JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i1.5886

AUDIT SISTEM INFORMASI MENGGUNAKAN COBIT 5 DOMAIN DSS001 DAN DSS005 (STUDI KASUS: PERPUSTAKAAN UPN "VETERAN" JAWA TIMUR)

Alya Fatin Fadhiyah Muhaimin Putri[1*], Imamah Nur Fadlilah[2], Afrida Lailiyah Hanim[3], Radhyana Gayatri Faradilla[4], Dhavina Ocxa Dwiyantie[5], Aisyatuz Zahroh[6], Eristya Maya Safitri[7]

[1,2,3,4,5,6]Universitas Pembangunan Nasional "Veteran" Jawa Timur; Jl. Rungkut Madya No.1, Gn. Anyar, Kec. Gn. Anyar, Kota SBY, Jawa Timur 60294; Telepon : (0623) 18706369

Received: 30 Desember 2024
Accepted: 14 Januari 2025
Published: 20 Januari 2025

Keywords:
Audit, COBIT 5, Domain DSS, Perpustakaan

Corespondent Email:
21082010132@student.upnjatim.ac.id

Abstrak. Teknologi informasi (TI) telah menjadi pilar utama dalam mendukung efisiensi layanan perpustakaan. Perpustakaan UPN "Veteran" Jawa Timur telah sistem berbasis web untuk meningkatkan layanan, namun menghadapi tantangan seperti minimnya SDM, kerusakan perangkat, dan ancaman siber yang dapat menurunkan kepercayaan pengguna, memicu kebocoran data, serta mengganggu proses akademik. Berdasarkan latar belakang tersebut penelitian ini bertujuan untuk mengevaluasi kapabilitas sistem informasi perpustakaan menggunakan framework COBIT 5 dengan domain DSS001 (*Manage Operations*) dan DSS005 (*Manage Security Services*). Metode penelitian yang digunakan adalah penelitian deskriptif melalui survei dan wawancara dengan pegawai perpustakaan. Hasil penelitian menunjukkan kapabilitas DSS001 berada pada level 2 (*Managed*), yang memerlukan kebijakan dan prosedur formal, sedangkan DSS005 berada pada level 3 (*Established*) dengan kebutuhan pengelolaan keamanan yang lebih terstruktur. Rekomendasi yang diberikan meliputi audit akses, pelatihan keamanan bagi karyawan, pembuatan jadwal evaluasi berkala, dan penerapan sistem pemantauan otomatis. Implementasi langkah-langkah ini diharapkan mampu meningkatkan struktur manajemen operasional dan keamanan, serta memastikan kelancaran layanan perpustakaan di era digital.

Abstract. *Information technology (IT) has become a key pillar in supporting the efficiency of library services. UPN "Veteran" East Java Library has a web-based system to improve services, but faces challenges such as lack of human resources, device damage, and cyber threats that can reduce user confidence, trigger data leaks, and disrupt academic processes. Based on this background, this study aims to evaluate the capabilities of library information systems using the COBIT 5 framework with domains DSS001 (Manage Operations) and DSS005 (Manage Security Services). The research method used is descriptive research through surveys and interviews with library employees. The results showed that DSS001 capability is at level 2 (Managed), which requires formal policies and procedures, while DSS005 is at level 3 (Established) with the need for more structured security management. Recommendations include access audits, security training for employees, creation of a regular evaluation schedule, and implementation of an automated monitoring system. The implementation of these measures is expected to improve the operational and security management structure, and ensure the smooth running of library services in the digital era.*

1. PENDAHULUAN

Teknologi informasi (TI) telah menjadi pilar utama dalam mendukung efisiensi layanan pendidikan, khususnya dalam pengelolaan perpustakaan. Sistem informasi memungkinkan pengelolaan koleksi digital, akses repository akademik, dan layanan peminjaman buku yang lebih terstruktur. Dalam konteks ini, Perpustakaan UPN "Veteran" Jawa Timur mulai menggunakan sistem berbasis web sejak Maret 2023 untuk menggantikan aplikasi desktop yang telah digunakan sebelumnya. Implementasi sistem baru ini bertujuan untuk mengatasi berbagai tantangan operasional, seperti antrian panjang pada peminjaman loker manual yang menggunakan kartu mahasiswa. Meskipun demikian, sistem ini menghadapi sejumlah tantangan baru, termasuk keterbatasan sumber daya manusia (hanya satu staf TI), kerusakan perangkat keras, dan ancaman keamanan siber. Misalnya, insiden peretasan situs repositori yang terjadi saat proses bisnis berjalan telah mengganggu akses ke data repository akademik, sehingga menyebabkan penundaan layanan informasi bagi mahasiswa dan staf akademik. Jika masalah-masalah ini tidak segera diatasi, dampaknya dapat berupa menurunnya kepercayaan pengguna terhadap sistem, meningkatnya risiko kebocoran data, hingga potensi gangguan proses akademik yang lebih luas. Oleh karena itu, urgensi untuk meningkatkan pengelolaan operasional dan keamanan sistem menjadi sangat penting untuk mendukung kelancaran layanan perpustakaan [1], [2].

Framework COBIT 5 menjadi salah satu pendekatan yang diakui dalam mengukur dan meningkatkan tata kelola TI organisasi. Dalam konteks perpustakaan berbasis web, *framework* ini relevan untuk memastikan kelancaran operasional dan keamanan sistem informasi. Domain DSS001 (*Manage Operations*) bertujuan mengelola proses operasional harian agar sesuai dengan standar yang ditentukan, termasuk penerapan prosedur operasional dan pemantauan infrastruktur TI, yang sangat penting untuk mendukung keandalan sistem [3]. Di sisi lain, domain DSS005 (*Manage Security Services*) berfokus pada melindungi sistem dan data dari ancaman keamanan melalui pengelolaan risiko, pemantauan insiden, dan penerapan langkah mitigasi. Mengingat meningkatnya ancaman siber dan kompleksitas pengelolaan data pengguna, penerapan kedua domain ini memiliki relevansi tinggi untuk mendukung urgensi audit dan meningkatkan efektivitas sistem informasi perpustakaan di era digital [1], [4].

Penelitian sebelumnya menunjukkan bahwa audit sistem informasi berbasis COBIT memberikan hasil signifikan dalam mengidentifikasi dan memperbaiki kelemahan sistem. Rahmaha et al. (2018) mengevaluasi domain DSS001 dan DSS003 di Perpustakaan UPN yang sama dan menemukan rendahnya *capability level* DSS003 akibat kurangnya dokumentasi formal untuk menangani masalah operasional. Studi ini merekomendasikan pengembangan prosedur standar dan pelatihan staf sebagai langkah perbaikan [2]. Selain itu, Shafira et al. (2014) mengevaluasi domain *Deliver, Service, and Support* (DSS) menggunakan COBIT 4.1 di institusi lain dan menemukan pengelolaan kapasitas hanya mencapai maturity level 1,1, menunjukkan perlunya peningkatan dalam perencanaan kapasitas sistem untuk memenuhi kebutuhan pengguna [3]. Namun, belum ada penelitian yang secara khusus mengevaluasi domain DSS005 untuk keamanan sistem informasi perpustakaan berbasis web. Padahal, aspek keamanan sangat penting di tengah meningkatnya ancaman siber yang dapat berdampak langsung pada keberlanjutan layanan perpustakaan [1].

Penelitian ini bertujuan untuk mengevaluasi *capability level* domain DSS001 (*Manage Operations*) dan DSS005 (*Manage Security Services*) pada sistem informasi Perpustakaan UPN "Veteran" Jawa Timur. Diperkirakan saat ini DSS001 berada pada *maturity level* 2 (*Managed Process*), yang berarti proses operasional sudah dilaksanakan tetapi belum sepenuhnya terdokumentasi dan distandarisasi. Adapun DSS005 mencapai *maturity level* 3 (*Established Process*), yang menunjukkan bahwa pengelolaan keamanan telah terdefinisi dengan baik dan diterapkan secara konsisten. Namun, kedua domain tersebut belum mencapai tingkat yang diharapkan, yaitu level 4 (*Predictable Process*), di mana proses seharusnya dapat dipantau, diukur, dan dioptimalkan secara konsisten. Untuk DSS001, direkomendasikan pengembangan prosedur operasional standar yang lebih terstruktur, peningkatan dokumentasi proses, serta pelatihan staf untuk memastikan proses dapat diulang secara efektif. Sementara itu, untuk DSS005, direkomendasikan penguatan sistem pemantauan keamanan berbasis log dan penerapan analisis risiko secara berkala untuk meningkatkan kesiapan menghadapi ancaman siber di masa mendatang. Dengan langkah-langkah tersebut, diharapkan tata kelola sistem informasi perpustakaan dapat mendukung efisiensi operasional dan keamanan sistem secara lebih optimal.

2. TINJAUAN PUSTAKA

2.1 Perpustakaan

Menurut [5], Perpustakaan Perguruan Tinggi merupakan perpustakaan yang terletak di dalam

perguruan tinggi, baik di unit-unit yang terkait maupun lembaga yang berafiliasi dengan perguruan tinggi tersebut. Tujuan utama adanya perpustakaan perguruan tinggi adalah mendukung perguruan tinggi dalam mencapai misi Tri Dharma Perguruan Tinggi (Pendidikan, penelitian, dan pengabdian kepada masyarakat). Perpustakaan menyediakan berbagai informasi dan materi yang diperlukan oleh sivitas akademika, termasuk mahasiswa, dosen, dan staf pengajar, untuk menunjang proses pembelajaran, penelitian, dan pengembangan ilmu pengetahuan. Selain itu, perpustakaan juga berfungsi sebagai tempat untuk mengakses literatur yang mencakup berbagai disiplin ilmu yang ada di perguruan tinggi, serta menjadi sarana untuk memperluas wawasan akademik bagi para penggunanya. Di perguruan tinggi, terdapat berbagai jenis perpustakaan yang beroperasi di bawah lembaga pendidikan tinggi, termasuk perpustakaan universitas, fakultas, akademik, dan sekolah tinggi.

2.2 Proses *Capability*

Proses *Capability* merupakan konsep yang sangat penting dalam *framework* COBIT 5, yang berhubungan dengan kemampuan suatu organisasi dalam mengelola dan mengoptimalkan proses-proses yang ada untuk mencapai tujuan strategis yang telah ditetapkan. Kemampuan (*capability*) merujuk pada tingkat kematangan, efisiensi, dan efektivitas setiap proses yang diterapkan dalam organisasi. Dalam konteks COBIT 5, proses *capability* berkaitan dengan bagaimana organisasi mampu menjalankan berbagai proses kontrol dengan pengendalian dan kinerja yang tepat untuk mendukung tujuan bisnis yang lebih besar. ISO/IEC 15504-2 menetapkan standar untuk mengevaluasi kualitas proses dalam *framework* COBIT. Penilaian *capability* dilakukan berdasarkan enam tingkat, mulai dari level 0 hingga 5, yang menggambarkan sejauh mana suatu diterapkan dengan baik dan dapat ditingkatkan [6].

Tabel 1. *Capability Level Criteria Assessment*

Capability Level	**Deskripsi**
Level 0: *Incomplete Process*	Proses belum dilaksanakan atau tidak berhasil mencapai tujuan yang diharapkan.
Level 1: *Performed Process*	Proses berjalan sesuai rencana dan tujuan, namun tidak ada standar atau dokumentasi yang jelas.
Level 2: *Managed Process*	Proses yang terdapat pada level 1 sekarang dijalankan dengan pendekatan manajerial, yang mencakup perencanaan, pemantauan, dan penyelarasan. Serta ada dokumentasi namun belum terstandarisasi.
Level 3: *Established Process*	Proses yang terdapat pada level 2 diimplementasikan dengan mematuhi prosedur dan kebijakan yang telah ditentukan, sehingga mampu menghasilkan output yang diharapkan.
Level 4: *Predictable Process*	Proses pada level 3 beroperasi secara konsisten dan terdapat pengukuran kinerja proses untuk memastikan stabilitas dan kemampuan dalam mencapai tujuan.
Level 5: *Optimising Process*	Proses pada level 4 berlangsung dengan baik dan terus diperbaiki secara berkelanjutan dengan berfokus pada peningkatan dan pengoptimalan kebutuhan bisnis yang terus berkembang.

2.3 COBIT 5

Cobit 5 (*Control Objectives for Information and Related Technologies*) merupakan kerangka kerja yang dikembangkan oleh ISACA dan ITGI untuk membantu organisasi dalam mengelola dan mengoptimalkan penggunaan teknologi informasi (TI) agar selaras dengan tujuan bisnis. COBIT 5 menyediakan panduan terstruktur yang memungkinkan organisasi untuk meningkatkan efisiensi, efektivitas, dan keamanan sistem informasi dalam mendukung pencapaian tujuan strategis mereka [7].

COBIT 5 terdiri dari serangkaian prinsip dan praktik yang dirancang untuk memastikan bahwa TI tidak hanya mendukung tujuan organisasi, tetapi juga berfungsi sebagai aset strategis yang memberikan nilai tambah, meminimalkan risiko, dan memastikan kepatuhan terhadap berbagai regulasi. Kerangka kerja ini mengintegrasikan berbagai aspek manajemen TI, mulai dari perencanaan, pengembangan, hingga evaluasi dan pemantauan kinerja TI [8]. COBIT 5 memiliki lima domain utama yang mencakup seluruh siklus hidup TI di dalam organisasi, yang masing-masing memiliki tujuan dan ruang lingkup tertentu. Berikut adalah penjelasan tentang lima domain utama dalam COBIT 5:

a) EDM (*Evaluate, Direct, and Monitor*): Pengawasan, pengendalian, dan pengambilan

keputusan strategis terkait penggunaan TI dalam organisasi.

b) APO (*Align, Plan, and Organize*): Perencanaan, pengaturan, dan penyusunan strategi TI untuk mendukung tujuan bisnis.
c) BAI (*Build, Acquire, and Implement*): Proses pengembangan dan penerapan solusi TI yang sesuai dengan kebutuhan bisnis.
d) DSS (*Deliver, Service, and Support*): Pengiriman, pelayanan, dan dukungan terhadap sistem informasi yang telah diimplementasikan.
e) MEA (*Monitor, Evaluate, and Assess*): Pemantauan dan penilaian terhadap kinerja TI untuk memastikan pencapaian tujuan organisasi.

2.4 Domain DS*S*

Domain DSS (*Deliver, Service, and Support*) merupakan salah satu domain penting dalam *framework* COBIT 5. Domain DSS berfokus pada pengelolaan dan penyampaian layanan serta dukungan terhadap sistem informasi yang ada di dalam organisasi. Domain ini merupakan perkembangan dari domain DS (*Deliver and Support*) yang terdapat pada COBIT 4.1, yang kemudian dikembangkan lebih lanjut oleh ISACA untuk mencakup berbagai aspek pengelolaan layanan TI yang lebih komprehensif TI [9].

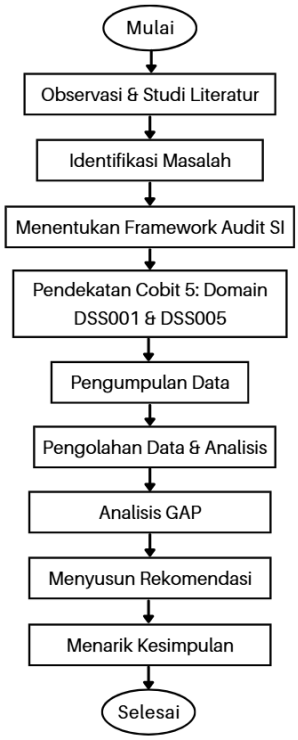
Domain DSS memiliki peran penting dalam memastikan sistem informasi yang diterapkan dapat berjalan dengan efektif, efisien, serta memberikan dukungan yang cukup dan nilai tambah bagi organisasi. Fokus utama dari domain ini adalah pada pengiriman dan pelayanan sistem informasi yang lancar, termasuk dukungan teknis untuk memastikan kelangsungan dan keamanan sistem. Selain itu, domain DSS juga mencakup pengelolaan data, pelatihan, serta pemeliharaan dan perbaikan layanan agar sesuai dengan kebutuhan organisasi. Dalam COBIT 5, domain DSS mencakup enam proses kontrol utama, yaitu:

a) DSS01 (*Manage Operations*): Proses ini berfokus pada pengelolaan operasi TI sehari-hari untuk memastikan sistem informasi dan infrastruktur TI berfungsi dengan baik dan efisien.
b) DSS02 (*Manage Service Request and Incident*): Proses ini berfokus pada penanganan permintaan layanan dan insiden yang terjadi dalam sistem informasi.
c) DSS03 (*Manage Problem*): Proses ini berfokus pada identifikasi dan penyelesaian akar masalah yang menyebabkan insiden berulang.
d) DSS04 (*Manage Continuity*): Proses ini memastikan kontinuitas operasional TI dalam situasi darurat atau bencana.
e) DSS05 (*Manage Security Service*): Proses ini berfokus pada pengelolaan layanan keamanan TI untuk melindungi sistem dan data organisasi dari ancaman eksternal dan internal.
f) DSS06 (*Manage Business Process Control*): Fokus dari proses ini adalah pengelolaan kontrol atas proses bisnis yang terkait dengan penggunaan sistem informasi.

3. METODE PENELITIAN

3.1 Tahapan Penelitian

Tahapan penelitian yang dilakukan ditunjukkan pada Gambar 1.



Gambar 1. Tahapan penelitian

3.2 Jenis Penelitian

Penelitian ini merupakan penelitian deskriptif. Menurut Sugiyono (2020) salah satu jenis penelitian deskriptif adalah survei, survei dilakukan untuk mengumpulkan fakta-fakta terkait fenomena yang sedang terjadi serta mendapatkan informasi faktual, baik mengenai kondisi sosial, ekonomi, maupun politik suatu kelompok atau wilayah tertentu. Penelitian deskriptif ini umumnya menggunakan pendekatan kuantitatif untuk memungkinkan penilaian terhadap tingkat kematangan (*maturity level*). [10]

Penelitian ini dilakukan secara langsung terhadap objek penelitian, yaitu Unit Pelaksana Akademik (UPA) Perpustakaan UPN Veteran Jawa Timur, dengan tujuan mendapatkan informasi yang relevan dan mendalam terkait tata kelola teknologi informasi yang diterapkan. Penelitian ini menggunakan pendekatan deskriptif, yang dirancang untuk

memberikan gambaran menyeluruh tentang kondisi yang ada, serta mendukung analisis dan evaluasi tata kelola TI berdasarkan kerangka kerja COBIT 5, khususnya domain DSS001 (*Manage Operations*) dan DSS005 (*Manage Security Service*). Penelitian ini diharapkan mampu memberikan rekomendasi serta rancangan model tata kelola baru yang sesuai dengan kebutuhan objek penelitian, dengan tujuan mendukung peningkatan kualitas pengelolaan teknologi informasi di Perpustakaan UPN "Veteran" Jawa Timur.

3.3 Pengumpulan Data

Pengumpulan data dilakukan menggunakan beberapa metode, yaitu:

a. Studi literatur bertujuan untuk meninjau teori, konsep, dan hasil penelitian sebelumnya terkait kerangka kerja COBIT 5, khususnya domain DSS001 *(Manage Operations)* dan DSS005 *(Manage Security Service)*. Informasi ini digunakan sebagai dasar dalam menganalisis dan mengevaluasi tata kelola TI di perpustakaan.
b. Observasi dilakukan secara langsung pada operasional sistem TI di perpustakaan, untuk mengidentifikasi proses kerja, efektivitas layanan, serta potensi masalah yang terjadi. Observasi ini memungkinkan peneliti memahami praktik nyata yang berlangsung di lapangan.
c. Wawancara dilakukan dengan Bapak Fatchullah, S.Sos., MA. selaku Sie Koordinator Layanan Perpustakaan sekaligus penanggung jawab TI di perpustakaan ini. Beliau merupakan responden dan narasumber utama dalam proses pengumpulan data. Wawancara ini bertujuan untuk mendapatkan informasi mendalam mengenai kendala yang dihadapi, penerapan sistem informasi, serta efektivitas tata kelola TI yang berlangsung. Responden dipilih berdasarkan peran dan keterlibatannya dalam pengelolaan operasional dan keamanan layanan perpustakaan.

3.4 Identifikasi Masalah

Pengelolaan teknologi informasi (TI) menjadi aspek penting dalam mendukung operasional dan layanan organisasi, termasuk perpustakaan perguruan tinggi. Salah satu kerangka kerja yang banyak digunakan untuk memastikan tata kelola TI yang efektif adalah COBIT 5 (*Control Objectives for Information and Related Technology*). COBIT 5 merupakan kerangka kerja yang dirancang untuk membantu organisasi dalam mengelola dan mengendalikan TI agar selaras dengan tujuan strategis organisasi. Kerangka kerja ini mencakup panduan untuk mengevaluasi, mengelola, dan meningkatkan proses TI melalui berbagai domain yang spesifik.

Salah satu domain utama dalam COBIT 5 adalah *Deliver, Service, and Support* (DSS). Domain ini berfokus pada proses-proses yang mendukung layanan teknologi informasi secara berkelanjutan, termasuk pengelolaan operasional, dukungan teknis, keamanan layanan, dan keberlanjutan sistem. DSS bertujuan untuk memastikan bahwa layanan TI berjalan secara efisien, aman, dan memberikan nilai tambah bagi organisasi. Penelitian ini akan berfokus pada dua sub-domain dalam DSS, yaitu DSS001 (*Manajemen Operasional*), yang bertugas mengatur efisiensi proses operasional sistem TI, dan DSS005 (*Manage Security Service*), yang menangani perlindungan serta keamanan data dan layanan TI untuk menjaga keberlanjutan operasional yang optimal.

3.5 Identifikasi Domain dan Proses Cobit

Pemetaan antara IT-related Goals dan COBIT 5 Processes menunjukkan bagaimana setiap proses dalam kerangka kerja COBIT 5 mendukung pencapaian tujuan-tujuan yang berkaitan dengan TI. Dalam hal ini, domain *Build, Acquire, and Implement* (BAI) berfokus pada pengembangan dan penerapan solusi TI, domain *Deliver, Service, and Support* (DSS) berfokus pada pengoperasian dan layanan TI secara berkelanjutan, sedangkan domain *Monitor, Evaluate, and Assess* (MEA) memastikan proses pemantauan, evaluasi, dan peningkatan berkelanjutan. [11]

Dalam domain DSS, proses DSS001 Mengelola Operasi bertujuan untuk mengelola kegiatan operasional TI, termasuk pengelolaan infrastruktur, aplikasi, dan sumber daya pendukung untuk memastikan kinerja yang konsisten, efisien, dan andal. Proses ini melibatkan aktivitas seperti pengelolaan tugas rutin, pemantauan layanan TI, serta respons terhadap insiden operasional untuk meminimalkan gangguan layanan.

Sementara itu, DSS005 Mengelola Layanan Keamanan berfokus pada perlindungan aset informasi dan pengelolaan risiko keamanan informasi. Proses ini mencakup identifikasi ancaman, pelaksanaan kontrol keamanan, penanganan insiden keamanan, dan kepatuhan terhadap kebijakan keamanan TI. DSS005 sangat penting untuk memastikan bahwa layanan TI berjalan dengan aman dan risiko keamanan dapat diminimalkan secara proaktif.

Dengan mengoptimalkan DSS001 dan DSS005, organisasi dapat menjaga kesinambungan operasional dan melindungi aset TI dari ancaman keamanan, sehingga mendukung tercapainya tujuan-tujuan strategis TI.

4. HASIL DAN PEMBAHASAN

4.1 *Mapping Enterprise Goals to IT Related Goals*

Pemetaan antara *Enterprise Goals* dan *IT Related Goals* menggunakan kerangka kerja COBIT 5 dilakukan untuk memastikan bahwa teknologi informasi yang diterapkan dalam organisasi dapat mendukung pencapaian tujuan bisnis yang lebih luas, seperti peningkatan efisiensi operasional, kepatuhan terhadap regulasi, serta peningkatan kualitas layanan kepada pelanggan.

Gambar 2. *Mapping Enterprise Goals to IT Related Goals*

Hasil pemetaan menunjukkan bahwa fokus utama sistem informasi perpustakaan adalah memastikan kelancaran operasional, seperti layanan yang andal, tersedia, dan aman, serta kepatuhan terhadap peraturan internal dan eksternal (terlihat pada *IT-related goals* 4, 5, 10). Fokus kedua adalah kepuasan pengguna, dengan prioritas pada layanan yang sesuai kebutuhan dan perlindungan data pengguna (*IT-related goals* 7, 8). Selanjutnya, efisiensi dalam penggunaan sumber daya TI menjadi perhatian penting untuk mendukung keberlanjutan sistem, termasuk integrasi teknologi dan proses bisnis (*IT-related goals* 11, 12). Terakhir, pengembangan kompetensi personel TI dan mendorong inovasi berbasis TI juga menjadi fokus untuk mendukung peningkatan layanan perpustakaan (*IT-related goals* 16, 17).

4.2 *Mapping IT Related Goals to IT Process*

Lalu pada tahap ini dibuat pemetaan antara *IT Related Goals* dengan subdomain DSS (*Deliver, Service, and Support*) adalah untuk memastikan bahwa implementasi dan pengelolaan teknologi informasi yang berkaitan dengan operasional dan keamanan layanan TI, seperti kelancaran operasional dan perlindungan data, dilakukan dengan mengacu pada praktik terbaik yang ada dalam framework COBIT 5.

IT Related Goals	DSS01 (Manage Operations)	DSS05 (Manage Security)
Alignment of IT and business strategy	P	S
IT compliance and support for business compliance with external laws and regulations	S	P
Commitment of executive management for making IT-related decisions	P	S
Managed IT-related business risk	P	P
Realized benefits from IT-enabled investments and services portfolio	S	P
Transparency of IT costs, benefits, and risk	S	S
Delivery of IT services in line with business requirements	P	P
Adequate use of applications, information, and technology solutions	P	S
IT agility	S	P
Security of information, processing infrastructure, and applications	S	P
Optimization of IT assets, resources, and capabilities	P	S
Enablement and support of business processes by integrating applications and technology	S	P
Delivery of programs delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S
Availability of reliable and useful information for decision making	P	S
IT compliance with internal policies	P	P
Competent and motivated business and IT personnel	S	S
Knowledge, expertise, and initiatives for business innovation	S	S

Gambar 3. *Mapping IT Goals to IT Process*

4.3 Pengumpulan Data

4.3.1 RACI *Chart*

RACI (Responsible, Accountable, Consulted, Informed) *Chart* digunakan untuk mendefinisikan peran dan tanggung jawab dalam pelaksanaan audit sistem informasi. Pada tabel berikut disusun RACI *Chart* berdasarkan hasil wawancara dengan pihak terkait di Perpustakaan UPN "Veteran" Jawa Timur. Tujuannya adalah untuk memperjelas siapa yang bertanggung jawab langsung *(Responsible)*, memiliki wewenang akhir *(Accountable)*, pemberi masukan *(Consulted)*, dan penerima informasi *(Informed)* pada setiap aktivitas dalam masing-masing sub-domain DSS001 dan DSS005.

Tabel 2. RACI DSS001

Aktivitas	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
DSS001.01 Evaluasi sistem tata kelola	Sie Koordinator Layanan	Sie Koordinator Layanan	Pengguna	Kepala Perpustakaan
DSS001.02 Mengelola layanan TI yang dialihdayakan	Sie Koordinator Layanan	Sie Koordinator Layanan	Tim Telematika	Kepala Perpustakaan
DSS001.03 Memantau infrastruktur TI	Sie Koordinator Layanan	Sie Koordinator Layanan	Tim Telematika	Kepala Perpustakaan
DSS001.04 Mengelola lingkungan	Sie Koordinator Layanan	Sie Koordinator Layanan	Sie Koordinator Layanan	Kepala Perpustakaan
DSS001.05 Mengelola fasilitas	Sie Koordinator Layanan	Sie Koordinator Layanan	Sie Koordinator Layanan	Kepala Perpustakaan

Tabel 3. RACI DSS005

Aktivitas	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
DSS001.01 Evaluasi sistem tata kelola	Sie Koordinator Layanan	Sie Koordinator Layanan	Tim Telematika	Kepala Perpustakaan
DSS001.02 Mengelola layanan TI yang dialihdayakan	Sie Koordinator Layanan	Sie Koordinator Layanan	Tim Telematika	Pengguna

DSS001.03 Memantau infrastruktur TI	Sie Koordinator Layanan	Sie Koordinator Layanan	Tim Telematika	Kepala Perpustakaan
DSS001.04 Mengelola lingkungan	Sie Koordinator Layanan	Sie Koordinator Layanan	Tim Telematika	Kepala Perpustakaan
DSS001.05 Mengelola fasilitas	Sie Koordinator Layanan	Sie Koordinator Layanan	Kepala Perpustakaan	Kepala Perpustakaan

Berdasarkan hasil pemetaan RACI, pada penelitian ini terindikasi bahwa terdapat kemungkinan individu dalam organisasi yang mengemban tanggung jawab di luar cakupan yang seharusnya[12]. Hal ini dibuktikan dengan pembagian tugas atau pekerjaan yang dilakukan tidak tepat dengan jabatan.

4.3.2 Analisis Data

Pada tahap ini, analisis data dilakukan untuk mendukung proses audit sistem informasi pada Perpustakaan UPN "Veteran" Jawa Timur menggunakan kerangka kerja COBIT 5.

Tabel 4. Analisis data domain DSS001

Sub-Domain	Aspek	Keterangan
DSS001.01 Evaluasi sistem tata kelola	Frekuensi evaluasi tata kelola, metode evaluasi, kendala evaluasi	Evaluasi dilakukan berdasarkan kebutuhan dan hanya saat ada laporan masalah, belum ada jadwal atau sistem evaluasi terstruktur.
DSS001.02 Mengelola layanan TI yang dialihdayakan	Pengelolaan layanan TI alih daya, alur komunikasi, koordinasi antar pihak, kendala dalam pengelolaan	Layanan TI dikelola bersama tim telematika (Pak Agus). Kendala utama adalah kurangnya tim khusus IT di perpustakaan dan kurangnya formalitas sistem pemantauan.
DSS001.03 Memantau infrastruktur TI	Proses pemantauan infrastruktur TI, penggunaan monitoring tools, rencana peningkatan	Pemantauan hanya dilakukan saat terjadi gangguan, belum ada sistem monitoring otomatis. Rencana: menggunakan sistem monitoring real-time.
DSS001.04 Mengelola lingkungan	Prosedur pengelolaan lingkungan, pentingnya dokumentasi, kendala yang dihadapi	Pengelolaan sudah dilakukan, tetapi belum terstandar atau terdokumentasi dengan baik.
DSS001.05 Mengelola fasilitas	Pengelolaan sudah dilakukan, tetapi belum terstandar atau terdokumentasi dengan baik.	Pengelolaan dilakukan berdasarkan kebutuhan mendesak, belum ada jadwal rutin atau sistem terpusat.

Analisis data dilakukan berdasarkan domain yang digunakan yaitu domain DSS001 seperti yang terlihat pada tabel 4 di atas dan domain DSS005 seperti yang terlihat pada tabel 5 berikut.

Tabel 5. Analisis data domain DSS005

Sub-Domain	Aspek	Keterangan
DSS005.01 Mengelola identitas dan hak akses	Proses pengelolaan identitas dan hak akses, kebijakan autentikasi	Hak akses telah terstruktur berdasarkan peran pengguna, dengan kebijakan autentikasi yang jelas.
DSS005.02 Melindungi informasi	Perlindungan data pengguna, kebijakan perlindungan informasi, tantangan dalam mempertahankan keamanan	Data pengguna dilindungi dengan baik, tidak ada laporan kebocoran data. Tantangan utama: menghadapi ancaman siber baru.
DSS005.03 Menjamin keamanan infrastruktur TI	Prosedur evaluasi keamanan infrastruktur, dokumentasi keamanan, penanganan insiden	Keamanan diperiksa secara berkala, namun belum ada jadwal formal atau dokumentasi yang sistematis.
DSS005.04 Mengelola kerentanan sistem	Pengelolaan kerentanan sistem, prosedur pembaruan keamanan, penanganan masalah keamanan	Ada insiden hack sebelumnya, namun telah diatasi. Pembaruan sistem dilakukan tetapi tidak ada dokumentasi formal atau jadwal yang jelas.
DSS005.05 Meningkatkan kesadaran keamanan	Program pelatihan keamanan, langkah meningkatkan kesadaran, metode komunikasi kepada staf	Belum ada pelatihan keamanan rutin. Langkah peningkatan kesadaran hanya berupa peringatan kecil kepada staf.

4.3.3 Validasi Data

Pada tahap ini, hasil wawancara ini disusun untuk mendokumentasikan informasi yang diperoleh selama proses wawancara terkait audit sistem informasi di Perpustakaan UPN "Veteran" Jawa Timur.

Tabel 6. Hasil wawancara domain DSS001

Sub-Domain	Pertanyaan	Jawaban Narasumber	Catatan Penting
DSS001.01 Evaluasi sistem tata kelola	Seberapa sering evaluasi tata kelola dilakukan?	Sesuai kebutuhan saja, tidak tentu dan tidak terjadwal.	Evaluasi sistem belum terjadwal dan hanya dilakukan saat ada laporan masalah dari pengguna.
	Apa rencana untuk meningkatkan pemantauan infrastruktur?	Menerapkan sistem monitoring otomatis untuk laporan real-time dan historis.	Sistem ini akan membantu deteksi masalah lebih awal.
DSS001.02 Mengelola layanan TI yang dialihdayakan DSS001.03 Memantau infrastruktur TI	Apa kendala utama dalam evaluasi?	Belum ada evaluasi terjadwal atau berbasis data yang jelas, sehingga sulit untuk memonitor dan memperbaiki sistem secara proaktif.	Perlu sistem evaluasi yang berkelanjutan dan berbasis data.
	Bagaimana prosedur pengelolaan lingkungan saat ini?	Sudah dilakukan dengan baik, tetapi belum sepenuhnya terstruktur atau terstandarisasi.	Perlu prosedur yang terstandar dan dokumentasi sistematis.
	Apa kendala layanan TI yang	Tidak ada tim khusus IT di	Pengelolaan masih

	dialihdayakan?	perpustakaan, sehingga koordinasi harus dilakukan dengan tim telematika (Pak Agus). Tidak ada sistem pemantauan formal.	bergantung pada tindakan reaktif.
	Bagaimana pengelolaan fasilitas saat ini?	Dilakukan dengan baik, tetapi masih kondisional (berdasarkan kebutuhan mendesak).	Perlu jadwal perawatan rutin dan sistem manajemen fasilitas yang terpusat.
DSS001.04 Mengelola lingkungan	Bagaimana menjaga komunikasi dengan tim alih daya?	Ada alur komunikasi dengan tim telematika, tetapi terkadang tidak selalu tersedia saat terjadi masalah.	Komunikasi perlu dioptimalkan agar respons lebih cepat.
DSS001.05 Mengelola fasilitas	Bagaimana proses pemantauan infrastruktur TI saat ini?	Tidak ada sistem monitoring berkelanjutan. Pemantauan dilakukan hanya saat terjadi gangguan.	Perlu sistem monitoring otomatis dan real-time.
DSS001.01 Evaluasi sistem tata kelola	Seberapa sering evaluasi tata kelola dilakukan?	Sesuai kebutuhan saja, tidak tentu dan tidak terjadwal.	Evaluasi sistem belum terjadwal dan hanya dilakukan saat ada laporan masalah dari pengguna.

Pertanyaan wawancara didasarkan pada topik sub domain yang terdapat dalam domain DSS001 seperti yang tercantum pada tabel di atas dan domain DSS005 yang tercantum pada tabel berikut.

Tabel 7. Hasil wawancara domain DSS005

Sub-Domain	Pertanyaan	Jawaban Narasumber	Catatan Penting
DSS005.01 Mengelola identitas dan hak akses	Bagaimana proses pengelolaan identitas dan hak akses?	Sudah ada pembagian akses yang jelas berdasarkan peran pengguna, dengan kebijakan autentikasi yang diterapkan.	Sistem hak akses sudah cukup baik.
	Apa langkah meningkatkan kesadaran keamanan?	Belum ada pelatihan rutin. Upaya peningkatan hanya berupa peringatan kecil kepada staf.	Kesadaran keamanan perlu ditingkatkan dengan pelatihan rutin dan langkah sistematis.
DSS005.02 Melindungi informasi	Bagaimana sistem menjaga keamanan informasi?	Data pengguna (seperti nama dan riwayat peminjaman) telah dilindungi. Tidak ada laporan kebocoran data hingga saat ini.	Keamanan data dinilai efektif, tetapi perlu penyesuaian terhadap ancaman baru.
DSS005.03 Menjamin keamanan infrastruktur TI	Apa tantangan terbesar dalam menjaga keamanan?	Mengikuti perkembangan ancaman terbaru (serangan siber).	Ancaman keamanan harus diantisipasi melalui protokol
		Perlu pembaruan protokol keamanan secara berkala.	terbaru.
DSS005.04 Mengelola kerentanan sistem	Bagaimana prosedur menjamin keamanan infrastruktur TI?	Keamanan diperiksa berkala, tetapi belum ada jadwal formal atau dokumentasi standar.	Dokumentasi dan jadwal evaluasi formal perlu ditingkatkan.
DSS005.05 Meningkatkan kesadaran keamanan	Bagaimana pengelolaan kerentanan sistem?	Pembaruan keamanan dilakukan, tetapi tidak ada jadwal spesifik dan belum terdokumentasi formal. Pernah ada insiden hack, tetapi langsung ditangani oleh tim telematika.	Pengelolaan kerentanan perlu lebih terstruktur, termasuk dokumentasi insiden.
DSS005.01 Mengelola identitas dan hak akses	Bagaimana proses pengelolaan identitas dan hak akses?	Sudah ada pembagian akses yang jelas berdasarkan peran pengguna, dengan kebijakan autentikasi yang diterapkan.	Sistem hak akses sudah cukup baik.

4.4 Pengolahan Data dan Analisis

4.4.1 DSS001 *Manage Operations*

Berdasarkan hasil wawancara dan analisis dokumen yang ada, selanjutnya dilakukan analisis data dengan melakukan rekapitulasi nilai rata-rata aktivitas masing-masing subproses.

Tabel 8. *Current Capability* DSS001 *Manage Operation*

Sub Proses DSS	Aktivitas	*Current Capability* (CC)
DSS001.01	Evaluasi sistem tata kelola	3
DSS001.02	Mengelola layanan TI yang dialihdayakan	2
DSS001.03	Memantau infrastruktur TI	1
DSS001.04	Mengelola lingkungan	2
DSS001.05	Mengelola fasilitas	2
Rata-rata		2

Sebagaimana tercantum pada tabel 4.1, berikut adalah hasil nilai kapabilitas saat ini untuk masing-masing sub proses dalam DSS001.

1. DSS001.01 - Evaluasi sistem tata kelola: level 3, yaitu *"Established"*. Karena tidak ada evaluasi sistem yang terjadwal atau terstruktur. Evaluasi hanya dilakukan ketika ada laporan masalah dari pengguna, dan belum ada sistem evaluasi yang berkelanjutan atau berbasis data yang jelas.
2. DSS001.02 - Mengelola layanan TI yang dialihdayakan: level 2, yaitu *"Managed"*. Karena layanan TI yang dialihdayakan masih dilakukan secara terkelola dengan adanya koordinasi langsung saat terjadi masalah. Meskipun ada alur komunikasi dengan tim terkait, namun tidak ada sistem pemantauan atau pengelolaan layanan yang formal.
3. DSS001.03 - Memantau infrastruktur TI: level 1, yaitu *"Performed"*. Karena tidak ada pemantauan yang terstruktur terhadap infrastruktur TI. Pemantauan dilakukan secara ad-hoc dan hanya berdasarkan insiden atau gangguan yang muncul. Tidak ada sistem monitoring yang berkelanjutan.
4. DSS001.04 - Mengelola lingkungan: level 2, yaitu *"Managed"*. Karena pengelolaan fasilitas dan lingkungan fisik dilakukan dengan baik meskipun prosedurnya belum sepenuhnya terstruktur atau terstandarisasi. Lingkungan fisik dikelola, tetapi mungkin masih kurang sistematis dalam hal dokumentasi dan perencanaan.
5. DSS001.05 - Mengelola fasilitas: level 2, yaitu *"Managed"*. Karena fasilitas dikelola dengan baik, tetapi proses pengelolaannya belum terstandarisasi atau terjadwal secara formal. Tindakan perawatan dan pengelolaan fasilitas lebih bersifat reaktif berdasarkan kebutuhan mendesak.

Berdasarkan hasil pada tabel di atas, dapat dilihat bahwa kapabilitas dalam DSS001 *Manage Operations* berada pada level 2 *(Managed)*, yang menunjukkan bahwa sistem kapabilitas organisasi dalam mengelola operasi layanan TI masih berada pada tahap yang terkelola namun belum sepenuhnya terstruktur dan terstandarisasi.

4.4.2 DSS005 *Manage Security Services*

Berdasarkan hasil wawancara untuk sub domain DSS005, maka dilakukan analisis data dengan melakukan rekapitulasi nilai rata-rata aktivitas masing-masing subproses.

Tabel 9. *Current Capability* DSS005 *Manage Security Services*

Sub Proses	**Aktivitas**	***Current***
DSS		***Capability*** **(CC)**
DSS005.01	Mengelola identitas dan hak akses	3
DSS005.02	Melindungi informasi	4
DSS005.03	Menjamin keamanan infrastruktur TI	3
DSS005.04	Mengelola kerentanan sistem	2
DSS005.05	Meningkatkan kesadaran keamanan	1
Rata-rata		3

Sebagaimana tercantum pada tabel 4.2, berikut adalah hasil nilai kapabilitas saat ini untuk masing-masing sub proses dalam DSS005.

1. DSS005.01 - Mengelola identitas dan hak akses: level 3, yaitu *"Established"*. Karena sistem perpustakaan sudah memiliki pembagian akses berdasarkan peran pengguna. Kebijakan keamanan seperti autentikasi untuk pengguna sudah diterapkan.
2. DSS005.02 - Melindungi informasi: level 4, yaitu *"Predictable"*. Karena data pribadi pengguna, seperti nama dan riwayat peminjaman buku, dilindungi dengan baik. Tidak ada laporan kebocoran data hingga saat ini.
3. DSS005.03 - Menjamin keamanan infrastruktur TI: level 3, yaitu *"Established"*. Karena keamanan infrastruktur diperiksa secara berkala, tetapi belum ada jadwal formal untuk evaluasi keamanan, serta langkah-langkah penanganan insiden disesuaikan dengan kebutuhan.
4. DSS005.04 - Mengelola kerentanan sistem: level 2, yaitu *"Managed"*. Karena pembaruan keamanan sistem dilakukan, tetapi tidak ada jadwal spesifik untuk pelaksanaannya. Belum ada pengelolaan kerentanan yang terdokumentasi formal.
5. DSS005.05 - Meningkatkan kesadaran keamanan: level 1, yaitu *"Performed"*. Karena pelatihan keamanan belum dilakukan secara rutin, meskipun ada upaya meningkatkan kesadaran keamanan di kalangan staf.

Berdasarkan hasil pada tabel di atas, dapat dilihat bahwa kapabilitas dalam DSS005 *Manage Security Services* berada pada level 3 *(Established)*, yang menunjukkan bahwa kapabilitas keamanan layanan di sistem perpustakaan sudah cukup baik dan diterapkan secara terstruktur.

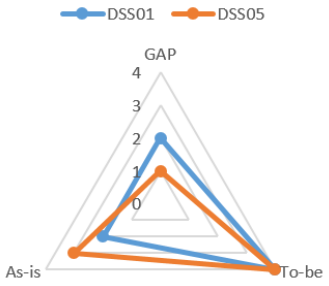
4.5 Analisis GAP

Setelah melakukan penilaian kapabilitas, analisis kesenjangan (*gap analysis*) dilakukan untuk membandingkan antara kondisi saat ini (*as-is*) dengan kondisi yang diharapkan (*to-be*) dalam pengelolaan operasional dan keamanan sistem informasi perpustakaan.

Tabel 10. Nilai GAP pada sub-domain

Sub Domain	*As-is*	*To-be*	GAP
DSS01 - *Manage Operations*	Level 2	Level 4	2
DSS05 - *Manage Security Services*	Level 3	Level 4	1

Berdasarkan tabel 4.3, pada domain DSS01 terdapat nilai kesenjangan sebesar 2 antara kondisi saat ini dengan kondisi yang diharapkan. Secara umum, pengelolaan operasional sistem informasi perpustakaan belum terstruktur dan terdokumentasi dengan baik. Banyak proses dilakukan secara ad-hoc tanpa sistem yang formal. Untuk mencapai level 4 yaitu *predictable*, dibutuhkan pengembangan kebijakan, prosedur formal, jadwal rutin evaluasi sistem, dan penerapan sistem monitoring berkelanjutan.



Gambar 4. *Spider chart* GAP sub-domain

Pada domain DSS05 nilai kesenjangannya sebesar 1. Keamanan sistem informasi perpustakaan telah dikelola dengan cukup baik, termasuk pengelolaan hak akses dan perlindungan data pribadi. Namun, untuk mencapai level 4 yaitu *predictable*, diperlukan peningkatan formalitas dalam pengelolaan keamanan, seperti jadwal pembaruan keamanan sistem, pelatihan rutin untuk staf, dan prosedur dokumentasi pengelolaan kerentanan.

4.6 Rekomendasi Perbaikan

Berdasarkan data pada level kapabilitas dan analisis gap, didapatkan rekomendasi perbaikan untuk proses DSS001 dan DSS005. Setiap rekomendasi perbaikan bertujuan untuk meningkatkan manajemen operasional dan keamanan sistem informasi di Perpustakaan UPN "Veteran" Jawa Timur. Dengan ini, diharapkan dapat mencapai level kapabilitas yang diharapkan yakni pada level 4 *(Predictable Process)*. Tim kelola IT dapat melakukan perbaikan dengan menyusun jadwal evaluasi dan pemeliharaan rutin, didukung oleh sistem pemantauan otomatis serta dashboard kinerja untuk memantau metrik operasional dan infrastruktur TI secara berkala. SLA yang terstandarisasi dengan pihak ketiga perlu diimplementasikan dan dipantau secara berkala, didukung oleh SOP yang jelas dan penggunaan CMMS untuk mengelola fasilitas. Selain itu, audit akses dan kontrol berbasis peran harus diperkuat, dengan kebijakan enkripsi data end-to-end dan pelaksanaan uji penetrasi rutin untuk mengidentifikasi kerentanan. Jadwal pembaruan keamanan, dokumentasi pengelolaan kerentanan, dan pelatihan staf mengenai kebijakan keamanan dan ancaman terkini juga harus dilakukan secara berkala untuk memastikan keamanan dan keberlanjutan sistem informasi.

5. KESIMPULAN

Berdasarkan hasil analisis terhadap kapabilitas sistem informasi Perpustakaan UPN “Veteran” Jawa Timur, dapat disimpulkan sebagai berikut.

a. Kapabilitas saat ini berada pada level 2 *(Managed)* untuk domain DSS001 dan level 3 *(Established)* untuk domain DSS005, yang menunjukkan pengelolaan operasional dan keamanan sudah berjalan namun belum mencapai level 4 *(Predictable)*.
b. Didapatkan beberapa rekomendasi yaitu membutuhkan kebijakan formal seperti penyusunan SOP, SLA terstandar, evaluasi berkala, dan pemantauan otomatis. Selain itu, sistem memerlukan audit akses, kebijakan enkripsi, jadwal audit keamanan rutin, pembaruan sistem, dan pelatihan staf.

Dengan implementasi rekomendasi tersebut, diharapkan kapabilitas sistem informasi dapat meningkat, sehingga mendukung layanan perpustakaan yang lebih aman dan efisien.

UCAPAN TERIMA KASIH

Terima kasih kepada semua pihak yang telah mendukung dan berkontribusi dalam penyelesaian

jurnal ini. Terima kasih khususnya kepada dosen pembimbing atas bimbingan dan arahan yang berharga, serta kepada keluarga dan teman-teman yang selalu memberikan dukungan moral. Semoga hasil penelitian ini bermanfaat bagi pengembangan ilmu pengetahuan.

DAFTAR PUSTAKA

[1] S. Humaira, G. F. Nama, dan R. A. Pradipta, "Analisis Tata Kelola Teknologi Informasi Menggunakan COBIT 5 Subdomain DSS01 Manage Operations (Studi Kasus PT. BRI BO Liwa)," Jurnal Informatika dan Teknik Elektro Terapan, vol. 12, no. 2, pp. 1410–1420, 2024.

[2] Rahmaha, et al., "Audit Sistem Informasi Perpustakaan UPN dengan COBIT 5 pada DSS001 dan DSS003," Jurnal Teknik Informatika dan Sistem Informasi, vol. 4, no. 3, pp. 490–499, Desember 2018.

[3] Shafira, et al., "Evaluasi Tata Kelola Teknologi Informasi Perpustakaan Menggunakan COBIT 4.1," Jurnal Sistem Informasi dan Manajemen, vol. 3, no. 2, pp. 215–226, 2014.

[4] ISACA, "COBIT 5: Framework for IT Governance and Management," ISACA Press, 2012.

[5] Herlina, H. (2006). Ilmu Perpustakaan Dan Informasi.

[6] Sihotang, H. T., Zarlis, M., Efendi, S., & Jollyta, D. (2019, August). Evaluation of Maturity Level of Information and Communication Technology (ICT) Governance with CobIT 5.0 Case Study: STMIK Pelita Nusantara Medan. In *Journal of Physics: Conference Series* (Vol. 1255, No. 1, p. 012046). IOP Publishing.

[7] Purwaningrum, O. (2021). Studi Literatur: Framework Cobit 5 Pada Tata Kelola Teknologi Informasi. *Scan: Jurnal Teknologi Informasi dan Komunikasi*, *16*(2), 7-14.

[8] Suryono, R. R., Darwis, D., & Gunawan, S. I. (2018). Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 (Studi Kasus: Balai Besar Perikanan Budidaya Laut Lampung). *Jurnal Teknoinfo*, *12*(1), 16-22

[9] Candra, R. K., Atastina, I., & Firdaus, Y. (2015). Audit teknologi informasi menggunakan framework COBIT 5 pada domain DSS (Deliver, Service, and Support)(Studi kasus: IGRACIAS Telkom University). *eProceedings of Engineering*, *2*(1).

[10] I. Susiyana, J. Triloka, & Sutedi, "Audit Sistem Informasi Perpustakaan Sekolah Menggunakan Frame Work Cobit 5 Pada SMAN 1 Terbanggi Besar Lampung Tengah," Seminar Nasional Hasil Penelitian dan Pengabdian Masyarakat 2023, Institut Informatika dan Bisnis Darmajaya, pp. 132, 2023.

[11] T. D. N. B. Mira, E. Sediyono, & A. Iriani, "Audit Pemanfaatan Sistem Informasi Akademik Di Universitas Kristen Wira Wacana Sumba Menggunakan Framework Cobit 5," JOINTER – Journal of Informatics Engineering, vol. 2, no. 2, 2021.

[12] S. Humaira, G. F. Nama, dan R. A. Pradipta, "Analisis Tata Kelola Teknologi Informasi Menggunakan COBIT 5 Subdomain DSS01 Manage Operations (Studi Kasus PT. BRI BO Liwa)," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 2, pp. 123–132, 2024.