JUSIBI (JURNAL SISTEM INFORMASI DAN E-BISNIS)
***p-ISSN* : 2655-7541** *Volume 8, Nomor , June 2026*
e-ISSN : 2745-5823 *Hal : 110~117*

AUDIT SISTEM INFORMASI KASIR APOTEK BERBASIS COBIT DSS05 UNTUK PERLINDUNGAN DATA LAYANAN

Surya Ade Saputera[1*], Korin Kusuma Ningrum[2], Dea Imelda Lika[3], Fransiska[4]
[1,2,3,4]Program Studi Sistem Informasi, Fakultas Teknik, Universitas Muhammadiyah Bengkulu
*Corresponding author : adesurya2012@gmail.com[1]

ABSTRAK

Pemanfaatan sistem informasi kasir pada apotek berperan penting dalam mendukung transaksi penjualan, pengelolaan persediaan obat, dan penyediaan laporan keuangan. Namun, peningkatan penggunaan sistem tersebut juga diikuti oleh risiko keamanan informasi, khususnya pada apotek skala kecil yang belum menerapkan pengelolaan keamanan secara terstruktur. Penelitian ini bertujuan untuk mengevaluasi tingkat pengelolaan keamanan sistem informasi kasir apotek dan menyusun rekomendasi perbaikan menggunakan kerangka kerja COBIT, khususnya domain DSS05 (Manage Security Services). Metode penelitian yang digunakan adalah audit sistem informasi dengan pendekatan kualitatif-deskriptif melalui observasi, wawancara, dan analisis dokumen. Hasil audit menunjukkan bahwa tingkat kapabilitas pengelolaan keamanan sistem informasi kasir apotek berada pada Level 2 (Managed Process) dengan nilai rata-rata 1,9. Subproses DSS05.01 memperoleh nilai 2,0, DSS05.02 sebesar 1,8, DSS05.03 sebesar 2,1, dan DSS05.05 sebesar 1,7, yang menunjukkan bahwa pengelolaan keamanan telah dilakukan namun belum terstandarisasi dan terdokumentasi secara formal. Berdasarkan temuan tersebut, penelitian ini merekomendasikan peningkatan pengelolaan keamanan menuju Level 3 (Established Process) melalui penyusunan kebijakan, prosedur, dan pengendalian keamanan yang lebih terstruktur guna meningkatkan perlindungan data dan keandalan layanan sistem informasi kasir apotek.

Kata Kunci
Audit Sistem Informasi; Keamanan Sistem Informasi; Sistem Informasi Kasir Apotek; COBIT; DSS05

ABSTRACT

The use of point-of-sale (POS) information systems in pharmacies plays a critical role in supporting sales transactions, inventory management, and financial reporting. However, the increasing reliance on such systems is accompanied by heightened information security risks, particularly in small-scale pharmacies where structured security management is often lacking. This study aims to evaluate the level of information security management of a pharmacy POS system and to formulate improvement recommendations using the COBIT framework, specifically the DSS05 (Manage Security Services) domain. The research adopts an information systems audit approach with a qualitative-descriptive method through observation, interviews, and document analysis. The audit results indicate that the overall capability level of information security management is at Level 2 (Managed Process) with an average score of 1.9. The capability scores for DSS05 sub-processes are 2.0 for malware protection (DSS05.01), 1.8 for access management (DSS05.02), 2.1 for data protection (DSS05.03), and 1.7 for security incident management (DSS05.05). These findings suggest that security practices have been implemented but are not yet standardized or formally documented. Therefore, this study recommends improving information security management toward Level 3 (Established Process) by developing structured policies, procedures, and controls to enhance data protection and service reliability of the pharmacy POS system.

Keywords
Information Systems Audit; Information Security; Pharmacy Point-of-Sale System; COBIT; DSS05

1. Pendahuluan

Perkembangan teknologi informasi yang pesat mendorong integrasi sistem informasi ke dalam berbagai proses bisnis untuk meningkatkan efisiensi dan kualitas layanan. Pada sektor kesehatan, pemanfaatan teknologi ini telah merambah operasional apotek melalui penggunaan sistem informasi kasir atau *Point of Sales* (POS) yang terintegrasi[1]. Sistem kasir berfungsi krusial untuk mendukung transaksi penjualan, pengelolaan persediaan obat, data pelanggan, hingga pelaporan keuangan yang menjadi dasar pengambilan keputusan manajerial [2], [3]. Namun, tingginya ketergantungan operasional pada sistem

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823

kasir ini berbanding lurus dengan meningkatnya risiko siber seperti akses tidak sah, manipulasi data transaksi, infeksi *malware*, hingga risiko kebocoran data layanan farmasi yang bersifat sensitif [4].

Kondisi tersebut diperparah oleh fenomena empiris di lapangan di mana apotek skala kecil dan menengah umumnya belum menempatkan aspek tata kelola keamanan informasi sebagai prioritas utama [5]. Berdasarkan hasil observasi awal dan wawancara pada Apotek Yenni, ditemukan berbagai kerentanan signifikan dalam pengelolaan operasional harian. Pengelolaan hak akses pengguna masih dilakukan secara sederhana tanpa pembatasan yang ketat, praktik berbagi akun (*shared account*) antar karyawan masih lumrah terjadi, dan belum tersedia kebijakan atau Prosedur Operasional Standar (SOP) keamanan yang terdokumentasi secara formal. Selain itu, belum ada mekanisme evaluasi atau audit keamanan sistem informasi secara berkala. Kerentanan-kerentanan ini menempatkan data transaksi dan layanan Apotek Yenni pada risiko tinggi terhadap insiden keamanan yang dapat mengganggu stabilitas operasional dan merusak kepercayaan konsumen.

Untuk memitigasi risiko tersebut secara terukur, diperlukan audit sistem informasi menggunakan standar tata kelola global, salah satunya adalah framework *Control Objectives for Information and Related Technology* (COBIT)[6][7]. Dalam penelitian ini, evaluasi difokuskan secara spesifik pada COBIT 5 domain DSS05 (*Manage Security Services*)[8]. Pemilihan domain DSS05 didasarkan pada relevansinya yang berfokus penuh pada operasional keamanan layanan informasi, perlindungan terhadap aset TI, manajemen identitas pengguna, hingga penanganan insiden keamanan secara taktis.

Beberapa penelitian terdahulu telah menerapkan framework COBIT dalam mengevaluasi tata kelola dan keamanan teknologi informasi di berbagai sektor. Hidayat et al. [8] mengaudit sistem keamanan informasi pada lingkungan perguruan tinggi menggunakan COBIT 5 domain DSS05, sementara Nuraeni dan Haryana [9] mengevaluasi domain DSS dan menemukan bahwa mayoritas proses keamanan organisasi masih berada pada tingkat kapabilitas yang rendah. Pada sektor pemerintahan dan korporasi, Hanafi et al.[10] serta Akbar dan Saputra [11] memanfaatkan COBIT 2019 untuk mengidentifikasi objektivitas keamanan layanan informasi dan mengukur *capability level* tata kelola organisasi. Lebih spesifik pada sektor kesehatan, Prandana et al. [12] melakukan evaluasi tata kelola sistem informasi rumah sakit menggunakan COBIT 5, dan Algiffary et al.[13] mengaudit keamanan Sistem Informasi Manajemen Rumah Sakit (SIMRS) menggunakan COBIT 2019.

Meskipun penelitian bertema audit keamanan dengan COBIT telah banyak dilakukan pada institusi berskala besar, pemerintahan, dan rumah sakit, studi yang secara khusus menguji keandalan sistem keamanan kasir pada apotek retail mandiri masih sangat terbatas. Penelitian sejenis yang dilakukan oleh Asmar dan Fajar[14] pada Apotek XYZ baru mengevaluasi tata kelola sistem informasi POS secara makro/umum, dan belum mengisolasi domain DSS05 untuk membedah aspek keamanan layanan informasi secara komprehensif. Untuk mempertegas posisi kebaruan (*novelty*) penelitian ini, ringkasan perbandingan dengan literatur terdahulu disajikan pada Tabel 1.

Tabel 1. Ringkasan Penelitian Terdahulu dan Posisi Penelitian Ini

Peneliti & Tahun	**Objek Penelitian**	**Framework**	**Fokus & Hasil Utama**
Nuraeni & Haryana (2016)[9]	Institusi Pendidikan	COBIT 5	Evaluasi domain DSS; mayoritas proses berada pada Level 1.
Prandana et al. (2019)[12]	Rumah Sakit Ganesha	COBIT 5	Tata kelola umum; *capability level* mencapai level 3 (2,77).
Hidayat et al. (2021) [15]	Pusat Data Universitas	COBIT 5 (DSS05)	Mengukur kapabilitas keamanan informasi akademik.
Hanafi et al. (2023)	Instansi Pemerintah	COBIT 2019	Menetapkan DSS05 sebagai *objective* penting keamanan TI.
Akbar & Saputra (2023) [11]	PT Telkom Akses	COBIT 2019	Pengukuran kinerja tata kelola TI; berada pada level 3.
Algiffary et al. (2023) [13]	Rumah Sakit	COBIT 2019	Mengaudit keamanan SIMRS; berada pada Level 3.
Asmar & Fajar (2025) [14]	Apotek XYZ	COBIT	Audit tata kelola umum sistem POS; berada pada level 2.
Rosyidah & Kurniawati (2026)[16]	Laboratorium Teknik Informatika	COBIT 5	Sebagian besar proses berada pada Level 2 (Managed) dengan rekomendasi peningkatan tata kelola.
Penelitian Ini (2026)	**Apotek Yenni**	**COBIT 5 (DSS05)**	**Audit kapabilitas mendalam pada 5 subproses keamanan data kasir.**

p-ISSN : 2655-7541
e-ISSN : 2745-5823

Berdasarkan tabel 1 penelitian terdahulu, dapat diketahui bahwa implementasi COBIT telah banyak digunakan pada sektor pendidikan, pemerintahan, perusahaan, laboratorium, dan rumah sakit untuk mengukur capability level tata kelola teknologi informasi. Namun penelitian yang secara khusus mengevaluasi keamanan layanan informasi pada sistem informasi kasir apotek menggunakan COBIT 5 domain DSS05 masih sangat terbatas. Selain itu, penelitian sebelumnya belum mengevaluasi secara komprehensif seluruh subdomain DSS05 yang terdiri dari DSS05.01 (*Protect Against Malware*), DSS05.02 (*Manage Network and Connectivity Security*), DSS05.03 (*Manage Endpoint Security*), DSS05.04 (*Manage User Identity and Logical Access*), dan DSS05.05 (*Manage Physical Access to IT Assets*).

Berdasarkan *research gap* tersebut, penelitian ini bertujuan untuk mengevaluasi tingkat capability level pengelolaan keamanan sistem informasi kasir Apotek Yenni menggunakan framework COBIT 5 domain DSS05, menganalisis kesenjangan antara capability level saat ini dengan tingkat yang diharapkan, serta menyusun rekomendasi perbaikan guna meningkatkan keamanan layanan informasi, perlindungan data, dan keandalan operasional sistem informasi apotek.

Penelitian ini bertujuan untuk mengevaluasi tingkat kapabilitas pengelolaan keamanan sistem informasi kasir pada Apotek Yenni menggunakan framework COBIT 5 domain DSS05. Selain itu, penelitian ini bertujuan untuk mengidentifikasi kesenjangan antara tingkat kapabilitas saat ini dengan tingkat yang diharapkan serta menyusun rekomendasi perbaikan yang dapat digunakan sebagai dasar peningkatan keamanan layanan informasi, perlindungan data, dan keandalan operasional sistem informasi apotek.

2. Metodologi Penelitian

Penelitian ini menggunakan metode deskriptif kuantitatif dengan pendekatan audit sistem informasi menggunakan framework Control Objectives for Information and Related Technology (COBIT 5) pada domain Deliver, Service and Support 05 (DSS05 – Manage Security Services). Domain DSS05 dipilih karena berfokus pada pengelolaan keamanan layanan informasi yang meliputi perlindungan terhadap malware, keamanan jaringan, keamanan perangkat, pengelolaan identitas pengguna, serta pengamanan akses terhadap aset teknologi informasi. Pendekatan ini digunakan untuk mengukur tingkat kapabilitas (*capability level*) pengelolaan keamanan sistem informasi kasir pada Apotek Yenni serta memberikan rekomendasi perbaikan berdasarkan hasil audit.

Tahapan penelitian dimulai dari identifikasi permasalahan, studi literatur, observasi lapangan, wawancara, penyusunan instrumen audit, penyebaran kuesioner, pengukuran capability level, analisis kesenjangan (*gap analysis*), penyusunan rekomendasi perbaikan, hingga penarikan kesimpulan. Alur penelitian ditunjukkan pada Gambar 1.

Objek penelitian adalah Sistem Informasi Kasir Apotek Yenni yang digunakan untuk mengelola transaksi penjualan obat, pengelolaan stok, serta penyusunan laporan operasional. Audit difokuskan pada aspek keamanan layanan informasi sesuai praktik terbaik COBIT 5 domain DSS05.

Pengumpulan data dilakukan melalui observasi, wawancara, dan penyebaran kuesioner. Observasi dilakukan untuk memperoleh gambaran mengenai kondisi aktual penerapan keamanan sistem informasi pada Apotek Yenni. Wawancara dilakukan secara langsung kepada pihak yang terlibat dalam pengelolaan dan penggunaan sistem informasi untuk memperoleh informasi mengenai prosedur keamanan yang telah diterapkan. Selanjutnya, kuesioner digunakan sebagai instrumen utama untuk mengukur capability level berdasarkan praktik COBIT 5 domain DSS05.

Karena Apotek Yenni merupakan organisasi dengan struktur yang relatif sederhana, penelitian ini menggunakan teknik purposive sampling, yaitu pemilihan responden berdasarkan keterlibatan langsung dalam penggunaan dan pengelolaan sistem informasi. Responden terdiri dari empat orang yang meliputi pemilik apotek, apoteker, kasir, dan pelayan apotek. Pemilik apotek berperan sebagai penanggung jawab kebijakan teknologi informasi, apoteker sebagai pengguna utama sistem, kasir sebagai pengelola transaksi, serta pelayan apotek sebagai pengguna operasional sistem.

Penentuan peran responden mengacu pada konsep Responsible, Accountable, Consulted, and Informed (RACI) yang digunakan dalam COBIT 5 untuk memastikan keterlibatan setiap pihak sesuai tanggung jawabnya.

Tabel 2. Mapping RACI Responden

Aktivitas DSS05	Pemilik	Apoteker	Kasir	Pelayan
DSS05.01 Protect Against Malware	A	R	C	I
DSS05.02 Manage Network and Connectivity Security	A	R	C	I
DSS05.03 Manage Endpoint Security	A	R	R	C
DSS05.04 Manage User Identity and Logical Access	A	R	R	C
DSS05.05 Manage Physical Access to IT Assets	A	R	C	R

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823

Keterangan:
A = Accountable
R = Responsible
C = Consulted
I = Informed

Instrumen penelitian berupa kuesioner yang disusun berdasarkan praktik COBIT 5 domain DSS05. Kuesioner terdiri atas lima subdomain dengan total 15 indikator penilaian, dimana setiap subdomain memiliki tiga indikator yang disusun sesuai tujuan pengendalian keamanan informasi.

Tabel 3. Indikator Penilaian Domain DSS05

Subdomain	**Indikator**
DSS05.01 Protect Against Malware	1. Antivirus aktif pada komputer, 2. Pembaruan antivirus dilakukan secara berkala, 3. Pemeriksaan malware dilakukan secara rutin.
DSS05.02 Manage Network and Connectivity Security	1. Jaringan menggunakan mekanisme autentikasi, 2. Akses jaringan dibatasi sesuai kebutuhan, 3. Konfigurasi jaringan dilakukan secara aman.
DSS05.03 Manage Endpoint Security	1. Komputer menggunakan sistem keamanan, 2. Pembaruan sistem operasi dilakukan secara berkala, 3. Backup data dilakukan secara rutin.
DSS05.04 Manage User Identity and Logical Access	1. Setiap pengguna memiliki akun sendiri, 2. Penggunaan password dilakukan secara individual, 3. Hak akses diberikan sesuai tugas pengguna.
DSS05.05 Manage Physical Access to IT Assets	1. Perangkat komputer ditempatkan pada lokasi yang aman, 2. Akses fisik dibatasi hanya untuk personel tertentu, 3. Terdapat pengamanan terhadap risiko kehilangan atau kerusakan perangkat.

Instrumen penelitian menggunakan skala Likert lima tingkat dengan rentang nilai 1 sampai 5, dimana nilai 1 menunjukkan kondisi sangat tidak sesuai dan nilai 5 menunjukkan kondisi sangat sesuai terhadap praktik keamanan informasi yang diukur.

Capability level dihitung berdasarkan rata-rata skor seluruh indikator menggunakan persamaan berikut.

$$\text{Capability Level} = \frac{\sum Skor\ Seluruh\ Indikator}{Jumlah\ Indikator} \quad (1)$$

Hasil perhitungan kemudian dikonversikan ke dalam capability level COBIT 5 sebagaimana ditunjukkan pada Tabel 3.

Tabel 4. Konversi Capability Level COBIT 5

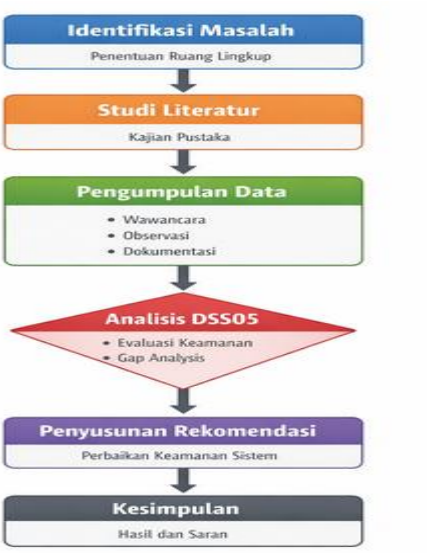
Nilai	**Capability Level**	**Kategori**
0,00 – 0,50	Level 0	Incomplete Process
0,51 – 1,50	Level 1	Performed Process
1,51 – 2,50	Level 2	Managed Process
2,51 – 3,50	Level 3	Established Process
3,51 – 4,50	Level 4	Predictable Process
4,51 – 5,00	Level 5	Optimizing Process

Selanjutnya dilakukan analisis kesenjangan (*gap analysis*) dengan membandingkan capability level saat ini (*current capability level*) terhadap capability level yang ditargetkan (*expected capability level*). Pada penelitian ini target capability level ditetapkan pada **Level 3 (Established Process)** karena pada level tersebut proses keamanan informasi telah terdokumentasi, distandarisasi, dan diterapkan secara konsisten dalam operasional organisasi. Perhitungan gap dilakukan menggunakan persamaan:

$$Gap = Target\ Capability\ Level - Current\ Capability\ Level \quad (2)$$

Semakin kecil nilai gap menunjukkan bahwa tingkat pengelolaan keamanan sistem informasi semakin mendekati kondisi yang diharapkan. Berdasarkan hasil capability level dan analisis gap tersebut, selanjutnya disusun rekomendasi perbaikan untuk masing-masing subdomain DSS05 sebagai dasar peningkatan keamanan layanan informasi pada Sistem Informasi Kasir Apotek Yenni. Tahapan penelitian dapat dilihat pada Gambar 1.

p-ISSN : 2655-7541
e-ISSN : 2745-5823



Gambar 1. Alur Penelitian
Sumber: Data Primer Penelitian 2026

3. Hasil dan Pembahasan

Hasil Pengukuran Instrumen Audit

Pengukuran tingkat pengelolaan keamanan sistem informasi kasir Apotek Yenni dilakukan menggunakan instrumen audit yang disusun berdasarkan domain DSS05 (Manage Security Services) pada framework COBIT 5. Pengumpulan data dilakukan melalui observasi, wawancara, dan penyebaran kuesioner kepada empat responden yang memiliki peran berbeda dalam pengelolaan sistem informasi, yaitu pemilik apotek, apoteker, kasir, dan pelayan apotek.

Pembagian peran responden mengacu pada konsep Responsible, Accountable, Consulted, and Informed (RACI). Pada Apotek Yenni, struktur organisasi yang relatif sederhana menyebabkan beberapa tanggung jawab keamanan sistem masih terpusat pada pihak tertentu. Pemilik apotek berperan sebagai pihak yang bertanggung jawab terhadap kebijakan pengelolaan sistem, apoteker sebagai pengelola operasional, kasir sebagai pengguna utama sistem transaksi, sedangkan pelayan apotek berperan sebagai pengguna yang memanfaatkan informasi yang dihasilkan sistem. Hasil penilaian berdasarkan masing-masing peran disajikan pada Tabel 5.

Tabel 5. Hasil Penilaian Berdasarkan Peran RACI

Peran	Nilai
Responsible	1,76
Accountable	2,12
Consulted	1,76
Informed	1,72
Rata-rata	1,84

Berdasarkan Tabel 5, peran *Accountable* memperoleh nilai tertinggi sebesar 2,12, sedangkan peran *Informed* memperoleh nilai terendah sebesar 1,72. Hal ini menunjukkan bahwa pengelolaan keamanan sistem informasi lebih dipahami oleh pihak yang bertanggung jawab secara langsung dibandingkan pengguna yang hanya menerima informasi operasional. Secara keseluruhan, nilai rata-rata sebesar 1,84 menunjukkan bahwa pengelolaan keamanan sistem informasi telah dilaksanakan, namun belum sepenuhnya terdokumentasi dan distandarisasi.

Capability Level Domain DSS05

Capability level dihitung berdasarkan rata-rata hasil penilaian instrumen audit yang kemudian dikonversi menggunakan model capability level COBIT 5. Selain pengukuran secara keseluruhan, penelitian ini juga mengidentifikasi *capability level* pada setiap subdomain DSS05 sebagaimana ditunjukkan pada Tabel 6.

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823

Tabel 6. Capability Level Domain DSS05

Subdomain	Current Level	Target Level	GAP
DSS05.01 *Protect Against Malware*	2,0	3	1,0
DSS05.02 *Manage Network and Connectivity Security*	1,8	3	1,2
DSS05.03 *Manage Endpoint Security*	2,1	3	0,9
DSS05.04 *Manage User Identity and Logical Access*	1,9	3	1,1
DSS05.05 *Manage Physical Access to IT Assets*	1,7	3	1,3
Rata-rata	1,90	3,00	1,10

Hasil pengukuran menunjukkan bahwa capability level rata-rata berada pada nilai 1,90 atau Level 2 (*Managed Process*)**.** Pada level ini proses keamanan sistem informasi telah dijalankan dan dikelola, namun pelaksanaannya masih bergantung pada kebiasaan pengguna serta belum didukung oleh prosedur operasional yang terdokumentasi secara formal.
Subdomain DSS05.03 (*Manage Endpoint Security*) memperoleh nilai tertinggi sebesar 2,1, yang menunjukkan bahwa pengamanan perangkat melalui penggunaan antivirus, pembaruan sistem operasi, dan pencadangan data telah diterapkan dengan cukup baik. Sebaliknya**,** DSS05.05 (*Manage Physical Access to IT Assets)* memperoleh nilai terendah sebesar 1,7, yang mengindikasikan bahwa pengamanan fisik terhadap perangkat dan aset teknologi informasi masih perlu ditingkatkan.

Analisis GAP
Analisis kesenjangan (gap analysis) dilakukan dengan membandingkan capability level saat ini terhadap target capability level yang ditetapkan pada Level 3 (Established Process). Level tersebut dipilih karena merepresentasikan proses keamanan yang telah terdokumentasi, terstandarisasi, dan diterapkan secara konsisten dalam organisasi.
Berdasarkan hasil perhitungan, diperoleh rata-rata capability level sebesar 1,90 sehingga menghasilkan nilai GAP sebesar 1,10 terhadap target yang diharapkan.
Gap terbesar terdapat pada DSS05.05 (Manage Physical Access to IT Assets) dengan nilai 1,3, yang menunjukkan bahwa pengamanan fisik perangkat, pembatasan akses terhadap aset teknologi informasi, serta mekanisme pengawasan masih belum optimal. Sementara itu, DSS05.03 (Manage Endpoint Security) memiliki gap terkecil sebesar 0,9, sehingga aspek keamanan perangkat telah mendekati kondisi yang diharapkan.
Hasil tersebut menunjukkan bahwa peningkatan tata kelola keamanan sistem informasi perlu difokuskan pada penyusunan prosedur keamanan, pengendalian akses pengguna, pengamanan aset fisik, serta dokumentasi aktivitas keamanan secara lebih terstruktur.

Pembahasan
Hasil penelitian menunjukkan bahwa pengelolaan keamanan sistem informasi kasir Apotek Yenni telah berada pada Capability Level 2 (*Managed Process*). Kondisi ini menunjukkan bahwa organisasi telah menyadari pentingnya keamanan sistem informasi dan telah menerapkan beberapa mekanisme pengendalian, namun implementasinya masih bersifat dasar dan belum sepenuhnya terstandarisasi.
Temuan ini sejalan dengan penelitian Asmar dan Fajar (2025)[14] yang melakukan audit sistem informasi Point of Sales pada apotek menggunakan COBIT dan memperoleh capability level pada Level 2, sehingga masih diperlukan penyusunan standar operasional prosedur serta peningkatan pengendalian keamanan sistem. Hasil penelitian ini juga konsisten dengan penelitian Rosyidah dan Kurniawati (2026)[16] yang menunjukkan bahwa tata kelola teknologi informasi pada laboratorium berada pada Level 2 (Managed Process) dan memerlukan penguatan melalui penyusunan SOP, pelatihan sumber daya manusia, serta monitoring secara berkala. Selain itu, penelitian Algiffary et al. (2023)[13] menjelaskan bahwa peningkatan keamanan sistem informasi dapat dilakukan melalui penguatan kontrol akses, pengamanan fisik perangkat, penerapan pencatatan aktivitas sistem (log monitoring), serta penyusunan kebijakan keamanan yang terdokumentasi. Rekomendasi tersebut relevan dengan kondisi Apotek Yenni yang masih memiliki kesenjangan terbesar pada aspek pengamanan fisik dan pengendalian akses pengguna.
Secara keseluruhan, hasil penelitian membuktikan bahwa penggunaan framework COBIT 5 domain DSS05 mampu memberikan gambaran tingkat kapabilitas keamanan sistem informasi sekaligus mengidentifikasi area yang memerlukan prioritas perbaikan. Implementasi rekomendasi yang dihasilkan diharapkan dapat meningkatkan capability level pengelolaan keamanan sistem informasi dari Level 2 (*Managed Process*) menuju Level 3 (*Established Process*) sehingga proses keamanan tidak lagi

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823

bergantung pada individu, melainkan telah menjadi bagian dari tata kelola organisasi yang terdokumentasi dan diterapkan secara konsisten.

4. Kesimpulan

Penelitian ini berhasil mengevaluasi tingkat pengelolaan keamanan sistem informasi kasir Apotek Yenni menggunakan framework COBIT 5 pada domain DSS05 (*Manage Security Services*). Berdasarkan hasil pengukuran yang dilakukan melalui observasi, wawancara, dan kuesioner terhadap pemilik apotek, apoteker, kasir, dan pelayan apotek, diperoleh nilai capability level rata-rata sebesar 1,84 yang berada pada Level 2 (*Managed Process*). Hasil tersebut menunjukkan bahwa proses pengelolaan keamanan sistem informasi telah dilaksanakan dan dikelola, namun belum sepenuhnya terdokumentasi, distandarisasi, dan diterapkan secara konsisten sesuai praktik tata kelola yang baik. Analisis capability pada setiap subdomain DSS05 menunjukkan bahwa aspek *Manage Endpoint Security* (DSS05.03) memiliki tingkat kapabilitas yang relatif lebih baik dibandingkan subdomain lainnya, sedangkan *Manage Physical Access to IT Assets* (DSS05.05) masih menjadi area yang memerlukan perhatian utama. Hasil analisis gap terhadap target Level 3 (*Established Process*) menghasilkan selisih sebesar 1,16, yang mengindikasikan masih perlunya peningkatan tata kelola keamanan sistem informasi, khususnya pada pengendalian akses pengguna, pengamanan fisik perangkat, dokumentasi kebijakan keamanan, serta mekanisme monitoring dan pencatatan aktivitas sistem. Berdasarkan hasil audit, rekomendasi perbaikan yang dapat diterapkan meliputi penyusunan Standar Operasional Prosedur (SOP) keamanan sistem informasi, penerapan pengelolaan hak akses berdasarkan peran pengguna, peningkatan pengamanan fisik aset teknologi informasi, pelaksanaan backup data secara berkala, serta peningkatan kesadaran keamanan melalui pelatihan bagi pengguna sistem. Implementasi rekomendasi tersebut diharapkan dapat meningkatkan capability level menuju Level 3 (*Established Process*) sehingga pengelolaan keamanan sistem informasi kasir Apotek Yenni menjadi lebih efektif, terdokumentasi, dan mampu mendukung keberlangsungan operasional apotek secara aman dan andal.

5. Daftar Pustaka

[1] D. Prasanti and S. S. Indriani, "Pengembangan Teknologi Informasi Dan Komunikasi Dalam Sistem E-Health Alodokter. Com," *J. Sosioteknologi*, vol. 17, no. 1, pp. 93–103, 2018.

[2] A. Ashifuddin and H. I. Huda, "Penerapan Sistem Informasi Keuangan dalam Mendukung Transparansi Laporan Keuangan UMKM Desa Kumejing Kabupaten Batang," *J. Ilm. Sist. Inf.*, 2026, [Online]. Available: https://api.semanticscholar.org/CorpusID:285002049

[3] S. Mauluddin, "Pengembangan Sistem Informasi Apotek (Studi Kasus: Apotek Leuwi Sehat Majalengka)," *JATI-Jurnal Teknol. dan Inf. UNIKOM*, vol. 2, 2015.

[4] S. R. Paminto[1] *et al.*, "Perlindungan Hukum Bagi Korban Pencurian Data Dan Informasi Pribadi Di Era Kejahatan Siber," *J. Dunia Ilmu Huk.*, 2024, [Online]. Available: https://api.semanticscholar.org/CorpusID:281938161

[5] F. Nurdiansyah, E. D. Daniati, and A. Ristyawan, "PENGEMBANGAN SISTEM INFORMASI KASIR APOTEK DENGAN METODE WATERFALL," *EDUSAINTEK J. Pendidikan, Sains dan Teknol.*, 2022, [Online]. Available: https://api.semanticscholar.org/CorpusID:259899698

[6] F. Habibi and S. Velma, "NETRALITAS BIROKRASI; SYSTEMATIC LITERATURE REVIEW," *J. Inov. dan Kreat.*, 2025, [Online]. Available: https://api.semanticscholar.org/CorpusID:284387881

[7] F. I. N. Mutiah, "ANALISIS DAN PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI PADA KANTOR IMIGRASI KELAS 1 TPI PONTIANAK MENGGUNAKAN METODE OCTAVE ALLEGRO DAN ISO/IEC 27001:2013," *Coding J. Komput. dan Apl.*, 2020, [Online]. Available: https://api.semanticscholar.org/CorpusID:270643548

[8] H. Kusbandono, D. Ariyadi, and T. Lestariningsih, "Tata kelola teknologi informasi." CV Nata Karya, 2019.

[9] A. Nuraeni and K. M. S. Haryana, "Penilaian tata kelola teknologi informasi dengan menambahkan unsur keamanan menggunakan framework cobit 5 pada domain dss," *J. Comput. Bisnis*, vol. 10, no. 2, pp. 89–105, 2016.

[10] R. Hanafi, M. Munir, S. Suwatno, and C. Furqon, "Identification of IT governance and management objectives and target process capability level in government institution," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 7, no. 2, pp. 290–308, 2023.

[11] H. Akbar and R. Saputra, "Evaluasi kinerja tata kelola teknologi informasi terhadap tools internal framework COBIT 2019," *Sebatik*, vol. 27, no. 2, pp. 589–605, 2023.

[12] D. Prandana, A. A. I. I. Paramitha, and I. Putra, "Evaluasi Tata Kelola Dan Audit Sistem

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823

Informasi Rumah Sakit Ganesha Dengan Menggunakan Kerangka Kerja Cobit 5," *J. Appl. Manag. Account. Sci.*, vol. 1, no. 1, pp. 65–75, 2019.

[13] A. Algiffary, M. I. Herdiansyah, and Y. N. Kunang, "Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI," *J. Appl. Comput. Sci. Technol.*, vol. 4, no. 1, pp. 19–26, 2023.

[14] I. F. Kurniati Asmar, "AUDIT SISTEM INFORMASI POINT OF SALES APOTEK XYZ Abstraksi Keywords : Pendahuluan Tinjauan Pustaka Metode Penelitian," vol. 6, no. 2, pp. 4–7, 2025.

[15] A. M. Hidayat, N. Afif, H. Kasim, and W. Saputra, "Evaluasi Kapabilitas Sistem Keamanan Informasi Pusat Teknologi dan Pangkalan Data Universitas X Menggunakan Process Assessment Model Framework Cobit 5 (Domain DSS05)," *J. INSYPRO (Information Syst. Process.*, 2021, [Online]. Available: https://api.semanticscholar.org/CorpusID:244629633

[16] U. A. Rosyidah, L. S. Kurniawati, S. Informasi, U. M. Jember, T. Informatika, and U. M. Jember, "Pengukuran dan Analisis Capability Level Tata Kelola IT di Laboratorium Teknik Informatika Menggunakan COBIT 5," vol. 7, no. 1, pp. 7–11, 2026.

6. Penulis

Surya Ade Saputera, M.Kom (Dosen)
Fakultas Teknik, Universitas Muhammadiyah Bengkulu

Korin Kusuma Ningrum (Mahasiswa)
Fakultas Teknik, Universitas Muhammadiyah Bengkulu

Fransiska (Mahasiswa)
Fakultas Teknik, Universitas Muhammadiyah Bengkulu

Dea Imelda Lika (Mahasiswa)
Fakultas Teknik, Universitas Muhammadiyah Bengkulu