ANALISIS KEAMANAN INFORMASI RUMAH SAKIT MENGGUNAKAN COBIT 2019 DENGAN FOKUS DOMAIN APO13 : *SYSTEMATIC LITERATURE REVIEW*

Dimaz Aidil Firdaus, Ilham
Sistem Informasi, Universitas Islam Negeri Sunan Ampel Surabaya
Jl. Dr. Ir. H. Soekarno No.682, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Indonesia
didimvanlast@gmail.com

ABSTRAK

Transformasi digital telah memberikan dampak besar pada sektor pelayanan kesehatan, termasuk dalam pengelolaan sistem informasi di fasilitas kesehatan. Namun, berbagai permasalahan terkait keamanan data seperti ancaman kebocoran informasi, serangan dunia maya, serta minimnya pemahaman petugas masih menjadi kendala utama. Studi ini menganalisis penerapan pengamanan data di rumah sakit dengan pendekatan kerangka kerja COBIT 2019, khususnya pada domain APO13 (Pengelolaan Keamanan) melalui tinjauan literatur sistematis. Hasil kajian mengungkapkan bahwa sebagian besar institusi kesehatan baru mencapai tingkat kematangan Level 2-3, belum memenuhi standar optimal Level 4, dengan tantangan utama pada kebijakan, sarana prasarana, dan sumber daya manusia. Solusi yang ditawarkan mencakup program pelatihan berkelanjutan, penyempurnaan regulasi keamanan, penguatan sistem proteksi, serta evaluasi rutin. Temuan ini diharapkan gara bisa menjadi acuan terhadap rumah sakit dalam mengembangkan memaksimalkan keamanan informasi untuk menjamin perlindungan data pasien dan kualitas layanan kesehatan.

Kata kunci : *COBIT 2019, APO13, fasilitas kesehatan, tata kelola teknologi informasi*

1. PENDAHULUAN

Perkembangan teknologi informasi (TI) telah membawa dampak signifikan dalam berbagai sektor, termasuk bidang kesehatan. Rumah sakit sebagai salah satu penyedia layanan kesehatan utama semakin bergantung pada sistem informasi untuk mendukung operasional, mulai dari rekam medis elektronik, manajemen pasien, hingga pertukaran data dengan pihak terkait. Sebagai instansi yang menggunakan teknologi informasi, keamanan selalu menjadi tantangan dan memastikan bahwa data dan informasi tidak rusak, tersedia, akurat, dan rahasia (A, Sardi et al.,2023). Dengan adanya Peraturan Menteri Kesehatan Indonesia No. 82 pada tahun 2013 mengenai Sistem Manajemen Informasi Rumah Sakit (SIMR) di mana semua rumah sakit diharuskan untuk mengelola dan mengembangkan dalam sistem manajemen rumah sakit untuk menciptakan layanan rumah sakit yang efektif, efisien, dan professional menajdi tantangan tersendiri dalam sektor kessehatan [8]. Adanya peraturan tersebut menjadikan masalah keamanan data juga dapat menjadi risiko tersendiri di rumah sakit, suatu tindakan diperlukan untuk melindungi organisasi dan pasien terhadap berbagai kasus pencurian data [6]. Keamanan teknologi informasi dalam rumah sakit tidak hanya berfungsi untuk melindungi data pasien, tetapi juga mempertahankan kepercayaan masyarakat terhadap layanan kesehatan. Jika sistem keamanan tidak memadai, ancaman seperti kebocoran data dan serangan siber dapat mengganggu operasional rumah sakit serta memengaruhi kualitas pelayanan yang diberikan kepada pasien[3]. Untuk meminimalkan hal tersebut, audit keamanan harus diterapkan. Audit keamanan sistem informasi rumah sakit merupakan prosedur pemeriksaan dan penilaian terhadap infrastruktur TI serta kebijakan keamanan yang diterapkan oleh fasilitas kesehatan. Tujuannya adalah memastikan perlindungan data pasien serta mencegah potensi ancaman, baik dari dalam maupun luar organisasi [1].

Audit teknologi informasi mengarah pada standar COBIT (*Control Objectives for Information and Associated Technologies*). Penelitin ini menggunakan kerangka kerja COBIT 2019 (*Control Objectives for Information and Related Technology*) yang merupakan. pembaruan dari COBIT 5 dengan peningkatan signifikan dalam struktur, panduan, dan alat yang tersedia [5]. COBIT 2019 merupakan Kerangka kerja yang komprehensif dan menyeluruh untuk mengelola teknologi informasi, yang dirancang untuk mendukung organisasi dalam mencapai tujuan bisnis melalui pemanfaatan teknologi informasi secara optimal [1]. Keragka kerja COBIT 2019 mencakup beberapa domain yang memiliki tujuan manajemen dan tata Kelola TI [7]. Salah satu domain dalam COBIT 2019 adalah APO (*Align, Plan, and Organize*). Domain APO terdiri dari 14 proses yang berkaitan dengan perencanaan strategis dan operasional untuk memastikan pengimplementasian yang optimal dari sumber daya teknologi informasi. Penelitian ini berfokus pada APO13 (*manage security*) untuk mengelola keamanan TI dan melindungi aset informasi dalam rumah sakit.

Penelitian ini bertujuan untuk mengevaluasi implementasi terkait dengan keamanan informasi rumah sakit dengan menggunakan kerangka kerja COBIT 2019 melalui metode Systematic Literature Review (SLR). Dengan memeriksa berbagai literatur terdahulu, penelitian ini berupaya menemukan berbagai tantangan secara mendalam, metode yang strategis dan praktik terbaik dalam mengelola suatu

risiko keamanan informasi dalam bidang kesehatan. Hasil penelitian ini diharapkan menjadi referensi yang berharga bagi para ahli TI di bidang kesehatan dan pembuat kebijakan untuk meningkatkan sistem keamanan informasi di te tengah pengembangan teknologi digital yang sangat cepat

2. TINJAUAN PUSTAKA

2.1. Sistem Informasi Manajemen Rumah Sakit (SIMRS)

SIMRS merupakan sebuah sistem terpadu yang bertujuan untuk mengoptimalkan pengelolaan data administratif, klinis, serta keuangan di fasilitas kesehatan guna meningkatkan kualitas pelayanan [1]. Sistem tersebut terdiri dari beberapa komponen, seperti manajemen farmasi, pencitraan medis, rekam medis digital, dan sistem laboratorium. Di Indonesia, penerapan SIMRS diatur dalam Peraturan Menteri Kesehatan Nomor 82 Tahun 2013 sebagai upaya untuk menciptakan pelayanan kesehatan yang lebih efisien dan akuntabel [8]. Namun, beberapa kendala seperti masalah integrasi sistem, keterbatasan kompetensi SDM, dan perlindungan data masih menjadi hambatan dalam implementasinya [2].

Beberapa studi sebelumnya telah menemukan berbagai kendala dalam penerapan SIMRS di beberapa rumah sakit. Penelitian oleh A. Algiffary, di RSUD Palembang BARI menunjukkan bahwa kapabilitas sistem informasi di rumah sakit tersebut belum maksimal, terutama pada domain APO13 COBIT 2019 yang masih berada di Tingkat 3. Beberapa faktor penghambat utamanya meliputi keterbatasan pelatihan bagi karyawan serta belum tersedianya pedoman kebijakan keamanan yang komprehensif [1]. Di sisi lain, hasil riset Y. A. Wilar, di RSUD Nabire mengungkapkan bahwa pengelolaan aspek keamanan data masih perlu ditingkatkan akibat kurangnya penyebarluasan kebijakan serta dukungan infrastruktur yang belum optimal [2].

Studi yang dilakukan oleh H. C. T. Amirta di RS Ernaldi Bahar, Sumatera Selatan, menemukan bahwa domain APO12 dan DSS05 berdasarkan standar COBIT 2019 masih berada di Level 1. Temuan ini mengindikasikan bahwa rumah sakit tersebut belum sepenuhnya siap dalam menangani risiko serta mengelola layanan keamanan data [9]. Fenomena serupa ditemukan dalam penelitian A, W. Aulia di RSUD Sekayu, di mana domain APO13 hanya mencapai Level 2. Kondisi ini memperlihatkan bahwa upaya perlindungan informasi masih bersifat dasar dan belum terorganisir secara terstruktur [12].

Berdasarkan temuan beberapa studi tersebut, terlihat bahwa Sistem Informasi Manajemen Rumah Sakit (SIMRS) di Indonesia masih memerlukan penyempurnaan signifikan dalam hal tata kelola TI, khususnya terkait perlindungan data. Penerapan standar internasional seperti COBIT 2019 menjadi krusial untuk menjamin sistem. Tidak hanya berfungsi optimal, tetapi juga mampu melindungi kerahasiaan dan keutuhan informasi medis pasien.

2.2. Keamanan Informasi dalam Rumah Sakit

Aspek keamanan data di rumah sakit memegang peranan penting mengingat tingginya sensitivitas informasi pasien, yang mencakup prinsip kerahasiaan, keakuratan, dan keteraksesan (CIA Triad) [11]. Risiko keamanan seperti serangan siber, kebocoran informasi, dan infeksi malware dapat mengancam kelancaran operasional rumah sakit [1]. Beberapa faktor yang berkontribusi terhadap risiko tersebut diantaranya:

a. Aspek Sumber Daya Manusia: N. Khan dan R. J. Rudman dalam penelitiannya mengungkap kompleksitas tantangan yang dialami rumah sakit di Afrika Selatan, khususnya terkait rendahnya kesadaran staf terhadap keamanan data dan ketidaksesuaian dengan standar regulasi. Temuan penelitian ini menekankan urgensi penerapan strategi terencana untuk mengatasi serangan siber seperti ransomware dan phishing, termasuk peningkatan program pelatihan serta penguatan sistem pengawasan [3].
b. Aspek Infrastruktur: Seperti hasil penelitian A, W. Aulia di RSUD Sekayu mengungkapkan bahwa tingkat penerapan keamanan informasi masih berada pada tahap kedua. Beberapa kendala utama yang ditemukan seperti sistem dokumentasi kebijakan keamanan yang belum terorganisir dengan baik, infrastruktur yang belum memadai, serta kurangnya kontrol hak akses terhadap data penting[12].

Berdasarkan penelitian terdahulu implementasi sistem keamanan data di fasilitas kesehatan Indonesia menghadapi tiga kendala utama, yaitu: pengaturan kebiakan organisasi yang belum optimal; kurangnya pemahaman staff terhadap aspek keamanan digital; dan terbatasnya sarana dan prasarana teknologi. Untuk mengatasi kondisi tersebut.

2.3. Framework COBIT 2019 dan Domain APO13

COBIT 2019 merupakan sebuah framework tata kelola mencakup beberapa domain yang memiliki tujuan manajemen dan tata Kelola TI [7]. Salah satu domain utamanya, APO13 (*Managed Security*), berfokus pada penguatan keamanan informasi melalui:

a. Regulasi Keamanan: Penetapan standar seperti ISO 27001 [8].
b. Pengelolaan Hak Akses: Penerapan prinsip *least privilege* untuk membatasi akses pengguna [11].
c. Pemantauan Sistem: Pelaksanaan audit rutin serta penggunaan alat seperti SIEM (*Security Information and Event Management*) [3].
d. Peningkatan Kesadaran **Staf**: Program edukasi mengenai ancaman seperti *phishing* dan kebijakan keamanan [2].

Beberapa penelitian menunjukkan bahwa implementasi domain APO13 di fasilitas kesehatan masih mengalami berbagai hambatan. Salah satunya adalah studi yang dilakukan N. A. Arimurti et al. (2024) di RSPAU dr. Suhardi Hardjolukito. Hasil penelitian menunjukkan bahwa domain APO11 dan APO12 - yang memiliki keterkaitan erat dengan

APO13 dalam hal manajemen kualitas dan mitigasi risiko - baru mencapai Level 2 pencapaian. Faktor penyebab pencapaian level 2 tersebut adalah ketidaklengkapan dokumentasi, belum adanya prosedur operasional baku, dan program pelatihan yang belum memadai [8].

Selain itu penelitian Moryanda mengungkapkan bahwa implementasi domain APO13 di Semen Padang Hospital masih memiliki keterbatasan. Meskipun framework tersebut telah diterapkan, pencapaian kapabilitasnya baru menyentuh Level 3. Hal tersebut terjadi karena proses adopsi inovasi teknologi yang berjalan lambat, serta belum standar regulasi sistem rekam medis digital belum sepenuhnya tercapai [6].

Dalam beberapa penelitian tersebut, tampak bahwa penerapan domain APO13 pada rumah sakit masih belum mencapai tingkat optimal. Untuk mengatasi tersebut, perlu pendekatan menyeluruh yang mencakup pembaruan kebijakan keamanan data, penguatan sumber daya manusia melalui program pelatihan terstruktur, dan implementasi audit serta pengawasan berkelanjutan. Langkah-langkah strategis tersebut bertujuan agar memaksimalkan manfaat penerapan kerangka kerja COBIT 2019 dalam meningkatkan kualitas layanan kesehatan berbasis teknologi informasi.

2.4. Audit dan Tata Kelola Keamanan Informasi Rumah Sakit

Audit keamanan informasi bertujuan untuk menilai efektivitas langkah-langkah pengamanan serta memastikan kesesuaian dengan regulasi seperti HIPAA dan Permenkes [3]. Proses audit mencakup:

a. Penilaian Risiko: Identifikasi kelemahan sistem menggunakan alat pemindaian kerentanan [1].
b. Pemeriksaan Kontrol: Evaluasi terhadap kebijakan, prosedur, dan infrastruktur keamanan [11].
c. Usulan Perbaikan: Peningkatan keamanan fisik (pemasangan CCTV, akses biometrik), teknis (penggunaan firewall, enkripsi), dan administratif (pelatihan staf) [8].

Seperti penelitian oleh A. W. Aulia yang melakukan audit terhadap RSUD Sekayu menunjukkan bahwa domain APO12 (Manajemen Risiko) dan APO13 (Manajemen Keamanan) masih berada pada level kapabilitas 2. Hal ini menandakan bahwa meskipun rumah sakit telah memulai implementasi tata kelola keamanan, kegiatan yang dilakukan belum terdokumentasi secara menyeluruh dan belum konsisten [12].

Hal serupa terjadi dalam penelitian R. S. A. Gusni di RS Bhayangkara Sespima Polri Jakarta. Analisis audit menemukan bahwa walaupun tingkat kematangan sistem telah mencapai Level 3, terdapat beberapa area yang masih memerlukan perbaikan signifikan, seperti program pentingnya pleatihan staff, pembaruan penilaian risiko, serta control akses fisik yang belum maksimal [11]. Kondisi tersebut menegaskan urgensi evaluasi berkala dan penguatan strategi mitigasi risiko untuk mencapai level kapabilitas yang lebih tinggi.

Berdasarkan penelitian sebelumnya, menunjukkan bahwa audit TI berbasis standar COBIT 2019 bisa menemukan masalah sistemastis dalam pengamanan data rumah sakit. Hasil audit tersebut bukan hanya untuk alat evaluasi, tetapi juga sebagai fondasi untuk perbaikan berkelanjutan yang berdampak langsung pada kualitas layanan kesehatan dan kepercayaan publik.

3. METODE PENELITIAN

Penelitian ini dibuat menggunakan metode Systematic Literature Review (SLR). SLR merupakan metode analisis yang digunakan dengan menggabungkan sejumlah penelitian terdahulu untuk mengidentifikasi dan menganalisis masalah yang terkait dengan objek penelitian saat ini[13]. Peninjauan penelitian menggunakan metode SLR dipilih berdasarkan pertanyaan penelitian (Research Question atau RQ) serta menggunakan kriteria inklusi dan eksklusi yang telah ditentukan oleh peneliti. Research Question (RQ) berperan sebagai metode yang merumuskan pertanyaan-pertanyaan utama yang akan dijawab dalam proses penelitian. Penerapan Research Question bertujuan untuk memastikan agar pertanyaan-pertanyaan dalam penelitian tidak ambigu, tertata dengan jelas, dan juga dapat diteliti terkait pada fokus penelitian.

Tabel 1. Research Question

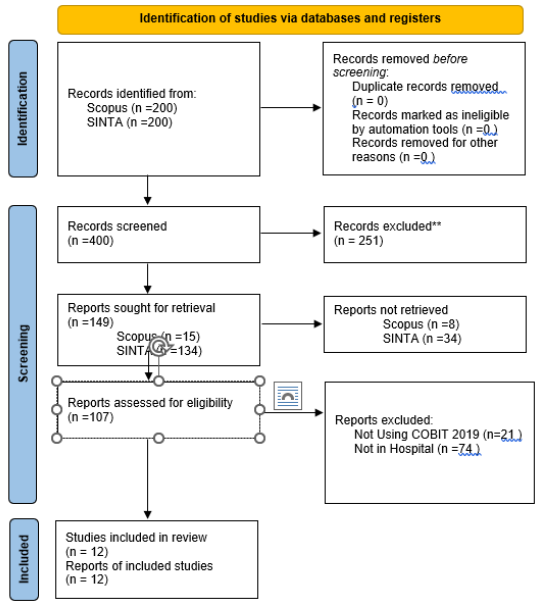
No	Research Question
1.	Apa saja tantangan yang dihadapi oleh rumah sakit dalam implementasi keamanan informasi, baik dari segi teknologi, kebijakan, maupun sumber daya manusia?
2.	Apa dampak yang mungkin terjadi jika sistem keamanan informasi di rumah sakit tidak dikelola dengan baik?
3.	Strategi dan pendekatan apa yang paling efektif dalam memitigasi risiko keamanan informasi di rumah sakit berdasarkan literatur sebelumnya?

Proses itu dilakukan dengan tujuan untuk menemukan beberapa sumber yang relevan dan memiliki keterkaitan, yang mampu mendukung dalam menjawab pertanyaan penelitian (*Research Question*/RQ) serta memberikan referensi tambahan yang sesuai

Tabel 2. Kriteria Inklusi dan Eksklusi

Kategori	Kriteria Inklusi	Kriteria Eksklusi
Sumber Data	Artikel dari *Scopus* dan *SINTA* (SINTA 1–4)	Artikel dari basis data selain *Scopus* dan *SINTA*
Framework	Menggunakan *COBIT 2019* sebagai kerangka utama	Menggunakan kerangka lain di luar *COBIT 2019*
Topik dan Konteks	Implementasi tata kelola TI di rumah sakit atau unit kesehatan	Fokus pada sektor medis (pendidikan, perusahaan, proyek, dll)
Aksesibilitas	Artikel tersedia dalam format *full-text*	Artikel tidak dapat diakses penuh (hanya abstrak/tidak tersedia)
Tahun Publikasi	Diterbitkan antara dalam kurun waktu tahun 2020–2025	Diterbitkan sebelum tahun 2019
Bahasa	Ditulis dalam bahasa Indonesia atau Inggris	Ditulis dalam bahasa lain
Jenis Publikasi	Jurnal ilmiah yang *peer-reviewed* atau *prosiding* terindex	Editorial, opini, ringkasan konferensi, atau jenis publikasi non ilmiah lainnya

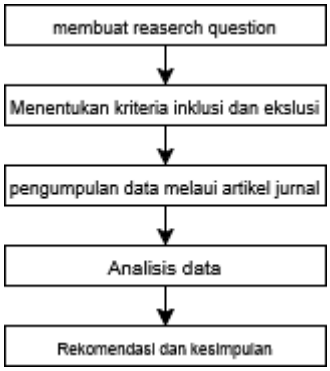
Tabel inklusi dan ekslusi tersebut bertujuan untk menentukan kriteria subjek yang di teliti agar relevan dengan penelitian.



Gambar 1. Diagram PRISMA dalam proses pemilihan artikel untuk membuat *Systematic Review*

Pengumpulan data dilakukan menggunakan metode PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Penelitian ini diawali dengan pencarian literatur pada database terindeks seperti Scopus, SINTA, dan Google Scholar menggunakan kata kunci spesifik, antara lain *'Cobit 2019'*, *'Rumah Sakit'*, dan *'Keamanan Informasi'*. Batasan tahun publikasi artikel yang digunakan adalah periode 2020 hingga 2025.

Dengan melakukan tinjauan awal terhadap literatur terkait keamanan TI di fasilitas kesehatan, penelitian ini menerapkan kriteria inklusi dan eksklusi. Pendekatan ini digunakan untuk memfilter referensi agar tetap relevan dan mendukung tujuan systematic literature review (SLR) yang dilakukan.



Gambar 2. Kerangka kerja penelitian

4. HASIL DAN PEMBAHASAN

Berdasarkan Hasil Tinjauan *Systematic Literatur Review* (SLR) dari 12 artikel ilmiah yang memenuhi kriteria inklusi, penelitian ini menentukan sejumlah hasil penting yang terkait dengan penerapan COBIT 2019, terutama pada domain APO13 di sektor kesehatan khususnya rumah sakit. Semua studi yang dianalisis berasal dari publikasi yang diakui Sinta dan Scopus, dengan konteks yang terkait dengan keamanan informasi dalam sektor rumah sakit.

Tabel 3. Hasil Artikle Acuan

No	Judul	Hasil
1	Audit Keamanan Sistem Informasi Manajemen Rumah Sakit dengan Framework COBIT 2019 pada RSUD Palembang BARI	Rumah Sakit Palembang BARI menghadapi berbagai risiko serius dalam pemanfaatan teknologi informasi, seperti potensi serangan malware, aktivitas peretasan, hingga pencurian data. Selain itu, tantangan dalam memenuhi regulasi terkait keamanan informasi turut menjadi perhatian utama. Ancaman-ancaman ini tidak hanya membahayakan kerahasiaan dan keutuhan data pasien, tetapi juga dapat merusak reputasi rumah sakit serta mengganggu jalannya manajemen dan operasional. Beberapa strategi mitigasi yang dinilai efektif meliputi identifikasi dan evaluasi risiko, penerapan kontrol keamanan yang tepat, kepatuhan terhadap standar keamanan informasi, serta peningkatan pemahaman staf mengenai pentingnya perlindungan sistem informasi. Meski demikian, pelaksanaan strategi ini masih

No	Judul	Hasil
		menghadapi hambatan, seperti lemahnya proses evaluasi sistem, kurangnya pemantauan serta pembaruan terhadap profil risiko, dan rendahnya kesadaran karyawan tentang keamanan informasi. Kendati begitu, dengan komitmen dan upaya berkelanjutan, Rumah Sakit Palembang BARI memiliki peluang besar untuk memperkuat sistem keamanan informasinya..
2	Analisis Keamanan Sistem Manajemen Informasi Rumah Sakit Umum Daerah Nabire	Studi ini menganalisis tingkat keamanan informasi di RSUD Nabire menggunakan framework COBIT 2019. Hasil penelitian menunjukkan bahwa implementasi keamanan informasi masih memiliki beberapa kelemahan, terutama dalam aspek kepatuhan terhadap kebijakan keamanan data dan kurangnya sosialisasi terkait keamanan informasi kepada staf. Rekomendasi yang diberikan mencakup peningkatan pelatihan bagi karyawan, pembaruan kebijakan keamanan, serta peningkatan infrastruktur TI untuk meningkatkan perlindungan data pasien.
3	ANALISIS RISIKO TEKNOLOGI INFORMASI DALAM MANAJEMEN RUMAH SAKIT: SYSTEMATIC LITERATURE REVIEW	Penelitian ini membahas berbagai risiko yang dihadapi dalam implementasi teknologi informasi di rumah sakit. Menggunakan pendekatan berbasis risiko, penelitian ini mengidentifikasi faktor-faktor yang dapat menghambat efektivitas sistem TI dalam manajemen rumah sakit, seperti serangan siber, kesalahan pengguna, dan kurangnya pemeliharaan sistem. Studi ini menyarankan penerapan strategi mitigasi risiko yang lebih efektif, termasuk peningkatan pengawasan keamanan dan peningkatan kesadaran staf terhadap keamanan informasi.
4	IoT medical device risks: Data security, privacy, confidentiality and compliance with HIPAA and COBIT 2019	Sistem keamanan informasi di rumah sakit yang diteliti di Afrika Selatan masih menghadapi tantangan besar, terutama dalam kepatuhan terhadap regulasi keamanan data. Kesadaran staf terhadap keamanan informasi masih rendah, yang meningkatkan risiko kesalahan manusia dalam pengelolaan data. Selain itu, infrastruktur TI yang ada belum memadai untuk menangani serangan siber yang semakin kompleks. Ancaman eksternal seperti serangan ransomware dan phishing menjadi ancaman terbesar, sementara ancaman internal, seperti akses tidak sah oleh karyawan dan kebocoran data yang tidak disengaja, juga menjadi faktor risiko utama. Kurangnya pemantauan dan evaluasi keamanan membuat sistem lebih rentan terhadap serangan.
5	Rancangan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus:PT XYZ)	Hasil penelitian menunjukkan bahwa keamanan teknologi informasi di rumah sakit masih menghadapi berbagai tantangan, terutama dalam aspek regulasi, infrastruktur, dan kesadaran staf terhadap keamanan data. Ancaman terbesar berasal dari serangan siber seperti ransomware dan phishing, serta risiko internal seperti akses tidak sah dan kebocoran data yang tidak disengaja. Kurangnya pemantauan dan evaluasi keamanan semakin meningkatkan kerentanan sistem.
6	Penerapan Kerangka Kerja Keamanan Informasi di Rumah Sakit: Tinjauan Literatur Sistematis	manajemen rumah sakit memiliki komitmen terhadap keamanan informasi, namun belum sepenuhnya didukung oleh kebijakan yang terdokumentasi dan terstandardisasi. Penerapan kerangka kerja seperti ISO/IEC 27001 telah dimulai, tetapi masih bersifat parsial dan belum menyeluruh. Sistem informasi memang sudah dimanfaatkan untuk menyimpan data medis pasien, namun mekanisme perlindungan seperti enkripsi dan kontrol akses belum berjalan secara optimal. Selain itu, keterbatasan sumber daya manusia dan minimnya pelatihan mengenai keamanan informasi juga menjadi tantangan utama. Audit internal serta penilaian risiko belum dilakukan secara rutin, sehingga menyulitkan proses identifikasi dan mitigasi ancaman keamanan. Kesimpulannya, penerapan kerangka kerja keamanan informasi masih dalam tahap awal dan belum merata, sehingga diperlukan penguatan kebijakan, peningkatan pelatihan, dan evaluasi sistem secara berkala agar keamanan informasi di rumah sakit dapat berjalan secara efektif dan menyeluruh.
7	TINJAUAN LITERATUR AUDIT TEKNOLOGI INFORMASI PADA COBIT 2019 FOKUS DOMAIN APO14	audit teknologi informasi berdasarkan kerangka kerja COBIT 2019, khususnya pada domain **APO14 (Managed Data)**, sangat penting untuk memastikan tata kelola data berjalan secara efektif di organisasi. Melalui tinjauan literatur dari berbagai penelitian sebelumnya, artikel ini mengidentifikasi bahwa aspek-aspek seperti klasifikasi data, kualitas data, keamanan, dan integritas data merupakan fokus utama dalam pengelolaan data yang baik. Penelitian-penelitian tersebut menunjukkan bahwa penerapan APO14 membantu organisasi dalam mengelola siklus hidup data, meminimalkan risiko kehilangan atau manipulasi data, serta meningkatkan efisiensi dan kepatuhan terhadap regulasi. Secara keseluruhan, artikel ini menyimpulkan bahwa domain APO14 dalam COBIT 2019 merupakan fondasi penting dalam mendukung tata kelola TI yang terstruktur, akuntabel, dan berorientasi pada nilai bisnis melalui pengelolaan data yang andal dan aman.
8	Penilaian Kapabilitas Tata Kelola Teknologi Informasi Menggunakan	Tata kelola TI di RSPAU dr. Suhardi Hardjolukito masih belum optimal, terutama pada domain APO11 (Managed Quality) dan APO12 (Managed Risk). Penilaian menunjukkan adanya kesenjangan dalam pengelolaan mutu dan risiko, seperti kurangnya dokumentasi, pelaporan, dan prosedur standar. Rekomendasi perbaikan difokuskan pada tiga aspek: people (pelatihan dan komunikasi), process (SOP dan

No	Judul	Hasil
	Kerangka Kerja Cobit 2019 dengan Fokus Domain APO pada RSPAU dr. Suhardi Hardjolukito	dokumentasi), dan technology (pemanfaatan fitur seperti data mining). Dengan perbaikan ini, diharapkan kualitas tata kelola TI dan layanan rumah sakit dapat meningkat.
9	Risk Management Evaluation in Hospital Management Information Systems Using Framework COBIT 2019 - Case Study: Ernaldi Bahar South Sumatera Hospital	mengevaluasi tingkat kapabilitas manajemen risiko TI di Rumah Sakit Ernaldi Bahar, Sumatera Selatan, dengan menggunakan kerangka kerja COBIT 2019. Penelitian ini menilai empat proses utama: EDM03 (Ensured Risk Optimization), APO12 (Managed Risk), DSS03 (Managed Problems), dan DSS05 (Managed Security Services). Hasil pengukuran menunjukkan bahwa proses EDM03 dan DSS03 berada pada level kapabilitas 3, sementara APO12 dan DSS05 hanya berada di level 1. Analisis kesenjangan menunjukkan bahwa proses APO12 dan DSS05 memiliki gap sebesar tiga tingkat dari target yang diharapkan, sedangkan EDM03 dan DSS03 memiliki gap satu tingkat. Studi ini menyimpulkan bahwa tata kelola risiko TI di rumah sakit masih belum terstruktur dengan baik, dan merekomendasikan perbaikan berbasis praktik terbaik COBIT 2019 untuk meningkatkan efektivitas sistem informasi manajemen rumah sakit (SIMRS).
10	Evaluasi Sistem Informasi Manajemen Rumah Sakit Menggunakan Framework COBIT 2019 (Studi Kasus: Semen Padang Hospital)	tata kelola SIMRS di Semen Padang Hospital masih memiliki berbagai tantangan, terutama dalam hal pengembangan sistem, integrasi data, dan pemenuhan regulasi. Penelitian ini menggunakan pendekatan COBIT 2019 dengan analisis 11 faktor desain dan menemukan bahwa tiga domain utama, yaitu EDM03 (Ensured Risk Optimization), APO12 (Managed Risk), dan APO13 (Managed Security), menjadi prioritas karena memiliki nilai kapabilitas tertinggi. Ketiganya mencerminkan fokus rumah sakit dalam mengelola risiko, meningkatkan keamanan informasi, serta menjaga kualitas manajemen data. Meski demikian, rumah sakit masih tergolong lambat dalam mengadopsi teknologi baru dan belum sepenuhnya memenuhi kebijakan rekam medis elektronik sesuai Permenkes No. 24 Tahun 2022. Penelitian ini merekomendasikan perbaikan tata kelola berdasarkan best practice COBIT 2019 agar SIMRS lebih efektif dan adaptif terhadap perkembangan teknologi dan regulasi.
11	Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019	tata kelola keamanan SIM-RS telah diterapkan dengan cukup baik dan berada pada tingkat kapabilitas Level 3 (Defined) dengan tingkat implementasi 73,25%. Penilaian dilakukan terhadap lima proses utama COBIT 2019, yaitu EDM03 (Risk Optimization), APO12 (Risk Management), APO13 (Security Management), APO14 (Data Management), dan DSS05 (Security Service Management). Semua proses berada satu tingkat di bawah level yang diharapkan (Gap = 1). Meski sistem sudah dilengkapi dengan firewall, enkripsi, dan SOP, masih ditemukan kelemahan seperti kurangnya pelatihan keamanan, lemahnya keamanan fisik, dan belum diperbaruinya profil risiko. Penelitian ini merekomendasikan peningkatan keamanan fisik, pelatihan personil, pemantauan sistem berkala, serta pembaruan profil risiko untuk meningkatkan efektivitas tata kelola keamanan informasi di RS Bhayangkara
12	Audit Tata Kelola Teknologi Informasi Di RSUD Sekayu Menggunakan Framework Cobit 2019	implementasi tata kelola TI di RSUD Sekayu belum sepenuhnya optimal. Penilaian dilakukan pada tiga domain utama: APO12 (Manajemen Risiko), APO13 (Manajemen Keamanan), dan BAI10 (Manajemen Konfigurasi). Hasil capability level menunjukkan bahwa domain APO12 dan BAI10 masing-masing berada pada level 1 (belum terorganisir sepenuhnya), sementara APO13 mencapai level 2 (aktivitas dasar telah dilakukan namun belum optimal). Analisis menunjukkan bahwa meskipun beberapa proses telah berjalan, masih banyak aktivitas penting yang belum diterapkan secara menyeluruh. Penelitian ini merekomendasikan agar RSUD Sekayu meningkatkan perencanaan dan dokumentasi aktivitas TI, serta memperkuat manajemen risiko, keamanan, dan konfigurasi agar mampu mencapai target kapabilitas yang lebih tinggi sesuai standar COBIT 2019.

4.1. Tingkata Kapabilitas

Berdasarkan kajian terhadap 12 jurnal ilmiah tersebut, dapat disimpulkan bahwa implementasi tata kelola dan keamanan sistem informasi di sejumlah rumah sakit, baik di dalam maupun luar negeri, menunjukkan kemampuan yang beragam. Namun, mayoritas institusi kesehatan tersebut belum mampu memenuhi standar ideal berdasarkan kerangka kerja COBIT 2019. Proses evaluasi yang paling banyak diteliti umumnya meliputi aspek pengelolaan risiko (APO12), pengendalian keamanan sistem (APO13), serta komponen EDM03 dan DSS05.

Tabel 4. Tingkat Kapabilitas Artikel Acuan

Judul	Domain	Level Kapabilitas
Audit Keamanan Sistem Informasi Manajemen Rumah Sakit dengan Framework COBIT 2019 pada RSUD Palembang BARI	EDM03, APO12, APO13, APO14, DSS05	3

Judul	Domain	Level Kapabilitas
Analisis Keamanan Sistem Manajemen Informasi Rumah Sakit Umum Daerah Nabire	Tidak dirinci	Tidak disebutkan eksplisit, indikasi < Level 3
IoT medical device risks: Data security, privacy, confidentiality and compliance with HIPAA and COBIT 2019	APO13	2
Penilaian Kapabilitas Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 2019 dengan Fokus Domain APO pada RSPAU dr. Suhardi Hardjolukito	APO11, APO12	2
Risk Management Evaluation in Hospital Management Information Systems Using Framework COBIT 2019 – Case Study: Ernaldi Bahar South Sumatera Hospital	EDM03, APO12, DSS03, DSS05	2
Evaluasi Sistem Informasi Manajemen Rumah Sakit Menggunakan Framework COBIT 2019 (Studi Kasus: Semen Padang Hospital)	EDM01, EDM03, EDM05, APO12, APO13, APO14, BAI09, BAI10, DSS02, DSS03, DSS04, DSS05, DSS06, MEA02, MEA03, MEA04	2
Audit Tata Kelola Teknologi Informasi Di RSUD Sekayu Menggunakan Framework Cobit 2019	APO12, APO13, BAI10	2
Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019	EDM03, APO12, APO13, APO14, DSS05	3

4.2. Gap Analys

Berdasarkan berbagai hasil penelitian, kemampuan tata kelola umumnya masih berada pada Level 2 sampai Level 3. Nilai rata-rata APO13 dari berbagai studi yang mengkaji bidang ini mencapai Level 3 (Defined), meskipun implementasinya belum dilakukan secara sistematis dan terukur.

Tabel 5. Gap RSUD Palembang BARI

Domain	*As It*	*To Be*	*Gap*
EDM03	3	4	1
APO12	3	4	1
APO13	3	4	1
APO14	3	4	1
DSS05	3	4	1

Berdasarkan hasil analisis gap, tingkat keamanan Sistem Informasi Manajemen Rumah Sakit (SIMRS) RSUD Palembang BARI saat ini baru mencapai Level 3 (Defined). Capaian ini masih di bawah standar ideal yang ditetapkan, yaitu Level 4 (Quantitative), sehingga teridentifikasi selisih satu level antara kinerja aktual dengan target yang diharapkan.

Tabel 6. Gap RSPAU dr. Suhardi Hardjolukito

Domain	*As It*	*To Be*	*Gap*
APO11	2	3	1
APO12	2	3	1

Hasil analisis gap menunjukkan bahwa tingkat tata Kelola teknologi infrmasi RSPAU dr. Suhardi Hardjolukito masih berada pada Level 2 (Defined) dan belum memenuhi target Level 3 (Quantitative). Dengan demikian, terdapat kesenjangan satu level antara kondisi saat ini dengan standar yang seharusnya dicapai.

Tabel 7. Gap Ernaldi Bahar South Sumatera Hospital

Domain	*As It*	*To Be*	*Gap*
EDM03	3	4	1
APO12	1	4	3
DSS03	3	4	1
DSS05	1	4	3

Hasil analisis gap menunjukkan bahwa tingkat manajemene resiko dan Manajemen sistem informasi rumah sakit Ernaldi Bahar Sumatera selatan masih berada pada Level 1-3 (Defined) dan belum memenuhi target Level 4 (Quantitative). Dengan demikian, terdapat kesenjangan satu level antara kondisi saat ini dengan standar yang seharusnya dicapai.

Tabel 8. Gap Semen Padang Hospital

Domain	*As It*	*To Be*	*Gap*
EDM01	1	4	3
EDM03	4	4	0
EDM05	1	4	3
APO12	4	4	0
APO13	4	4	0
APO14	3	4	1
BAI09	1	4	3
BAI10	1	4	3
DSS02	1	4	3
DSS03	1	4	3
DSS04	1	4	3
DSS05	3	4	1
DSS06	1	4	3
MEA02	1	4	3
MEA03	3	4	1
MEA04	1	4	3

Hasil analisis gap menunjukkan bahwa tingkat Manajemen sistem informasi rumah sakit Semen Padang masih berada pada Level 1-4 (Defined) dan beberapa domain belum memenuhi target Level 4 (Quantitative). Dengan demikian, terdapat

kesenjangan 1-3 level antara kondisi saat ini dengan standar yang seharusnya dicapai.

Tabel 9. Gap RSUD Sekayu

Domain	*As It*	*To Be*	*Gap*
APO12	2	4	2
APO13	3	4	1
BAI10	2	4	2

Hasil analisis gap menunjukkan bahwa tingkat tata Kelola teknologi infrmasi RSUD Sekayu masih berada pada Level 2-3 (Defined) dan belum memenuhi target Level 4 (Quantitative). Dengan demikian, terdapat kesenjangan 1-2 level di antara saat ini dengan standar yang seharusnya dicapai.

Tabel 10. Rumah Sakit Bhayangkara Sespima Polri Jakarta

Domain	*As It*	*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 gap menunjukkan bahwa tingkat Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta masih berada pada Level 3 (Defined) dan belum memenuhi target Level 4 (Quantitative). Dengan demikian, terdapat kesenjangan satu level antara kondisi saat ini dengan standar yang seharusnya dicapai.

Hasil analisis gap mengungkapkan bahwa semua objek yang telah diteliti masih memiliki perbedaan 1-3 level dibandingkan dengan standar kapabilitas yang ditetapkan.

4.3. Rekomendasi Mitigasi

Untuk mengatasi temuan dari penilaian kapabilitas dan gap analys, terdapat beberapa rekomendasi mitigasi yang dapat diimplementasikan guna memperkuat tata kelola keamanan informasi di rumah sakit.

a. Peningkatan pelatihan dan kesadaran keamanan.
   Upaya peningkatan keamanan informasi di rumah sakit harus diawali dengan pelatihan menyeluruh bagi seluruh staf untuk mengatasi rendahnya pemahaman akan ancaman siber dan prosedur operasional yang aman. Pelatihan berkala yang mencakup materi dasar keamanan siber, tata cara pengoperasian sistem, serta penanganan insiden perlu diwajibkan bagi semua karyawan, didukung dengan modul e-learning yang mudah diakses. Langkah ini diharapkan dapat menumbuhkan kesadaran kolektif dalam menjaga keamanan data pasien secara menyeluruh.
b. Pembaruan dan Dokumentasi Kebijakan Keamanan.
   Ketidak aktualan kebijakan dan lemahnya dokumentasi menjadi penyebab utama kerentanan sistem. Oleh karena itu, rumah sakit perlu melakukan tinjauan tahunan kebijakan keamanan yang mencakup dan Menerapkan sistem dokumentasi terpusat untuk pemabruan kebijakan keamanan.
c. Penerapan keamanan fisik dan sistem.
   Penggunaan pengamanan fisik dan sistem menjadi hal penting dalam perlindungan data rumah sakit. Meskipun penggunaan aspek digital seperti firewall telah diimplementasikan, pengendalian akses fisik kerap terabaikan. Solusi komprehensif meliputi penerapan biometrik untuk akses ruang server, sistem pengawasan CCTV, serta proteksi perangkat lunak melalui lisensi resmi dan antivirus terkini.
d. Audit dan monitoring berkala.
   Pelaksanaan audit internal tahunan memungkinkan identifikasi dini terhadap kerentanan sistem dan penyimpangan prosedural, sementara monitoring real-time memfasilitasi deteksi aktivitas mencurigakan seperti akses tidak sah. Implementasi kedua mekanisme tersebut secara terpadu tidak hanya memperkuat postur keamanan tetapi juga meningkatkan responsivitas terhadap insiden, sehingga menjamin kelangsungan layanan kesehatan digital yang berkualitas.
e. Pembaruan dan pemantauan profilrisiko TI.
   Manajemen risiko TI yang efektif memerlukan pembaruan profil risiko secara berkala setiap enam bulan untuk mengantisipasi ancaman siber terkini seperti ransomware dan zero-day exploits. Dengan mengintegrasikan temuan audit dan indikator berbasis teknologi seperti tingkat kerentanan sistem, rumah sakit dapat membangun kerangka manajemen risiko yang dinamis dan responsif, sehingga mengurangi potensi gangguan terhadap keamanan data pasien dan kelancaran operasional layanan kesehatan.

5. KESIMPULAN DAN SARAN

Berdasarkan kajian literatur sistematis terhadap 12 penelitian terkait, studi ini menyimpulkan bahwa implementasi pengamanan data di rumah sakit menggunakan domain APO13 COBIT 2019 masih menghadapi berbagai hambatan, terutama terkait tingkat kematangan sistem yang umumnya berada pada Level 2-3 dan belum mencapai standar ideal (Level 4). Beberapa faktor penghambat utama meliputi keterbatasan pemahaman staff, tidak adanya dokumen kebijakan yang memadai, serta infrastruktur pengamanan yang belum optimal. Untuk mengatasi masalah ini, diperlukan pendekatan terpadu yang mencakup pendidikan berkelanjutan bagi staf, penyusunan regulasi yang komprehensif, serta penerapan teknologi pengawasan modern. Penelitian lanjutan dapat mengembangkan pendekatan ini melalui penelitian Berbasis observasi atau memperluas analisis dengan mencakup domain-domain lain dalam kerangka kerja COBIT 2019 untuk mendapatkan gambaran yang lebih menyeluruh.

DAFTAR PUSTAKA

[1] A. Algiffary, M. Izman Herdiansyah, and Yesi Novaria Kunang, "Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI," *Journal of Applied Computer Science and Technology*, vol. 4, no. 1, pp. 19–26, Jun. 2023, doi: 10.52158/jacost.v4i1.505.

[2] Y. A. Wilar, K. Yuliawan, and A. A. Natsir, "Analisis Keamanan Sistem Manajemen Informasi Rumah Sakit Umum Daerah Nabire," *MAHESA : Malahayati Health Student Journal*, vol. 3, no. 10, pp. 3365–3374, Oct. 2023, doi: 10.33024/mahesa.v3i10.11246.

[3] N. Khan and R. J. Rudman, "IoT medical device risks: Data security, privacy, confidentiality and compliance with HIPAA and COBIT 2019," *South African Journal of Business Management*, vol. 56, no. 1, Feb. 2025, doi: 10.4102/sajbm.v56i1.4796.

[4] H. Carolina, E. Sitompul, M. Fahrezi, and A. Wulansari, "ANALISIS RISIKO TEKNOLOGI INFORMASI DALAM MANAJEMEN RUMAH SAKIT: SYSTEMATIC LITERATURE REVIEW," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 1, pp. 69–74, Feb. 2024, doi: 10.36040/jati.v8i1.8721.

[5] A. M. Fikri, H. S. Priastika, N. Octaraisya, S. Sadriansyah, and L. H. Trinawati, "Rancangan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: PT XYZ)," *INFORMATION MANAGEMENT FOR EDUCATORS AND PROFESSIONALS : Journal of Information Management*, vol. 5, no. 1, p. 1, Dec. 2020, doi: 10.51211/imbi.v5i1.1410.

[6] I. Mardiyana *et al.*, "Penerapan Kerangka Kerja Keamanan Informasi di Rumah Sakit: Tinjauan Literatur Sistematis," *Jutisi : Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, no. 2, p. 729, Aug. 2023, doi: 10.35889/jutisi.v12i2.1260.

[7] A. Zai, Muhammad Alva Hendi, and Asro Nasiri, "TINJAUAN LITERATUR AUDIT TEKNOLOGI INFORMASI PADA COBIT 2019 FOKUS DOMAIN APO14," *Jurnal Informatika Teknologi dan Sains (Jinteks)*, vol. 5, no. 4, pp. 607–611, Dec. 2023, doi: 10.51401/jinteks.v5i4.3507.

[8] N. A. Arimurti, W. A. Nurtrisha, and F. Falahah, "Penilaian Kapabilitas Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 2019 dengan Fokus Domain APO pada RSPAU Dr. Suhardi Hardjolukito," *Jurnal Teknologi dan Manajemen Informatika*, vol. 10, no. 1, pp. 13–23, Jun. 2024, doi: 10.26905/jtmi.v10i1.10939.

[9] H. C. T. Amirta, M. I. Jambak, P. P. Suarli, Y. Utama, A. Wedhasmara, and P. E. Sevtiyuni, "Risk Management Evaluation in Hospital Management Information Systems Using Framework COBIT 2019 - Case Study: Ernaldi Bahar South Sumatera Hospital," *Sriwijaya Journal of Informatics and Applications*, vol. 4, no. 1, Apr. 2023, doi: 10.36706/sjia.v4i1.52.

[10] R. Moryanda, V. Pujani, and Y. Marpaung, "Evaluasi Sistem Informasi Manajemen Rumah Sakit Menggunakan Framework COBIT 2019 (Studi Kasus: Semen Padang Hospital)," *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 9, no. 3, pp. 299–306, Jan. 2024, doi: 10.25077/teknosi.v9i3.2023.299-306.

[11] R. S. A. Gusni, Kraugusteeliana, dan I. W. W. Pradnyana, "Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019," *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)*, Jakarta, Indonesia, 15 September 2021, e-ISBN 978-623-93343-4-5.

[12] A. W. Aulia, M. Ulfa, Suyanto, dan T. Ibadi, "Audit Tata Kelola Teknologi Informasi di RSUD Sekayu Menggunakan Framework COBIT 2019," *Jurnal Riset Sistem Informasi dan Teknik Informatika (JURASIK)*, vol. 8, no. 2, pp. 816–828, Agustus 2023, doi: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik.

[13] F. Z. Nisa', G. D. Febrianti, and N. N. Ajrina, "Systematic Literature Review: Analisis Implementasi Manajemen Risiko TI Menggunakan Framework COBIT di Sektor Industri Jasa," *Bulletin of Computer Science Research*, vol. 4, no. 1, pp. 66–74, Dec. 2023, doi: 10.47065/bulletincsr.v4i1.313.