

Jurnal JTik (Jurnal Teknologi Informasi dan Komunikasi)

DOI: <https://doi.org/10.35870/jtik.v9i3.3528>

Evaluasi Tata Kelola Keamanan Informasi Menggunakan Framework COBIT 5 Domain APO13 dan DSS05 (Studi Kasus: Klinik Pratama Rawat Jalan Watumas)

Tarwoto¹, Oktafia Heng Huice², Sri Wahyuningsih^{3*}

^{1,2,3*} Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto, Kota Banyumas, Provinsi Jawa Tengah, Indonesia.

article info

Article history:

Received 10 December 2024

Received in revised form

20 December 2024

Accepted 15 January 2025

Available online Juli 2025.

Keywords:

Evaluation; Information Security; Security Management; Security Service Management; COBIT 5.

Kata Kunci:

Evaluation; Information Security; Security Management; Security Service Management; COBIT 5.

abstract

The Watumas Outpatient Pratama Clinic is an institution that utilizes Information Technology (IT) to assist its operations and health services. IT empowerment in this clinic is carried out by the department responsible for the technology applied, including the management and storage of highly sensitive patient data. Considering the importance of protecting the data and information collected, a good security system is needed to protect the clinic from potential threats that could be detrimental. Evaluation of the quality of information security management is necessary to ensure that the information technology used is safe and trustworthy. This research adopts a qualitative approach through the use of the COBIT 5 framework, especially in the APO13 (Managing Security) and DSS05 (Managing Security Services) stages, to assess the level of information security implemented. Data was collected through observation, interviews, and the use of assessment sheet instruments. The research results show that both stages are at level 2 (Managed Process), while the level expected by the clinic is level 3 (Established Process). This indicates that there is a gap of one level in each process. This research also provides several recommendations for improving information security management by considering the gaps that arise.

abstract

Klinik Pratama Rawat Jalan Watumas adalah sebuah lembaga yang memanfaatkan Teknologi Informasi (TI) dalam membantu operasional dan pelayanan kesehatannya. Pemberdayaan TI di klinik ini dilakukan oleh departemen yang bertanggung jawab atas teknologi yang diterapkan, termasuk dalam pengelolaan dan penyimpanan data pasien yang bersifat sangat sensitif. Mengingat pentingnya perlindungan terhadap data dan informasi yang dihimpun, maka diperlukan sistem keamanan yang baik untuk melindungi klinik dari potensi ancaman yang dapat merugikan. Evaluasi terhadap mutu pengelolaan keamanan informasi diperlukan dalam menjamin bahwa teknologi informasi yang digunakan sudah aman dan dapat dipercaya. Penelitian ini mengadopsi pendekatan kualitatif melalui pemanfaatan framework COBIT 5, khususnya dalam tahapan APO13 (Mengelola Keamanan) dan DSS05 (Mengelola Layanan Keamanan), untuk menilai tingkat keamanan informasi yang diterapkan. Data dikumpulkan melalui observasi, wawancara, dan penggunaan instrumen lembar penilaian. Hasil penelitian menunjukkan bahwa kedua tahapan tersebut berada pada level 2 (Managed Process), sementara tingkat yang diharapkan oleh klinik adalah level 3 (Established Process). Hal ini menandakan adanya kesenjangan (gap level) sebesar satu level di setiap proses. Penelitian ini juga memberikan beberapa rekomendasi untuk meningkatkan pengelolaan keamanan informasi melalui mempertimbangkan kesenjangan yang timbul.

Corresponding Author. Email: sriwhyunsh@gmail.com ^{3}.

Copyright 2025 by the authors of this article. Published by Lembaga Otonom Lembaga Informasi dan Riset Indonesia (KITA INFO dan RISET). This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. 

1. Pendahuluan

Klinik Pratama Rawat Jalan Watumas merupakan fasilitas kesehatan yang berkomitmen untuk meningkatkan layanan kepada pasien dengan memanfaatkan *teknologi informasi* (TI). Penggunaan TI di klinik ini mencakup berbagai aspek operasional, termasuk manajemen administrasi pasien, pengelolaan data kesehatan, serta manajemen sumber daya manusia. Selain itu, klinik juga menerapkan sistem berbagi file untuk mempermudah akses administrasi antarunit dan data medis. Tujuan utama dari penerapan TI ini adalah untuk meningkatkan efisiensi dan kualitas layanan. Meskipun demikian, terdapat beberapa masalah terkait keamanan data dan informasi yang dihimpun dalam sistem klinik (Ilham Akbar Sodik & Nugraheni, 2022). Salah satu tantangan utama yang dihadapi adalah minimnya jaminan keamanan data, terutama dalam hal perlindungan data pasien. Akses terhadap data sensitif di klinik hanya boleh dilakukan oleh pihak yang berwenang. Namun, penggunaan sistem *file-sharing* untuk transfer data antar unit meningkatkan kemungkinan terjadinya akses yang tidak sah. Selain itu, ada potensi ancaman dari luar berupa upaya peretasan yang menunjukkan bahwa sistem yang ada saat ini masih rentan terhadap serangan siber.

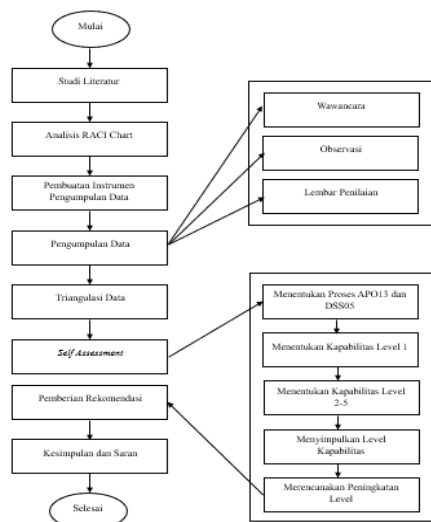
Ancaman tersebut dapat membuka peluang bagi pihak yang tidak berwenang untuk mengakses data yang berisiko merusak privasi pasien dan merugikan reputasi klinik secara keseluruhan (Algiffary *et al.*, 2023). Sebagai penyedia layanan kesehatan, Klinik Pratama Rawat Jalan Watumas perlu memberikan perhatian serius terhadap pengelolaan *keamanan informasi*. Semakin banyak sistem informasi yang diterapkan, semakin besar pula jumlah data sensitif yang harus dilindungi. *Keamanan informasi* yang baik menjadi faktor kunci dalam mempertahankan kepercayaan pasien serta menjaga reputasi klinik. Menurut teori *keamanan informasi*, ada tiga aspek utama yang harus dilindungi, yaitu "kerahasiaan" (*confidentiality*), "integritas" (*integrity*), dan "ketersediaan" (*availability*). *Kerahasiaan* memastikan bahwa data hanya dapat diakses oleh entitas yang berwenang, *integritas* menjamin bahwa data tidak dapat diubah oleh pihak yang tidak sah, sementara *ketersediaan* memastikan bahwa data dapat diakses saat dibutuhkan (Vansuri *et al.*, 2023). Untuk menjaga

kerahasiaan serta kepercayaan dalam penyimpanan data pasien dan operasional klinik, ketiga aspek tersebut menjadi dasar dalam pengelolaan *keamanan informasi*. Menghadapi permasalahan ini, pengamanan informasi tidak hanya cukup dilakukan melalui pendekatan teknis, seperti penggunaan *firewall* atau enkripsi data. Diperlukan pendekatan manajerial yang terstruktur dan berkelanjutan. *COBIT 5*, yang merupakan singkatan dari "*Control Objectives for Information and Related Technology*", adalah framework yang dapat digunakan untuk mengevaluasi dan meningkatkan tata kelola *keamanan informasi*. Framework ini memberikan panduan dalam tata kelola dan manajemen TI yang seimbang antara manfaat dan risiko penggunaan sumber daya TI, yang pada akhirnya dapat membantu mencapai tujuan organisasi (Imania, 2024). *COBIT 5* mencakup beberapa domain yang relevan dalam pengelolaan *keamanan informasi*, seperti *APO13 "Manage Security"* dan *DSS05 "Manage Security Services"*. *APO13* berfokus pada pengimplementasian manajemen keamanan yang menyeluruh, sedangkan *DSS05* mengelola layanan keamanan di tingkat operasional. Kedua domain ini memungkinkan organisasi untuk melakukan evaluasi secara menyeluruh mengenai tata kelola keamanan informasi, terutama yang berkaitan dengan pengelolaan risiko dan ancaman yang ada (Sinaga *et al.*, 2021).

Penelitian sebelumnya juga mendukung penggunaan *COBIT 5* sebagai alat untuk evaluasi *keamanan informasi*. Simamora & Vieri Putra (2024) dalam penelitiannya berjudul "Evaluasi Tata Kelola Keamanan Sistem Informasi Menggunakan Framework *COBIT 5* (Studi Kasus: PT BPR XYZ)" bertujuan untuk mengevaluasi *keamanan sistem informasi* pada PT BPR XYZ, sebuah lembaga bank pengkreditan rakyat yang menghadapi risiko serangan siber tinggi. Dalam penelitian tersebut, evaluasi di domain *APO13* dan *DSS05* menunjukkan bahwa tingkat kesiapan dan kemampuan *keamanan data* berada di level 3, sementara tingkat yang diinginkan adalah level 4, yang menunjukkan adanya kesenjangan sebesar satu level (Simamora & Putra Kartika, 2024). Selain itu, penelitian M. Khairul Anamr *et al.* (2023) mengenai penerapan *COBIT 2019*, yang berfokus pada domain *APO13* dan *DSS05*, memberikan pemahaman lebih dalam mengenai pengelolaan keamanan sistem informasi.

Penelitian ini menyarankan agar institusi pendidikan, seperti STMIK Amik Riau, merancang kebijakan dan prosedur keamanan yang efektif untuk melindungi data akademik dan informasi sensitif lainnya. Implementasi standar keamanan informasi yang sesuai dapat mengurangi risiko yang ditimbulkan oleh ancaman eksternal serta kebocoran data internal, sekaligus meningkatkan tingkat kematangan tata kelola keamanan sistem informasi di masa depan (Anam *et al.*, 2023). Dengan penerapan framework *COBIT 5*, khususnya di domain *APO13* dan *DSS05*, Klinik Pratama Rawat Jalan Watumas dapat melakukan evaluasi dan memperkuat pengelolaan keamanan informasi yang ada. Evaluasi ini diharapkan dapat memberikan saran yang bermanfaat untuk meningkatkan pengelolaan keamanan informasi di klinik, sekaligus menjaga kepercayaan pasien terhadap kerahasiaan dan keamanan data mereka.

2. Metodologi Penelitian



Gambar 1. Metodologi Penelitian

Gambar 1 menggambarkan langkah-langkah yang diambil dalam penelitian ini. Tahap pertama dimulai dengan melakukan studi literatur, yang bertujuan untuk mengidentifikasi dan memeriksa studi-studi sebelumnya yang membahas fenomena yang relevan dengan masalah yang diteliti dalam studi ini. Tujuan dari studi literatur ini adalah untuk memperoleh pemahaman dasar mengenai konsep dan teori dasar tentang keamanan informasi, serta bagaimana

framework *COBIT 5* diterapkan, khususnya dalam domain *APO13* dan *DSS05*. Tahap berikutnya adalah menganalisis diagram *RACI* atau "Responsible, Accountable, Consulted, and Informed" dalam setiap proses pada *COBIT 5* yang terkait dengan keamanan data. Diagram ini membantu dalam menentukan fungsi dan tanggung jawab masing-masing pihak dalam setiap tahap. Setelah itu, tahap ketiga adalah penyusunan instrumen penelitian untuk mengumpulkan data, yang dilakukan setelah analisis *RACI Chart*. Instrumen ini meliputi pedoman wawancara dan lembar penilaian yang digunakan untuk menilai seberapa efektif tata kelola keamanan informasi di klinik. Instrumen ini dirancang untuk mengumpulkan informasi yang relevan dan akurat dari pihak-pihak yang terlibat dalam pengelolaan keamanan data.

Tahap keempat melibatkan pengumpulan data melalui berbagai metode, termasuk observasi, lembar penilaian, dan wawancara dengan pihak terkait. Pemahaman langsung tentang praktik keamanan data di lapangan diperoleh melalui observasi, sementara lembar penilaian dan wawancara memberikan perspektif dari pihak yang bertanggung jawab atas pengelolaan dan keamanan data. Tahap kelima adalah triangulasi data setelah data terkumpul. Proses ini membandingkan informasi yang diperoleh dari berbagai sumber untuk meningkatkan validitas data, dengan tujuan agar hasil penelitian menjadi lebih akurat dan dapat diandalkan. Pada tahap keenam, dilakukan *self-assessment* berdasarkan tahapan *COBIT 5* yang telah ditentukan (*APO13* dan *DSS05*) untuk mengevaluasi seberapa baik praktik keamanan informasi perusahaan telah sesuai dengan standar yang ada. Hasil evaluasi ini memberikan gambaran tentang kekuatan dan kelemahan dalam pengelolaan keamanan data. Berdasarkan hasil *self-assessment*, tahap ketujuh adalah pemberian rekomendasi yang bertujuan untuk memenuhi standar dan praktik terbaik yang ada dalam *COBIT 5*, serta untuk memperbaiki dan meningkatkan tata kelola *keamanan informasi* di organisasi. Terakhir, hasil penelitian disimpulkan, dan saran untuk penelitian lebih lanjut diberikan. Kesimpulan ini menguraikan hasil utama dari penelitian dan menawarkan rekomendasi yang dapat digunakan dalam proyek-proyek mendatang untuk mengembangkan tata kelola *keamanan data* (Dzikri Imany *et al.*, 2019).

3. Hasil dan Pembahasan

Hasil

Analisis RACI Chart

RACI Chart atau "*Responsible, Accountable, Consulted, Informed*" adalah alat yang digunakan untuk mengidentifikasi dan menentukan fungsi serta tanggung jawab dalam sebuah organisasi. Dalam kerangka kerja *COBIT 5*, *RACI Chart* diterapkan untuk seluruh proses guna membantu menetapkan peran yang jelas dalam manajemen keamanan informasi. *RACI Chart* mencakup empat peran utama: *Responsible*, yang merujuk pada pihak yang bertanggung jawab langsung untuk melaksanakan suatu proses; *Accountable*, yaitu individu yang memiliki otoritas penuh dan memberikan arahan terkait pelaksanaan proses; *Consulted*, yaitu pihak yang memberikan saran atau panduan dalam pelaksanaan tugas; dan *Informed*, yang merupakan individu yang perlu menerima informasi tentang perkembangan

atau hasil proses. Berdasarkan analisis menggunakan *RACI Chart*, peran *Responsible* dan *Accountable* dianggap sangat penting dalam evaluasi *keamanan informasi* karena keduanya terlibat langsung dalam pelaksanaan dan pengambilan keputusan terkait pengelolaan keamanan informasi (Triyunsari & Sutabri, 2023). Di Klinik Pratama Rawat Jalan Watumas, pemetaan *RACI Chart* dilakukan melalui tahap menganalisis kewajiban dan peran setiap bagian dalam struktur organisasi klinik. Tujuan dari pemetaan ini adalah untuk menyelaraskan peran dalam *RACI Chart* dengan posisi yang ada di dalam struktur organisasi klinik, guna memastikan bahwa pengelolaan keamanan informasi dapat dilaksanakan secara efektif dan sesuai dengan standar yang telah ditetapkan. Tabel 1 menunjukkan pemetaan *RACI Chart* pada tahap *APO13* yang menggambarkan alokasi peran utama berdasarkan jabatan yang ada di klinik (Hardiansyah & Tyroni Mursityo, 2020).

Tabel 1. Analisis RACI Chart Proses APO13

Komponen	Peran	Jabatan
<i>Responsible</i>	<i>IT Administrator</i>	<i>Teknisi IT</i>
	<i>Information Security Officer</i>	<i>Staf Keamanan Informasi</i>
<i>Accountable</i>	<i>Chief Information Security Officer</i>	<i>Kepala Departemen IT</i>
	<i>Clinic Operations Manager</i>	<i>Manajer Operasional Klinik</i>

Berdasarkan Tabel 1, posisi *IT Administrator* dalam struktur organisasi klinik disebut *Teknisi IT*, yang ditetapkan sebagai entitas *Responsible* dalam menjawab lembar penilaian dokumen pada tahapan *APO13*. Hal ini sesuai dengan struktur organisasi saat ini, di mana *Teknisi IT* memiliki tanggung jawab yang setara dengan peran *IT Administrator*, yaitu mengelola, mengawasi, dan memastikan bahwa sistem *TI* berfungsi secara optimal untuk mendukung operasional klinik. Untuk peran *Information Security Officer* dalam struktur organisasi, jabatan ini setara dengan *Staf Keamanan Informasi*, yang berperan sebagai pihak *Responsible*. Pihak ini bertanggung jawab untuk mengimplementasikan kebijakan dan prosedur *keamanan data* di klinik serta memastikan bahwa semua tugas terkait pengelolaan *keamanan data*, seperti menjaga data sensitif dan mengurangi risiko, dilakukan sesuai dengan aturan yang ditetapkan oleh organisasi. Di sisi lain, peran *Chief Information Security Officer* dalam struktur organisasi dikenal sebagai *Kepala Departemen IT*, yang berfungsi sebagai pihak

Accountable dengan otoritas penuh untuk membuat keputusan mengenai kebijakan dan praktik *keamanan informasi* klinik. Pihak ini juga bertanggung jawab memastikan bahwa semua komponen *keamanan informasi* di klinik dikelola dengan baik dan memenuhi persyaratan yang diperlukan untuk melindungi data dan sistem klinik.

Selanjutnya, peran *Clinic Operations Manager* dalam struktur organisasi dikenal dengan sebutan *Manajer Operasional Klinik*, yang juga berfungsi sebagai pihak *Accountable*. Tanggung jawab utama peran ini adalah memastikan bahwa operasional klinik berjalan lancar, termasuk pengelolaan sumber daya dan proses yang mendukung *keamanan informasi*. Sebagai entitas yang bertanggung jawab, *Manajer Operasional Klinik* memiliki kewenangan untuk memastikan bahwa semua regulasi dan prosedur terkait *keamanan data* diikuti dengan baik di seluruh operasional klinik, serta berperan penting dalam pengambilan keputusan strategis terkait *keamanan informasi*. *Teknisi IT* berfungsi mirip dengan

IT Administrator dalam *RACI Chart*, yang bertanggung jawab atas pengelolaan dan penyelesaian masalah terkait sistem *teknologi informasi* di klinik. Sementara itu, *Kepala Departemen IT*, yang setara

dengan *Chief Information Security Officer*, memiliki peran utama dalam memastikan *keamanan data* di klinik.

Tabel 2. Analisis RACI Chart Proses DSS05

Komponen	Peran	Jabatan
<i>Responsible</i>	<i>IT Administrator</i>	<i>Teknisi IT</i>
	<i>Information Security Officer</i>	<i>Staf Keamanan Informasi</i>
<i>Accountable</i>	<i>Chief Information Security Officer</i>	<i>Kepala Departemen IT</i>
	<i>Clinic Operations Manager</i>	<i>Manajer Operasional Klinik</i>

Berdasarkan tabel 2, posisi *IT Administrator* dalam struktur organisasi dikenal dengan sebutan *Teknisi IT*, yang ditunjuk sebagai pihak *Responsible* untuk mengelola dan memantau pemeliharaan layanan *TI* yang terkait dengan proses *DSS05*. *Teknisi IT* bertanggung jawab untuk memastikan bahwa sistem *TI* berjalan secara optimal dan memenuhi kebutuhan operasional klinik. Sementara itu, peran *Information Security Officer* dalam struktur organisasi disebut *Staf Keamanan Informasi*, yang juga ditunjuk sebagai pihak *Responsible* dalam proses *DSS05*. *Staf Keamanan Informasi* bertanggung jawab untuk mengimplementasikan kebijakan dan prosedur keamanan informasi terkait dengan pemeliharaan dan pengelolaan data, serta memastikan bahwa data yang dipelihara tetap aman dan sesuai dengan standar yang berlaku. Selanjutnya, *Chief Information Security Officer* dalam struktur organisasi disebut *Kepala Departemen IT*, yang berperan sebagai entitas *Accountable* dalam proses *DSS05*.

Kepala Departemen IT memiliki wewenang penuh untuk mengambil keputusan mengenai kebijakan dan pengelolaan sistem *TI* yang berhubungan dengan pemeliharaan serta keamanan informasi dan data klinik. Posisi *Clinic Operations Manager*, yang dalam organisasi dikenal dengan sebutan *Manajer Operasional Klinik*, juga berperan sebagai pihak *Accountable* untuk memastikan kelancaran operasional klinik, termasuk pemeliharaan dan pengelolaan sistem *TI* yang mendukung kegiatan operasional. *Manajer Operasional Klinik* berperan dalam pengambilan keputusan strategis terkait dengan pengelolaan *TI* dan keamanan informasi. *Teknisi IT* berfungsi serupa dengan *IT Administrator* pada *RACI Chart* Proses *DSS05*, yaitu sebagai entitas yang bertanggung jawab atas pengelolaan dan

pemeliharaan sistem *TI* klinik. Sementara itu, *Kepala Departemen IT*, yang setara dengan *Chief Information Security Officer*, memiliki peran utama dalam memastikan pengelolaan keamanan data dan kebijakan *TI* di klinik.

Manage Security (APO13)

APO13 adalah tahap dalam *COBIT 5* yang berfokus pada penjabaran, pengelolaan, dan pengendalian keamanan informasi serta pengelolaan risiko informasi pada tingkat yang dapat diterima oleh organisasi. Tujuan dari tahap ini adalah untuk memastikan bahwa dampak dari ancaman terhadap keamanan data tetap berada dalam batas yang ditentukan oleh organisasi. Dalam hal ini, penerapan tahap *APO13* dan *DSS05* dari *COBIT 5* di Klinik Pratama Rawat Jalan Watumas dapat membantu mengevaluasi dan memperkuat sistem keamanan informasi yang ada. Dengan menerapkan kedua domain ini, klinik dapat memastikan bahwa kebijakan dan prosedur pengamanan yang efektif diterapkan untuk mengelola risiko serta melindungi data sensitif, seperti data pasien, agar tetap aman dan rahasia (Aftaa Aulia *et al.*, 2021). Pada penilaian level berikutnya, sejumlah *Generic Practices* dan *Generic Work Products* dihasilkan, berupa Dokumen Pedoman Tata Kelola *TI*, yang mencakup Prosedur Pengamanan *TI* dan Dokumen Prosedur Operasi lengkap dengan langkah-langkah prosedural serta diagram alir. Hasil penilaian pada level ini menunjukkan bahwa proses telah mencapai status *largely achieved*, sehingga penilaian bisa dilanjutkan ke level berikutnya. Namun, penilaian dihentikan pada level 3 karena salah satu atribut pada level tersebut hanya mencapai status *partially achieved*, yaitu pada atribut proses 3.2 (*PA 3.2*). Dengan demikian, proses penilaian berakhir pada level 2 *Managed Process*, meskipun pada level 3 *Established*

Process, atribut 3.1 (PA 3.1) telah mencapai status *largely achieved*, sementara atribut 3.2 (PA 3.2) hanya tercapai pada status *partially achieved*. Berdasarkan hasil evaluasi tersebut, proses ini tidak dapat dilanjutkan ke level berikutnya karena salah satu atribut proses

belum mencapai status *largely achieved* (Shaharani Azpriyenne Cahyono *et al.*, 2023). Evaluasi keseluruhan pada tahapan APO13 dapat dilihat pada Tabel 3.

Tabel 3. Penilaian Proses APO13

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5				
	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
	L	L	L	L	P				
			2						

Pada tabel 3, dapat dijelaskan bahwa evaluasi pada tahap APO13 mencapai level 2, yaitu "Managed Process", dengan catatan bahwa pada level 3, atribut pada tahap 3.1 (PA 3.1) memenuhi kriteria "Largely Achieved", sementara atribut pada tahap 3.2 (PA 3.2) hanya mencapai status "Partially Achieved". Berdasarkan wawancara yang dilakukan, Klinik Pratama Rawat Jalan Watumas mengharapkan bahwa proses APO13 dapat mencapai level 3. Oleh karena itu, terdapat kesenjangan (gap) satu level antara kondisi yang tercapai saat ini dan level yang diinginkan oleh klinik.

Manage Security Services (DSS05)

DSS05 adalah salah satu tahapan dalam framework COBIT 5 yang bertujuan untuk memperkuat layanan keamanan informasi dalam organisasi, dengan fokus untuk memastikan bahwa risiko keamanan informasi tetap berada dalam batas yang aman sesuai dengan standar yang telah ditetapkan. Praktik dasar dan produk kerja yang dihasilkan dalam evaluasi tahap ini mencakup Dokumen Prosedur Operasi Instalasi dan Monitoring Software, kegiatan klasifikasi data, log untuk Firewall & Antivirus, Dokumen Prosedur Operasi Hak Akses, Dokumen Prosedur Operasi Lisensi Software, serta dokumen prosedur terkait

pengamanan TI. Meskipun proses klasifikasi data telah diterapkan di Klinik Pratama Rawat Jalan Watumas, tidak ditemukan dokumen yang menjabarkan prosedur klasifikasi data yang diterapkan oleh klinik (Fitri Afifah *et al.*, 2022). Pada evaluasi tahap berikutnya, praktik umum dan produk kerja yang dikembangkan mencakup Dokumen Prosedur Operasi Instalasi dan Monitoring Software untuk bagian Prosedur Pengamanan Software, Dokumen Prosedur Operasi Pengelolaan Masalah TI dalam Diagram Alir, serta prosedur terkait pengelompokan klasifikasi masalah. Selain itu, Dokumen Prosedur Operasi Pengelolaan Hak Akses juga termasuk dalam prosedur pemberian hak akses TI. Evaluasi pada tahap ini berhenti pada level 3 untuk atribut tahap kedua (PA 3.2), yang mencapai kriteria *partially achieved*, sementara atribut pada proses sebelumnya sudah memenuhi kriteria *largely achieved* (Hafizh Abiyyu Firdaus *et al.*, 2024). Karena salah satu atribut proses belum mencapai kriteria *largely achieved*, penilaian pada proses DSS05 di Klinik Pratama Rawat Jalan Watumas tidak berhasil mencapai level berikutnya. Gambaran evaluasi untuk proses DSS05 dapat dilihat pada Tabel 4.

Tabel 4. Penilaian Proses DSS05

Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
	L	L	L	L	P				
			2						

Tabel 4 menunjukkan bahwa proses DSS05 yang diterapkan di Klinik Pratama Rawat Jalan Watumas sudah menginjak level 2 "Managed Process", yang memiliki catatan bahwa di level 3, atribut PA 3.1 telah

mencapai kriteria berhasil dicapai secara signifikan, sementara PA 3.2 baru mencapai kriteria tercapai sebagian. Hasil wawancara yang dilakukan menunjukkan bahwa pihak manajemen Klinik

Pratama Rawat Jalan Watumas menginginkan agar pencapaian pada proses DSS05 dapat mencapai level 3. Terdapat kesenjangan atau perbedaan sebesar satu level pada proses DSS05 yang perlu diperbaiki untuk mencapai target tersebut.

Manage Security (APO13)

Analisis menunjukkan bahwa tahapan *APO13* “*Manage Security*” di Klinik Pratama Rawat Jalan Watumas saat ini berada pada level 2, yaitu “*Managed Process*”. Klinik ini berkeinginan untuk meningkatkan proses tersebut ke level 3, yaitu “*Established Process*”, di mana prosedur-prosedur sudah terstandarisasi dan tujuan dari setiap proses dapat tercapai dengan baik (Khairunnisa *et al.*, 2024). Rekomendasi pertama untuk meningkatkan tata kelola keamanan informasi pada proses *APO13* adalah menyusun dokumen studi kasus bisnis yang berkaitan dengan keamanan informasi. Dokumen ini bertujuan untuk memperkuat pemahaman pemangku kepentingan mengenai kebijakan keamanan informasi yang diberlakukan di klinik. Rekomendasi kedua adalah penguatan manajemen keamanan informasi melalui penerapan standar internasional, yaitu ISO/IEC 27001:2013. Selain itu, dibutuhkan analisis untuk mengidentifikasi area-area yang perlu ditingkatkan dalam aspek keamanan. Rekomendasi ketiga mencakup pelaksanaan audit keamanan informasi secara komprehensif dan rutin, dengan menggunakan standar seperti *ISO/IEC 27001*, *ITIL Security*

Management, atau standar lokal seperti *Indeks KAMI*. Audit ini akan membantu memastikan bahwa prosedur-prosedur keamanan yang telah diterapkan berjalan efektif dan sesuai dengan standar yang berlaku. Rekomendasi keempat berfokus pada peningkatan pemahaman mengenai keamanan informasi di seluruh satuan kerja. Langkah ini bertujuan untuk meningkatkan kesadaran tentang pentingnya keamanan data serta mengurangi risiko perpindahan data ke pihak yang tidak berwenang. Satuan kerja TI perlu diberikan pelatihan khusus agar mampu menangani tugas yang memerlukan keahlian tertentu dan sertifikasi yang sesuai. Rekomendasi kelima menyarankan agar Dokumen Pedoman Tata Kelola TI diperbarui dengan mencakup informasi mengenai infrastruktur dan lingkungan kerja yang diperlukan untuk mengelola keamanan informasi secara optimal. Rekomendasi keenam adalah penyusunan kebijakan untuk memantau dan melaporkan tahapan manajemen *keamanan informasi* sesuai dengan kriteria yang ditetapkan. Kebijakan ini akan melengkapi rekomendasi lainnya agar proses *APO13* dapat mencapai level 3 yang diinginkan. Enam rekomendasi tersebut dirangkum dalam Tabel 5, yang menunjukkan langkah-langkah yang harus diambil untuk meningkatkan proses *APO13* di Klinik Pratama Rawat Jalan Watumas dan memperkuat tata kelola keamanan informasi agar mencapai target yang diinginkan.

Tabel 5. Rekomendasi Proses APO13

No	Rekomendasi	Outcome
1.	Menyusun dokumen terkait studi kasus bisnis tentang Sistem Manajemen Keamanan Informasi di klinik.	APO13-02
2.	Menyusun dokumen tertulis yang berisi rekomendasi untuk meningkatkan Sistem Manajemen Keamanan Informasi di Klinik Pratama Rawat Jalan Watumas.	APO13-01, APO13-03
3.	Melaksanakan audit manajemen keamanan data melalui tahapan yang mendetail dan berkala dengan memanfaatkan “standar internasional/nasional” yang sesuai.	APO13-01
4.	Memperkaya wawasan tentang keamanan data di semua satuan kerja klinik.	APO13-03
5.	Memperbarui Dokumen Tata Kelola TI melalui tahap memperkaya informasi mengenai infrastruktur dan lingkungan kerja minimal yang diperlukan dalam melangsungkan manajemen keamanan data.	APO13-02
6.	Menambahkan kebijakan dalam Dokumen Tata Kelola TI untuk memantau dan melaporkan tahapan manajemen keamanan data.	APO13-02

Manage Security Services (DSS05)

Rekomendasi pertama untuk meningkatkan kualitas proses *DSS05* di Klinik Pratama Rawat Jalan Watumas adalah untuk “melengkapi dokumen yang menguraikan evaluasi ancaman keamanan informasi potensial”. Berdasarkan temuan evaluasi, klinik ini belum memiliki dokumen yang merinci potensi ancaman yang dapat memengaruhi keamanan informasi yang dimilikinya. Dokumen tersebut perlu mencakup daftar ancaman yang dapat membantu klinik dalam meminimalkan risiko secara lebih rinci (Ricky Perdana Kusuma, 2019). Dokumen ini sangat penting sebagai bagian dari strategi mitigasi risiko di lingkungan klinik. Rekomendasi kedua adalah untuk “memperbarui Dokumen Prosedur Operasi Pengelolaan Hak Akses” dengan menambahkan capaian observasi berkala pada hak akses pengguna. Peninjauan berkala ini bertujuan untuk memastikan kesesuaian hak akses dengan peran pengguna guna mencegah kesalahan atau penyalahgunaan (Ardhyka *et al.*, 2023). Proses ini perlu dilaksanakan secara rutin untuk memastikan bahwa hak akses yang diberikan sesuai dengan kebutuhan tiap unit kerja di klinik. Rekomendasi ketiga berfokus pada “pengelolaan berkas berharga dan perangkat output”, seperti laptop dan printer, dengan memastikan perlindungan fisik yang memadai terhadap aset-aset *TI* yang sensitif (Gede *et al.*, 2023). Berdasarkan observasi, klinik belum sepenuhnya menerapkan manajemen yang memadai terhadap dokumen dan perangkat output tersebut. Pengelolaan ini sangat penting untuk mencegah potensi kebocoran data, terutama dalam situasi di mana data dapat berpindah antar departemen melalui sistem berbagi file. Oleh karena itu, diperlukan kontrol keamanan tambahan untuk melindungi data klinik (Heriyanto, 2023).

Rekomendasi keempat adalah untuk “mendokumentasikan klasifikasi data secara tertulis”. Meskipun klinik sudah melakukan klasifikasi data dalam sistemnya, belum ada dokumentasi lengkap yang menjelaskan metode dan kategori klasifikasi tersebut. Dokumentasi ini sangat penting untuk memperjelas pengelolaan data yang digunakan oleh klinik. Rekomendasi kelima mencakup “meningkatkan pemantauan terhadap infrastruktur yang terkait dengan keamanan informasi”. Kurangnya pemantauan yang memadai dapat menyebabkan insiden yang mengganggu operasional klinik (Cut Azlina Effendy *et al.*, 2024). Oleh karena itu, pemantauan yang menyeluruh terhadap infrastruktur *TI* harus dilaksanakan untuk mengidentifikasi dan menangani risiko dari sumber internal, seperti kerusakan perangkat keras atau perangkat lunak, serta risiko eksternal, seperti bencana alam (Ramanda *et al.*, 2024). Rekomendasi keenam melibatkan “pengujian keamanan sistem informasi yang digunakan di klinik”. Pengujian ini mencakup *penetration testing* dan *vulnerability assessment* untuk memverifikasi keamanan sistem secara keseluruhan. Hasil observasi menunjukkan bahwa klinik hanya melakukan pengawasan terhadap log firewall dan antivirus, yang tidak cukup untuk memenuhi standar pengujian yang lebih lengkap. *Penetration testing* diperlukan untuk mendeteksi kelemahan dalam keamanan aplikasi, sistem, atau jaringan (Yudi Mulyanto *et al.*, 2022), dan temuan dari pengujian ini dapat mengonfirmasi hasil dari *vulnerability assessment* (Irawadi Alwi & Budi Ilmawan, 2021). Rekomendasi-rekomendasi tersebut dirangkum dalam Tabel 6, yang memuat langkah-langkah peningkatan yang dapat diambil untuk proses *DSS05* di Klinik Pratama Rawat Jalan Watumas.

Tabel 6. Rekomendasi Proses DSS05

No	Rekomendasi	Outcome
1.	“Menyusun dokumen terkait studi kasus bisnis tentang Sistem Manajemen Keamanan Informasi di klinik.”	DSS05-01, DSS05-02
2.	“Menyusun dokumen tertulis yang berisi rekomendasi untuk meningkatkan Sistem Manajemen Keamanan Informasi di Klinik Pratama Rawat Jalan Watumas.”	DSS05-03
3.	“Melaksanakan audit manajemen keamanan informasi secara mendetail dan berkala dengan menggunakan standar internasional/nasional yang sesuai.”	DSS05-05
4.	“Meningkatkan pengetahuan tentang keamanan informasi di seluruh satuan kerja klinik.”	DSS05-01

5.	“Memperbarui Dokumen Tata Kelola TI dengan menambahkan informasi mengenai infrastruktur dan lingkungan kerja minimal yang diperlukan untuk menjalankan manajemen keamanan informasi.”	DSS05-01
6.	“Menambahkan kebijakan dalam Dokumen Tata Kelola TI untuk memantau dan melaporkan proses manajemen keamanan informasi.”	DSS05-04

Pembahasan

Berdasarkan hasil evaluasi dan analisis yang telah dilakukan terhadap proses *Manage Security* (APO13) dan *Manage Security Services* (DSS05) di Klinik Pratama Rawat Jalan Watumas, dapat disimpulkan beberapa langkah perbaikan yang penting untuk meningkatkan tata kelola keamanan informasi di klinik ini. Penerapan rekomendasi-rekomendasi yang disarankan diharapkan dapat memperkuat pengelolaan keamanan informasi yang lebih efektif, mengurangi risiko kebocoran data, serta meningkatkan kepercayaan pasien terhadap kualitas layanan yang diberikan. Pada tahap *APO13*, Klinik Pratama Rawat Jalan Watumas berada pada level 2 (*Managed Process*). Meskipun telah ada penerapan prosedur dasar untuk mengelola keamanan informasi, klinik masih membutuhkan peningkatan untuk mencapai level 3 (*Established Process*), di mana prosedur-prosedur tersebut sudah terstandarisasi dan diterapkan secara konsisten di seluruh unit kerja. Hal ini sejalan dengan temuan dalam penelitian Aftaa Aulia *et al.* (2021), yang menyatakan bahwa pencapaian tingkat kematangan yang lebih tinggi dalam tata kelola keamanan informasi memerlukan standar yang jelas dan prosedur yang lebih terperinci.

Untuk meningkatkan proses *APO13*, beberapa rekomendasi yang diberikan antara lain adalah penerapan standar internasional seperti *ISO/IEC 27001:2013* (Anam *et al.*, 2023) dan pelaksanaan audit keamanan informasi secara berkala. Audit ini penting untuk memastikan bahwa kebijakan dan prosedur yang diterapkan berjalan efektif dalam mengelola risiko dan melindungi data sensitif, seperti data pasien, dari ancaman yang mungkin timbul. Hal ini sejalan dengan pendapat Hardiansyah & Tyroni Mursityo (2020) yang menyarankan bahwa audit keamanan yang rutin dapat membantu mengevaluasi kesiapan sistem keamanan dalam menghadapi ancaman yang terus berkembang. Selain itu, penting untuk meningkatkan pemahaman tentang keamanan informasi di seluruh satuan kerja klinik. Pelatihan khusus untuk pegawai yang menangani data sensitif

akan membantu mengurangi risiko kebocoran data akibat kesalahan manusia atau akses yang tidak sah, sesuai dengan temuan Algiffary *et al.* (2023) yang menekankan pentingnya pelatihan dalam mengurangi kerentanannya terhadap ancaman. Pada tahap *DSS05*, yang berfokus pada pengelolaan layanan keamanan informasi, klinik perlu meningkatkan pengelolaan terhadap ancaman yang dapat memengaruhi keamanan data. Salah satu rekomendasi utama adalah menyusun dokumen yang menguraikan evaluasi ancaman keamanan informasi potensial. Seperti yang disarankan oleh Ricky Perdana Kusuma (2019), dokumen ini akan membantu klinik dalam mengidentifikasi dan memitigasi ancaman secara lebih terperinci. Tanpa dokumen yang jelas, risiko terhadap keamanan informasi akan semakin tinggi, karena ancaman yang mungkin muncul tidak dapat dikelola secara efektif. Selanjutnya, pembaruan pada Dokumen Prosedur Operasi Pengelolaan Hak Akses juga perlu dilakukan, dengan menambahkan capaian observasi berkala pada hak akses pemakai. Peninjauan berkala ini bertujuan untuk memastikan bahwa akses data hanya diberikan kepada pihak yang berwenang dan sesuai dengan peran mereka dalam organisasi, sebagaimana yang diungkapkan oleh Ardhyka *et al.* (2023).

Hal ini akan membantu mencegah potensi kesalahan atau penyalahgunaan akses oleh individu yang tidak berwenang. Penting juga untuk mengelola perangkat keras dan perangkat output, seperti laptop dan printer, dengan memastikan perlindungan fisik yang memadai terhadap aset-aset TI yang sensitif. Gede *et al.* (2023) menunjukkan bahwa pengelolaan perangkat keras yang memadai dapat mencegah kebocoran data, terutama ketika data berpindah antar departemen. Oleh karena itu, kontrol keamanan tambahan harus diterapkan untuk memastikan bahwa perangkat tersebut terlindungi dari potensi ancaman fisik yang bisa membahayakan data. Selain itu, dokumentasi yang jelas mengenai klasifikasi data di klinik juga perlu diperbaiki. Meskipun klinik sudah melakukan klasifikasi data dalam sistemnya, belum ada

dokumentasi yang menjelaskan metode dan kategori klasifikasi yang diterapkan. Hal ini penting untuk memberikan kejelasan dalam pengelolaan data yang digunakan oleh klinik, sesuai dengan temuan Fitri Afifah *et al.* (2022), yang menyarankan bahwa dokumentasi klasifikasi data yang lengkap akan membantu dalam menjaga konsistensi dan keamanan data. Rekomendasi lainnya adalah meningkatkan pemantauan terhadap infrastruktur TI yang terkait dengan keamanan informasi. Kurangnya pemantauan yang memadai dapat menyebabkan gangguan operasional yang dapat merugikan klinik, sebagaimana dikatakan oleh Cut Azlina Effendy *et al.* (2024). Pemantauan menyeluruh terhadap infrastruktur TI akan membantu mengidentifikasi dan menangani risiko yang muncul, baik dari sumber internal maupun eksternal, sehingga memastikan bahwa sistem tetap berfungsi dengan baik dan aman. Terakhir, pengujian keamanan sistem informasi yang lebih komprehensif, seperti *penetration testing* dan *vulnerability assessment*, juga diperlukan untuk mendeteksi potensi kelemahan dalam sistem yang ada. Hasil pengujian ini akan memberikan gambaran lebih jelas mengenai kerentanannya, yang kemudian dapat diperbaiki sebelum ancaman tersebut menyebabkan kerusakan yang signifikan (Irawadi Alwi & Budi Ilmawan, 2021).

4. Kesimpulan dan Saran

Berdasarkan temuan evaluasi tata kelola *keamanan informasi* yang dilakukan di Klinik Pratama Rawat Jalan Watumas menggunakan framework COBIT 5, khususnya pada domain APO13 dan DSS05, terdapat beberapa kesimpulan yang dapat diambil. Proses yang diterapkan di klinik ini pada kedua domain tersebut berada pada level 2 (*Managed Process*), dengan sebagian besar indikator pada level 1 dan 2 mencapai kriteria *Largely Achieved*. Namun, meskipun telah ada pengelolaan yang baik, pada level 3, atribut PA 3.1 telah mencapai kriteria *Largely Achieved*, sedangkan PA 3.2 hanya mencapai kriteria *Partially Achieved*. Hal ini menunjukkan adanya ruang untuk perbaikan lebih lanjut. Klinik Pratama Rawat Jalan Watumas menginginkan agar proses APO13 dan DSS05 dapat mencapai level 3 (*Established Process*), yang berarti terdapat kesenjangan antara kondisi yang tercapai saat ini dengan level yang diinginkan, yaitu satu

tingkat. Beberapa rekomendasi untuk meningkatkan proses APO13 termasuk menyusun dokumen studi kasus bisnis terkait keamanan informasi, memperkenalkan kebijakan yang lebih komprehensif, serta melakukan audit rutin untuk memastikan efektivitas pengelolaan keamanan informasi. Peningkatan pengetahuan pemangku kepentingan melalui pelatihan dan sosialisasi juga sangat dianjurkan, selain memperbarui Dokumen Pedoman Tata Kelola TI yang mencakup infrastruktur dan lingkungan kerja yang lebih memadai untuk mendukung implementasi keamanan yang lebih baik. Sementara itu, untuk DSS05, rekomendasi yang perlu dipertimbangkan adalah melengkapi dokumen yang menguraikan ancaman terhadap keamanan informasi, memperbarui dokumentasi klasifikasi data, serta melaksanakan pengujian *penetration test* dan *vulnerability assessment* secara berkala untuk mendeteksi celah dalam sistem.

Saran untuk meningkatkan tata kelola *keamanan informasi* di Klinik Pratama Rawat Jalan Watumas adalah dengan mempertimbangkan penerapan proses lainnya dalam COBIT 5, seperti EDM03 (*Ensure Risk Optimisation*), APO12 (*Manage Risk*), dan BAI06 (*Manage Changes*). Selain itu, penerapan standar atau kerangka kerja lain yang relevan, seperti ISO/IEC 27001, ITIL for Information Security, dan ISO 31000, juga dapat dipertimbangkan untuk memperbarui dan memperkuat sistem pengelolaan *keamanan informasi*. Dengan mengimplementasikan rekomendasi-rekomendasi tersebut, diharapkan Klinik Pratama Rawat Jalan Watumas dapat mencapai tingkat kematangan yang lebih tinggi dalam tata kelola *keamanan informasi*, serta mengurangi risiko yang dapat membahayakan kerahasiaan dan integritas data pasien.

5. Daftar Pustaka

- Aditya, I. G. W., Juliharta, I. G. P. K., & Putri, I. G. A. P. D. (2023). PENERAPAN FRAMEWORK COBIT 2019 DALAM AUDIT TATA KELOLA SISTEM INFORMASI PADA LPD DESA BERABAN. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 7(4), 2592-2599. <https://doi.org/10.36040/jati.v7i4.7142>.

- Alfifah, U. (2022). Analysis of the Platform E-Learning Utilization on DSS05 Domain Using the COBIT 5 Framework at Private Universities in Riau Archipelago. *Sistemasi: Jurnal Sistem Informasi*, 11(1), 179-185. <https://doi.org/10.32520/stmsi.v11i1.1679>.
- Algiffary, A., Herdiansyah, M. I., & Kunang, Y. N. (2023). Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI. *Journal of Applied Computer Science and Technology*, 4(1), 19-26. <https://doi.org/10.52158/jacost.505>.
- Alwi, E. I., & Ilmawan, L. B. (2021). Analisis Keamanan Sistem Informasi Akademik (SIKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment. *INFORMAL: Informatics Journal*, 6(3), 131-135.
- Anam, M. K., Putri, S. D., Yuliana, D., Yumami, E., & Lestari, T. P. (2023). Application Of the Cobit 2019 Framework to Analyse the Security Of Academic Information Systems. *Decode: Jurnal Pendidikan Teknologi Informasi*, 3(2), 296-309. <https://doi.org/10.51454/decode.v3i2.192>.
- Ardhyka, R., Fidaiyah, A., & Meiyanti, R. (2023). Analisis Manajemen Risiko IT Menggunakan COBIT5 Pada Domain APO12. *Jurnal Informasi dan Teknologi*, 30-38. <https://doi.org/10.37034/jidt.v5i1.325>.
- Aulia, N. A., Antoni, D., Syamsuar, D., & Cholil, W. (2021). Sistem tata kelola keamanan teknologi informasi berbasis framework COBIT 5 (Studi kasus: SMA Negeri 1 Palembang). *Jurnal Informatika*, 9(2), 30-37.
- Cahyono, S. A., Mukaromah, S., & Wulansari, A. (2023). Perancangan Alat Ukur Tingkat Kapabilitas Manajemen Perubahan SPBE Menggunakan Kerangka Kerja Cobit 5. *Jurnal Ilmiah Teknik Informatika dan Komunikasi*, 3(3), 49-56. <https://doi.org/10.55606/juitik.v3i3.615>.
- Devanti, K., Parwita, W. G. S., & Sandika, I. K. B. (2019). Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Pada Pt. Bisma Tunas Jaya Sentral. *Jurnal Sistem Informasi Dan Komputer Terapan Indonesia (JSIKTI)*, 2(2), 65-76.
- Effendy, C. A., Paramarta, V., & Purwanda, E. (2024). Peran teknologi informasi, pengelolaan sumber daya manusia, dan sistem informasi rumah sakit dalam meningkatkan kinerja rumah sakit (Kajian literatur). *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, 7(4), 13479-13489. <https://doi.org/10.31004/jrpp.v7i4.34703>.
- Hardiansyah, R., Mursityo, Y. T., & Suprpto, S. (2020). Evaluasi Proses Tata kelola Keamanan Informasi Menggunakan COBIT 5 Dengan Proses APO13, DSS04 dan DSS05 (Studi Pada DISKOMINFO Kabupaten Sidoarjo). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 4(4), 1116-1124.
- Heriyanto, H. (2023). Analisis perbandingan regulasi dan perlindungan hukum atas privasi data pasien di tiga Negara Asia Tenggara (Indonesia, Singapura, dan Laos). *Jurnal Ners*, 7(2), 1247-1259. <https://doi.org/10.31004/jn.v7i2.16760>.
- Imany, Y. D., Putra, W. H. N., & Herlambang, A. D. (2019). Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 3(6), 5926-5935.
- Kusuma, R. P. (2020). Audit Teknologi Informasi Menggunakan Framework Cobit 5 Pada Domain Dss (Deliver, Service, and Support)(Studi Kasus: Konsultan Manajemen Pusat). *Jurnal Digit: Digital of Information Technology*, 9(1), 97-109.
- Mulyanto, Y., Herfandi, H., & Kirana, R. C. (2022). Analisis Keamanan Wireless Local Area Network (Wlan) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi Kasus: Rs H. Lmanambai

- Abdulkadir). *Jurnal Informatika Teknologi dan Sains (Jinteks)*, 4(1), 26-35.
<https://doi.org/10.51401/jinteks.v4i1.1528>.
- Ramanda, R., & Jaya, J. N. U. (2024). Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 4.1 Pada Telkom Penajam. *Journal of Software Engineering and Information System (SEIS)*, 63-75.
<https://doi.org/10.37859/seis.v4i2.6837>.
- Simamora, F. (2024). Evaluasi Tata Kelola Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (Studi Kasus: PT Bpr Xyz). *JCOSIS (Journal Computer Science and Information Systems)*, 1(1), 8-13.
<https://doi.org/10.61567/jcosis.v1i1.174>.
- Sinaga, R., Samsinar, S., & Afriany, R. (2021). Information System Security Audit Based on the DSS05 Framework Cobit 5 at Higher Education XX. *Berkala Sainstek*, 9(1), 35.
- Sodik, I. A., & Nugraheni, D. M. K. (2022). Implementation Cobit 2019 for Evaluation of Health Clinic Information System Governance in Central Java. *Jurnal Teknik Informatika (Jutif)*, 3(6), 1549-1556.
<https://doi.org/10.20884/1.jutif.2022.3.6.361>.
- Triyunsari, D. (2023). Analisis Tingkat Kematangan Manajemen Layanan Pegawai Berbasis Teknologi Informasi Menggunakan Framework COBIT 5 Pada SMA Negeri 19 Palembang. *Indonesian Journal of Multidisciplinary on Social and Technology*, 1(2), 146-153.
<https://doi.org/10.31004/ijmst.v1i2.141>.
- Vansuri, R., Fauzi, A., Prasetyo, E. T., Negara, R., Ramadhan, R., Restu, A. M., & Firmansyah, R. R. (2023). Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi. *Jurnal Ilmu Multidisplin*, 2(1), 106-113.
<https://doi.org/10.38035/jim.v2i1>.