level 5	Rekomendasi: Terapkan COBIT 2019 & ISO 27001:2022 dengan mengumpulkan data insiden dengan log harian dan laporan mingguan, meningkatkan server dan MySQL, menggunakan Grafana/Zabbix dengan backup S3, dan memberikan pelatihan rutin untuk meningkatkan kinerja dan ketahanan.

Tabel 13. Rekomendasi Domain DSS03

No	Rekomendasi Domain DSS03	
1	Tujuan Proses TI Domain DSS03	Meningkatkan ketersediaan, memperbaiki tingkat layanan, mengurangi biaya, meningkatkan kenyamanan dan kepuasan pelanggan dengan mengurangi jumlah masalah operasional, dan mengidentifikasi akar penyebab sebagai bagian dari penyelesaian masalah
2.	Titik Kritis	Titik kritis 4 : Unit IT yang kurang terlatih dalam pengelolaan *website.*
3.	Rekomendasi untuk mencapai capability level 3	Rekomendasi: Terapkan COBIT 2019 & ISO 27001:2022 dengan mengaktifkan klasifikasi/prioritas insiden berbasis ITSM, mengotomatiskan analisis akar penyebab, meningkatkan server (EPYC 7302P, RAM 32GB, NVMe 1TB), mengoptimalkan MySQL, dan menyelesaikan insiden berdasarkan prioritas bisnis.
4.	Rekomendasi untuk mencapai capability level 4	Rekomendasi: Terapkan COBIT 2019 & ISO 27001:2022 dengan mengaktifkan pemantauan waktu nyata (Zabbix/Prometheus + Grafana/Kibana), laporan insiden mingguan otomatis, pencadangan log terpusat, dan, jika perlu, peningkatan server dan MySQL untuk deteksi dan respons yang lebih baik.
5.	Rekomendasi untuk mencapai capability level 5	Rekomendasi: Terapkan COBIT 2019 & ISO 27001:2022 dengan mengumpulkan data insiden dengan log harian dan laporan mingguan, meningkatkan server dan MySQL, menggunakan Grafana/Zabbix dengan backup S3, dan memberikan pelatihan rutin untuk meningkatkan kinerja dan ketahanan.

Tabel 14. Rekomendasi Domain DSS04

No	Rekomendasi Domain DSS04	
1	Tujuan Proses TI Domain DSS04	Beradaptasi dengan cepat, melanjutkan operasi bisnis, dan menjaga ketersediaan sumber daya dan informasi pada tingkat yang dapat diterima oleh

		perusahaan jika terjadi gangguan yang signifikan (misalnya, ancaman, peluang, tuntutan).
2.	Titik Kritis	Titik kritis 1 : Database yang mengalami overload menyebabkan pembaruan informasi pada website tidak optimal. Titik kritis 2 : Spesifikasi server yang kurang memadai untuk menjalankan website saat terjadi lonjakan pengguna.
3.	Rekomendasi untuk mencapai capability level 3	Rekomendasi: Berdasarkan COBIT 2019 & ISO 27001:2022, nilai ancaman terhadap kelangsungan bisnis dan mitigasi melalui basis data terkluster, penyeimbangan beban, perangkat keras berspesifikasi tinggi, NIC cepat, pencadangan yang kuat, pemantauan berkelanjutan, pemasangan patch, dan latihan ketahanan rutin.
4.	Rekomendasi untuk mencapai capability level 4	Rekomendasi: Sesuai COBIT 2019 & ISO 27001:2022 A.8.34, lakukan tinjauan pasca-pelatihan dan pengujian failover non-produksi, tingkatkan tempat pengujian jika RTO melebihi target untuk memastikan penanganan beban yang realistis, metrik yang akurat, dan peningkatan layanan yang berkelanjutan.
5.	Rekomendasi untuk mencapai capability level 5	Rekomendasi: Sesuai COBIT 2019 & ISO 27001:2022 A.8.6, perbarui rencana kesinambungan pasca-tinjauan untuk mempertahankan kapasitas lonjakan ≥1,5×, kurangi failover dari 90-an menjadi 60-an melalui peningkatan perangkat keras, redundansi, pemantauan, dan latihan dua tahunan untuk ketahanan dan peningkatan.

SIMPULAN

Audit dilakukan melalui tahapan identifikasi titik kritis (APO12, BAI10, DSS02, DSS03, DSS04) melalui wawancara, penentuan tujuan bisnis, penyelarasan tujuan, proses TI, penentuan responden, penyebaran kuesioner kapabilitas, analisis nilai gap, dan pemberian rekomendasi. Hasil kapabilitas menunjukkan bahwa APO12 BAI10, DSS02, DSS03, dan DSS04 berada pada level 2. Rekomendasi disusun untuk meningkatkan setiap domain ke level 5 sesuai target pimpinan RSUD X dengan mengacu pada COBIT 2019 dan ISO 27001:2022. Rekomendasi difokuskan pada peningkatan manajemen risiko TI, manajemen aset layanan, penanganan insiden, serta kesiapan dan kesinambungan operasi bisnis selama gangguan.

DAFTAR PUSTAKA

Algiffary, M. A., Herdiansyah, M. I., & Kunang, Y. N. (2023). *JOURNAL OF APPLIED COMPUTER SCIENCE AND TECHNOLOGY (JACOST) Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI*. *4*(1), 19–26.

Bayu, K., Sudana, O., Wirdiani, A., & Paramartha, A. (2021). Evaluation of IT Governance at Office X using the COBIT 5 Framework. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *9*(1), 1. https://doi.org/10.24843/jim.2021.v09.i01.p01

Belo, G. I., Wiranti, Y. T., & Atrinawati, L. H. (2020). Perancangan Tata Kelola Teknologi Informasi Menggunakan COBIT 2019 Pada PT Telekomunikasi Indonesia Regional

Kalimantan. *JUSIKOM PRIMA (Jurnal Sistem Informasi Ilmu Komputer Prima)*, *4*(1), 23–30.
Dawis, A. M., Meylani, Y., Heryana, N., Alfathoni, M. A. M., Sriwahyuni, E., Ristiyana, R., Januarsi, Y., Wiratmo, P. A., Dasman, S., Mulyani, S., Agit, A., Shoffa, S., & Baali, Y. (2023). *Pengantar Metodologi Penelitian*.
Moryanda, R., Pujani, V., & Marpaung, Y. (2024). Evaluasi Sistem Informasi Manajemen Rumah Sakit Menggunakan Framework COBIT 2019 (Studi Kasus: Semen Padang Hospital). *Jurnal Nasional Teknologi Dan Sistem Informasi*, *9*(3), 299–306. https://doi.org/10.25077/teknosi.v9i3.2023.299-306
Nachrowi, E., Yani Nurhadryani, & Heru Sukoco. (2020). Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(4), 764–774. https://doi.org/10.29207/resti.v4i4.2265
Padmi, I. A. A., Githa, D. P., & Susila, A. A. N. H. (2022). Audit Tata Kelola Teknologi Informasi Rumah Sakit Umum X Menggunakan Framework Cobit 2019. *JITTER-Jurnal Ilmiah Teknologi Dan Komputer*, *3*(1), 894–901. https://ojs.unud.ac.id/index.php/jitter/article/view/83146/43131
Putra, S. D., Herman, H., & Yudhana, A. (2023). Audit Tata Kelola Academic Information System Menggunakan Framework Cobit 2019. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(3), 467–474. https://doi.org/10.25126/jtiik.20231036361
Safitri, A., Syafii, I., & Adi, K. (2021). Identifikasi Level Pengelolaan Tata Kelola SIPERUMKIM Kota Salatiga berdasarkan COBIT 2019. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(3), 429–438. https://doi.org/10.29207/resti.v5i3.3060
Solikin, I., & Fauzi, A. (2023). Audit Sistem Infomasi Manajemen Rumah Sakit Menggunakan Framework Cobit 2019 (Studi Kasus Rsud Muaradua). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *8*(3), 934–946. https://doi.org/10.29100/jipi.v8i3.4004
Sukamto, A. S., Novriando, H., & Reynaldi, A. (2021). Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: UPT TIK Universitas Tanjungpura Pontianak). *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *7*(2), 210. https://doi.org/10.26418/jp.v7i2.47859
Sukmajaya, I. B., & Johanes Fernandes Andry. (2019). Audit Sistem Informasi Pada Aplikasi Accurate Menggunakan Model Cobit Framework 4.1 (Studi Kasus: PT. Setia Jaya Teknologi). *Seminar Nasional Teknoka*, *2*(2502–8782), 42–51.
Utama, D. P., Muhammad, A. H., & Purwanto, A. (2023). Audit Manajemen Masalah Teknologi Informasi Menggunakan Kerangka Kerja Cobit 2019 Domain Dss03. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *8*(3), 839–846. https://doi.org/10.29100/jipi.v8i3.3946
Wahyuningtyas, C. A., Purnawan, I. K. A., & Mandenni, N. M. I. M. (2019). Audit Tata Kelola TI Perusahaan X Dengan COBIT 5. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *7*(3), 244–252. https://ojs.unud.ac.id/index.php/merpati/article/view/54250/32985
Widarja, R., & Maulana Sulthon, B. (2023). Audit Layanan Tata Kelola Informasi Rumah Sakit St. Carolus Menggunakan COBIT 2019. *RESOLUSI : Rekayasa Teknik Informatika Dan Informasi*, *4*(1), 21–30. https://djournals.com/resolusi