3. HASIL DAN PEMBAHASAN

3.1 Tahap Perencanaan

Tahap perencanaan dilaksanakan sebagai langkah awal dalam proses evaluasi tata kelola teknologi informasi pada sistem informasi JB Class di Balai Tekkomdik DIY. Evaluasi ini dilatarbelakangi oleh belum adanya penilaian formal terhadap pengelolaan sistem tersebut berdasarkan *framework* tata kelola yang berstandar. Kondisi tersebut mengakibatkan belum tersedianya informasi yang memadai mengenai sejauh mana pengelolaan sistem telah memenuhi prinsip-prinsip pengendalian teknologi informasi yang baik. Berdasarkan hasil penelusuran awal, sistem JB Class belum dilengkapi dengan fitur keamanan tambahan seperti autentikasi dua faktor maupun pengiriman kode OTP pada saat proses daftar. Ketiadaan fitur tersebut meningkatkan potensi risiko penyalahgunaan akses, khususnya jika identitas pengguna diketahui oleh pihak yang tidak berwenang. Sebagai dasar pelaksanaan evaluasi, ditetapkan penggunaan *framework* COBIT 2019 yang menawarkan pendekatan berbasis proses dan menyediakan alat ukur *capability level* untuk menilai kemampuan pengelolaan TI secara objektif dan terstruktur. Pada tahap ini, dilakukan penyusunan pendekatan evaluasi serta perancangan instrumen pengumpulan data yang terdiri dari tiga metode utama, yaitu wawancara, observasi, dan studi dokumen. Ketiga metode tersebut dirancang saling melengkapi untuk memperoleh data yang menyeluruh dan valid sebagai landasan dalam proses analisis dan penilaian pada tahap selanjutnya.

3.2 Tahap Pengumpulan Data

1. Penetapan *Framework* dan Domain Evaluasi

Framework COBIT 2019 digunakan dalam penelitian ini karena menyediakan struktur proses serta alat ukur *capability level* yang sistematis dan relevan dalam menilai tingkat kapabilitas tata kelola TI. Berdasarkan karakteristik dan kebutuhan evaluasi terhadap sistem informasi JB Class, ditetapkan dua domain utama sebagai fokus analisis, yaitu *Deliver, Service and Support* (DSS) serta *Monitor, Evaluate and Assess* (MEA). Domain DSS berfokus pada proses layanan dan dukungan operasional TI, sedangkan domain MEA mencakup aspek pemantauan, evaluasi, dan penjaminan efektivitas sistem. Seluruh proses dalam kedua domain tersebut, yakni DSS01.01 hingga DSS06.03 dan MEA01.01 hingga MEA04 dijadikan objek awal evaluasi dengan mengacu pada indikator aktivitas dalam *framework* COBIT 2019. Untuk memperoleh hasil evaluasi yang mendalam dan terfokus, penelitian ini kemudian memusatkan analisis pada tiga proses utama. Pemilihan dilakukan berdasarkan capaian *capability level*, gap antara kondisi saat ini dan kondisi yang diharapkan, serta urgensi masing-masing proses terhadap keberlangsungan layanan TI.

Adapun ketiga proses yang dianalisis secara mendalam adalah sebagai berikut:

1. DSS01.03, karena menunjukkan capaian *capability level* 0 dengan target level 3, sehingga memiliki kesenjangan tertinggi dan memerlukan perbaikan mendasar terhadap proses pengelolaan insiden yang ada.
2. DSS05.02, karena telah mencapai *capability level* 1 sesuai dengan target yang ditetapkan, sehingga merepresentasikan proses yang telah berjalan optimal pada tingkat dasar.
3. MEA04, karena seluruh aktivitasnya berada pada tingkat Not Achieved (N), yang menunjukkan belum adanya perencanaan maupun pelaksanaan proses assurance secara formal terhadap sistem.

2. Metode Pengumpulan Data (Triangulasi)

Pengumpulan data dilakukan melalui tiga pendekatan utama, yaitu studi dokumen, observasi, dan wawancara. Ketiga pendekatan tersebut digunakan untuk menjamin validitas dan kelengkapan data yang diperoleh. Dalam prosesnya, peneliti didampingi oleh tim IT dari Balai Tekkomdik untuk membantu memahami struktur sistem JB Class, menelaah dokumen teknis, serta memverifikasi hasil observasi dan wawancara. Sebanyak 150 butir pertanyaan audit disusun berdasarkan 29 aktivitas proses dari domain DSS dan MEA dalam *framework* COBIT 2019, yang terdiri atas 127 butir untuk domain DSS dan 23 butir untuk domain MEA. Namun demikian, dalam tahap analisis *capability level*, hanya 3 hingga 5 pertanyaan paling representatif yang digunakan untuk setiap proses. Pendekatan ini diterapkan agar evaluasi dapat dilakukan secara lebih terfokus, mendalam, dan relevan dengan konteks implementasi sistem JB Class.

A. Domain DSS

DSS01 – Mengelola Operasional (*Managed Operations*)

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

Proses ini bertujuan untuk memastikan bahwa infrastruktur teknologi informasi dipantau secara berkala guna menjaga ketersediaan dan performa layanan sistem informasi. Evaluasi terhadap proses ini dilakukan dengan pendekatan triangulasi, yaitu melalui studi dokumen, observasi, dan wawancara, berdasarkan indikator dalam *framework* COBIT 2019. Hasil pengumpulan data disajikan dalam 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:

Kode	Pertanyaan	Jawaban
		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 *overload*, 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: 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 *real-time*, 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*)

Proses ini bertujuan untuk memastikan bahwa infrastruktur jaringan dan konektivitas sistem JB Class telah dilindungi dari potensi ancaman eksternal, serta menggunakan protokol komunikasi yang aman. Evaluasi dilakukan untuk meninjau penerapan pengamanan jaringan, penggunaan enkripsi data, serta sistem pertahanan terhadap akses tidak sah. Hasil pengumpulan data disajikan 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	Apakah data dikirim menggunakan protokol aman (HTTPS, SSL)?	**Studi Dokumen:** Terdapat dokumen konfigurasi teknis yang menunjukkan penerapan HTTPS untuk pengamanan koneksi.
		Observasi: Hasil observasi menunjukkan bahwa URL sistem JB Class menampilkan HTTPS, yang menandakan koneksi telah menggunakan enkripsi SSL.
		Wawancara: Tim IT menyatakan bahwa sistem JB Class menggunakan HTTPS sebagai protokol utama dalam komunikasi data untuk menjaga kerahasiaan dan keamanan data pengguna.
D523	Apakah ada firewall atau proteksi dari serangan luar?	**Studi Dokumen:** Terdapat dokumen konfigurasi jaringan dan kebijakan akses yang menunjukkan penerapan firewall pada server yang digunakan JB Class.
		Observasi: Hasil observasi tidak terdapat informasi dalam tampilan sistem JB Class mengenai konfigurasi firewall, namun dokumentasi menunjukkan penggunaan firewall aktif di tingkat server.
		Wawancara: Tim IT menyampaikan bahwa firewall aktif digunakan di server Kominfo untuk membatasi akses yang tidak sah dan melindungi sistem dari serangan luar.

B. Domain MEA

MEA04 – Memberikan Jaminan (*Provide Assurance*)

Proses ini bertujuan untuk mengevaluasi sejauh mana Balai Tekkomdik telah menerapkan mekanisme assurance atau penjaminan terhadap sistem JB Class, baik melalui prosedur internal maupun oleh pihak eksternal. Fokus evaluasi mencakup keberadaan prosedur formal, cakupan pengujian terhadap aspek keamanan dan kontrol akses, serta frekuensi dan dokumentasi dari pelaksanaan assurance tersebut. Hasil pengumpulan data disajikan dalam 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?	**Studi Dokumen:** Tidak ditemukan dokumen resmi atau SOP terkait assurance.
		Observasi: Tidak terdapat menu, fitur, atau informasi evaluasi sistem di JB Class.
		Wawancara: Tim menyampaikan belum ada prosedur assurance formal; evaluasi hanya dilakukan teknis oleh tim internal.
M42		**Studi Dokumen:**

	Apakah proses assurance tersebut mencakup pengujian keamanan sistem, pengaturan akses pengguna, dan efektivitas fitur yang tersedia?	Tidak tersedia laporan pengujian atau standar evaluasi aspek keamanan dan kontrol akses.
		Observasi: Tidak ditemukan dokumentasi atau alat ukur evaluasi keamanan dan akses.
		Wawancara: Tim menyatakan pengecekan dilakukan berkala jika ada kendala, namun tidak terdokumentasi.
M43	Seberapa rutin proses assurance dilakukan dan apakah hasilnya diperbarui secara berkala?	**Studi Dokumen:** Tim menyatakan pengecekan dilakukan berkala jika ada kendala, namun tidak terdokumentasi.
		Observasi: Tidak terdapat histori pembaruan terkait evaluasi sistem.
		Wawancara: Tim menyampaikan evaluasi dilakukan saat terjadi gangguan atau pengembangan fitur, tanpa jadwal khusus.

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 pendekatan *capability level*. Setiap proses dievaluasi berdasarkan aktivitas utamanya, kemudian diberikan skor capaian, rating aktivitas, serta ditentukan *capability level* yang menggambarkan kondisi sebenarnya dari implementasi proses. Dari 29 proses dalam domain DSS dan MEA yang menjadi objek awal evaluasi, penelitian ini difokuskan pada tiga proses utama, yaitu DSS01.03, DSS05.02, dan MEA04. Pemilihan ketiga proses tersebut didasarkan pada pertimbangan capaian *capability level*, gap, serta urgensi terhadap keberlangsungan layanan sistem informasi. Hasil analisis ini memberikan gambaran menyeluruh mengenai kondisi aktual tata kelola TI pada sistem JB Class dan menjadi dasar dalam penyusunan rekomendasi perbaikan yang relevan serta sesuai dengan standar COBIT 2019.

A. Analisis domain DSS

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	*Capability level*		Analisis	
					As-Is	*To-be*	*As-is*	*To-be*
D131	Pemantauan performa dan status infrastruktur	70%	L	Monitoring dilakukan via Grafana, namun belum optimal	0	3	Tidak ada aktivitas Level 1 yang mencapai *Fully Achieved* (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 sebenarnya 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 tidak dilengkapi prosedur formal untuk evaluasi dan tindak lanjut. 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 *Fully Achieved* (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 level kapabilitas yang lebih tinggi melalui evaluasi berkala dan dokumentasi yang lebih sistematis.

B. Analisis domai MEA

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 *assurance* yang dijalankan atau terdokumentasi. Semua aktivitas dinilai *Not Achieved (N)*.	Berdasarkan faktor desain, assurance formal, pengujian sistem, dan siklus evaluasi berkala seharusnya tersedia dan terdokumentasi secara sistematis karena berperan penting dalam menjamin keandalan sistem serta memenuhi ekspektasi pemangku kepentingan.
M42	Pelaksanaan assurance (pengujian keamanan, akses, fitur)	0%	N	Belum pernah dilakukan aktivitas assurance dalam konteks pengujian sistem.				
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.