



AUDIT SISTEM INFORMASI JB CLASS DENGAN PENGUKURAN *CAPABILITY LEVEL* KINERJA DAN KEAMANAN MENGGUNAKAN COBIT 2019 (STUDI KASUS: BALAI TEKKOMDIK DIY)

Paramadina Evita Pertiwi¹, Ulfi Saidata Aesy², Arif Himawan³

¹²³ Fakultas Teknik dan Teknologi Informasi, Program Studi Sistem Informasi, Universitas Jenderal Achmad vYani Yogyakarta, Indonesia

Article Info:

Dikirim:
Direvisi:
Diterima:
Tersedia Online:

Penulis Korespondensi:

Paramadina Evita Pertiwi
Universitas Jenderal Achmad Yani
Yogyakarta, Yogyakarta, Indonesia
Email: paramadinaep@gmail.com

Abstrak: *JB Class merupakan sistem informasi pembelajaran berbasis web yang dikembangkan oleh Balai Tekkomdik DIY untuk mendukung digitalisasi pendidikan di Daerah Istimewa Yogyakarta. Seiring meningkatnya pemanfaatan sistem JB Class, perlu dilakukan audit untuk menilai kinerja dan keamanannya. Penelitian ini bertujuan mengevaluasi sistem JB Class menggunakan framework Control Objectives for Information and Related Technology (COBIT) 2019 dengan fokus pada domain Deliver, Service and Support (DSS) dan Monitor, Evaluate and Assess (MEA). Penelitian dilakukan dengan metode triangulasi data, yaitu wawancara, observasi, dan studi dokumen. Hasil evaluasi menunjukkan bahwa sebagian besar proses masih berada pada capability level 0 dan 1. Proses DSS05.02 menjadi satu-satunya yang mencapai level 1, sedangkan proses seperti DSS01.03 dan MEA04 masih berada pada level 0. Ditemukan bahwa dokumentasi belum lengkap dan belum tersedia kontrol sistematis terhadap risiko keamanan serta evaluasi berkala. Oleh karena itu, direkomendasikan adanya penguatan dokumentasi, penyusunan kebijakan formal, dan pelaksanaan audit sistem secara berkala.*

Kata kunci: *audit system informasi, DSS, MEA*

Abstract: *JB Class is a web-based learning information system developed by Balai Tekkomdik DIY to support education digitalization in the Special Region of Yogyakarta. As the system's usage grows, an audit is needed to assess its performance and security. This study aims to evaluate JB Class using the Control Objectives for Information and Related Technology (COBIT) 2019 framework, focusing on the Deliver, Service and Support (DSS) and Monitor, Evaluate and Assess (MEA) domains. The research employs a data triangulation method through interviews, observations, and document studies. The results show that most processes are still at capability levels 0 and 1. DSS05.02 is the only process that reached level 1, while processes such as DSS01.03 and MEA04 remain at level 0. It was found that the documentation is incomplete and systematic control over security risks and regular system evaluations are lacking. Therefore, strengthening documentation, establishing formal policies, and conducting regular audits are recommended.*

Keywords: *Information system audit, DSS, MEA*

1. PENDAHULUAN

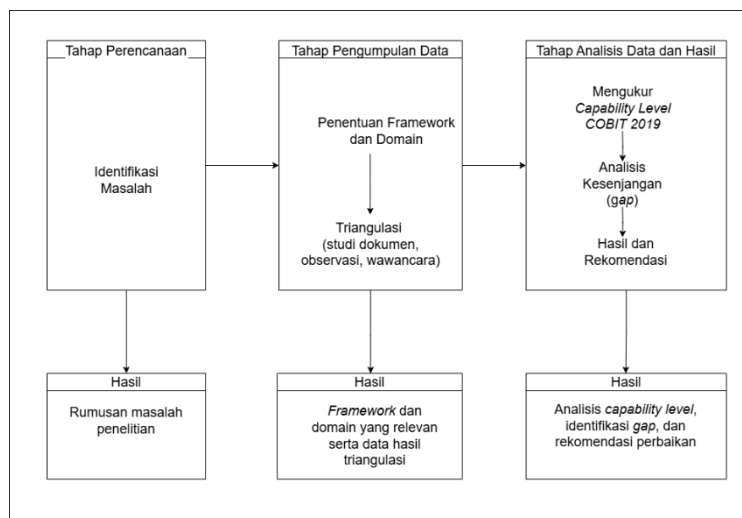
Teknologi informasi telah menjadi bagian penting dalam perubahan berbagai sektor, khususnya pendidikan [1]. Saat ini, sistem informasi tidak hanya berfungsi sebagai alat bantu dalam proses pembelajaran, tetapi juga memegang peranan penting dalam pengelolaan data akademik dan administratif secara efisien serta terintegrasi [2]. Pemanfaatan sistem ini membuka peluang bagi instansi pendidikan untuk meningkatkan kualitas layanan pembelajaran secara menyeluruh. Sistem informasi pendidikan juga memberikan fleksibilitas dalam proses pembelajaran, memungkinkan integrasi antara metode daring dan luring [3]. Seiring meningkatnya kompleksitas dan cakupan sistem informasi di lingkungan pendidikan, evaluasi berkala menjadi suatu keharusan [4]. Evaluasi tersebut diperlukan untuk memastikan bahwa sistem mampu beroperasi secara optimal, aman, serta memenuhi kebutuhan pengguna [5]. Audit sistem informasi menjadi salah satu pendekatan yang banyak

digunakan untuk menilai performa sistem serta memberikan *feedback* bagi pengembangan sistem ke depan [6]. *Framework* COBIT 2019 telah banyak digunakan dalam audit sistem informasi karena kemampuannya dalam memberikan penilaian terstruktur terhadap proses TI berbasis *capability level* [7]. Beberapa studi terdahulu menunjukkan efektivitas COBIT dalam mengukur kinerja dan kontrol sistem informasi, khususnya melalui domain *Deliver, Service, and Support (DSS)* dan *Monitor, Evaluate, and Assess (MEA)* [8]. Selain itu, pendekatan *capability level* yang ditawarkan oleh COBIT 2019 juga dinilai relevan untuk mengukur tingkat kematangan proses TI dalam menjamin kualitas layanan dan keamanan secara berkelanjutan di sektor pendidikan [9]. Namun, sebagian penelitian fokus pada sistem informasi kepegawaian, absensi, dan layanan perusahaan, sementara penelitian yang menyoroti sistem pembelajaran daring pada instansi pemerintah daerah masih sangat terbatas. Oleh karena itu, penelitian ini difokuskan pada salah satu sistem informasi pembelajaran yang dikembangkan oleh instansi pemerintah daerah, yaitu sistem JB Class.

Balai Teknologi Komunikasi dan Pendidikan DIY (Balai Tekkomdik DIY) telah mengembangkan sistem informasi JB Class sebagai sarana pendukung pembelajaran berbasis teknologi. Sistem ini digunakan oleh siswa, guru, dan orang tua. Namun, hingga saat ini belum pernah dilakukan audit sistem informasi secara menyeluruh terhadap JB Class. Beberapa permasalahan masih ditemukan dalam implementasinya, antara lain belum tersedianya proses verifikasi pengguna saat registrasi. Oleh karena itu, penelitian ini bertujuan untuk melakukan audit terhadap sistem JB Class menggunakan *framework* COBIT 2019 pada domain DSS dan MEA. Tujuan utama dari penelitian ini adalah untuk mengevaluasi tingkat kapabilitas sistem dalam aspek kinerja layanan dan keamanan, serta memberikan rekomendasi yang dapat digunakan untuk meningkatkan keandalan dan efektivitas sistem di masa mendatang. Dengan pendekatan ini, penelitian diharapkan dapat memberikan gambaran nyata di lapangan mengenai audit sistem informasi pembelajaran berbasis COBIT 2019, khususnya di lingkungan instansi pemerintahan daerah.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode triangulasi, yaitu studi dokumen, observasi, dan wawancara. Tujuan penelitian adalah mengevaluasi *capability level* sistem informasi JB Class berdasarkan *framework* COBIT 2019 pada domain *Deliver, Service, and Support (DSS)* dan *Monitor, Evaluate, and Assess (MEA)*. COBIT 2019 merupakan *framework* tata kelola teknologi informasi yang mendukung perencanaan strategi, pengelolaan operasional, serta evaluasi manajemen TI secara lebih optimal [10]. *Framework* ini memiliki dua tujuan utama, yaitu tata kelola dan manajemen. Tujuan tata kelola hanya mencakup satu domain, yakni *Evaluate, Direct, and Monitor (EDM)*, sedangkan tujuan manajemen terdiri dari empat domain: *Align, Plan, and Organize (APO)*, *Build, Acquire, and Implement (BAI)*, *Deliver, Service, and Support (DSS)*, serta *Monitor, Evaluate, and Assess (MEA)* [11]. Namun, dalam penelitian ini hanya dua domain yang digunakan dalam penelitian ini, yaitu DSS dan MEA, karena relevan dengan aspek kinerja dan keamanan sistem informasi. Audit dilakukan melalui tiga tahap utama: perencanaan, pengumpulan data, serta analisis dan evaluasi hasil. Ketiga tahapan ini ditampilkan secara sistematis pada Gambar 1.



Gambar 1 Alur Penelitian

2.1 TAHAP PERENCANAAN

Tahapan ini bertujuan mengidentifikasi permasalahan utama yang menjadi dasar pelaksanaan audit. JB Class dipilih karena belum pernah dievaluasi secara formal sejak digunakan. Permasalahan yang ditemukan antara lain adalah tidak tersedianya verifikasi pengguna pada saat registrasi, serta beberapa kendala teknis dalam implementasi harian. Permasalahan ini menjadi dasar untuk merumuskan fokus audit terhadap *capability level* sistem.

2.2 TAHAP PENGUMPULAN DATA

1. Penentuan *Framework* dan Domain

Tahap awal pengumpulan data adalah menetapkan *framework* audit yang digunakan. Penelitian ini menggunakan COBIT 2019, *framework* tata kelola TI yang menilai kapabilitas proses berdasarkan skala *capability level*. Dari lima domain utama yang tersedia, dipilih dua domain yang paling relevan dengan konteks sistem JB Class, yaitu *Deliver, Service, and Support* (DSS) dan *Monitor, Evaluate, and Assess* (MEA). Pemilihan ini didasarkan pada fokus evaluasi terhadap aspek kinerja layanan, pengelolaan insiden, serta pemantauan efektivitas sistem informasi.

2. Metode Triangulasi

Setelah domain yang akan dievaluasi ditentukan, data dikumpulkan dengan metode triangulasi, yang mencakup tiga pendekatan utama:

1. Wawancara

Dilakukan dengan tim teknis pengembang dan pengguna kunci JB Class untuk menggali pemahaman terkait proses bisnis, kendala operasional, dan harapan pengembangan sistem ke depan.

2. Observasi

Dilakukan secara langsung terhadap sistem JB Class untuk meninjau fitur-fitur utama, alur operasional, serta masalah teknis yang muncul dalam praktik penggunaan.

3. Studi Dokumen

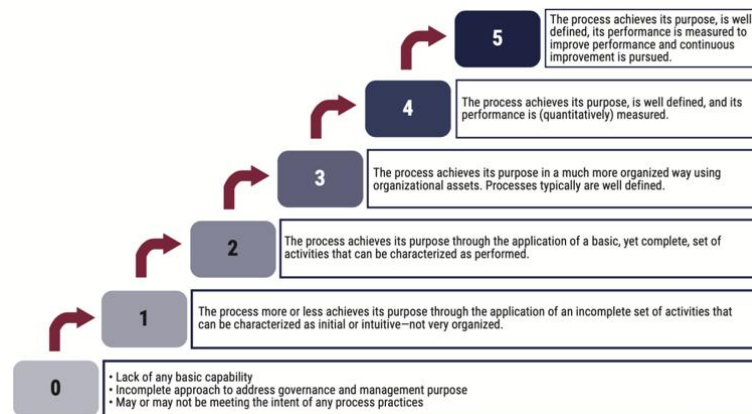
Mencakup analisis dokumen internal seperti panduan pengguna, SOP, dan notulen teknis, yang memberikan gambaran tentang struktur pengelolaan dan prosedur sistem.

Data dari ketiga pendekatan ini digunakan untuk menilai proses-proses dalam domain DSS dan MEA, sesuai dengan mekanisme penilaian COBIT 2019 yang mempertimbangkan *rating activity* dan *design factors* dalam menentukan *capability level* dan kesenjangan (*gap*) dari kondisi saat ini. Hasil dari tahapan ini, menentukan *framework* dan domain yang relevan serta penggunaan metode triangulasi.

2.3 TAHAP ANALISIS DATA DAN HASIL

1. Mengukur *Capability level* COBIT 2019

Capability level digunakan untuk menilai sejauh mana suatu proses telah dijalankan dan diimplementasikan dalam suatu organisasi [12]. Proses evaluasi dilakukan berdasarkan standar COBIT 2019, yang mengklasifikasikan *capability level* dari level 0 hingga level 5, sebagaimana ditampilkan pada Gambar 2.



Gambar 2 Capability Level

Evaluasi terhadap *capability level* dilakukan dengan merujuk pada empat kategori *rating process activities*, sebagaimana tercantum dalam Tabel 2.3. Setiap kategori berfungsi untuk menilai sejauh mana aktivitas dalam suatu proses telah dilaksanakan secara konsisten dan terdokumentasi. Penilaian ini digunakan untuk mengidentifikasi apakah suatu proses belum mencapai, telah sesuai, atau melampaui standar yang ditetapkan [13].

Tabel 1 *Rating Process Activities*

Kode	Management objectives	Target capability level
N	<i>Not Achieved</i> (Tidak Tercapai)	0% - 15%
P	<i>Partially Achieved</i> (Sebagian Tercapai)	15% - 50%
L	<i>Largely Achieved</i> (Sebagian Besar Tercapai)	50% - 85%
F	<i>Fully Achieved</i> (Sepenuhnya Tercapai)	85% - 100%

Berdasarkan pedoman COBIT 2019, penilaian *capability level* dilakukan secara bertahap dan berjenjang, di mana suatu proses hanya dapat ditingkatkan ke level berikutnya apabila seluruh aktivitas pada level sebelumnya telah mencapai kategori *Fully Achieved (F)* [14]. Prinsip evaluasi ini diperkuat oleh temuan Yolanda dan Wulandari Ginting (2003) yang menegaskan bahwa penilaian *capability level* tidak dapat dilanjutkan ke tingkat yang lebih tinggi apabila syarat pada level sebelumnya belum sepenuhnya terpenuhi [15]. Oleh karena itu, pada proses yang dievaluasi dalam penelitian ini, *capability level* ditetapkan pada Level 0 karena belum seluruh aktivitas pada Level 1 mencapai kriteria *Fully Achieved (F)*.

2. Analisis Kesenjangan (*gap*)

Analisis kesenjangan dilakukan untuk mengidentifikasi perbedaan antara kondisi saat ini dengan kondisi yang diharapkan berdasarkan standar COBIT 2019. Analisis ini digunakan untuk menentukan proses mana yang perlu diperbaiki guna mencapai level yang diharapkan.

3. Hasil dan Rekomendasi

Berdasarkan hasil analisis *capability level* dan kesenjangan, dirumuskan rekomendasi yang ditujukan untuk meningkatkan efektivitas dan keamanan sistem. Rekomendasi ini difokuskan pada perbaikan proses, peningkatan kualitas layanan, serta pencapaian *capability level* yang lebih optimal dan berkelanjutan.

3. HASIL DAN PEMBAHASAN

3.1 TAHAP PERENCANAAN

Tahap perencanaan merupakan langkah awal dalam evaluasi tata kelola sistem informasi JB Class yang dikelola oleh Balai Tekkomdik DIY. Evaluasi ini dilatarbelakangi oleh belum dilakukannya penilaian formal berbasis kerangka kerja standar, sehingga belum tersedia informasi yang memadai mengenai kesesuaian pengelolaan sistem terhadap prinsip-prinsip tata kelola TI yang baik. Penelusuran awal mengidentifikasi kelemahan pada aspek keamanan, khususnya ketiadaan fitur autentikasi dua faktor dan pengiriman kode OTP saat proses login atau aktivitas yang bersifat sensitif. Kondisi ini meningkatkan potensi risiko penyalahgunaan akses oleh pihak yang tidak berwenang. Sebagai pedoman evaluasi, digunakan framework COBIT 2019, yang menawarkan pendekatan berbasis proses dengan skala *capability level* untuk menilai tingkat kematangan pengelolaan TI secara sistematis. Pada tahap ini, disusun pula rancangan instrumen pengumpulan data menggunakan metode triangulasi meliputi wawancara, observasi, dan studi dokumen guna memperoleh data yang komprehensif dan valid sebagai dasar analisis pada tahapan berikutnya.

3.2 TAHAP PENGUMPULAN DATA

1. Penetapan *Framework* dan Domain Evaluasi

Penelitian ini menetapkan framework COBIT 2019 sebagai dasar evaluasi karena menyediakan struktur proses yang komprehensif serta alat ukur *capability level* untuk menilai tingkat kematangan tata kelola TI secara sistematis. Berdasarkan karakteristik sistem JB Class dan kebutuhan evaluasi, dipilih dua domain utama, yaitu *Deliver, Service and Support (DSS)* dan *Monitor, Evaluate and Assess (MEA)*. Domain DSS mencakup proses-proses yang berkaitan dengan operasional sistem dan pengelolaan layanan keamanan, seperti pemantauan infrastruktur dan perlindungan jaringan. Sementara itu, domain MEA berfokus pada pemantauan kinerja, evaluasi efektivitas kontrol, serta kegiatan penjaminan mutu sistem. Seluruh proses dalam kedua domain tersebut (DSS01.01 hingga DSS06.03 dan MEA01.01 hingga MEA04) dijadikan objek awal evaluasi dengan mengacu pada indikator aktivitas dalam COBIT 2019. Untuk memperoleh hasil yang lebih terfokus dan mendalam, penelitian ini memusatkan analisis pada tiga proses utama yang dipilih berdasarkan capaian *capability level*, kesenjangan (*gap*) antara kondisi saat ini dan kondisi yang diharapkan, serta urgensi proses terhadap keberlangsungan layanan TI.

2. Metode Pengumpulan Data (Triangulasi)

Pengumpulan data dilakukan melalui tiga pendekatan utama, yaitu studi dokumen, observasi, dan wawancara. Pendekatan ini dirancang secara triangulatif agar saling melengkapi dan meningkatkan validitas serta kedalaman data yang diperoleh. Selama prosesnya, peneliti didampingi oleh tim IT dari Balai Tekkomdik untuk memahami struktur sistem JB Class, menelaah dokumen teknis, serta memverifikasi hasil observasi dan wawancara. Dalam proses evaluasi, disusun total 150 butir pertanyaan audit yang mengarah pada 29 proses dalam domain DSS dan MEA dari framework COBIT 2019, terdiri atas 127 pertanyaan untuk domain DSS dan 23 pertanyaan untuk domain MEA. Namun demikian, untuk menjaga ketelitian analisis dan menghindari pemecahan data yang terlalu luas, penelitian ini menerapkan teknik *sampling* purposif, yakni dengan memilih 3 hingga 5 pertanyaan yang paling representatif untuk setiap proses. Pemilihan dilakukan berdasarkan tingkat relevansi, kekuatan indikator aktivitas proses yang diwakili, serta kesesuaian konteks dengan implementasi sistem JB Class. Pendekatan ini dianggap lebih efektif dalam menghasilkan evaluasi yang terarah, mendalam, dan tetap selaras dengan prinsip-prinsip COBIT 2019.

Berdasarkan proses yang dievaluasi, tiga di antaranya dipilih untuk dianalisis lebih dalam, yaitu DSS01.03, DSS05.02, dan MEA04. Pemilihan ini didasarkan pada capaian *capability level*, kesenjangan antara kondisi saat ini dan kondisi yang diharapkan, serta urgensi proses terhadap keberlangsungan layanan TI. DSS01.03 dipilih karena menunjukkan capaian *capability level* 0, sementara targetnya adalah level 3, mencerminkan kesenjangan paling signifikan dalam aspek pemantauan infrastruktur. Di sisi lain, DSS05.02 telah mencapai level 1 sesuai target, merepresentasikan proses yang telah berjalan optimal pada tingkat dasar. Adapun MEA04 dipilih karena seluruh aktivitasnya berada pada tingkat *Not Achieved (N)*, menunjukkan belum adanya pelaksanaan mekanisme assurance secara formal terhadap sistem.

A. Domain DSS

DSS01 – Mengelola Operasional (*Managed Operations*)

DSS01.03 – Memantau Infrastruktur TI (*Monitor IT Infrastructure*)

Pengumpulan data pada proses DSS01.03 menunjukkan bahwa sistem JB Class telah menerapkan pemantauan infrastruktur melalui alat seperti Grafana, yang memungkinkan pemantauan kondisi server secara *real-time*. Meskipun pengelolaan teknis sudah tersedia, belum ditemukan dokumentasi formal terkait jadwal dan hasil pemantauan, serta mekanisme notifikasi belum berjalan otomatis dan masih bergantung pada pengecekan manual. Temuan lengkap dari triangulasi data disajikan pada Tabel 2.

Tabel 2 Pertanyaan dan Jawaban Metode Triangulasi - DSS01.03

Kode	Pertanyaan	Jawaban
D131	Apakah sistem JB Class menggunakan alat pemantauan infrastruktur TI secara real-time, seperti Zabbix atau fitur bawaan dari layanan hosting/cloud?	Studi Dokumen: Terdapat dokumentasi teknis internal yang menunjukkan bahwa sistem JB Class menggunakan Grafana sebagai alat monitoring infrastruktur. Dokumentasi ini mencakup konfigurasi dashboard serta parameter performa yang dimonitor.
		Observasi: Hasil observasi menunjukkan bahwa sistem JB Class menggunakan Grafana untuk memantau kondisi server secara real-time, seperti penggunaan CPU, memori, dan status layanan. Akses ke dashboard ini terbatas pada tim teknis Balai dan pihak terkait.
		Wawancara: Tim IT menjelaskan bahwa Grafana digunakan sebagai alat pemantauan utama untuk infrastruktur TI. Alat ini membantu tim dalam mendeteksi gangguan secara dini dan menjaga kestabilan sistem.
D132	Apakah sistem memiliki mekanisme alert atau notifikasi dini untuk mendeteksi potensi gangguan pada infrastruktur, seperti server mendekati <i>overload</i> , storage hampir penuh, atau koneksi jaringan terputus?	Studi Dokumen: Terdapat dokumentasi internal mengenai konfigurasi sistem monitoring menggunakan Grafana.
		Observasi: Berdasarkan tampilan dashboard Grafana, ditemukan fitur alert berupa ikon lonceng yang menandakan adanya notifikasi apabila terjadi kondisi abnormal pada server. Notifikasi ini hanya terlihat saat dashboard dibuka secara manual, dan tidak dikirimkan melalui email atau media lain.
		Studi Dokumen:

Kode	Pertanyaan	Jawaban
		Tim IT menyampaikan bahwa sistem pemantauan menggunakan Grafana dengan alert aktif di dalam dashboard. Namun, notifikasi tidak dikirim ke luar sistem (seperti ke email atau perangkat seluler), sehingga pengecekan harus dilakukan secara manual oleh tim teknis.
D133	Seberapa rutin tim IT Balai Tekkomdik melakukan pemantauan terhadap performa server, jaringan, atau komponen lain yang terkait dengan sistem JB Class?	Studi Dokumen: Tidak ditemukan dokumen yang menjelaskan jadwal atau prosedur tertulis terkait frekuensi pemantauan rutin terhadap performa infrastruktur TI.
		Observasi: Berdasarkan observasi, tim IT Balai Tekkomdik melakukan pemantauan sistem setiap hari dengan memastikan sistem dapat diakses dan layanan berjalan normal. Dashboard Grafana juga digunakan untuk memantau kondisi server secara <i>real-time</i> , namun tidak ditemukan dokumentasi hasil pemantauan yang disusun secara berkala.
		Wawancara: tim IT menyampaikan bahwa pemantauan infrastruktur dilakukan setiap hari, baik melalui pengecekan langsung maupun dengan bantuan Grafana. Fokus pemantauan meliputi performa server, ketersediaan layanan, dan deteksi potensi gangguan.
D134	Jika dari hasil pemantauan ditemukan potensi gangguan pada infrastruktur TI yang dikelola oleh Kominfo, bagaimana prosedur yang dilakukan oleh tim IT Balai Tekkomdik dalam menindaklanjutinya?	Studi Dokumen: Tidak ditemukan dokumen SOP atau panduan tertulis yang menjelaskan secara rinci prosedur penanganan atau koordinasi apabila ditemukan potensi gangguan pada infrastruktur TI yang berada di bawah tanggung jawab Dinas Kominfo.
		Observasi: Observasi dilakukan secara tidak langsung. Tim IT Balai Tekkomdik menunjukkan dokumentasi percakapan (chat) dengan pihak Dinas Kominfo sebagai bukti koordinasi saat terjadi gangguan sistem.
		Wawancara: Berdasarkan wawancara dengan tim IT Balai Tekkomdik, jika terdapat potensi gangguan, tim akan melakukan pengecekan awal secara mandiri. Selanjutnya, koordinasi dilakukan secara informal, salah satunya melalui platform komunikasi seperti Discord. Hingga saat ini belum terdapat prosedur formal yang dijadikan acuan dalam proses tersebut.

DSS05 – Mengelola Layanan Keamanan (*Managed Security Services*)

DSS05.02 – Mengelola Keamanan Jaringan dan Konektivitas (*Manage Network and Connectivity Security*)

Pada DSS05.02, sistem JB Class telah dilindungi oleh infrastruktur jaringan dari Dinas Kominfo, menggunakan protokol komunikasi aman (HTTPS), dan dilengkapi dengan firewall aktif pada tingkat server. Namun, aspek dokumentasi formal terkait kebijakan keamanan dan prosedur pelaksanaan masih belum memadai. Rincian hasil triangulasi data ditampilkan dalam Tabel 3.

Tabel 3 Pertanyaan dan Jawaban Metode Triangulasi - DSS05.02

Kode	Pertanyaan	Jawaban
D521	Bagaimana keamanan jaringan internet sistem dijaga?	Studi Dokumen: Terdapat dokumen teknis yang menjelaskan bahwa pengamanan jaringan dilakukan oleh Dinas Kominfo.
		Observasi: Tampilan sistem JB Class tidak menyediakan informasi atau indikator terkait status keamanan jaringan. Informasi mengenai pengamanan jaringan diperoleh dari dokumentasi teknis dan penjelasan tim IT.
		Wawancara: Tim IT menyampaikan bahwa sistem JB Class dilindungi oleh infrastruktur jaringan milik Kominfo.
D522		Studi Dokumen:

Kode	Pertanyaan	Jawaban
	Apakah data dikirim menggunakan protokol aman (HTTPS, SSL)?	<p>Terdapat dokumen konfigurasi teknis yang menunjukkan penerapan HTTPS untuk pengamanan koneksi.</p> <p>Observasi: Hasil observasi menunjukkan bahwa URL sistem JB Class menampilkan HTTPS, yang menandakan koneksi telah menggunakan enkripsi SSL.</p> <p>Wawancara: Tim IT menyatakan bahwa sistem JB Class menggunakan HTTPS sebagai protokol utama dalam komunikasi data untuk menjaga kerahasiaan dan keamanan data pengguna.</p>
D523	Apakah ada firewall atau proteksi dari serangan luar?	<p>Studi Dokumen: Terdapat dokumen konfigurasi jaringan dan kebijakan akses yang menunjukkan penerapan firewall pada server yang digunakan JB Class.</p> <p>Observasi: Hasil observasi tidak terdapat informasi dalam tampilan sistem JB Class mengenai konfigurasi firewall, namun dokumentasi menunjukkan penggunaan firewall aktif di tingkat server.</p> <p>Wawancara: Tim IT menyampaikan bahwa firewall aktif digunakan di server Kominfo untuk membatasi akses yang tidak sah dan melindungi sistem dari serangan luar.</p>

B. Domain MEA

MEA04 – Memberikan Jaminan (*Provide Assurance*)

Hasil pengumpulan data pada proses MEA04 menunjukkan bahwa belum terdapat mekanisme assurance yang terdokumentasi secara formal. Proses evaluasi sistem dilakukan secara *ad-hoc* dan belum mencakup pengujian terhadap keamanan, kontrol akses, maupun evaluasi fungsional secara berkala. Temuan ini mencerminkan bahwa aspek assurance belum terintegrasi dalam tata kelola sistem JB Class. Detail hasil pengumpulan data dapat dilihat pada Tabel 4.

Tabel 4 Pertanyaan dan Jawaban Metode Triangulasi – MEA04

Kode	Pertanyaan	Jawaban
M41	Apakah Balai Tekkomdik memiliki prosedur resmi untuk melakukan assurance atau penjaminan terhadap sistem JB Class, baik secara internal maupun oleh pihak luar?	<p>Studi Dokumen: Tidak ditemukan dokumen resmi atau SOP terkait assurance.</p> <p>Observasi: Tidak terdapat menu, fitur, atau informasi evaluasi sistem di JB Class.</p> <p>Wawancara: Tim menyampaikan belum ada prosedur assurance formal; evaluasi hanya dilakukan teknis oleh tim internal.</p>
M42	Apakah proses assurance tersebut mencakup pengujian keamanan sistem, pengaturan akses pengguna, dan efektivitas fitur yang tersedia?	<p>Studi Dokumen: Tidak tersedia laporan pengujian atau standar evaluasi aspek keamanan dan kontrol akses.</p> <p>Observasi: Tidak ditemukan dokumentasi atau alat ukur evaluasi keamanan dan akses.</p> <p>Wawancara: Tim menyatakan pengecekan dilakukan berkala jika ada kendala, namun tidak terdokumentasi.</p>
M43	Seberapa rutin proses assurance dilakukan dan apakah hasilnya diperbarui secara berkala?	<p>Studi Dokumen: Tim menyatakan pengecekan dilakukan berkala jika ada kendala, namun tidak terdokumentasi.</p> <p>Observasi: Tidak terdapat histori pembaruan terkait evaluasi sistem.</p> <p>Wawancara: Tim menyampaikan evaluasi dilakukan saat terjadi gangguan atau pengembangan fitur, tanpa jadwal khusus.</p>

3.3 TAHAP ANALISI DATA DAN HASIL

Tahap ini menjelaskan proses analisis data yang diperoleh melalui wawancara, observasi, dan studi dokumen terhadap sistem informasi JB Class. Analisis dilakukan berdasarkan *framework* COBIT 2019 dengan menggunakan skala *capability level* sebagai dasar penilaian. Setiap proses dievaluasi berdasarkan aktivitas utamanya, disertai pemberian skor capaian, rating aktivitas, dan penetapan *capability level* yang mencerminkan kondisi saat ini. Dari 29 proses pada domain DSS dan MEA yang menjadi objek awal evaluasi, penelitian ini memfokuskan analisis pada tiga proses utama: DSS01.03, DSS05.02, dan MEA04. Pemilihan ketiganya didasarkan pada capaian *capability level*, tingkat kesenjangan (*gap*) antara kondisi saat ini dan kondisi yang diharapkan, serta urgensinya terhadap keberlangsungan dan keamanan layanan sistem. Hasil analisis ini memberikan gambaran menyeluruh terhadap kondisi tata kelola TI yang berjalan, sekaligus menjadi dasar penyusunan rekomendasi peningkatan yang sesuai dengan prinsip COBIT 2019.

A. Analisis domain DSS dan MEA

1. DSS01.03 – Memantau Infrastruktur TI (*Monitor IT Infrastructure*)

Proses ini bertujuan untuk mengevaluasi pelaksanaan monitoring infrastruktur teknologi informasi pada sistem JB Class, termasuk efektivitas pemantauan kinerja dan respons terhadap gangguan. Hasil evaluasi terhadap empat aktivitas utama dalam proses DSS01.03 disajikan pada Tabel 5.

Tabel 5 Penilaian dan Analisis Hasil – DSS01.03

Kode	Aktivitas	Skor (%)	Rating	Keterangan	<i>Capability level</i>		Analisis	
					<i>As-Is</i>	<i>To-be</i>	<i>As-is</i>	<i>To-be</i>
D131	Pemantauan performa dan status infrastruktur	70%	L	Monitoring dilakukan via Grafana, namun belum optimal	0	3	Tidak ada aktivitas Level 1 yang mencapai <i>Fully Achieved</i> (F), hanya L dan P.	Berdasarkan faktor desain: kebutuhan monitoring infrastruktur tinggi, risiko sistem, dan stabilitas.
D132	Sistem alert terhadap gangguan	50%	P	Ada fitur alert di Grafana, namun belum terintegrasi dengan sistem eksternal.				
D133	Dokumentasi hasil monitoring dan pelaksanaan rutin	40%	P	Monitoring dilakukan setiap hari, namun belum terdokumentasi secara lengkap dan rutin.				
D134	Evaluasi dan tindak lanjut terhadap temuan monitoring	30%	P	Evaluasi belum dilakukan secara sistematis, tidak ada prosedur formal.				

Berdasarkan hasil evaluasi, proses DSS01.03 menunjukkan *capability level* 0 dengan target level 3, yang berarti terdapat kesenjangan signifikan antara kondisi saat ini dan kondisi yang diharapkan. Aktivitas monitoring infrastruktur telah dijalankan menggunakan tools seperti Grafana, namun belum sepenuhnya optimal karena hasil monitoring belum terdokumentasi secara rutin dan belum tersedia prosedur formal yang mendukung proses evaluasi dan tindak lanjut hasil monitoring. Selain itu, sistem alert belum terintegrasi secara menyeluruh dengan sistem eksternal, sehingga respons terhadap gangguan belum terkoordinasi secara efektif. Dengan skor aktivitas yang hanya mencapai L (*Largely Achieved*) dan P (*Partially Achieved*), tidak ada satupun aktivitas yang berada pada tingkat *Fully Achieved* (F), mengindikasikan perlunya penguatan prosedur dan dokumentasi untuk mencapai tingkat kapabilitas yang ditetapkan.

2. DSS05.02 - Mengelola Keamanan Jaringan dan Konektivitas (*Manage Network and Connectivity Security*)

Proses ini bertujuan untuk mengevaluasi efektivitas mekanisme perlindungan sistem JB Class terhadap ancaman malware dan akses tidak sah. Evaluasi dilakukan terhadap tiga aktivitas utama dalam proses DSS05.02, dengan hasil yang disajikan pada Tabel 6.

Tabel 6 Penilaian dan Analisis Hasil – DSS05.02

Kode	Aktivitas	Skor (%)	Rating	Keterangan	Capability level		Analisis	
					As-Is	To-be	As-is	To-be
D521	Pengamanan jaringan di tingkat infrastruktur server	90%	F	Keamanan jaringan telah diterapkan dengan firewall dan kontrol akses oleh Kominfo.	1	2	Semua aktivitas Level 1 telah mencapai <i>Fully Achieved</i> (F).	Berdasarkan faktor desain: keamanan jaringan merupakan elemen strategis yang mendukung kestabilan layanan, perlindungan data, dan integritas sistem, sehingga perlu diterapkan secara formal dan dimonitor aktif.
D522	Penggunaan protokol aman (HTTPS) untuk pengiriman data	100%	F	Sistem sudah sepenuhnya menggunakan HTTPS dengan sertifikat SSL aktif.				
D523	Proteksi dari serangan luar (firewall)	85%	F	Firewall aktif digunakan di server untuk membatasi akses dan melindungi sistem.				

Proses ini telah menunjukkan kinerja optimal dengan seluruh aktivitas pada level 1 tercapai secara penuh (*Fully Achieved*), sehingga *capability level* saat ini berada pada level 1, sesuai dengan target yang ditetapkan. Sistem JB Class telah menerapkan berbagai mekanisme pengamanan seperti penggunaan firewall, protokol HTTPS dengan sertifikat SSL, serta pengamanan jaringan yang dikendalikan oleh pihak Kominfo. Capaian ini menunjukkan bahwa perlindungan terhadap ancaman malware telah menjadi bagian integral dari pengelolaan TI, meskipun masih dapat ditingkatkan lebih lanjut untuk mencapai *capability level* yang lebih tinggi melalui evaluasi berkala dan dokumentasi yang lebih sistematis.

3. MEA04 – Memberikan Jaminan (*Provide Assurance*)

Proses ini ditujukan untuk menilai keberadaan dan efektivitas aktivitas penjaminan sistem informasi, yang mencakup penyusunan prosedur, pelaksanaan pengujian, dan siklus evaluasi berkala. Hasil evaluasi terhadap tiga aktivitas utama dalam proses MEA04 disajikan pada Tabel 7.

Tabel 7 Penilaian dan Analisis Hasil – MEA04

Kode	Aktivitas	Skor (%)	Rating	Keterangan	Capability level		Analisis	
					As-Is	To-be	As-is	To-be
M41	Penyusunan prosedur assurance	0%	N	Tidak terdapat SOP atau prosedur formal untuk assurance, baik internal maupun eksternal.	0	2	Tidak ada aktivitas <i>assurance</i> yang dijalankan atau terdokumentasi. Semua aktivitas dinilai <i>Not Achieved</i> (N).	Berdasarkan faktor desain, assurance formal, pengujian sistem, dan siklus evaluasi berkala seharusnya tersedia dan terdokumentasi secara sistematis karena
M42	Pelaksanaan assurance (pengujian)	0%	N	Belum pernah dilakukan aktivitas				

Kode	Aktivitas	Skor (%)	Rating	Keterangan	Capability level		Analisis	
					As-Is	To-be	As-is	To-be
	keamanan, akses, fitur)			assurance dalam konteks pengujian sistem.				berperan penting dalam menjamin keandalan sistem serta memenuhi ekspektasi pemangku kepentingan.
M43	Penjadwalan dan pembaruan hasil assurance	0%	N	Tidak ada siklus evaluasi atau pembaruan hasil assurance karena aktivitas belum pernah dilakukan.				

Proses ini merupakan salah satu titik lemah utama dalam tata kelola TI JB Class, karena seluruh aktivitasnya dinilai *Not Achieved* (N). Tidak ditemukan adanya prosedur formal untuk pelaksanaan assurance, termasuk pengujian keamanan, kontrol akses, maupun efektivitas fitur sistem. Selain itu, tidak terdapat siklus evaluasi atau pembaruan hasil assurance yang terdokumentasi. Dengan *capability level* 0 dan target level 2, diperlukan perencanaan dan penerapan prosedur assurance yang komprehensif untuk memastikan keandalan dan keamanan sistem secara berkelanjutan. Proses ini juga penting dalam memenuhi ekspektasi pemangku kepentingan serta memperkuat tata kelola berbasis risiko.

B. Hasil dan Rekomendasi Perbaikan

Berdasarkan hasil evaluasi terhadap aktivitas dalam setiap proses, ditemukan adanya gap antara kondisi saat ini dan target yang diharapkan. Sebagai tindak lanjut atas temuan tersebut, disusun rekomendasi perbaikan yang bersifat praktis dan terarah guna mendorong peningkatan *capability level* serta memperkuat tata kelola TI pada sistem JB Class. Rincian hasil audit dan rekomendasi disajikan pada Tabel 8.

Table 8 Hasil dan Rekomendasi Perbaikan

Proses	Gap	Hasil	Keterangan	Rekomendasi
DSS01.03	3	Tidak Sesuai Standar	Infrastruktur telah dimonitor, tetapi tidak didokumentasikan dan belum ada evaluasi formal.	<ol style="list-style-type: none"> 1. Menyusun SOP monitoring infrastruktur yang mencakup frekuensi pemantauan, jenis parameter yang harus diawasi, dan mekanisme pelaporan. 2. Mengaktifkan dan mengintegrasikan sistem alert ke media eksternal (misalnya email, WhatsApp, atau Telegram) untuk notifikasi otomatis bila terjadi gangguan. 3. Membuat laporan hasil monitoring harian atau mingguan untuk disimpan sebagai dokumentasi formal.
DSS05.02	1	Sesuai Standar	Sistem telah memenuhi standar minimum untuk keamanan jaringan, meskipun masih bisa ditingkatkan pada sisi monitoring otomatis dan dokumentasi pelengkap	<ol style="list-style-type: none"> 1. Menyusun dokumentasi kebijakan keamanan jaringan secara formal agar praktik yang sudah berjalan memiliki landasan yang kuat. 2. Meningkatkan visibilitas keamanan melalui dashboard pemantauan realtime untuk mendeteksi aktivitas mencurigakan dan mempercepat respons terhadap ancaman. 3. Melakukan evaluasi dan uji coba berkala terhadap konfigurasi firewall dan kontrol akses untuk memastikan efektivitas perlindungan jaringan.

MEA04	2	Tidak Sesuai Standar	Proses assurance terhadap sistem JB Class belum dirancang, dilaksanakan, maupun terdokumentasi. Belum tersedia SOP, kegiatan evaluasi, ataupun pelaporan hasil. Diperlukan upaya penyusunan prosedur, pelaksanaan pengujian sistem secara berkala, dan pelibatan pihak independen guna menjamin keandalan layanan.	<ol style="list-style-type: none"> 1. Menyusun SOP assurance sistem JB Class yang mencakup tujuan, ruang lingkup, frekuensi pelaksanaan, serta pihak yang bertanggung jawab, guna memastikan sistem berjalan sesuai dengan standar keamanan dan keandalan layanan. 2. Melaksanakan kegiatan evaluasi sistem secara berkala yang mencakup aspek keamanan, kontrol akses, dan efektivitas fitur, agar potensi kelemahan dapat diidentifikasi dan diperbaiki lebih awal. 3. Mendokumentasikan hasil evaluasi sistem dalam format laporan yang dapat ditinjau secara berkala, sehingga proses assurance menjadi terstruktur dan dapat dijadikan dasar dalam pengambilan keputusan pengembangan sistem selanjutnya.
-------	---	----------------------	--	---

Hasil evaluasi terhadap tiga proses utama dalam domain DSS dan MEA yakni DSS01.03 (*Monitor IT Infrastructure*), DSS05.02 (*Manage Network and Connectivity Security*), dan MEA04 (*Provide Assurance*) menunjukkan adanya variasi tingkat pencapaian *capability level*. Proses DSS01.03 dan MEA04 berada pada kondisi *tidak sesuai standar*, masing-masing dengan gap sebesar tiga dan dua tingkat dari level yang diharapkan. Temuan ini mengindikasikan lemahnya dokumentasi formal, ketiadaan prosedur evaluasi yang sistematis, serta belum adanya pelaksanaan kegiatan penjaminan mutu terhadap sistem informasi. Sebaliknya, proses DSS05.02 telah memenuhi target *capability level* dengan seluruh aktivitas pada level 1 mencapai status *Fully Achieved*. Namun, masih diperlukan penyempurnaan lebih lanjut dalam hal dokumentasi kebijakan keamanan dan pemantauan otomatis guna meningkatkan ketahanan sistem terhadap ancaman eksternal. Sebagai tindak lanjut atas temuan tersebut, disusun rekomendasi perbaikan yang mencakup, penyusunan prosedur operasional standar (SOP) untuk aktivitas monitoring dan assurance, integrasi sistem notifikasi dengan media eksternal, pelaksanaan evaluasi berkala terhadap aspek keamanan dan kontrol akses, serta pendokumentasian hasil evaluasi secara sistematis. Rekomendasi ini diharapkan dapat menjadi dasar perbaikan berkelanjutan yang sejalan dengan prinsip tata kelola TI dalam kerangka COBIT 2019.

4. KESIMPULAN

Hasil evaluasi tata kelola teknologi informasi pada sistem JB Class berdasarkan *framework* COBIT 2019 menunjukkan adanya variasi tingkat *capability level* pada tiga proses utama yang dianalisis, yaitu DSS01.03 (*Monitor IT Infrastructure*), DSS05.02 (*Manage Network and Connectivity Security*), dan MEA04 (*Provide Assurance*). Proses DSS01.03 memperoleh *capability level* 0 dari target level 3, yang mencerminkan belum optimalnya implementasi monitoring infrastruktur, baik dari segi dokumentasi, sistem notifikasi, maupun evaluasi tindak lanjut. Proses DSS05.02 berada pada *capability level* 1 dan telah memenuhi target, menandakan bahwa aspek keamanan jaringan telah diterapkan secara dasar, namun masih terdapat ruang perbaikan dalam penguatan kontrol dan monitoring. Sementara itu, MEA04 juga menunjukkan *capability level* 0 dari target level 2, dengan temuan bahwa belum terdapat mekanisme assurance formal yang terdokumentasi ataupun dilaksanakan secara rutin. Temuan ini menegaskan perlunya perbaikan dalam bentuk penyusunan prosedur, penguatan dokumentasi, dan pelaksanaan evaluasi secara sistematis agar setiap proses dapat memenuhi target kapabilitasnya. Secara umum, evaluasi ini memberikan gambaran kondisi aktual pengelolaan TI pada sistem JB Class dan dapat menjadi dasar perumusan strategi peningkatan yang selaras dengan prinsip tata kelola berbasis COBIT 2019.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Balai Teknologi Komunikasi dan Pendidikan (Balai Tekkomdik) DIY atas dukungan dan kerja sama yang diberikan selama proses penelitian. Ucapan terima kasih juga disampaikan kepada tim IT JB Class yang telah bersedia memberikan informasi, akses data, serta waktu untuk mendukung kelancaran pengumpulan data melalui wawancara dan observasi. Penelitian ini tidak akan terlaksana tanpa kontribusi dan partisipasi semua pihak terkait.