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 prinsipprinsip 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 login atau saat pengguna melakukan aktivitas yang bersifat sensitif. 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 kematangan 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

3.2.1 Penetapan Framework dan Domain Evaluasi

Penelitian ini menggunakan framework COBIT 2019 ditetapkan dua domain utama yang relevan, yaitu DSS dan MEA DSS01.01 hingga DSS06.03, serta MEA01.01 hingga MEA04. Pemilihan proses dengan menggunakan perangkat faktor desain menghasilkan 3 domain dengan skor tertinggi, gap tertinggi yaitu domain terkait keamanan dan resiko informasi antara lain APO12, APO13 dan DSS05.

3.2.2 Metode Pengumpulan Data (Triangulasi)

Pengumpulan data dilakukan melalui tiga pendekatan utama, yaitu studi dokumen, observasi, dan wawancara. Ketiga pendekatan ini digunakan secara terpadu untuk memastikan validitas dan kelengkapan informasi yang diperoleh. Dalam proses ini, penulis didampingi oleh programmer dari tim IT Balai Tekkomdik dalam memahami struktur sistem JB Class, menelaah dokumentasi teknis, serta memverifikasi temuan hasil observasi dan wawancara.

1. DSS01.03

   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

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	**Studi Dokumen:** Terdapat dokumentasi internal mengenai konfigurasi sistem monitoring menggunakan Grafana.
		Observasi:

Kode	Pertanyaan	Jawaban
	overload, storage hampir penuh, atau koneksi jaringan terputus?	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.

2. DSS05.02

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

Kode	Pertanyaan	Jawaban

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.

3. MEA04

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

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	Apakah proses assurance tersebut mencakup pengujian keamanan sistem, pengaturan akses pengguna, dan efektivitas fitur yang tersedia?	**Studi Dokumen:** 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 Analisis Data dan Hasil

Tahap ini memuat hasil analisis terhadap seluruh proses dalam domain DSS dan MEA berdasarkan *framework* COBIT 2019. Setiap proses dievaluasi dengan mengacu pada aktivitas utama yang ditetapkan dalam *framework*, dan dianalisis menggunakan data dari wawancara, observasi**,** serta studi dokumen. Seluruh data kemudian diolah menjadi skor capaian dan rating aktivitas, yang digunakan untuk menentukan *capability level* masing-masing proses. Hasil analisis ini memberikan gambaran menyeluruh mengenai *capability level* tata kelola TI pada sistem JB Class, serta mengidentifikasi *gap* antara kondisi saat ini dan kondisi yang diharapkan. Evaluasi ini menjadi dasar dalam menyusun rekomendasi peningkatan proses tata kelola TI yang lebih efektif dan sesuai standar.

1.DSS01.03 – Analisis Data

Proses DSS01.03 – Mengelola Masalah dipilih karena menunjukkan capaian capability level paling rendah, yaitu level 0. Hal ini mengindikasikan bahwa aktivitas-aktivitas dasar dalam proses ini belum sepenuhnya berjalan atau terdokumentasi. Evaluasi dilakukan untuk menelaah bagaimana proses monitoring infrastruktur dilakukan dalam sistem JB Class, serta sejauh mana prosedur formal dan mekanisme tindak lanjut diterapkan. Hasil pengumpulan data terhadap proses ini disajikan sebagai berikut.

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	30%	P	Evaluasi belum dilakukan secara sistematis, tidak ada prosedur				

Kode	Aktivitas	Skor (%)	Rating	Keterangan	*Capability level*		Analisis	
					As-Is	*To-be*	*As-is*	*To-be*
	monitoring			formal.				

Karena DSS01.03 belum mencapai aktivitas dasar pada level 1, maka pengukuran terhadap level selanjutnya belum dapat dilakukan. Seluruh aktivitas pada level ini masih berada pada tingkat *Partially Achieved* (P) atau *Largely Achieved (P)*, namun belum memenuhi syarat minimum untuk *Fully Achieved (F)*. Hal ini menandakan perlunya pembenahan mendasar terlebih dahulu agar proses ini dapat ditingkatkan ke level yang lebih tinggi secara sistematis.

Sebagai tindak lanjut, rekomendasi perbaikan berikut disusun agar proses DSS01.03 dapat mencapai *capability level* 3 secara bertahap:

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.

2.DSS05.02 – Analisis Data

Proses DSS05.02 – Mengelola Malware dipilih sebagai representasi dari proses yang telah berjalan cukup baik, dengan capaian capability level yang sesuai harapan (level 1). Proses ini berfokus pada perlindungan sistem dari ancaman eksternal, penerapan enkripsi data, dan pengamanan jaringan. Evaluasi dilakukan untuk meninjau sejauh mana kebijakan dan konfigurasi teknis telah diterapkan dalam sistem JB Class. Hasil pengumpulan data untuk proses ini disajikan pada bagian berikut.

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.				

Seluruh aktivitas pada level 1 telah dinyatakan *Fully Achieved* (F), yang menunjukkan bahwa praktik perlindungan dasar terhadap jaringan telah diterapkan secara menyeluruh. Namun demikian, untuk dapat naik ke level berikutnya (level 2), dibutuhkan dokumentasi formal dan mekanisme evaluasi berkala yang lebih sistematis. Tanpa adanya struktur kebijakan tertulis dan pengukuran berkelanjutan, pengembangan ke level lebih tinggi belum dapat dinilai secara objektif.

Sebagai langkah peningkatan, berikut adalah rekomendasi perbaikan yang dapat diterapkan agar proses DSS05.02 dapat mencapai *capability level* 2:

1. Menyusun dokumentasi kebijakan keamanan jaringan secara formal agar praktik yang sudah berjalan memiliki landasan yang kuat.
2. Meningkatkan visibilitas keamanan melalui dashboard pemantauan real-time 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.

3. MEA04 – Analisis Data

Proses MEA04 – Managed Assurance menjadi fokus evaluasi karena merupakan proses yang belum dijalankan sama sekali, dengan semua aktivitas berada pada tingkat *Not Achieved*. Proses ini berkaitan dengan penerapan prosedur assurance atau penjaminan terhadap sistem informasi, yang mencakup pengujian keamanan, akses, serta efektivitas fitur. Evaluasi difokuskan pada ketersediaan kebijakan, mekanisme evaluasi berkala, dan dokumentasi hasil assurance. Rincian data terhadap proses ini disajikan dalam tabel berikut.

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.				

Karena tidak terdapat satu pun aktivitas assurance yang dijalankan, baik secara formal maupun informal, maka proses MEA04 dinilai berada pada *capability level* 0. Hal ini mengindikasikan bahwa belum tersedia fondasi yang memadai untuk pengukuran pada level berikutnya. Padahal, berdasarkan faktor desain COBIT 2019, mekanisme assurance seharusnya tersedia untuk menjamin keandalan sistem, mendukung pengambilan keputusan, dan memenuhi ekspektasi pemangku kepentingan.

Sebagai dasar peningkatan proses, berikut rekomendasi perbaikan yang perlu diterapkan agar proses MEA04 dapat mencapai *capability level* 2:

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.