BAB 4
HASIL PENELITIAN

4.1 RINGKASAN HASIL PENELITIAN

Penelitian ini mengevaluasi sistem informasi JB Class yang dikembangkan oleh Balai Tekkomdik DIY, berfokus pada aspek kinerja dan keamanan. Audit ini penting karena sistem JB Class belum pernah dievaluasi menggunakan standar tata kelola TI, sehingga tingkat kesesuaiannya dengan prinsip pengelolaan dan keamanan yang baik belum diketahui. Evaluasi dilakukan menggunakan *framework* COBIT 2019 dengan fokus pada domain DSS dan MEA. Data dikumpulkan melalui wawancara, observasi langsung terhadap sistem, serta studi dokumen internal, kemudian dianalisis menggunakan pendekatan *capability level*.

4.2 HASIL PENELITIAN

4.2.1 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 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.

4.2.2 TAHAP PENGUMPULAN DATA

Tahap pengumpulan data dilaksanakan di Balai Tekkomdik DIY pada periode 8 hingga 28 Mei 2025. Tujuan dari tahap ini adalah untuk memperoleh data yang dibutuhkan dalam mengevaluasi tata kelola TI pada sistem informasi JB Class, dengan mengacu pada *framework* COBIT 2019. Penilaian dilakukan dengan menggunakan pendekatan *capability level* yang terdapat dalam *framework* tersebut.

1. **Penetapan *Framework* dan Domain Evaluasi**

   Penelitian ini menggunakan *framework* COBIT 2019 karena menyediakan struktur proses dan alat ukur yang dapat digunakan untuk menilai kapabilitas pengelolaan TI secara terukur dan sistematis. Berdasarkan karakteristik dan ruang lingkup sistem JB Class, ditetapkan dua domain utama yang relevan, yaitu DSS dan MEA. Seluruh proses dalam kedua domain tersebut dijadikan objek evaluasi, meliputi DSS01.01 hingga DSS06.03, serta MEA01.01 hingga MEA04. Setiap proses dianalisis berdasarkan aktivitas-aktivitas yang dijelaskan dalam *framework* dan dinilai tingkat pencapaiannya melalui *capability level*.

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. Penulis menyusun total 150 butir pertanyaan yang merepresentasikan 29 aktivitas proses dari domain DSS dan MEA. Pertanyaan tersebut terdiri atas 127 untuk domain DSS dan 23 untuk domain MEA. Seluruh daftar pertanyaan beserta hasil

pengumpulan data secara lengkap dicantumkan dalam Lampiran 5 sebagai dasar evaluasi terhadap seluruh proses dalam domain DSS dan MEA.

Namun demikian, dalam tahap pengolahan dan analisis data, tidak seluruh pertanyaan digunakan secara langsung untuk penilaian *capability level*. Hal ini didasarkan pada pendekatan efektivitas dan relevansi analisis dalam *framework* COBIT 2019, yang memberikan fleksibilitas untuk memusatkan evaluasi pada indikator yang paling menggambarkan pencapaian suatu proses. Oleh karena itu, untuk setiap proses dipilih sebanyak 3 hingga 5 pertanyaan yang paling representatif, agar penilaian dapat dilakukan secara lebih fokus, mendalam, dan sesuai dengan konteks implementasi sistem JB Class.

A. Domain DSS

DSS01 – Mengelola Operasional (*Managed Operations*)

DSS01.01 – Melaksanakan Prosedur Operasional (*Perform Operational Procedures*)

Proses ini bertujuan untuk memastikan bahwa seluruh aktivitas operasional teknologi informasi dijalankan sesuai dengan prosedur yang telah ditetapkan. Untuk mengevaluasi penerapan proses ini, data dikumpulkan melalui pendekatan triangulasi yang melibatkan studi dokumen, observasi, dan wawancara. Hasil pengumpulan data disajikan dalam Tabel 4.1.

Tabel 4.1 Pertanyaan dan Jawaban Metode Triangulasi – DSS01.01

Kode	Pertanyaan	Jawaban
D111	Apakah tersedia SOP atau panduan operasional tertulis untuk pengelolaan sistem JBClass?	**Studi Dokumen:** Tersedia dokumen panduan operasional tertulis untuk pengguna sistem JB Class, mencakup panduan bagi guru, siswa, dan orang tua.
		Observasi: Berdasarkan hasil observasi, pengguna menjalankan aktivitas sesuai dengan langkah-langkah yang tercantum dalam panduan.
		Wawancara: Tim IT menjelaskan bahwa panduan operasional sengaja disusun untuk meminimalkan kesalahan penggunaan sistem oleh *end-user* (guru, siswa, dan orang tua). Selain itu, panduan ini juga membantu mengurangi beban support teknis karena pengguna dapat menyelesaikan masalah dasar secara mandiri. Panduan disusun

Kode	Pertanyaan	Jawaban
		berdasarkan alur sistem dan fitur utama JB Class, seperti pembuatan akun, manajemen kelas, unggah materi, hingga evaluasi.
D112	Seberapa sering SOP tersebut digunakan dalam praktik operasional harian?	**Studi Dokumen:** Panduan tertulis JB Class tersedia untuk setiap jenis pengguna. Dokumen ini memuat langkah-langkah penggunaan sistem secara teknis, namun tidak mencantumkan frekuensi atau kewajiban penggunaan dalam kegiatan operasional harian.
		Observasi: Panduan tidak digunakan secara rutin setiap hari. Pengguna cenderung merujuk panduan hanya pada kondisi tertentu, seperti saat awal penggunaan sistem, adanya perubahan fitur, atau ketika mengalami kendala teknis.
		Wawancara: Tim IT menjelaskan bahwa panduan berfungsi sebagai referensi teknis yang digunakan sesuai kebutuhan. Panduan tidak digunakan setiap hari, namun biasanya dirujuk saat *onboarding* pengguna baru.
D113	Bagaimana sistem mendokumentasikan pelaksanaan prosedur operasional harian?	**Studi Dokumen:** Tidak ditemukan dokumen SOP atau panduan kerja tertulis yang menjelaskan bagaimana pelaksanaan prosedur operasional harian harus dicatat.
		Observasi: Melalui pengamatan terhadap aktivitas tim IT di lingkungan kantor Balai Tekkomdik, tidak ditemukan dokumen, formulir, atau media lain yang menunjukkan adanya pencatatan pelaksanaan prosedur operasional harian. Proses kerja berjalan rutin, namun tidak terdokumentasi secara formal.
		Wawancara: Tim IT menyampaikan bahwa prosedur operasional seperti pengecekan sistem dan pengelolaan layanan dilakukan secara rutin, namun tidak ada pencatatan atau bukti pelaksanaannya yang dituangkan dalam dokumen.
D114	Jika ada perubahan dalam sistem, apakah SOP langsung diperbarui dan disosialisasikan?	**Studi Dokumen:** Tersedia dokumen panduan pengguna JB Class dalam bentuk PDF yang dapat diunduh melalui sistem. Panduan menjelaskan langkahlangkah penggunaan sistem oleh guru, siswa, dan orang tua. Namun, dokumen tersebut tidak menyertakan riwayat versi atau tanggal revisi yang menunjukkan pembaruan resmi setelah perubahan sistem dilakukan.
		Observasi:

Kode	Pertanyaan	Jawaban
		Ditemukan bahwa isi panduan telah disesuaikan dengan tampilan dan fitur terbaru, terlihat dari penggunaan tangkapan layar antarmuka terbaru. Namun, tidak ditemukan informasi versi atau catatan pembaruan.
		Wawancara: Tim IT menyampaikan bahwa jika terdapat perubahan sistem atau penambahan fitur yang signifikan, file panduan akan diperbarui dan diunggah ulang ke halaman panduan di sistem JB Class. Pengguna dapat langsung mengakses dan mengunduh panduan terbaru secara mandiri. Sosialisasi dilakukan melalui kegiatan seperti FGD bersama pihak sekolah.

DSS01.02 – Mengelola Layanan TI yang Dialihdayakan (*Manage Outsourced IT Services*)

Proses ini bertujuan untuk memastikan bahwa kerja sama dengan pihak ketiga dalam penyediaan layanan teknologi informasi dikelola secara efektif dan terdokumentasi. Evaluasi terhadap proses ini dilakukan melalui pendekatan triangulasi, yaitu studi dokumen, observasi, dan wawancara, yang disusun berdasarkan indikator dalam *framework* COBIT 2019. Hasil pengumpulan data disajikan dalam Tabel 4.2.

Tabel 4.2 Pertanyaan dan Jawaban Metode Triangulasi – DSS01.02

Kode	Pertanyaan	Jawaban
D121	Apakah terdapat layanan pihak ketiga (misalnya *hosting*, *cloud*, atau domain) yang digunakan dalam JB Class?	**Studi Dokumen:** Terdapat dokumen kerja sama internal antara Balai Tekkomdik dengan Dinas Kominfo yang menjelaskan penempatan server sistem JB Class di lingkungan Kominfo. Dokumen ini menunjukkan bahwa infrastruktur server tidak sepenuhnya dikelola secara internal, melainkan bekerja sama dengan instansi lain.
		Observasi: Server JB Class secara fisik ditempatkan di lingkungan Dinas Kominfo. Tim IT Balai tetap mengelola sistem, namun ketergantungan terhadap dukungan infrastruktur seperti ruang server, jaringan, dan listrik menunjukkan adanya peran pihak eksternal dalam penyediaan layanan.
		Wawancara: Tim pengembang JB Class menyampaikan bahwa meskipun server adalah milik Balai, penempatannya berada di lingkungan Dinas

Kode	Pertanyaan	Jawaban
		Kominfo sebagai bentuk kerja sama. Kominfo bertanggung jawab dalam menyediakan dukungan infrastruktur, termasuk ruang server dan koneksi jaringan.
D122	Apakah ada perjanjian layanan (SLA) yang mengatur jaminan keamanan dan kinerja?	**Studi Dokumen:** Terdapat dokumen kerja sama antara Balai Tekkomdik dan Dinas Kominfo yang mencantumkan beberapa kesepakatan seperti waktu tang*gap* (*response time*) dan waktu pemulihan (*recovery time*).
		Observasi: Berdasarkan observasi, dokumen kerja sama tersedia dan digunakan sebagai acuan dalam hubungan layanan antara Balai Tekkomdik dan Dinas Kominfo. Namun, isi kontrak tidak ditampilkan secara terbuka karena bersifat internal. Sistem JB Class sendiri berjalan tanpa *downtime* signifikan, sehingga tidak terdapat pelacakan *uptime* secara harian.
		Wawancara: Tim IT Balai Tekkomdik menyampaikan bahwa *response time* dan *recovery time* telah diatur dalam kontrak kerja sama, tetapi waktu penyelesaian bersifat fleksibel dan disesuaikan dengan tingkat kesulitan insiden yang terjadi.
D123	Apakah dilakukan pemantauan rutin terhadap dan kepatuhan penyedia layanan berdasarkan SLA?	**Studi Dokumen:** Terdapat dokumen perjanjian kerja sama antara Balai Tekkomdik dan Dinas Kominfo yang mencantumkan klausul terkait tanggung jawab dan dukungan teknis, namun tidak dijelaskan secara rinci mekanisme pemantauan rutin.
		Observasi: Berdasarkan pengamatan, terdapat beberapa laporan dari Dinas Kominfo terkait pemeliharaan sistem dan gangguan teknis. Namun, belum ditemukan dokumentasi rutin dari pihak Balai yang menunjukkan evaluasi atau pemantauan terhadap layanan secara sistematis.
		Wawancara: Tim teknis menyampaikan bahwa Dinas Kominfo kadang menyampaikan laporan teknis terkait insiden seperti bug, gangguan koneksi, atau pemeliharaan sistem. Namun, laporan tersebut belum digunakan secara rutin sebagai bagian dari evaluasi terhadap kepatuhan SLA.
D124	Apakah Balai Tekkomdik mewajibkan penyedia layanan untuk memenuhi standar keamanan seperti ISO 27001	**Studi Dokumen:** Terdapat dokumen kerja sama internal antara Balai Tekkomdik dan Dinas Kominfo, namun tidak secara eksplisit mencantumkan

Kode	Pertanyaan	Jawaban
	atau peraturan pemerintah terkait data *protection*?	kewajiban pemenuhan terhadap standar keamanan tertentu seperti ISO 27001.
		Observasi: Sistem JB Class telah menggunakan protokol HTTPS sebagai bentuk pengamanan data saat transmisi. Infrastruktur server berada di bawah pengelolaan Dinas Kominfo, yang telah menerapkan standar keamanan sesuai kebijakan internal instansi pemerintah.
		Wawancara: Tim IT menyampaikan bahwa untuk sisi sistem JB Class mereka mengikuti standar keamanan umum seperti penggunaan HTTPS dan pengaturan hak akses. Sementara untuk sisi infrastruktur, mereka mempercayakan kepada Dinas Kominfo yang telah memiliki standar keamanan tersendiri sebagai penyedia layanan infrastruktur.

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 4.3.

Tabel 4.3 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

Kode	Pertanyaan	Jawaban
		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

Kode	Pertanyaan	Jawaban
		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.

DSS01.04 – Mengelola Lingkungan Fisik (*Manage the Physical Environment*)

Proses ini bertujuan untuk memastikan bahwa lingkungan fisik infrastruktur teknologi informasi dikelola secara aman dan sesuai standar yang berlaku. Evaluasi terhadap proses ini dilakukan menggunakan pendekatan triangulasi melalui studi dokumen, observasi, dan wawancara. Hasil pengumpulan data disajikan dalam Tabel 4.4.

Tabel 4.4 Pertanyaan dan Jawaban Metode Triangulasi – DSS01.04

Kode	Pertanyaan	Jawaban
D141	Dimana lokasi penyimpanan data JB Class (server fisik, data center, atau *cloud*)?	**Studi Dokumen:** Terdapat dokumen kerja sama antara Balai Tekkomdik dan Dinas Kominfo yang menjelaskan bahwa server sistem JB Class merupakan milik Balai Tekkomdik, namun secara fisik ditempatkan di lingkungan Dinas Kominfo.
		Observasi: Sistem JB Class dijalankan pada server fisik milik Balai Tekkomdik yang ditempatkan di lingkungan Dinas Kominfo. Dukungan infrastruktur seperti jaringan, listrik, dan ruang server disediakan oleh Kominfo.
		Wawancara: Tim IT Balai Tekkomdik menjelaskan bahwa data sistem disimpan di server fisik milik Balai Tekkomdik. Penempatan server di Dinas Kominfo merupakan kebijakan dari Pemda DIY untuk memusatkan infrastruktur layanan teknologi, dengan pembagian tugas di mana Balai mengelola sistem dan Kominfo mendukung infrastruktur.
D142	Siapa saja yang memiliki wewenang untuk mengakses infrastruktur TI sistem JBClass?	**Studi Dokumen:** Terdapat dokumen internal yang mencantumkan pihak-pihak yang memiliki

Kode	Pertanyaan	Jawaban
		wewenang untuk mengakses infrastruktur TI sistem JB Class.
		Observasi: Berdasarkan observasi, akses terhadap infrastruktur diberikan kepada tim IT Balai Tekkomdik untuk operasional sistem, Dinas Kominfo untuk pengelolaan fisik server, serta pihak rekanan untuk dukungan teknis.
		Wawancara: Tim IT Balai Tekkomdik memiliki akses untuk pemeliharaan sistem. Dinas Kominfo memiliki akses pada ruang server sebagai penyedia infrastruktur, sementara rekanan diberikan akses teknis terbatas sesuai kebutuhan proyek.
D143	Bagaimana sistem menjamin keamanan fisik dari infrastruktur IT-nya? (seperti kerusakan, pencurian)	**Studi Dokumen:** Terdapat dokumen kerja sama antara Balai Tekkomdik dan Dinas Kominfo yang mencantumkan penempatan server di ruang server dengan pengelolaan keamanan fisik oleh pihak Kominfo
		Observasi: Tidak dilakukan observasi langsung ke ruang server. Informasi diperoleh melalui penjelasan tim IT dan dokumentasi berupa foto dan video yang ditunjukkan.
		Wawancara: Tim IT menyampaikan bahwa keamanan fisik merupakan tanggung jawab Dinas Kominfo. Server ditempatkan di ruang server tertutup yang diawasi oleh CCTV, dilengkapi sistem pengontrol suhu, dan pemantauan fisik lainnya.
D144	Bagaimana sistem mendeteksi dan merespons potensi ancaman lingkungan seperti panas berlebih, kebocoran air, atau kebakaran?	**Studi Dokumen:** Terdapat dokumen kerja sama antara Balai Tekkomdik dan Dinas Kominfo yang mencantumkan bahwa server JB Class ditempatkan di ruang server milik Dinas Kominfo. Namun, dokumen tersebut belum menjelaskan secara rinci prosedur deteksi atau respons terhadap potensi ancaman lingkungan.
		Observasi: Tidak dilakukan observasi langsung ke ruang server. Informasi diperoleh melalui penjelasan tim IT dan dokumentasi berupa foto dan video yang ditunjukkan.
		Wawancara: Tim IT menyampaikan bahwa pengelolaan ancaman lingkungan seperti suhu tinggi, kelembaban, dan risiko kebakaran merupakan tanggung jawab Dinas Kominfo. Dinas Kominfo telah menyediakan sistem pendingin

Kode	Pertanyaan	Jawaban
		ruangan, pengawasan suhu, serta proteksi tambahan seperti alarm kebakaran.

DSS01.05 – Mengelola Operasional (*Manage Operations*)

Proses ini bertujuan untuk memastikan bahwa operasional harian, seperti pemantauan sistem, *backup* data, dan penanganan gangguan, dilaksanakan secara konsisten dan terdokumentasi. Evaluasi terhadap proses ini dilakukan dengan pendekatan triangulasi melalui studi dokumen, observasi, dan wawancara. Hasil pengumpulan data disajikan dalam Tabel 4.5.

Tabel 4.5 Pertanyaan dan Jawaban Metode Triangulasi – DSS01.05

Kode	Pertanyaan	Jawaban
D151	Apakah kegiatan operasional harian seperti *backup* data, pemantauan layanan, atau perbaikan bug dilakukan secara rutin?	**Studi Dokumen:** Terdapat dokumen teknis internal yang mencantumkan proses seperti monitoring sistem dan *backup*.
		Observasi: Monitoring dilakukan secara kombinasi otomatis melalui dashboard Grafana dan pengecekan manual oleh tim IT. Sistem dipantau untuk memastikan layanan dapat diakses dan berjalan normal.
		Wawancara: Tim IT menyampaikan bahwa setiap hari dilakukan monitoring infrastruktur seperti ketersediaan layanan dan performa sistem. *Backup* data meliputi database dan konfigurasi sistem, dilakukan secara rutin, bekerja sama dengan Kominfo sebagai penyedia server.
D152	Bagaimana kontrol terhadap akun pengguna dilakukan secara rutin, misalnya dalam hal pembuatan, penghapusan, atau pengelolaan hak akses?	**Studi Dokumen:** Tidak ditemukan dokumen formal yang menjelaskan prosedur manajemen akun pengguna.
		Observasi: Terdapat fitur di halaman admin untuk melihat statistik seperti jumlah materi yang diunggah oleh guru atau aktivitas siswa, namun belum terdapat sistem log histori perubahan akun secara lengkap.
		Wawancara: Pengguna membuat akun secara mandiri sesuai peran (guru, siswa, orang tua). Tim IT hanya melakukan pengelolaan terbatas seperti menonaktifkan akun atas permintaan sekolah atau menyesuaikan hak akses bila terjadi kesalahan. Proses dilakukan secara manual melalui panel admin.

Kode	Pertanyaan	Jawaban
D153	Apakah terdapat prosedur tertulis atau panduan kerja untuk menjalankan tugas operasional harian?	**Studi Dokumen:** Tidak ditemukan dokumen teknis atau kebijakan yang menjelaskan keberadaan log aktivitas (audit trail) secara detail dalam sistem JB Class.
		Observasi: Berdasarkan observasi, sistem JB Class hanya menampilkan ringkasan aktivitas seperti jumlah materi yang diunggah atau soal yang dibuat, dan itu hanya dapat diakses oleh admin. Pengguna biasa tidak dapat melihat ringkasan aktivitas mereka secara langsung.
		Wawancara: Tim IT menyampaikan bahwa sistem JB Class belum memiliki fitur log aktivitas yang mendetail. Saat ini hanya tersedia tampilan ringkasan untuk admin. Pencatatan teknis dilakukan melalui log server, bukan dari sistem JB Class secara langsung.

DSS02 – Mengelola Permintaan Layanan dan Insiden (*Managed Service Requests and Incidents*)

DSS02.01 – Mengelola Pertanyaan dan Permintaan Layanan Pengguna (*Manage User Queries and Service Requests*)

Proses ini bertujuan untuk memastikan bahwa penanganan permintaan layanan dan pertanyaan dari pengguna dilakukan secara efisien, terdokumentasi, dan dapat ditindaklanjuti dengan baik. Hasil pengumpulan data disajikan dalam Tabel 4.6.

Tabel 4.6 Pertanyaan dan Jawaban Metode Triangulasi -DSS02.01

Kode	Pertanyaan	Jawaban
D211	Bagaimana pengguna (guru, siswa, atau orang tua) mengajukan pertanyaan atau permintaan layanan terkait sistem JB Class?	**Studi Dokumen:** Terdapat informasi kontak teknis pengguna pada halaman utama JB Class. Namun belum tersedia SOP khusus yang mengatur proses permintaan layanan.
		Observasi: Pada landing page JB Class, tercantum informasi kontak Balai dan daftar kontak person teknis yang bisa dihubungi pengguna.
		Wawancara: Tim IT menyampaikan pertanyaan atau kendala melalui WhatsApp dengan menghubungi kontak yang tertera. Belum tersedia sistem ticketing atau portal mandiri.
D212		**Studi Dokumen:**

Kode	Pertanyaan	Jawaban
	Apakah tersedia kanal resmi seperti email, formulir, atau fitur dalam sistem untuk permintaan layanan?	Pada landing page JB Class hanya tercantum alamat email sebagai kanal resmi.
		Observasi: Berdasarkan observasi, hanya terdapat alamat email yang ditampilkan pada halaman utama JB Class.
		Wawancara: Pengguna dapat mengirimkan permintaan melalui email yang sudah ada pada landing page, namun pengelolaan masih dilakukan secara manual.
D213	Bagaimana tim mencatat dan memverifikasi permintaan dari pengguna?	**Studi Dokumen:** Terdapat dokumen pencatatan manual berupa draf oleh tim IT Balai Tekkomdik menggunakan Excel.
		Observasi: Permintaan pengguna dicatat secara manual tanpa sistem pelacakan digital.
		Wawancara: Permintaan ditindaklanjuti langsung oleh tim IT. Verifikasi dilakukan secara informal berdasarkan tingkat urgensi masalah.

DSS02.02 – Mencatat dan Mengklasifikasikan Insiden (*Register and Classify Incidents*)

Proses ini bertujuan untuk memastikan bahwa setiap insiden teknis yang terjadi dapat dicatat dan diklasifikasikan secara tepat sebagai dasar untuk penanganan serta evaluasi sistem yang lebih baik. Hasil pengumpulan data disajikan dalam Tabel 4.7.

Tabel 4.7 Pertanyaan dan Jawaban Metode Triangulasi – DSS02.02

Kode	Pertanyaan	Jawaban
D221	Apakah terdapat mekanisme untuk mencatat insiden yang terjadi, seperti bug, error, atau gangguan teknis?	**Studi Dokumen:** Terdapat dokumen internal yang menunjukkan pencatatan insiden seperti bug atau gangguan teknis yang ditangani oleh tim IT maupun pihak rekanan pengembang. Pencatatan dilakukan secara manual dan belum terdokumentasi dalam SOP formal atau sistem terpusat.
		Observasi: Tidak ditemukan form pelaporan atau fitur pencatatan insiden pada tampilan sistem JB Class. Pemantauan menunjukkan bahwa pencatatan insiden dilakukan secara informal melalui laporan teknis atau komunikasi digital antara tim IT Balai Tekkomdik dan pihak

Kode	Pertanyaan	Jawaban
		rekanan, terutama jika jumlah insiden yang ditangani cukup banyak.
		Wawancara: Tim IT Balai Tekkomdik menyampaikan bahwa penanganan insiden dilakukan secara situasional. Jika jumlah insiden yang ditangani oleh rekanan cukup banyak, maka rekanan akan mengirimkan laporan teknis kepada tim IT. Untuk insiden kecil, komunikasi dilakukan langsung melalui pesan atau chat. Belum tersedia sistem pencatatan insiden yang terintegrasi dan formal.
D222	Apakah insiden diklasifikasikan berdasarkan dampaknya terhadap kinerja atau keamanan sistem, seperti tingkat keparahan?	**Studi Dokumen:** Tidak tersedia dokumen yang menjelaskan klasifikasi insiden berdasarkan tingkat keparahan.
		Observasi: Tidak ditemukan fitur di sistem JB Class untuk pengelompokan insiden berdasarkan kategori atau dampaknya.
		Wawancara: Tim IT menyampaikan bahwa insiden tidak diklasifikasikan secara formal. Penanganan lebih mengandalkan penilaian langsung berdasarkan urgensi.
D223	Apakah insiden dicatat dalam sistem log atau platform manajemen insiden?	**Studi Dokumen:** Tidak ditemukan penggunaan sistem log khusus atau platform pelaporan insiden.
		Observasi: Tidak ada tampilan atau sistem di JB Class yang mendukung pencatatan atau pelacakan insiden.
		Wawancara: Tim IT menyampaikan bahwa pernah menggunakan Trello yang disiapkan oleh rekanan, namun saat ini sudah tidak digunakan. Saat ini pencatatan dilakukan informal dan langsung ditangani tanpa sistem pencatatan.
D224	Apakah pernah terjadi insiden yang berdampak pada kebocoran data atau gangguan besar?	**Studi Dokumen:** Terdapat dokumen laporan teknis yang menjelaskan riwayat gangguan ringan, namun tidak ada catatan kejadian kebocoran data atau gangguan besar.
		Observasi: Tidak terlihat informasi insiden besar ditampilkan pada sistem JB Class.
		Wawancara: Tim IT menyampaikan bahwa tidak pernah terjadi kebocoran data atau gangguan besar yang mengganggu operasional. Gangguan hanya bersifat ringan, seperti bug kecil dan dapat ditangani segera.

Kode	Pertanyaan	Jawaban
D225	Apakah data insiden digunakan dalam laporan evaluasi performa sistem?	**Studi Dokumen:** Terdapat dokumen evaluasi internal yang menunjukkan bahwa insiden menjadi bagian dari bahan pertimbangan dalam perbaikan sistem.
		Observasi: Sistem tidak menampilkan laporan evaluasi berbasis insiden atau fitur penilaian performa sistem dari histori gangguan.
		Wawancara: Tim IT menyampaikan bahwa evaluasi dilakukan secara teknis berdasarkan pengalaman dan insiden yang berulang, meskipun belum selalu terdokumentasi secara resmi.

DSS02.03 Menutup Insiden (*Escalate and Resolve Incidents*)

Proses ini bertujuan untuk memastikan bahwa insiden teknis yang tidak dapat diselesaikan secara langsung dapat dievaluasi, dikoordinasikan, dan diselesaikan secara tepat sesuai tingkat urgensinya. Hasil pengumpulan data disajikan dalam Tabel 4.8.

Tabel 4.8 Pertanyaan dan Jawaban Metode Triangulasi – DSS02.03

Kode	Pertanyaan	Jawaban
D231	Apa yang dilakukan ketika insiden tidak bisa diselesaikan oleh tim internal Balai Tekkomdik?	**Studi Dokumen:** Terdapat dokumen kerja sama dengan pihak rekanan yang menjadi dasar koordinasi teknis saat eskalasi insiden diperlukan.
		Observasi: Tidak ditemukan fitur atau modul dalam sistem JB Class untuk proses eskalasi insiden. Namun, terdapat dokumentasi komunikasi manual seperti riwayat chat dan laporan teknis yang menunjukkan keterlibatan pihak rekanan.
		Wawancara: Jika insiden tidak dapat ditangani secara internal, dilakukan eskalasi kepada pihak ketiga melalui komunikasi langsung, sesuai kesepakatan kerja sama yang telah ada. Namun, hingga saat ini belum tersedia SOP teknis yang mendetail terkait alur eskalasi tersebut. Proses penanganan insiden lebih mengandalkan pengalaman teknis tim.
D232	Apakah ada target waktu penyelesaian (SLA) untuk tiap kategori insiden?	**Studi Dokumen:** Terdapat dokumen internal berisi target penyelesaian insiden harian dan bulanan, namun belum dibagi berdasarkan kategori tingkat keparahan.

Kode	Pertanyaan	Jawaban
		Observasi: Tidak ditemukan pengaturan SLA berbasis kategori insiden pada sistem JB Class. Namun, dokumen target internal menjadi acuan teknis penanganan.
		Tim IT menyampaikan bahwa waktu penyelesaian mengacu pada target kerja internal dan tingkat urgensi, tetapi belum ditentukan dalam bentuk SLA terstruktur berdasarkan kategori insiden.
D233	Apakah ada proses dokumentasi langkah-langkah penyelesaian insiden?	**Studi Dokumen:** Terdapat dokumen dari pihak rekanan yang mencatat penyelesaian insiden teknis, terutama untuk kasus kompleks. Belum ditemukan sistem dokumentasi internal Balai yang terdokumentasi rapi.
		Observasi: Tidak ada tampilan dokumentasi historis penyelesaian insiden pada sistem. Namun, beberapa dokumen seperti laporan hasil perbaikan atau screenshot penanganan insiden disediakan oleh pihak rekanan.
		Wawancara: Tim IT menyampaikan bahwa insiden ringan biasanya ditangani langsung tanpa dokumentasi, sedangkan insiden besar terkadang disertai laporan dari pihak rekanan. Balai belum menyusun sistem dokumentasi internal secara konsisten.
D234	Apakah pengguna diberi informasi mengenai progres dan hasil penanganan insiden?	**Studi Dokumen:** Tidak ditemukan dokumen kebijakan atau SOP mengenai pemberitahuan progres penanganan insiden kepada pengguna.
		Observasi: Tidak ditemukan dokumen atau sistem yang menunjukkan notifikasi status penanganan insiden secara rutin.
		Wawancara: Tim IT menyampaikan bahwa pemberitahuan kepada pengguna dilakukan secara informal, biasanya melalui WhatsApp. Namun tidak rutin, dan tidak seluruh pengguna menerima informasi tersebut.
D235	Bagaimana sistem memantau apakah insiden yang sama terulang kembali?	**Studi Dokumen:** Terdapat log server yang dikelola oleh Dinas Kominfo yang dapat digunakan untuk melacak kejadian insiden, termasuk yang berulang. Namun, log ini belum diintegrasikan dengan sistem JB Class.
		Observasi: Tidak ditemukan fitur dalam sistem JB Class yang mencatat atau mendeteksi insiden berulang secara otomatis. Monitoring insiden

Kode	Pertanyaan	Jawaban
		lebih mengandalkan analisis manual dari data log server.
		Wawancara: Tim IT menyampaikan bahwa pemantauan insiden dilakukan secara teknis melalui log server yang ada di Kominfo. Namun, log tersebut belum dimanfaatkan secara maksimal untuk mendeteksi pola insiden berulang dalam sistem JB Class.

DSS02.04 Menutup Insiden (*Close Incidents*)

Proses ini bertujuan untuk memastikan bahwa setiap insiden yang telah ditangani ditutup secara resmi, tervalidasi, dan terdokumentasi untuk mendukung evaluasi berkelanjutan. Hasil pengumpulan data disajikan dalam Tabel 4.9.

Tabel 4.9 Pertanyaan dan Jawaban Metode Triangulasi – DSS02.04D

Kode	Pertanyaan	Jawaban
D241	Apakah insiden yang selesai ditutup secara resmi dan terdokumentasi?	**Studi Dokumen:** Tidak ditemukan dokumen atau SOP yang menjelaskan prosedur penutupan insiden, termasuk format laporan penyelesaian atau status penutupan resmi.
		Observasi: Sistem JB Class tidak menyediakan fitur status penanganan insiden, seperti "sedang ditangani" atau "selesai". Tidak terlihat alur penutupan insiden secara sistematis.
		Wawancara: Tim IT menyampaikan bahwa tidak terdapat mekanisme formal untuk menutup insiden. Setelah insiden diang*gap* selesai secara teknis, proses penanganan dihentikan tanpa pencatatan penutupan.
D242	Apakah ada proses validasi sebelum insiden diang*gap* selesai?	**Studi Dokumen:** Tidak ditemukan dokumen atau SOP formal yang menjelaskan proses validasi sebelum penutupan insiden.
		Observasi: Tidak ditemukan tampilan validasi dalam sistem, namun terdapat catatan yang menunjukkan proses pengecekan.
		Wawancara: Tim IT menjelaskan bahwa sebelum menyatakan insiden selesai, dilakukan pengecekan fungsional untuk memastikan gangguan sudah teratasi.
D243		**Studi Dokumen:**

Kode	Pertanyaan	Jawaban
	Apakah dilakukan review terhadap insiden besar?	Terdapat catatan internal yang menunjukkan adanya review teknis terhadap insiden berdampak besar.
		Observasi: Belum tersedia dokumentasi evaluasi yang konsisten atau format review standar dalam sistem.
		Wawancara: Tim IT menyampaikan bahwa review dilakukan secara diskusi teknis untuk analisis penyebab dan langkah perbaikan, namun belum tersusun sebagai laporan formal.
D244	Apakah pengguna diminta memberikan umpan balik setelah insidennya ditangani?	**Studi Dokumen:** Tidak tersedia dokumen atau kebijakan tentang pengumpulan umpan balik dari pengguna.
		Observasi: Sistem JB Class tidak menyediakan fitur survei, form feedback, atau mekanisme umpan balik setelah insiden ditangani.
		Wawancara: Tim IT menyampaikan bahwa belum ada kebijakan atau sistem pengumpulan umpan balik. Evaluasi disimpulkan dari kondisi sistem pasca penanganan.

DSS03 – Mengelola Masalah (*Managed Problems*)

DSS03.01 Mengidentifikasi dan Mengklasifikasikan Masalah (*Identify and Classify Problems*)

Proses ini bertujuan untuk memastikan bahwa masalah dalam sistem dapat diidentifikasi secara dini dan diklasifikasikan berdasarkan penyebab, dampak, dan frekuensi kemunculannya sebagai dasar perbaikan yang efektif. Hasil pengumpulan data disajikan dalam Tabel 4.10.

Tabel 4.10 Pertanyaan dan Jawaban Metode Triangulasi – DSS03.01

Kode	Pertanyaan	Jawaban
D311	Bagaimana sistem atau tim mendeteksi adanya masalah dalam sistem?	**Studi Dokumen:** Terdapat dokumentasi internal teknis yang menunjukkan penggunaan Grafana untuk pemantauan performa server, serta pengecekan fungsionalitas sistem secara berkala.
		Observasi: Sistem JB Class tidak memiliki fitur otomatis untuk mendeteksi masalah. Namun, tim teknis memantau kondisi sistem menggunakan dashboard Grafana yang menampilkan parameter performa.

Kode	Pertanyaan	Jawaban
		Wawancara: Tim IT Balai Tekkomdik menjelaskan bahwa deteksi masalah dilakukan dengan memantau performa sistem melalui Grafana dan manual melakukan pengecekan fungsionalitas. Beberapa masalah terdeteksi melalui pola insiden atau pertanyaan pengguna yang berulang.
D312	Bagaimana tim membedakan antara kesalahan pengguna dan masalah sistem, dan bagaimana klasifikasinya?	**Studi Dokumen:** Tidak ditemukan dokumen atau panduan tertulis terkait klasifikasi masalah berdasarkan sumber (user atau sistem).
		Observasi: Sistem JB Class tidak memiliki fitur yang mencatat atau memisahkan masalah berdasarkan penyebab teknis atau kesalahan pengguna.
		Wawancara: Tim IT menyampaikan bahwa masalah dikategorikan secara informal berdasarkan pola pertanyaan yang berulang. Jika banyak pengguna mengalami hal serupa, maka diasumsikan fitur tersebut perlu evaluasi. Namun, proses ini belum didukung oleh klasifikasi atau dokumentasi formal.
D313	Apakah ada metode khusus untuk mengidentifikasi masalah tersembunyi?	**Studi Dokumen:** Tidak ditemukan dokumen atau prosedur teknis terkait metode identifikasi masalah tersembunyi.
		Observasi: Sistem tidak memiliki fitur analisis log atau pelacakan otomatis terhadap potensi masalah tersembunyi.
		Wawancara: Tim IT menyampaikan bahwa belum diterapkan metode khusus untuk mendeteksi masalah tersembunyi. Identifikasi bergantung pada laporan pengguna atau pengecekan manual.
D314	Apakah masalah dikelompokkan berdasarkan frekuensi atau dampaknya?	**Studi Dokumen:** Terdapat catatan teknis internal yang mencantumkan daftar masalah berulang berdasarkan jumlah laporan. Namun, belum dalam bentuk sistem klasifikasi formal.
		Observasi: Belum tersedia fitur klasifikasi masalah dalam sistem. Namun terdapat daftar prioritas teknis yang dibuat manual.
		Wawancara: Tim IT menyampaikan bahwa beberapa masalah dikelompokkan berdasarkan intensitas laporan atau seberapa besar dampaknya. Daftar prioritas ini digunakan

Kode	Pertanyaan	Jawaban
		untuk perbaikan, tetapi belum diformalkan dalam kebijakan atau sistem.

DSS03.02 Menyelidiki dan Mendiagnosis Masalah (*Investigate and Diagnose Problems*)

Proses ini bertujuan untuk memastikan bahwa setiap masalah yang terjadi dapat dianalisis secara menyeluruh untuk menemukan akar penyebabnya serta mendukung upaya perbaikan yang berkelanjutan. Hasil pengumpulan data disajikan dalam Tabel 4.11.

Tabel 4.11 Pertanyaan dan Jawaban Metode Triangulasi – DSS03.02

Kode	Pertanyaan	Jawaban
D321	Bagaimana proses identifikasi akar penyebab dari suatu masalah dilakukan?	**Studi Dokumen:** Terdapat dokumen teknis yang menunjukkan praktik analisis akar penyebab menggunakan pengecekan manual dan analisis log server. Namun, belum ada SOP formal atau metode baku seperti RCA (*Root Cause Analyst*) atau diagram sebab-akibat.
		Observasi: Sistem JB Class tidak memiliki fitur penelusuran akar masalah secara otomatis. Proses identifikasi dilakukan secara teknis oleh tim melalui monitoring dan log server.
		Wawancara: Tim IT menjelaskan bahwa identifikasi akar masalah dilakukan dengan memeriksa log server dan melakukan pengecekan manual berdasarkan pengalaman teknis. Belum ada prosedur standar atau pelaporan hasil investigasi secara sistematis.
D322	Apakah digunakan alat bantu seperti *log analyzer* atau *error tracker*?	**Studi Dokumen:** Tidak ditemukan dokumen atau bukti penggunaan alat bantu khusus seperti log analyzer atau sistem error tracking otomatis.
		Observasi: Sistem JB Class tidak memiliki fitur terintegrasi dengan alat analisis kesalahan seperti *error tracker*.
		Wawancara: Tim IT menyampaikan bahwa mereka menggunakan log server dan dashboard Grafana untuk membantu menganalisis performa dan kesalahan, namun belum menggunakan tools khusus seperti *log analyzer* atau *error tracking* otomatis.
D323		**Studi Dokumen:**

Kode	Pertanyaan	Jawaban
	Apakah proses investigasi ini melibatkan pihak eksternal?	Terdapat tangkapan layar komunikasi via WhatsApp dan discord antara tim IT Balai Tekkomdik dan pihak rekanan yang menunjukkan keterlibatan pihak eksternal dalam proses investigasi masalah sistem, terutama pada gangguan teknis yang tidak dapat ditangani internal.
		Observasi: Tidak terdapat tampilan atau fitur dalam sistem yang menunjukkan kolaborasi dengan pihak eksternal dalam penyelidikan masalah.
		Wawancara: Tim IT Balai Tekkomdik menyampaikan bahwa pihak rekanan pengembang pernah dilibatkan dalam investigasi, terutama untuk permasalahan kode atau konfigurasi sistem. Bantuan dilakukan melalui pemeriksaan langsung terhadap sistem dan diskusi teknis.
D324	Apakah hasil investigasi masalah didokumentasikan secara sistematis?	**Studi Dokumen:** Tidak ditemukan dokumen atau sistem internal yang digunakan untuk mencatat hasil investigasi secara konsisten.
		Observasi: Sistem JB Class tidak menyediakan fitur untuk mencatat hasil investigasi atau pelacakan penyebab masalah.
		Wawancara: Tim IT menyampaikan bahwa hasil investigasi belum terdokumentasi secara sistematis. Laporan dari rekanan terkadang tersedia dalam bentuk file atau chat, tetapi tidak dikumpulkan dalam sistem dokumentasi yang terstruktur.

DSS03.03 Mencatat Kesalahan yang Dikenal (*Raise Known Errors*)

Proses ini bertujuan untuk memastikan bahwa kesalahan teknis yang telah dikenali terdokumentasi secara formal dan digunakan sebagai dasar dalam mempercepat penanganan serta mencegah terulangnya masalah yang sama di masa mendatang. Hasil pengumpulan data disajikan dalam Tabel 4.12.

Tabel 4.12 Pertanyaan dan Jawaban Metode Triangulasi – DSS03.03

Kode	Pertanyaan	Jawaban
D331	Apakah ada dokumentasi atau basis data terkait kesalahan yang sudah dikenal (*known errors*)?	**Studi Dokumen:** Tidak ditemukan dokumen atau arsip resmi yang mencatat daftar *known errors*.
		Observasi: Tidak terdapat fitur atau menu dalam sistem JB Class yang menyediakan informasi atau daftar *known errors*.

Kode	Pertanyaan	Jawaban
		Wawancara: Tim IT menyampaikan bahwa beberapa kesalahan teknis umum sudah diketahui oleh tim dan ditangani sesuai pengalaman, namun belum dicatat secara formal sebagai *known errors* dalam sistem atau dokumen.
D332	Apakah masalah yang pernah terjadi digunakan sebagai referensi untuk mencegah masalah serupa?	**Studi Dokumen:** Tidak ditemukan dokumen yang menjelaskan mekanisme pencegahan masalah berulang berdasarkan riwayat insiden.
		Observasi: Sistem JB Class tidak memiliki fitur histori atau pencatatan untuk referensi pencegahan masalah serupa.
		Wawancara: Tim IT menyampaikan bahwa meskipun belum ada dokumentasi, pengalaman terhadap masalah yang pernah terjadi digunakan sebagai acuan teknis untuk mencegah terulangnya masalah.
D333	Apakah solusi tetap (*permanent fix*) disiapkan untuk tiap masalah yang sudah dikenali?	**Studi Dokumen:** Tidak ditemukan dokumen atau kebijakan tentang solusi jangka panjang (*permanent fix*) untuk masalah yang telah diketahui.
		Observasi: Tidak terdapat tampilan atau catatan pada sistem JB Class yang menunjukkan adanya *permanent fix* atau sistem perbaikan berkelanjutan.
		Wawancara: Tim IT menjelaskan bahwa solusi terhadap masalah biasanya langsung diterapkan saat gangguan terjadi.
D334	Apakah dokumentasi kesalahan dimanfaatkan untuk meningkatkan efisiensi penanganan masalah?	**Studi Dokumen:** Terdapat beberapa catatan internal dan pengalaman teknis yang digunakan dalam menyelesaikan masalah berulang, meskipun belum seluruhnya terdokumentasi secara sistematis.
		Observasi: Sistem JB Class tidak menyediakan histori error atau fitur pelacakan untuk referensi efisiensi penanganan.
		Wawancara: Tim IT menyampaikan bahwa error yang pernah terjadi dimanfaatkan sebagai referensi teknis dalam penanganan berikutnya. Pengetahuan disimpan dalam bentuk pengalaman dan diskusi internal, bukan dalam sistem dokumentasi resmi.

DSS04 – Mengelola Keberlangsungan Layanan (*Managed Continuity*)

DSS04.01 Menentukan Kebutuhan Keberlangsungan (*Define Continuity Requirements*)

Proses ini bertujuan untuk memastikan bahwa kebutuhan akan keberlangsungan layanan sistem telah diidentifikasi, termasuk identifikasi risiko, toleransi *downtime*, dan kebutuhan pemantauan sistem secara berkelanjutan. Hasil pengumpulan data disajikan dalam Tabel 4.13.

Tabel 4.13 Pertanyaan dan Jawaban Metode Triangulasi – DSS04.01

Kode	Pertanyaan	Jawaban
D411	Apa saja risiko utama yang dapat mengganggu kontinuitas layanan?	**Studi Dokumen:** Tidak ditemukan dokumen formal seperti analisis risiko, *business continuity plan* (BCP) atau dokumen manajemen risiko yang memuat daftar risiko utama yang memengaruhi keberlangsungan layanan JB Class.
		Observasi: Sistem JB Class tidak memiliki fitur atau tampilan yang menunjukkan pemetaan risiko atau dokumentasi manajemen risiko internal.
		Wawancara: Tim IT menyampaikan bahwa risiko utama yang dihadapi meliputi terbatasnya anggaran operasional dan pengembangan, ketergantungan pada tenaga teknis tertentu, serta kebutuhan pembaruan sistem agar sesuai dengan perkembangan teknologi dan keamanan.
D412	Berapa batas toleransi waktu *downtime* yang dianggap wajar?	**Studi Dokumen:** Tidak ditemukan dokumen kebijakan resmi atau SLA (*Service Level Agreement*) yang mengatur batas toleransi downtime sistem JB Class.
		Observasi: Sistem JB Class tidak menampilkan informasi waktu pemulihan atau indikator toleransi downtime.
		Wawancara: Tim IT menyampaikan bahwa toleransi waktu *downtime* bersifat situasional, berkisar 5–15 menit tergantung pada tingkat kesulitan permasalahan teknis.
D413	Apakah ketersediaan sistem dipantau secara terus-menerus?	**Studi Dokumen:** Terdapat dokumen teknis internal yang menunjukkan bahwa tim menggunakan dashboard Grafana untuk pemantauan performa dan status sistem. Namun, belum tersedia SOP pemantauan formal.

Kode	Pertanyaan	Jawaban
		Observasi: Sistem JB Class tidak menyediakan fitur *real-time* monitoring kepada pengguna. Namun, berdasarkan observasi, tim melakukan pemantauan menggunakan alat terpisah (Grafana).
		Wawancara: Tim IT menyampaikan bahwa pemantauan sistem dilakukan setiap hari dengan bantuan Grafana yang memantau kondisi server secara otomatis, disertai pengecekan manual oleh tim untuk memastikan aksesibilitas dan kestabilan layanan.

DSS04.02 Menyusun Rencana Keberlangsungan (*Establish Continuity Plans*)

Proses ini bertujuan untuk memastikan bahwa organisasi memiliki rencana formal untuk menjaga keberlangsungan layanan, termasuk strategi pemulihan bencana, pengelolaan pencadangan data, dan penetapan tanggung jawab teknis. Hasil pengumpulan data disajikan dalam Tabel 4.14.

Tabel 4.14 Pertanyaan dan Jawaban Metode Triangulasi – DSS04.02

Kode	Pertanyaan	Jawaban
D421	Apakah tersedia dokumen formal tentang rencana pemulihan bencana?	**Studi Dokumen:** Tidak ditemukan dokumen formal atau kebijakan tertulis yang menjelaskan rencana pemulihan bencana pada sistem JB Class.
		Observasi: Berdasarkan pengamatan, baik pada tampilan sistem maupun arsip dokumentasi internal, belum ditemukan adanya rencana pemulihan bencana yang terdokumentasi secara formal atau terintegrasi dalam sistem.
		Wawancara: Tim IT menyatakan bahwa hingga saat ini belum tersedia dokumen resmi mengenai disaster *recovery plan*. Jika terjadi bencana, langkah-langkah penanganan akan dilakukan secara situasional sesuai kondisi yang dihadapi.
D422	Bagaimana prosedur *backup* data dilakukan?	**Studi Dokumen:** Tidak ditemukan dokumen formal berupa SOP *backup*. Terdapat catatan internal yang menjelaskan bahwa proses *backup* dilakukan secara berkala dan mencakup data penting serta konfigurasi sistem.
		Observasi:

Kode	Pertanyaan	Jawaban
		Dari hasil pengamatan, tidak ditemukan fitur khusus pada tampilan sistem JB Class yang menunjukkan status atau alur *backup*. Namun, dokumentasi internal menunjukkan bahwa proses *backup* dilaksanakan di lingkungan server yang dikelola oleh Kominfo.
		Wawancara: Tim IT menyampaikan bahwa proses *backup* dilakukan secara rutin dan melibatkan kerja sama teknis dengan Kominfo. Proses ini belum sepenuhnya terdokumentasi dalam bentuk SOP yang lengkap.
D423	Apakah *backup* dilakukan secara otomatis dan terjadwal?	**Studi Dokumen:** Tidak ditemukan dokumen formal berupa SOP terkait proses *backup* otomatis. Namun, terdapat catatan internal yang menunjukkan bahwa *backup* dilakukan secara rutin dan sebagian menggunakan sistem penjadwalan otomatis, terutama untuk database.
		Observasi: Hasil peninjauan terhadap dokumen internal menunjukkan bahwa *backup* untuk database telah dijadwalkan secara otomatis. Namun masih ada *backup* untuk file konfigurasi atau folder tertentu dilakukan secara manual.
		Wawancara: Tim IT menyatakan bahwa *backup* dilakukan dengan kombinasi antara proses otomatis dan manual. Belum semua komponen sistem dicakup dalam proses *backup* otomatis.
D424	Siapa yang bertanggung jawab terhadap implementasi rencana ini?	**Studi Dokumen:** Tidak ditemukan dokumen formal seperti SK atau kebijakan resmi yang menetapkan penanggung jawab. Namun, terdapat catatan internal yang menyebutkan bahwa tim IT Balai menjalankan peran tanggung jawab tersebut.
		Observasi: Observasi menunjukkan bahwa tanggung jawab terhadap keberlangsungan layanan, termasuk *backup*, dilakukan oleh tim internal Balai.
		Wawancara: Tim IT menegaskan bahwa pihaknya bertanggung jawab penuh terhadap pelaksanaan rencana keberlangsungan, dengan dukungan teknis dari Kominfo dalam penyediaan infrastruktur server.

DSS04.03 Menerapkan dan Memelihara Rencana Keberlangsungan (*Implement and Maintain Continuity Plans*)

Proses ini bertujuan untuk memastikan bahwa rencana keberlangsungan layanan sistem telah diterapkan, diuji secara berkala, dan diperbarui berdasarkan evaluasi agar tetap relevan dan efektif saat menghadapi gangguan nyata. Hasil pengumpulan data disajikan dalam Tabel 4.15.

Tabel 4.15 Pertanyaan dan Jawaban Metode Triangulasi – DSS04.03

Kode	Pertanyaan	Jawaban
D431	Apakah rencana pemulihan dan keberlangsungan layanan pernah diuji coba?	**Studi Dokumen:** Tidak ditemukan dokumen yang menunjukkan adanya kegiatan simulasi atau pengujian rencana pemulihan layanan.
		Observasi: Tidak terdapat fitur atau catatan dalam sistem JB Class yang menunjukkan pelaksanaan uji coba atau simulasi keberlangsungan layanan.
		Wawancara: Tim IT menyampaikan bahwa belum pernah dilakukan simulasi formal. Pengalaman gangguan server pada masa pandemi digunakan sebagai respon insiden nyata, bukan sebagai bentuk pengujian terencana.
D432	Bagaimana hasil pengujian tersebut digunakan untuk perbaikan?	**Studi Dokumen:** Tidak ditemukan dokumen atau laporan evaluasi hasil simulasi.
		Observasi: Tidak tersedia catatan atau fitur sistem yang menunjukkan tindak lanjut dari pengujian.
		Wawancara: Tim IT menyampaikan bahwa tidak ada pengujian yang dilakukan, sehingga belum ada evaluasi atau perbaikan formal berdasarkan hasil pengujian.
D433	Seberapa sering rencana kontinuitas ditinjau ulang?	**Studi Dokumen:** Tidak ditemukan dokumen atau catatan evaluasi berkala atas rencana keberlangsungan.
		Observasi: Tidak terdapat menu atau fitur dalam sistem yang menampilkan jadwal peninjauan berkala.
		Wawancara: Tim IT menyatakan bahwa evaluasi hanya dilakukan ketika terjadi gangguan besar dan belum memiliki jadwal tinjauan rutin karena belum ada dokumen formal rencana keberlangsungan.
D434		**Studi Dokumen:**

Kode	Pertanyaan	Jawaban
	Apakah rencana pemulihan terdokumentasi dan mudah diakses oleh tim?	Tidak ditemukan dokumen formal yang dapat diakses bersama oleh tim teknis.
		Observasi: Tidak tersedia repositori khusus yang menyimpan rencana pemulihan secara sistematis.
		Wawancara: Tim IT menyampaikan bahwa belum tersedia dokumen pemulihan dalam format tertulis yang dapat diakses secara kolektif. Penanganan gangguan dilakukan berdasarkan pengalaman teknis.

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

DSS05.01 Melindungi dari Malware (*Protect Against Malware*)

Proses ini bertujuan untuk memastikan bahwa sistem memiliki mekanisme perlindungan terhadap ancaman malware, baik melalui infrastruktur maupun pengamanan pada sisi aplikasi. Evaluasi dilakukan untuk menilai kesiapan proteksi, efektivitas pemindaian file, serta pencatatan insiden keamanan. Hasil pengumpulan data disajikan dalam Tabel 4.16.

Tabel 4.16 Pertanyaan dan Jawaban Metode Triangulasi – DSS05.01

Kode	Pertanyaan	Jawaban
D511	Apakah sistem memiliki mekanisme perlindungan dari malware?	**Studi Dokumen:** Terdapat dokumen teknis yang menunjukkan bahwa perlindungan dari malware dilakukan di tingkat server oleh Kominfo, seperti firewall dan pemindaian rutin.
		Observasi: Tidak ditemukan fitur perlindungan malware secara langsung dalam sistem JB Class, namun dokumentasi menunjukkan bahwa pengamanan aktif dijalankan di server.
		Wawancara: Tim IT menyampaikan bahwa perlindungan dari malware dilakukan melalui infrastruktur server Kominfo dengan firewall, pemantauan akses, dan pengamanan dasar. Belum tersedia proteksi khusus pada sistem JB Class itu sendiri.
D512	Apakah sistem secara otomatis memindai file yang diunggah oleh pengguna?	**Studi Dokumen:** Tidak ditemukan dokumen internal yang memuat prosedur keamanan terkait pemindaian otomatis file unggahan.
		Observasi: Tidak ditemukan fitur pemindaian otomatis pada antarmuka sistem JB Class.

Kode	Pertanyaan	Jawaban
		Wawancara: Tim IT menyampaikan bahwa pemindaian otomatis belum diterapkan pada file yang diunggah. Perlindungan difokuskan pada kontrol akses dan pencegahan manual.
D513	Bagaimana pembaruan keamanan sistem dilakukan?	**Studi Dokumen:** Tidak ditemukan dokumen kebijakan atau prosedur tertulis terkait pembaruan keamanan sistem JB Class.
		Observasi: Tidak tersedia menu atau informasi dalam sistem JB Class yang menunjukkan mekanisme pembaruan keamanan atau catatan aktivitas update.
		Wawancara: Tim IT Balai Tekkomdik menyampaikan bahwa pembaruan keamanan dilakukan di tingkat server, dan sering kali melibatkan bantuan dari rekanan pengembang serta Dinas Kominfo. Jika ditemukan potensi celah keamanan atau kerentanan, tim akan berkoordinasi dengan pihak terkait untuk membersihkan risiko tersebut, termasuk update manual dan penyesuaian sistem. Namun, proses ini belum dilakukan melalui sistem pembaruan otomatis atau prosedur formal yang terdokumentasi.
D514	Apakah ada log insiden terkait ancaman keamanan yang tercatat?	**Studi Dokumen:** Terdapat dokumentasi bahwa log sistem disimpan melalui server Kominfo sebagai bagian dari monitoring keamanan.
		Observasi: Belum ada fitur pelaporan insiden khusus di sistem JB Class, namun server mencatat log aktivitas.
		Wawancara: Tim IT menyampaikan bahwa aktivitas sistem terekam dalam log server dan digunakan untuk pemantauan keamanan jika terjadi gangguan atau aktivitas mencurigakan.

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 4.17.

Tabel 4.17 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.

DSS05.03 Mengelola Keamanan Endpoint (*Manage Endpoint Security*)

Proses ini bertujuan untuk memastikan bahwa perangkat *endpoint* yang digunakan untuk mengakses sistem JB Class terlindungi dari potensi ancaman keamanan. Evaluasi difokuskan pada keberadaan mekanisme pembatasan akses berdasarkan perangkat, kebijakan pengamanan perangkat kerja internal, serta kemampuan sistem dalam mengenali dan mencegah akses dari perangkat yang tidak sah. Rangkaian temuan hasil pengumpulan data disajikan pada Tabel 4.18.

Tabel 4.18 Pertanyaan dan Jawaban Metode Triangulasi – DSS05.03

Kode	Pertanyaan	Jawaban
D531	Apakah ada pembatasan akses berdasarkan perangkat pengguna (misal. 1 akun pengguna hanya bisa menggunakan 1 *device*)?	**Studi Dokumen:** Terdapat dokumen internal yang menjelaskan bahwa sistem tidak membatasi akses berdasarkan perangkat pengguna, dan mengizinkan login dari berbagai perangkat selama menggunakan akun yang sah.
		Observasi: Tidak ditemukan fitur yang membatasi akses perangkat. Sistem JB Class memungkinkan login dari berbagai perangkat tanpa notifikasi atau validasi perangkat.
		Wawancara: Tim IT menyampaikan bahwa pengguna dapat mengakses akun JB Class dari lebih dari satu perangkat, selama kredensial sesuai. Belum ada pembatasan berbasis perangkat.
D532	Bagaimana kebijakan keamanan diberlakukan untuk perangkat internal?	**Studi Dokumen:** Tidak ditemukan dokumen kebijakan atau panduan teknis yang mengatur pengamanan perangkat internal seperti laptop staf.
		Observasi: Tidak terlihat konfigurasi khusus dalam sistem maupun lingkungan kerja terkait pengamanan perangkat internal.
		Wawancara: Tim IT menyampaikan bahwa belum tersedia kebijakan formal mengenai pengamanan perangkat kerja internal. Penggunaan perangkat masih diserahkan sepenuhnya kepada masing-masing staf.
D533	Apakah endpoint seperti laptop staf dienkripsi dari potensi kebocoran data?	**Studi Dokumen:** Tidak ditemukan dokumen yang menjelaskan penerapan enkripsi pada perangkat endpoint milik staf.
		Observasi: Tidak terdapat tanda atau konfigurasi pengamanan enkripsi di perangkat yang digunakan.
		Wawancara:

Kode	Pertanyaan	Jawaban
		Tim IT menyampaikan bahwa belum ada kebijakan enkripsi pada perangkat endpoint. Fokus keamanan lebih diarahkan pada akses server, bukan perangkat lokal.
D534	Apakah sistem memiliki mekanisme untuk mengenali dan memblokir perangkat yang tidak terdaftar/mencurigakan saat mencoba mengakses akun pengguna?	**Studi Dokumen:** Tidak ditemukan dokumen yang menjelaskan kebijakan atau prosedur pendeteksian perangkat mencurigakan.
		Observasi: Sistem JB Class tidak menunjukkan fitur validasi atau pemblokiran otomatis terhadap perangkat yang tidak dikenal.
		Wawancara: Tim IT menyampaikan bahwa sistem belum memiliki mekanisme untuk mengenali atau memblokir perangkat tidak sah selama informasi login benar.

DSS05.04 Mengelola Identitas dan Akses Pengguna (*Manage User Identity and Logical Access*)

Proses ini bertujuan untuk memastikan bahwa perangkat *endpoint* seperti laptop, komputer, atau perangkat lain yang digunakan untuk mengakses sistem telah dikelola secara aman, guna mencegah risiko kebocoran atau penyalahgunaan data. Evaluasi difokuskan pada kebijakan akses perangkat, enkripsi, serta deteksi perangkat tidak sah. Hasil pengumpulan data disajikan dalam Tabel 4.18.

Tabel 4.19 Pertanyaan dan Jawaban Metode Triangulasi – DSS05.04

Kode	Pertanyaan	Jawaban
D541	Bagaimana proses pendaftaran dan aktivasi akun dilakukan?	**Studi Dokumen:** Terdapat panduan pengguna (guru, siswa, orang tua) yang menjelaskan langkah-langkah pendaftaran akun JB Class, termasuk pengisian data pada formulir pendaftaran. Akun bisa langsung digunakan tanpa aktivasi dari admin.
		Observasi: Pada sistem JB Class, akun dapat dibuat langsung melalui laman pendaftaran dan akan aktif secara otomatis tanpa perlu verifikasi atau persetujuan manual dari admin.
		Wawancara: Tim IT menyampaikan bahwa pendaftaran akun dilakukan mandiri melalui sistem JB Class. Setelah formulir diisi, akun langsung aktif dan bisa digunakan tanpa proses aktivasi tambahan.

Kode	Pertanyaan	Jawaban
D542	Apakah ada validasi seperti verifikasi email atau OTP?	**Studi Dokumen:** Tidak ditemukan dokumen atau panduan teknis yang menjelaskan adanya verifikasi email atau OTP saat pendaftaran akun.
		Observasi: Sistem JB Class tidak menampilkan fitur atau alur verifikasi akun melalui email atau OTP. Pengguna bisa langsung masuk setelah mendaftar.
		Wawancara: Tim IT menyampaikan bahwa sistem belum menerapkan validasi tambahan seperti email verifikasi atau OTP.
D543	Apakah setiap peran (guru, siswa, orang tua) memiliki hak akses yang berbeda?	**Studi Dokumen:** Dalam panduan pengguna JB Class disebutkan bahwa masing-masing peran (guru, siswa, dan orang tua) memiliki fitur dan menu yang berbeda sesuai kebutuhan.
		Observasi: Tampilan antarmuka sistem menunjukkan perbedaan akses berdasarkan peran. Guru memiliki akses ke manajemen kelas dan tugas, sedangkan siswa hanya dapat mengakses materi dan mengerjakan tugas.
		Wawancara: Tim IT Balai Tekkomdik menjelaskan bahwa sistem JB Class telah mengatur hak akses berbeda untuk setiap peran. Guru, siswa, dan orang tua hanya dapat mengakses fitur yang sesuai dengan kebutuhan dan tanggung jawab masing-masing.
D544	Apakah terdapat sistem autentikasi ganda (2FA) untuk akun dengan hak akses sensitif?	**Studi Dokumen:** Tidak ditemukan dokumen atau pengaturan terkait implementasi autentikasi dua faktor.
		Observasi: Tidak tersedia fitur 2FA dalam sistem JB Class, baik untuk pengguna biasa maupun admin.
		Wawancara: Tim IT menyampaikan bahwa saat ini sistem belum mendukung autentikasi ganda, dan semua akun cukup dengan satu lapis login saja
D545	Bagaimana sistem mengelola akun siswa yang pindah sekolah atau terkena sanksi drop out? Apakah akun tersebut langsung dicabut atau masih tersimpan?	**Studi Dokumen:** Tidak ditemukan dokumen formal yang menjelaskan prosedur penonaktifan akun siswa karena pindah sekolah atau *drop out*.
		Observasi: Tidak terlihat fitur sistem yang secara otomatis mencabut akses siswa karena perubahan status.
		Wawancara: Tim IT menyampaikan bahwa akun akan dinonaktifkan oleh admin jika ada laporan dari sekolah. Jika siswa pindah ke sekolah lain

Kode	Pertanyaan	Jawaban
		dan akan menggunakan kembali JB Class, maka siswa harus membuat akun baru secara mandiri melalui proses pendaftaran ulang.

DSS05.05 Mengelola Insiden Terkait Keamanan (*Manage Security-Related Incidents*)

Proses ini bertujuan untuk memastikan bahwa setiap insiden keamanan, seperti akses ilegal atau aktivitas mencurigakan, dapat terdeteksi dan ditangani secara tepat. Evaluasi difokuskan pada pencatatan insiden, pembagian tanggung jawab, mekanisme pelaporan, serta tindak lanjut terhadap insiden yang berdampak besar. Hasil pengumpulan data disajikan dalam Tabel 4.20.

Tabel 4.20 Pertanyaan dan Jawaban Metode Triangulasi – DSS05.05

Kode	Pertanyaan	Jawaban
D551	Bagaimana sistem mencatat insiden keamanan seperti login mencurigakan atau akses ilegal?	**Studi Dokumen:** Tidak ditemukan dokumen atau kebijakan yang mengatur pencatatan insiden keamanan dalam sistem JB Class.
		Observasi: Sistem JB Class belum menyediakan fitur pencatatan insiden keamanan secara otomatis, seperti pencatatan login mencurigakan atau akses ilegal.
		Wawancara: Tim IT menyampaikan bahwa insiden keamanan belum tercatat secara otomatis dalam sistem. Pemantauan aktivitas dilakukan melalui log server oleh Kominfo, tetapi belum tersedia sistem khusus untuk pencatatan insiden dalam JB Class.
D552	Siapa yang bertanggung jawab terhadap penanganan insiden keamanan tersebut?	**Studi Dokumen:** Terdapat dokumen internal yang menunjukkan bahwa tanggung jawab penanganan insiden berada pada tim IT Balai Tekkomdik.
		Observasi: Tidak terlihat pembagian tanggung jawab atau informasi peran tim secara langsung dalam sistem JB Class.
		Wawancara: Tim IT menyampaikan bahwa insiden keamanan ditangani oleh tim internal Balai, dan jika menyangkut infrastruktur server atau jaringan, maka Kominfo turut terlibat dalam penanganannya.
D553		**Studi Dokumen:**

Kode	Pertanyaan	Jawaban
	Apakah ada prosedur pelaporan dan eskalasi jika insiden terdeteksi?	Tidak ditemukan SOP atau pedoman tertulis mengenai pelaporan dan eskalasi insiden keamanan.
		Observasi: Sistem JB Class belum menyediakan fitur pelaporan insiden maupun jalur eskalasi formal.
		Wawancara: Tim IT menyampaikan bahwa hingga kini belum tersedia prosedur formal. Penanganan dilakukan secara langsung dan spontan oleh tim jika terjadi insiden, tanpa alur pelaporan yang terstruktur.
D554	Bagaimana tindak lanjut dilakukan terhadap insiden yang berdampak besar?	**Studi Dokumen:** Tidak ditemukan dokumen atau laporan evaluasi tindak lanjut terhadap insiden besar.
		Observasi: Tidak terdapat jejak atau arsip penanganan insiden berdampak besar yang tercatat secara sistematis.
		Wawancara: Tim IT menyampaikan bahwa jika terjadi insiden seperti gangguan besar atau server down, tindakan pemulihan dilakukan langsung oleh tim. Namun, belum ada dokumentasi evaluasi atau laporan tertulis yang dibuat sebagai tindak lanjut.

DSS06 – Mengelola Kontrol Proses Bisnis (*Managed Business Process Controls*)

DSS06.01 Menyesuaikan Kebutuhan Bisnis dan Kontrol (*Align Business Functional and Control Requirements*)

Proses ini bertujuan untuk memastikan bahwa fungsi-fungsi sistem disesuaikan dengan kebutuhan pengguna serta dilengkapi kontrol yang memadai untuk mendukung kelancaran proses bisnis. Evaluasi difokuskan pada kesesuaian fitur, proses pengujian, pembatasan akses, serta kontrol terhadap perubahan sistem. Hasil pengumpulan data disajikan dalam Tabel 4.21.

Tabel 4.21 Pertanyaan dan Jawaban Metode Triangulasi – DSS06.01

Kode	Pertanyaan	Jawaban
D611	Apakah fitur-fitur JB Class sudah sesuai dengan kebutuhan?	**Studi Dokumen:** Terdapat dokumen internal seperti notulen FGD dan laporan bimbingan teknis yang memuat masukan pengguna terkait pengembangan fitur.
		Observasi:

Kode	Pertanyaan	Jawaban
		Tampilan sistem menunjukkan fitur-fitur seperti input nilai, tugas, dan akses materi yang dibedakan menurut peran pengguna.
		Wawancara: Tim IT menyampaikan bahwa fitur disesuaikan dengan kebutuhan pengguna, terutama guru dan siswa. Masukan diperoleh melalui kegiatan teknis seperti FGD atau pelatihan.
D612	Apakah fitur-fitur baru selalu diuji kontrolnya sebelum dirilis ke pengguna?	**Studi Dokumen:** Terdapat dokumentasi internal pengujian fitur secara manual oleh tim pengembang dan rekanan, meskipun belum dalam bentuk standar uji formal.
		Observasi: Tidak terdapat penanda status pengujian dalam sistem, namun fitur diuji sebelum dirilis.
		Wawancara: Tim IT menyampaikan bahwa pengujian dilakukan sebelum rilis, dengan skenario dasar penggunaan dan perbaikan dilakukan jika ditemukan kesalahan.
D613	Apakah ada kontrol terhadap proses seperti input nilai, pengiriman tugas, dan akses materi?	**Studi Dokumen:** Terdapat dokumen panduan penggunaan yang menjelaskan langkah-langkah proses input nilai, pengiriman tugas, dan akses materi. Namun, belum tersedia kebijakan kontrol atau audit teknis yang tertulis secara formal.
		Observasi: Terdapat menu dan hak akses pengguna yang membedakan otoritas antara guru, siswa, dan orang tua.
		Wawancara: Tim IT menjelaskan bahwa sistem menggunakan pembatasan berbasis peran. Namun belum ada audit atau pengawasan aktivitas berbasis log.
D614	Bagaimana proses perubahan fitur dikontrol agar tidak mengganggu fungsionalitas yang sudah berjalan?	**Studi Dokumen:** Terdapat dokumen teknis internal berupa catatan pengujian manual sebelum rilis fitur baru, tetapi belum dilengkapi mekanisme rollback atau prosedur regresi yang baku.
		Observasi: Tidak tersedia tampilan rollback otomatis atau pengujian terjadwal di dalam sistem.
		Wawancara: Tim IT menyampaikan bahwa pengujian dilakukan sebelum perubahan dirilis, untuk mencegah gangguan pada fitur yang ada. Namun belum dilakukan pencatatan versi atau uji regresi sistematis.

DSS06.02 Mengendalikan Pemrosesan Informasi (*Control the Processing of Information*)

Proses ini bertujuan untuk memastikan bahwa setiap informasi yang diproses dalam sistem JB Class dikendalikan secara akurat, aman, dan sesuai dengan ketentuan teknis maupun fungsional. Evaluasi dilakukan terhadap aspek validasi input, perlindungan dari manipulasi data, serta kemampuan sistem untuk menangani kesalahan input. Hasil pengumpulan data disajikan dalam Tabel 4.22.

Tabel 4.22 Pertanyaan dan Jawaban Metode Triangulasi – DSS06.02

Kode	Pertanyaan	Jawaban
D621	Bagaimana sistem memastikan keakuratan data yang dimasukkan oleh pengguna?	**Studi Dokumen:** Terdapat dokumentasi mengenai validasi data teknis seperti keharusan pengisian dan format isian.
		Observasi: Sistem memiliki validasi sederhana seperti field wajib dan format email.
		Wawancara: Sistem belum memiliki verifikasi menyeluruh, hanya validasi teknis sederhana.
D622	Apakah ada validasi input otomatis saat pengguna mengisi data?	**Studi Dokumen:** Terdapat dokumen teknis yang menjelaskan skema validasi input dasar.
		Observasi: Sistem menampilkan peringatan jika isian tidak sesuai format atau tidak lengkap.
		Wawancara: Validasi dilakukan melalui pembatasan teknis seperti format email dan panjang karakter. Tidak terdapat validasi lintas data atau validasi bisnis yang lebih kompleks.
D623	Bagaimana sistem menghindari manipulasi atau perubahan tidak sah terhadap informasi?	**Studi Dokumen:** Terdapat dokumen hak akses pengguna, namun belum ada dokumentasi log audit.
		Observasi: Sistem menerapkan pembatasan hak akses per peran. Namun, belum tersedia fitur audit trail atau mekanisme pelacakan perubahan informasi yang terdokumentasi secara formal.
		Wawancara: Tim IT menjelaskan bahwa pengendalian dilakukan melalui pembatasan akses, namun saat ini belum ada sistem yang secara otomatis mencatat atau memantau perubahan data oleh pengguna. Hal ini meningkatkan risiko terjadinya manipulasi atau perubahan tidak sah yang tidak terdeteksi.
D624		**Studi Dokumen:**

Kode	Pertanyaan	Jawaban
	Apakah sistem memiliki mekanisme *rollback* jika terjadi kesalahan input data?	Tidak tersedia dokumentasi maupun fitur rollback.
		Observasi: Tidak ditemukan fitur undo, rollback, atau pemulihan data otomatis yang dapat diakses oleh pengguna.
		Wawancara: Tim IT menyampaikan koreksi kesalahan input hanya bisa dilakukan secara manual oleh admin.

DSS06.03 Memelihara Kontrol Proses Bisnis (*Maintain Business Process Controls*)

Proses ini bertujuan untuk memastikan bahwa seluruh proses bisnis yang berjalan dalam sistem telah didokumentasikan, dipantau, dan dievaluasi secara berkelanjutan. Evaluasi mencakup dokumentasi alur kerja, pemantauan sistem, audit internal, serta pemanfaatan masukan dari pengguna dalam pengembangan sistem. Hasil pengumpulan data disajikan dalam Tabel 4.23.

Tabel 4.23 Pertanyaan dan Jawaban Metode Triangulasi – DSS06.03

Kode	Pertanyaan	Jawaban
D631	Apakah semua alur kerja sistem terdokumentasi dengan baik?	**Studi Dokumen:** Terdapat panduan pengguna (guru, siswa, orang tua) yang menjelaskan langkah-langkah penggunaan fitur sesuai peran masing-masing.
		Observasi: Panduan dapat diakses pada halaman awal sistem JB Class dan menunjukkan alur penggunaan fitur, meskipun belum dalam bentuk diagram proses formal.
		Wawancara: Tim IT menyampaikan bahwa panduan disusun berdasarkan alur penggunaan fitur dan diperbarui jika ada perubahan sistem.
D632	Apakah dilakukan pemantauan terhadap pelaksanaan proses dalam sistem?	**Studi Dokumen:** Tidak ditemukan laporan evaluasi formal atau dokumentasi monitoring proses bisnis.
		Observasi: Sistem tidak memiliki dasbor evaluasi proses bisnis. Namun, penggunaan Grafana secara rutin membantu memantau kelancaran dan performa sistem.
		Wawancara: Tim IT menyampaikan bahwa pemantauan dilakukan melalui Grafana untuk melihat

Kode	Pertanyaan	Jawaban
		status layanan, kestabilan sistem, dan akses pengguna.
D633	Apakah dilakukan audit internal terhadap proses-proses bisnis dalam sistem JB Class?	**Studi Dokumen:** Tidak ditemukan laporan audit atau dokumen kebijakan audit proses bisnis.
		Observasi: Tidak terdapat fitur audit internal dalam sistem JB Class.
		Wawancara: Tim IT menyampaikan bahwa evaluasi dilakukan jika terdapat kendala atau masukan dari pengguna. Belum ada proses audit internal secara berkala.
D634	Bagaimana feedback dari pengguna digunakan untuk memperbaiki alur proses?	**Studi Dokumen:** Terdapat dokumen notulensi FGD dan kegiatan teknis yang mencatat masukan dari pengguna.
		Observasi: Tidak tersedia fitur umpan balik dalam sistem JB Class. Namun, dokumentasi menunjukkan adanya pertemuan pengguna.
		Wawancara: Tim IT menyampaikan bahwa feedback dikumpulkan melalui FGD, pelatihan, atau diskusi daring, dan menjadi bahan pertimbangan dalam pengembangan sistem.

B. Domain MEA (*Monitor, Evaluate and Assess*)

MEA01 – Memantau Kinerja dan Kepatuhan (*Monitor Performance and Conformance*)

MEA01.01 - Memantau Kinerja Sistem (*Monitor System Performance*)

Proses ini bertujuan untuk memastikan bahwa kinerja sistem informasi JB Class dipantau secara berkala, berdasarkan indikator yang relevan dengan kebutuhan pengguna maupun tujuan operasional. Evaluasi difokuskan pada penetapan indikator performa, pengaruh terhadap kepuasan pengguna, serta dokumentasi kejadian penurunan kinerja. Hasil pengumpulan data disajikan dalam Tabel 4.24.

Tabel 4.24 Pertanyaan dan Jawaban Metode Triangulasi – MEA01.01

Kode	Pertanyaan	Jawaban
M111	Apa saja indikator utama yang digunakan untuk menilai performa sistem JB Class?	**Studi Dokumen:** Terdapat dokumen internal yang mencatat indikator performa seperti kecepatan akses, ketersediaan layanan, dan stabilitas sistem.
		Observasi:

Kode	Pertanyaan	Jawaban
		Belum tersedia fitur pada sistem JB Class yang menampilkan indikator performa secara langsung, seperti waktu respons atau penggunaan sumber daya.
		Wawancara: Tim IT menjelaskan bahwa indikator utama yang digunakan adalah kecepatan akses sistem, ketersediaan layanan, serta aksesibilitas URL. Namun, belum dirumuskan dalam standar tertulis atau pedoman evaluasi kinerja formal.
M112	Apakah performa sistem JB Class memengaruhi kenyamanan atau kepuasan pengguna seperti guru dan siswa?	**Studi Dokumen:** Terdapat dokumen berupa catatan masukan pengguna dari kegiatan teknis seperti pelatihan dan FGD.
		Observasi: Sistem belum memiliki fitur penilaian kepuasan pengguna secara langsung.
		Wawancara: Tim IT menyampaikan bahwa performa sistem sangat berpengaruh terhadap kenyamanan pengguna. Keluhan seperti lambatnya akses atau gangguan layanan sering diterima melalui pesan langsung (misalnya WhatsApp).
M113	Apakah indikator performa ditentukan berdasarkan kebutuhan pengguna, standar internal, atau keduanya?	**Studi Dokumen:** Terdapat catatan internal yang menunjukkan bahwa indikator ditetapkan berdasarkan praktik teknis dan kebutuhan pengguna
		Observasi: Tidak ditemukan acuan resmi dalam sistem terhadap target performa tertentu.
		Wawancara: Tim IT menyampaikan bahwa indikator ditentukan berdasarkan pengalaman teknis dan umpan balik pengguna, belum berdasarkan standar atau dokumen kebijakan formal.
M114	Pernahkah sistem JB Class mengalami penurunan kinerja secara signifikan?	**Studi Dokumen:** Terdapat catatan teknis yang mencatat insiden penurunan performa dan langkah-langkah penanganan.
		Observasi: Tidak tersedia notifikasi publik dalam sistem terkait gangguan performa.
		Wawancara: Tim IT menyampaikan bahwa sistem pernah mengalami penurunan performa saat beban tinggi, dan perbaikan segera dilakukan. Namun, belum tersedia prosedur atau laporan tertulis yang menjelaskan alur penanganan secara sistematis.

MEA01.02 - Memantau Efektivitas Kontrol (*Monitor Control Effectiveness*)

Proses ini bertujuan untuk memastikan bahwa kontrol yang diterapkan dalam sistem JB Class dipantau secara berkala untuk menilai sejauh mana efektivitasnya dalam mendukung pengelolaan sistem yang aman dan andal. Evaluasi difokuskan pada metode penilaian efektivitas kontrol, penggunaan metrik atau indikator, pemanfaatan hasil evaluasi untuk perbaikan, serta frekuensi peninjauan ulang. Hasil pengumpulan data disajikan dalam Tabel 4.25.

Tabel 4.25 Pertanyaan dan Jawaban Metode Triangulasi – MEA01.02

Kode	Pertanyaan	Jawaban
M121	Bagaimana cara tim mengevaluasi apakah kontrol yang diterapkan di sistem berjalan dengan efektif?	**Studi Dokumen:** Terdapat dokumen teknis yang menunjukkan pengujian kontrol melalui percobaan langsung terhadap sistem.
		Observasi: Tidak terdapat pelaporan formal dalam sistem, tetapi terdapat aktivitas pemantauan berbasis teknis.
		Wawancara: Tim IT menjelaskan bahwa evaluasi dilakukan secara teknis dan informal saat sistem diuji atau saat terjadi kendala.
M122	Apakah ada ukuran atau metrik khusus yang digunakan untuk menilai efektivitas kontrol tersebut?	**Studi Dokumen:** Tidak ditemukan dokumen metrik formal.
		Observasi: Tidak ada indikator pengukuran di dalam sistem.
		Wawancara: Tim IT menyatakan belum menggunakan metrik kuantitatif, evaluasi hanya bersifat teknis dan kualitatif.
M123	Apakah hasil evaluasi kontrol digunakan sebagai dasar perbaikan sistem?	**Studi Dokumen:** Terdapat dokumen internal yang menunjukkan korelasi antara hasil evaluasi dan perbaikan sistem, meskipun tidak lengkap.
		Observasi: Tidak ada fitur dokumentasi pembaruan yang dikaitkan dengan evaluasi.
		Wawancara: Tim IT menyampaikan bahwa hasil evaluasi teknis menjadi dasar revisi fitur, walau dokumentasi masih terbatas.
M124	Seberapa sering kontrol tersebut ditinjau ulang untuk memastikan tetap relevan dan efektif?	**Studi Dokumen:** Terdapat dokumen yang menunjukkan bahwa kontrol sistem dipantau setiap hari. Namun belum terdokumentasi secara resmi.
		Observasi: Belum ditemukan laporan evaluasi berkala.

Kode	Pertanyaan	Jawaban
		Wawancara: Tim menyebutkan pemantauan dilakukan setiap hari oleh tim teknis. Namun belum ada siklus evaluasi tahunan atau per triwulan yang terdokumentasi.

MEA01.03 - Memantau Kepatuhan terhadap Regulasi Eksternal (*Monitor Compliance with External Requirements*)

Proses ini bertujuan untuk memastikan bahwa sistem JB Class telah mematuhi kebijakan dan regulasi eksternal yang berlaku, seperti ketentuan pemerintah, regulasi sektor pendidikan, dan peraturan perundang-undangan terkait perlindungan data. Evaluasi dilakukan untuk meninjau tingkat penyesuaian sistem terhadap regulasi, cara pemantauan kebijakan eksternal, keterlibatan pihak luar, serta dokumentasi perubahan akibat regulasi baru. Hasil pengumpulan data disajikan dalam Tabel 4.26.

Tabel 4.26 Pertanyaan dan Jawaban Metode Triangulasi – MEA01.03

Kode	Pertanyaan	Jawaban
M131	Apakah sistem JB Class telah disesuaikan dengan peraturan perundang-undangan yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP)?	**Studi Dokumen:** Terdapat dokumen internal yang menyebutkan penerapan prinsip dasar keamanan data, meskipun belum secara eksplisit merujuk ke UU PDP
		Observasi: Tidak ditemukan keterangan dalam sistem JB Class terkait kepatuhan terhadap regulasi seperti UU PDP.
		Wawancara: Tim IT menyampaikan bahwa meskipun belum secara eksplisit disesuaikan dengan UU PDP, prinsip pembatasan akses dan keamanan data telah diterapkan. Penyesuaian akan dilakukan seiring dengan arahan resmi dari instansi terkait.
M132	Bagaimana cara tim memastikan bahwa sistem tetap mematuhi kebijakan dan regulasi dari pihak eksternal, seperti pemerintah atau dinas pendidikan?	**Studi Dokumen:** Terdapat dokumen internal dan kebijakan dari Pemerintah Daerah, termasuk instruksi penempatan server di lingkungan Kominfo sebagai bagian dari pemenuhan kebijakan infrastruktur dan keamanan data.
		Observasi: Tidak ditemukan fitur di dalam sistem JB Class yang secara eksplisit menunjukkan pemantauan atau pembaruan kebijakan eksternal.
		Wawancara:

Kode	Pertanyaan	Jawaban
		Tim IT menyampaikan bahwa pemantauan terhadap regulasi dilakukan berdasarkan arahan dari Dinas Pendidikan atau Pemerintah Daerah. Instruksi seperti penempatan server di Kominfo dijadikan bagian dari penyesuaian sistem terhadap kebijakan eksternal. Namun, belum tersedia sistem dokumentasi berkala atau mekanisme formal untuk menindaklanjuti regulasi secara terstruktur.
M133	Apakah sistem JB Class pernah menjalani audit atau pemeriksaan oleh pihak luar terkait kepatuhan terhadap regulasi?	**Studi Dokumen:** Tidak ditemukan dokumen atau laporan audit dari pihak eksternal.
		Observasi: Tidak ada informasi atau histori audit dalam sistem.
		Wawancara: Tim IT menyampaikan bahwa belum ada audit formal, namun sistem mengikuti arahan dari pemerintah atau dinas terkait.
M134	Bagaimana proses dokumentasi dilakukan saat ada perubahan sistem untuk menyesuaikan dengan peraturan baru yang berlaku?	**Studi Dokumen:** Tidak tersedia dokumen formal terkait dokumentasi perubahan sistem berdasarkan regulasi.
		Observasi: Tidak ditemukan histori atau catatan perubahan sistem terkait regulasi.
		Wawancara: Penyesuaian langsung dilakukan tanpa pelaporan atau pencatatan formal, sehingga histori perubahan regulasi belum terdokumentasi.

MEA02 - Mengevaluasi Sistem Pengendalian Internal (*Assess the System of Internal Control*)

Proses ini bertujuan untuk menilai sejauh mana sistem pengendalian internal telah diterapkan dan berjalan secara efektif di dalam sistem informasi JB Class. Evaluasi difokuskan pada mekanisme pemantauan aktivitas pengguna, keberadaan prosedur formal, pelaksanaan audit internal, serta tindak lanjut terhadap potensi pelanggaran atau kelemahan pengendalian. Hasil pengumpulan data disajikan dalam Tabel 4.27.

Tabel 4.27 Pertanyaan dan Jawaban Metode Triangulasi – MEA02

Kode	Pertanyaan	Jawaban
M21	Apakah terdapat sistem atau mekanisme yang memantau	**Studi Dokumen:** Tidak ditemukan dokumen resmi mengenai sistem pemantauan aktivitas pengguna.

Kode	Pertanyaan	Jawaban
	aktivitas pengguna di platform JB Class?	**Observasi:** Sistem belum menampilkan fitur audit log pengguna, namun admin dapat melihat data aktivitas dasar seperti jumlah materi yang diunggah guru.
		Wawancara: Tim IT menyampaikan bahwa pemantauan dilakukan secara manual dan terbatas. Belum ada sistem otomatis untuk deteksi aktivitas tidak wajar.
M22	Bagaimana cara tim menilai apakah sistem pengendalian internal sudah berjalan efektif?	**Studi Dokumen:** Tidak ditemukan dokumen evaluasi pengendalian internal.
		Observasi: Tidak terdapat alat ukur formal di dalam sistem.
		Wawancara: Tim IT menyampaikan, evaluasi dilakukan berdasarkan kestabilan sistem dan minimnya keluhan pengguna.
M23	Apakah pernah ditemukan pelanggaran terhadap pengendalian internal?	**Studi Dokumen:** Tidak ditemukan laporan pelanggaran.
		Observasi: Tidak terdapat catatan pelanggaran dalam sistem.
		Wawancara: Tim IT menyatakan belum pernah ada pelanggaran serius. Jika ada kesalahan teknis, langsung diperbaiki.
M24	Apakah ada dokumen resmi mengenai prosedur pengendalian internal?	**Studi Dokumen:** Tidak ditemukan SOP atau dokumen pengendalian internal yang dipublikasikan.
		Observasi: Tidak terdapat panduan pengendalian internal dalam sistem.
		Wawancara: Tim IT menyampaikan bahwa belum ada prosedur resmi. Koordinasi hanya dilakukan secara informal, terutama dengan pihak eksternal seperti Kominfo atau rekanan.
M25	Apakah ada audit internal secara rutin untuk menilai efektivitas pengendalian yang ada? Apakah ada audit internal secara rutin untuk menilai efektivitas pengendalian yang ada?	**Studi Dokumen:** Tidak ditemukan laporan audit.
		Observasi: Tidak ada riwayat atau indikator pelaksanaan audit.
		Wawancara: Tim IT menyampaikan belum pernah dilakukan audit internal. Evaluasi hanya jika ada masalah.
M26	Jika audit menemukan masalah atau kekurangan, apakah hasilnya digunakan untuk memperbaiki prosedur pengendalian internal?	**Studi Dokumen:** Tidak ditemukan dokumen tindak lanjut hasil audit.
		Tidak tersedia histori perubahan sistem yang terkait audit.

Kode	Pertanyaan	Jawaban
		Wawancara: Tim IT menyampaikan Karena belum pernah dilakukan audit, belum ada tindak lanjut formal.

MEA03 - Kepatuhan terhadap Persyaratan Eksternal (*Compliance with External Requirements*)

Proses ini bertujuan untuk menilai sejauh mana sistem JB Class mematuhi standar, regulasi, dan kebijakan dari pihak eksternal, seperti peraturan pemerintah, kebijakan dinas pendidikan, serta standar keamanan informasi seperti ISO 27001. Evaluasi mencakup penyesuaian sistem terhadap regulasi, proses verifikasi kepatuhan, dokumentasi perubahan, serta penyediaan informasi kepada pengguna. Hasil pengumpulan data disajikan dalam Tabel 4.28.

Tabel 4.28 Pertanyaan dan Jawaban Metode Triangulasi – MEA03

Kode	Pertanyaan	Jawaban
M31	Apakah sistem JB Class telah memenuhi standar dari pihak luar seperti ISO 27001, UU ITE, atau kebijakan Dinas Pendidikan?	**Studi Dokumen:** Terdapat dokumen internal yang menunjukkan upaya pemenuhan prinsip dasar keamanan seperti pembatasan hak akses dan penyimpanan data di server aman.
		Observasi: Tidak terdapat tampilan atau fitur dalam sistem yang menyatakan kesesuaian dengan standar eksternal.
		Wawancara: Tim IT menyampaikan bahwa belum ada audit atau sertifikasi resmi terhadap standar seperti ISO atau UU ITE, namun prinsip dasar keamanan sudah diterapkan.
M32	Apakah tim memiliki daftar regulasi yang harus dipatuhi oleh sistem?	**Studi Dokumen:** Tidak ditemukan dokumen daftar regulasi eksternal sebagai acuan.
		Observasi: Tidak terdapat referensi regulasi di sistem.
		Wawancara: Tim IT menyampaikan belum tersedia daftar tertulis, regulasi disesuaikan secara situasional berdasarkan arahan dari instansi.
M33	Bagaimana proses verifikasi dilakukan untuk memastikan sistem telah mematuhi peraturan yang berlaku?	**Studi Dokumen:** Terdapat dokumentasi FGD yang memuat pembahasan tentang penyesuaian sistem terhadap arahan kebijakan.
		Observasi: Tidak ditemukan prosedur formal dalam sistem.
		Wawancara:

Kode	Pertanyaan	Jawaban
		Tim IT menyampaikan bahwa penyesuaian dilakukan sesuai arahan, misalnya dari FGD. Namun belum ada proses verifikasi formal atau unit khusus yang menangani kepatuhan regulasi.
M34	Apakah sistem mencatat perubahan yang dilakukan terkait regulasi?	**Studi Dokumen:** Tidak ditemukan dokumentasi perubahan sistem yang dikaitkan dengan regulasi.
		Observasi: Tidak terdapat histori perubahan terkait regulasi.
		Wawancara: Tim IT menyampaikan bahwa pencatatan belum dilakukan secara formal, perubahan langsung diterapkan oleh pengembang.
M35	Apakah pengguna JB Class mendapatkan informasi tentang hak dan perlindungan data mereka?	**Studi Dokumen:** Tidak tersedia kebijakan privasi atau pernyataan pengguna di dokumen atau sistem.
		Observasi: Tidak terdapat halaman tentang perlindungan data pengguna.
		Wawancara: Tim IT menyampaikan bahwa saat ini belum tersedia kebijakan privasi dalam sistem.

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 4.29.

Tabel 4.29 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.

4.2.3 TAHAP ANALISIS DATA DAN HASIL

Tahap ini memuat hasil analisis terhadap seluruh proses dalam domain DSS dan MEA berdasarkan *framework* COBIT 2019. Proses yang dianalisis mencakup 29 proses, dimulai dari DSS01.01 - Melaksanakan Prosedur Operasional hingga MEA04 - Memberikan Jaminan. 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.

A. Analisis Data Domain DSS dan MEA

Domain DSS (Deliver, Service and Support)

1. DSS01.01 - Melaksanakan Prosedur Operasional (*Perform Operational Procedures*)

Proses DSS01.01 pada sistem JB Class belum didukung oleh SOP formal yang menjelaskan pelaksanaan kegiatan operasional TI secara menyeluruh.

Dokumen yang tersedia berupa panduan penggunaan sistem, yang bersifat teknis dan tidak mencakup aspek prosedural pelaksanaan harian. Selain itu, pelaksanaan operasional belum dijalankan secara konsisten setiap hari, dan tidak tersedia dokumentasi yang mencatat pelaksanaan maupun pembaruan prosedur secara versi. Seluruh aktivitas pada proses ini sebagian besar berada pada kategori *Partially Achieved* dan *Not Achieved*, sehingga capaian *capability level* saat ini berada pada Level 0. Temuan ini mengindikasikan perlunya penguatan dalam aspek dokumentasi, pengendalian, serta pemantauan berkelanjutan agar proses ini dapat mencapai Level 2 sesuai target berdasarkan pertimbangan faktor desain. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.1 (Lampiran 7, halaman 167).

2. DSS01.02 - Mengelola Layanan TI yang Dialihdayakan (*Manage Outsourced IT Services*)

Proses DSS01.02 mengatur pengelolaan layanan TI yang diserahkan kepada pihak ketiga melalui kerja sama formal. Hasil evaluasi menunjukkan bahwa meskipun telah terdapat dokumen kontrak kerja sama yang mencantumkan peran dan tanggung jawab masing-masing pihak, sejumlah aspek krusial belum diatur secara memadai. Kesepakatan tingkat layanan (SLA) belum disusun secara formal, pemantauan performa hanya bergantung pada laporan dari pihak ketiga tanpa adanya evaluasi internal, serta standar keamanan belum dijadikan bagian eksplisit dalam perjanjian. Dari empat aktivitas yang dievaluasi, hanya satu aktivitas yang mencapai kategori *Fully Achieved*, sementara tiga lainnya berada pada tingkat *Partially Achieved*. Berdasarkan hasil penilaian tersebut, *capability level* saat ini berada pada Level 0, dengan target pengembangan pada Level 3, sejalan dengan tingginya tingkat ketergantungan terhadap pihak ketiga, risiko operasional, serta kebutuhan dokumentasi formal yang ditentukan dalam faktor desain. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.2 (Lampiran 7, halaman 167 - 168).

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

Proses DSS01.03 mencakup kegiatan pemantauan terhadap performa dan status infrastruktur TI untuk mendukung keberlangsungan layanan. Berdasarkan hasil evaluasi, pemantauan telah dilakukan secara rutin menggunakan Grafana, namun pelaksanaannya belum sepenuhnya optimal. Dokumentasi hasil pemantauan belum disusun secara sistematis, dan belum tersedia prosedur formal untuk evaluasi maupun tindak lanjut. Fitur *alert* telah tersedia, tetapi belum terintegrasi dengan sistem eksternal sehingga penanganan masih dilakukan secara manual. Seluruh aktivitas berada pada kategori *Partially Achieved* dan *Largely Achieved*, tanpa satupun yang mencapai *Fully Achieved*, sehingga *capability level* saat ini berada pada Level 0. Target pengembangan ditetapkan pada Level 3, mengingat kebutuhan monitoring yang tinggi, potensi risiko layanan, dan pentingnya stabilitas infrastruktur. Rincian hasil evaluasi proses ini dapat dilihat pada Tabel Lampiran 7.3 (Lampiran 7, halaman 168).

4. DSS01.04 - Mengelola Lingkungan Fisik (*Manage the Physical Environment*)

Proses DSS01.04 mencerminkan bahwa pengelolaan lingkungan fisik terhadap sistem JB Class telah dilakukan dengan cukup baik, terutama dalam aspek penempatan server, pembatasan akses fisik, serta penyediaan sistem proteksi seperti CCTV, sistem pendingin, dan alarm kebakaran. Lokasi server telah ditetapkan secara jelas, berada di lingkungan Dinas Kominfo dengan kepemilikan dan pengelolaan yang tercantum dalam dokumen kerja sama. Akses fisik juga telah dibatasi hanya untuk personel teknis tertentu sesuai pembagian tugas dalam dokumen internal. Meskipun begitu, masih terdapat kekurangan dalam penyusunan dokumen formal berupa SOP dan dokumentasi risiko yang berkaitan dengan ancaman lingkungan seperti kebakaran atau kebocoran. Satu dari empat aktivitas masih berada pada kategori *Largely Achieved*, sehingga *capability level* saat ini belum memenuhi syarat untuk mencapai Level 1 secara penuh. Target

pengembangan diarahkan pada Level 2, mengingat pentingnya perlindungan fisik terhadap aset TI dalam menjaga ketersediaan dan keberlanjutan layanan. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.4 (Lampiran 7, halaman 169).

5. DSS01.05 - Mengelola Operasional (*Manage Operations*)

Proses DSS01.05 menjelaskan bahwa pelaksanaan operasional harian, seperti monitoring dan pencadangan data, telah dilakukan secara rutin oleh pengelola sistem JB Class. Namun, kegiatan tersebut belum didukung oleh kebijakan atau prosedur formal dalam bentuk SOP, sehingga belum terdapat mekanisme pengendalian yang terdokumentasi secara sistematis. Selain itu, pengelolaan akun pengguna masih dilaksanakan secara manual tanpa adanya prosedur tertulis yang jelas. Aktivitas pencatatan penggunaan sistem juga belum dilengkapi dengan sistem audit log, sehingga pemantauan terhadap aktivitas pengguna dan administrator belum dapat dilakukan secara komprehensif. Berdasarkan hasil evaluasi, seluruh aktivitas berada pada kategori *Partially Achieved* dan *Largely Achieved*, tanpa ada yang mencapai *Fully Achieved*. Oleh karena itu, *capability level* saat ini berada pada Level 0**,** dengan target pengembangan pada Level 2**,** mengacu pada pentingnya keandalan operasional, kontrol akses, dan dokumentasi aktivitas pengguna sebagaimana tercantum dalam faktor desain. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.5 (Lampiran 7, halaman 169 - 170).

6. DSS02.01 - Mengelola Pertanyaan dan Permintaan Layanan Pengguna (*Manage User Queries and Service Requests*)

Proses DSS02.01 menjelaskan bahwa sistem JB Class telah menyediakan saluran komunikasi seperti WhatsApp dan email untuk menampung pertanyaan serta permintaan layanan dari pengguna. Meskipun mekanisme ini telah memfasilitasi interaksi antara pengguna dan pengelola sistem, pelaksanaannya masih bersifat manual dan belum didukung oleh prosedur standar atau sistem yang terdokumentasi secara formal. Prosedur operasional baku, seperti SOP atau formulir layanan, belum tersedia, dan pencatatan

permintaan hanya dilakukan secara manual tanpa adanya pelacakan melalui sistem digital. Kondisi ini menyebabkan pengelolaan permintaan layanan belum berjalan secara konsisten dan tidak memiliki rekam jejak yang dapat dievaluasi. Berdasarkan hasil penilaian, seluruh aktivitas dalam proses ini berada pada kategori *Partially Achieved* dan *Largely Achieved*, tanpa satupun yang mencapai *Fully Achieved*, sehingga *capability level* saat ini berada pada Level 0. Target pengembangan ditetapkan pada Level 2, mengingat kebutuhan akan pengelolaan permintaan yang terstruktur dan terdokumentasi guna meningkatkan efektivitas layanan, kepuasan pengguna, dan keandalan sistem. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.6 (Lampiran 7, halaman 170).

7. DSS02.02 - Mencatat dan Mengklasifikasikan Insiden (*Register and Classify Incidents*)

Proses DSS02.02 menjelaskan bahwa pencatatan insiden pada sistem JB Class masih dilakukan secara manual dan belum didukung oleh sistem pelaporan yang terstruktur. Pencatatan insiden saat ini hanya tersedia dalam bentuk laporan teknis informal, tanpa pemanfaatan platform khusus maupun sistem log yang terdokumentasi. Selain itu, mekanisme klasifikasi insiden berdasarkan jenis dan dampaknya belum diterapkan, sehingga penanganan insiden berlangsung sementara dan tidak mengikuti standar baku. Prosedur operasional seperti SOP juga belum tersedia, sehingga tidak terdapat alur kerja formal yang mengatur proses pencatatan dan klasifikasi insiden. Meskipun beberapa insiden telah dimanfaatkan dalam evaluasi teknis internal, penggunaan data tersebut belum dilakukan secara sistematis dan belum terdokumentasi secara formal. Seluruh aktivitas dalam proses ini berada pada kategori *Partially Achieved* dan *Largely Achieved*, tanpa ada yang mencapai *Fully Achieved*, sehingga *capability level* saat ini berada pada Level 0. Target pengembangan ditetapkan pada Level 2, sejalan dengan tingginya urgensi pengelolaan insiden dalam menjamin kontinuitas layanan, mendukung pembelajaran organisasi, serta mendorong peningkatan kualitas

sistem. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.7 (Lampiran 7, halaman 171).

8. DSS02.03 - Menutup Insiden (*Escalate and Resolve Incidents*)

Proses DSS02.03 menjelaskan bahwa insiden yang tidak dapat diselesaikan oleh tim internal Balai Tekkomdik umumnya diteruskan melalui koordinasi dengan pihak rekanan. Meskipun praktik tersebut telah berlangsung, mekanisme eskalasi belum didukung oleh prosedur formal atau sistem dokumentasi yang terstandar. Beberapa aspek penting juga belum diimplementasikan secara sistematis, seperti penetapan target waktu penyelesaian berdasarkan klasifikasi insiden, pencatatan langkah penyelesaian, serta pemberian informasi progres kepada pengguna. Komunikasi masih dilakukan secara informal melalui whatsApp dan discord, sementara pemantauan terhadap insiden berulang belum terintegrasi dalam sistem JB Class. Seluruh aktivitas berada pada kategori *Partially Achieved* dan *Largely Achieved*, tanpa capaian pada tingkat *Fully Achieved*, sehingga *capability level* saat ini berada pada Level 0. Target peningkatan ditetapkan pada Level 2, mempertimbangkan kebutuhan akan proses eskalasi insiden yang terdokumentasi dan terstruktur demi menjaga keandalan layanan serta mencegah insiden berulang. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.8 (Lampiran 7, halaman 172).

9. DSS02.04 - Menutup Insiden (*Close Incidents*)

Proses DSS02.04 menjelaskan bahwa aktivitas penutupan insiden pada sistem JB Class belum dilaksanakan secara formal maupun terdokumentasi. Validasi teknis terhadap insiden berskala besar memang telah dilakukan melalui diskusi internal, namun belum tersedia prosedur standar atau sistem yang mengatur proses penutupan insiden secara terstruktur. Selain itu, belum terdapat mekanisme untuk menghimpun umpan balik dari pengguna sebagai bagian dari evaluasi pasca insiden. Kondisi ini menunjukkan bahwa proses belum dijalankan secara konsisten, sehingga tidak terdapat rekam jejak yang dapat digunakan untuk pembelajaran maupun peningkatan layanan.

Berdasarkan hasil penilaian, seluruh aktivitas berada pada kategori *Not Achieved* dan *Partially Achieved*, dengan capaian *capability level* saat ini berada pada Level 0**.** Target pengembangan diarahkan pada Level 2**,** sejalan dengan pentingnya penutupan insiden yang terdokumentasi dan terstandar untuk memastikan penyelesaian yang valid serta mendukung proses evaluasi berkelanjutan. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.9 (Lampiran 7, halaman 173).

10. DSS03.01 - Mengidentifikasi dan Mengklasifikasikan Masalah (*Identify and Classify Problems*)

Proses DSS03.01 menjelaskan bahwa kegiatan identifikasi dan klasifikasi masalah pada sistem JB Class telah dilakukan, namun belum sepenuhnya terdokumentasi maupun didukung oleh sistem yang terstruktur. Monitoring teknis telah dilaksanakan dengan bantuan aplikasi seperti Grafana, tetapi aktivitas klasifikasi penyebab, identifikasi masalah tersembunyi, serta pengelompokan berdasarkan frekuensi atau dampak masih dilakukan secara manual dan belum mengacu pada prosedur standar. Tidak terdapat metode formal dalam mendeteksi masalah tersembunyi melalui analisis log atau pendekatan proaktif lainnya. Selain itu, pengelompokan permasalahan masih bersifat teknis tanpa dokumentasi yang memadai. Seluruh aktivitas dalam proses ini berada pada kategori *Not Achieved*, *Partially Achieved*, dan *Largely Achieved*, tanpa adanya aktivitas yang mencapai *Fully Achieved*, sehingga *capability level* saat ini berada pada Level 0. Target pengembangan ditetapkan pada Level 2, mengacu pada pentingnya dokumentasi dan klasifikasi masalah sebagai dasar peningkatan kualitas layanan serta upaya menjaga stabilitas operasional secara berkelanjutan. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.10 (Lampiran 7, halaman 173 - 174).

11. DSS03.02 - Menyelidiki dan Mendiagnosis Masalah (*Investigate and Diagnose Problems*)

Proses DSS03.02 menjelaskan bahwa kegiatan investigasi terhadap akar penyebab masalah telah dilakukan oleh tim pengelola sistem JB Class, namun

pelaksanaannya belum ditunjang oleh metode diagnosis yang terstandar seperti *Root Cause Analysis* (RCA) maupun prosedur formal lainnya. Proses identifikasi masih bersifat teknis dan belum terdokumentasi secara sistematis. Penggunaan alat bantu investigasi seperti *log analyzer* atau *error tracker* belum diterapkan, sehingga analisis hanya mengandalkan dashboard dan pencatatan log secara manual. Selain itu, hasil investigasi belum didokumentasikan secara sistematis dan sebagian hanya tersedia dalam bentuk file atau komunikasi informal. Seluruh aktivitas dalam proses ini berada pada kategori *Not Achieved*, *Partially Achieved*, dan *Largely Achieved*, tanpa ada aktivitas yang mencapai *Fully Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 2, mengacu pada pentingnya dokumentasi hasil investigasi, penggunaan metode terstandar, dan dukungan alat teknis sebagai upaya meningkatkan efisiensi penanganan masalah serta menjaga keberlangsungan layanan. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.11 (Lampiran 7, halaman 174).

12. DSS03.03 - Mencatat Kesalahan yang Dikenal (*Raise Known Errors*)

Proses DSS03.03 menjelaskan bahwa pencatatan *known errors* pada sistem JB Class belum dilakukan secara formal dan sistematis. Meskipun beberapa kesalahan telah dikenali oleh tim pengelola secara teknis, pencatatannya belum terdokumentasi dalam bentuk resmi atau sistem pencatatan yang terstruktur. Riwayat masalah yang pernah terjadi belum sepenuhnya dimanfaatkan sebagai referensi untuk penanganan insiden selanjutnya, dan pendekatan yang digunakan masih bersifat reaktif. Kebijakan mengenai solusi jangka panjang atau *permanent fix* juga belum tersedia, sehingga proses perbaikan tidak diarahkan pada penyelesaian berkelanjutan. Seluruh aktivitas dalam proses ini berada pada kategori *Not Achieved* dan *Partially Achieved*, tanpa ada yang mencapai *Fully Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 2, mengacu pada pentingnya dokumentasi *known errors* sebagai acuan perbaikan, pencegahan gangguan berulang, dan peningkatan

efisiensi dalam penanganan masalah. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.12 (Lampiran 7, halaman 175).

13. DSS04.01 - Menentukan Kebutuhan Keberlangsungan (*Define Continuity Requirements*)

Proses DSS04.01 menunjukkan bahwa kebutuhan keberlangsungan layanan pada sistem JB Class belum ditetapkan secara formal dan terdokumentasi. Risiko utama terhadap keberlangsungan sistem telah dikenali oleh tim teknis, namun belum didukung oleh analisis risiko yang tersusun secara sistematis. Batas toleransi terhadap *downtime* juga belum ditentukan dalam bentuk kebijakan atau perjanjian layanan. Sementara itu, pemantauan terhadap ketersediaan sistem telah dilakukan secara rutin dengan bantuan tools seperti Grafana, tetapi pelaksanaannya belum didukung oleh prosedur tertulis maupun dokumentasi hasil monitoring. Seluruh aktivitas dalam proses ini berada pada kategori *Not Achieved*, *Partially Achieved*, dan *Largely Achieved*, tanpa adanya capaian *Fully Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 2, sejalan dengan pentingnya penetapan kebutuhan keberlangsungan yang terdokumentasi, sebagai dasar dalam menjaga aksesibilitas dan keandalan sistem secara berkelanjutan. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.13 (Lampiran 7, halaman 175 - 176).

14. DSS04.02 - Menyusun Rencana Keberlangsungan (*Establish Continuity Plans*)

Proses DSS04.02 menunjukkan bahwa beberapa aktivitas terkait keberlangsungan layanan pada sistem JB Class telah mulai dilaksanakan, terutama dalam bentuk pencadangan sistem secara rutin dan penunjukan tanggung jawab teknis. Meskipun demikian, seluruh aktivitas tersebut belum didukung oleh dokumen formal seperti *disaster recovery plan*, SOP atau surat keputusan resmi terkait struktur tanggung jawab. Otomatisasi proses pencadangan juga belum mencakup seluruh komponen sistem, dan belum terdokumentasi dalam kebijakan yang baku. Berdasarkan hasil evaluasi,

seluruh aktivitas dalam proses ini masih berada pada kategori *Not Achieved* dan *Largely Achieved*, tanpa capaian *Fully Achieved*, sehingga *capability level* saat ini berada pada Level 0. Target pengembangan diarahkan pada Level 3, mengingat pentingnya penyusunan rencana keberlangsungan yang terdokumentasi secara menyeluruh untuk menjamin pemulihan layanan secara cepat dan efektif dalam situasi bencana atau gangguan operasional. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.14 (Lampiran 7, halaman 176 - 177).

15. DSS04.03 - Menerapkan dan Memelihara Rencana Keberlangsungan (*Implement and Maintain Continuity Plans*)

Proses DSS04.03 menunjukkan bahwa penerapan rencana keberlangsungan layanan pada sistem JB Class belum dilaksanakan secara formal. Belum terdapat bukti pelaksanaan simulasi pemulihan layanan, evaluasi hasil pengujian, maupun dokumentasi yang terdokumentasi secara sistematis. Seluruh kegiatan dalam proses ini masih bersifat reaktif dan hanya dilakukan ketika terjadi gangguan berskala besar, tanpa ada siklus peninjauan yang terjadwal secara rutin. Selain itu, tidak ditemukan dokumentasi rencana keberlangsungan yang dapat diakses atau digunakan secara kolektif oleh pihak terkait. Berdasarkan hasil evaluasi, seluruh aktivitas berada pada kategori *Not Achieved* dan *Partially Achieved*, tanpa adanya aktivitas yang mencapai *Fully Achieved*. Dengan demikian, *capability level* saat ini ditetapkan pada Level 0, sementara target pengembangan diarahkan pada Level 3, mempertimbangkan pentingnya dokumentasi formal, pelaksanaan simulasi, dan evaluasi berkelanjutan untuk menjamin keberlangsungan layanan sistem pembelajaran digital. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.15 (Lampiran 7, halaman 1767).

16. DSS05.01 - Melindungi dari Malware (*Protect Against Malware*)

Proses DSS05.01 menunjukkan bahwa perlindungan terhadap malware pada sistem JB Class masih berfokus pada sisi server yang dikelola oleh Dinas Kominfo, sementara sistem JB Class sendiri belum dilengkapi dengan

mekanisme perlindungan yang memadai dan terintegrasi. Fitur penting seperti pemindaian otomatis terhadap file unggahan pengguna, pembaruan keamanan yang terjadwal, serta sistem pencatatan dan pelaporan insiden belum tersedia secara optimal. Pemindaian unggahan masih belum diterapkan, dan pembaruan keamanan hanya dilakukan jika ditemukan masalah, tanpa jadwal yang tetap. Sementara itu, log insiden memang tersimpan di server, namun belum tersedia mekanisme pelaporan atau pemantauan insiden secara khusus dalam sistem JB Class. Seluruh aktivitas dalam proses ini berada pada kategori *Partially Achieved* dan *Largely Achieved*, tanpa satu pun yang mencapai *Fully Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 3, sesuai dengan pentingnya pengamanan sistem terhadap ancaman malware dalam menjaga integritas, keamanan data, dan kelangsungan layanan sistem pembelajaran digital. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.16 (Lampiran 7, halaman 177 - 178).

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

Proses DSS05.02 menunjukkan bahwa sistem JB Class telah dilengkapi dengan pengamanan jaringan dan konektivitas yang memadai, serta telah diterapkan secara optimal sesuai dengan kebutuhan layanan digital pendidikan. Seluruh aktivitas dalam proses ini berada pada kategori *Fully Achieved*, yang mencerminkan keberhasilan pelaksanaan kontrol keamanan jaringan secara menyeluruh. Infrastruktur server telah dilindungi melalui penggunaan firewall dan pengelolaan akses yang dilaksanakan oleh Dinas Kominfo, serta pengiriman data telah diamankan melalui protokol HTTPS dengan dukungan sertifikat SSL aktif. Selain itu, sistem juga telah memiliki mekanisme perlindungan dari ancaman eksternal melalui firewall yang berfungsi untuk membatasi dan mengendalikan lalu lintas jaringan. Berdasarkan hasil evaluasi, *capability level* saat ini berada pada Level 1, dan ditargetkan mencapai Level 2 sesuai arahan faktor desain yang menekankan pentingnya keamanan jaringan

dalam menjaga stabilitas layanan, perlindungan data, dan integritas sistem. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.17 (Lampiran 7, halaman 178 - 179).

18. DSS05.03 - Mengelola Keamanan Endpoint (*Manage Endpoint Security*)

Proses DSS05.03 menunjukkan bahwa pengelolaan keamanan endpoint pada sistem JB Class belum menjadi fokus utama dalam praktik pengelolaan keamanan secara menyeluruh. Sistem belum dilengkapi dengan kebijakan maupun mekanisme pembatasan perangkat pengguna, sehingga akses dapat dilakukan dari berbagai perangkat tanpa kontrol yang ketat. Selain itu, belum tersedia kebijakan formal terkait keamanan perangkat kerja internal, serta tidak diterapkan enkripsi pada perangkat endpoint yang digunakan oleh staf. Sistem juga belum memiliki kemampuan untuk mendeteksi perangkat tidak dikenal, selama kredensial login dinyatakan valid. Seluruh aktivitas dalam proses ini berada pada kategori *Not Achieved* dan *Partially Achieved*, tanpa adanya aktivitas yang mencapai *Fully Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 2, dengan mempertimbangkan pentingnya kebijakan keamanan endpoint, dokumentasi teknis, serta penerapan kontrol pengamanan terstruktur guna melindungi data dan menjaga integritas sistem. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.18 (Lampiran 7, halaman 179).

19. DSS05.04 - Mengelola Identitas dan Akses Pengguna (*Manage User Identity and Logical Access*)

Proses DSS05.04 menunjukkan bahwa pengelolaan identitas dan akses pengguna pada sistem JB Class belum sepenuhnya memenuhi indikator pada Level 1. Meskipun sistem telah menerapkan pengaturan hak akses berdasarkan peran pengguna, sejumlah aspek krusial lainnya masih belum optimal. Proses pendaftaran akun dilakukan secara mandiri tanpa validasi tambahan atau aktivasi oleh admin, sehingga belum menjamin keamanan identitas pengguna secara menyeluruh. Selain itu, sistem belum dilengkapi dengan mekanisme

verifikasi saat pendaftaran, seperti penggunaan OTP atau konfirmasi melalui email, serta belum mendukung autentikasi dua faktor (2FA), bahkan untuk akun dengan akses sensitif. Pengelolaan terhadap akun siswa yang sudah tidak aktif, seperti yang berpindah atau keluar dari sekolah, masih dilakukan secara manual dan belum terdokumentasi secara sistematis. Berdasarkan hasil evaluasi, dua dari lima aktivitas berada pada kategori *Not Achieved* dan satu lainnya *Partially Achieved*. Oleh karena itu, *capability level* saat ini berada pada Level 0, dengan target pengembangan pada Level 2, mengingat pentingnya kontrol identitas dan akses untuk menjamin keamanan sistem, privasi pengguna, dan integritas layanan digital. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.19 (Lampiran 7, halaman 180).

20. DSS05.05 - Mengelola Insiden Terkait Keamanan (*Manage Security-Related Incidents*)

Proses DSS05.05 menunjukkan bahwa penanganan insiden keamanan pada sistem JB Class masih bersifat reaktif dan belum terstruktur secara formal. Meskipun tanggung jawab terhadap insiden telah dijalankan secara fungsional dan tercantum dalam dokumen internal, sistem belum memiliki mekanisme pencatatan insiden secara otomatis maupun fitur peringatan dini yang dapat membantu deteksi awal. Prosedur pelaporan dan eskalasi insiden belum tersedia dalam bentuk kebijakan atau SOP formal, sehingga penanganan insiden dilakukan tanpa acuan yang terdokumentasi. Selain itu, insiden berdampak besar belum disertai dengan proses evaluasi dan tindak lanjut yang terdokumentasi secara sistematis. Dari hasil evaluasi, hanya satu dari empat aktivitas Level 1 yang mencapai *Fully Achieved*, sementara lainnya berada pada kategori *Partially Achieved* dan *Not Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 3, mengacu pada pentingnya pengelolaan insiden keamanan sebagai aspek krusial dalam menjaga kerahasiaan, integritas, dan ketersediaan sistem layanan pendidikan digital. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.20 (Lampiran 7, halaman 180 - 181).

21. DSS06.01 - Menyesuaikan Kebutuhan Bisnis dan Kontrol (*Align Business Functional and Control Requirements*)

Proses DSS06.01 menunjukkan bahwa penyesuaian sistem JB Class terhadap kebutuhan pengguna telah mulai dilakukan, namun belum didukung oleh proses yang terdokumentasi secara formal. Penyesuaian fitur telah dilakukan melalui kegiatan seperti FGD, tetapi belum dilandasi oleh analisis kebutuhan yang sistematis. Pengujian terhadap fitur baru sebelum implementasi juga telah dilakukan, namun belum dilengkapi dengan dokumentasi yang baku atau prosedur pengujian standar. Kontrol terhadap aktivitas penting seperti pengelolaan nilai, tugas, dan materi pembelajaran masih belum memadai, karena tidak tersedia kebijakan teknis maupun mekanisme audit penggunaan. Selain itu, kontrol terhadap perubahan fitur belum sepenuhnya diterapkan, termasuk belum tersedianya prosedur *rollback* dan pencatatan versi sistem. Berdasarkan hasil evaluasi, tidak ada aktivitas Level 1 yang mencapai *Fully Achieved*, dengan sebagian besar aktivitas berada pada kategori *Partially Achieved* dan satu aktivitas *Not Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 3, dengan mengacu pada faktor desain yang menekankan pentingnya dokumentasi, standarisasi, serta peninjauan berkala dalam pengelolaan kebutuhan bisnis dan kontrol sistem. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.21 (Lampiran 7, halaman 181 - 182).

22. DSS06.02 - Mengendalikan Pemrosesan Informasi (*Control the Processing of Information*)

Proses DSS06.02 menunjukkan bahwa pengendalian terhadap pemrosesan informasi pada sistem JB Class belum berjalan secara optimal. Validasi data yang diterapkan masih terbatas pada aspek teknis dasar, seperti pengecekan format atau kelengkapan isian, dan belum mencakup validasi lintas data maupun kesesuaian terhadap aturan bisnis. Meskipun hak akses pengguna telah diterapkan, sistem belum dilengkapi dengan mekanisme audit trail yang dapat melacak perubahan data, serta belum tersedia fitur *rollback* untuk memulihkan

kesalahan input secara efisien. Koreksi data masih dilakukan secara manual karena sistem belum mendukung pemulihan otomatis. Berdasarkan hasil evaluasi, tidak ada aktivitas Level 1 yang mencapai *Fully Achieved*, dengan dua aktivitas berada pada *Partially Achieved*, satu *Largely Achieved*, dan satu lainnya *Not Achieved*. Oleh karena itu, *capability level* saat ini ditetapkan pada Level 0, dengan target pengembangan pada Level 3, mengacu pada pentingnya pengendalian proses informasi untuk menjamin akurasi, integritas, dan keamanan data dalam mendukung pelaksanaan proses bisnis. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.22 (Lampiran 7, halaman 182).

23. DSS06.03 - Memelihara Kontrol Proses Bisnis (*Maintain Business Process Controls*)

Proses DSS06.03 menunjukkan bahwa pemeliharaan kontrol terhadap proses bisnis pada sistem JB Class telah mulai dilakukan, namun belum secara menyeluruh dan terdokumentasi secara formal. Dukungan terhadap kontrol proses terlihat melalui adanya panduan penggunaan sistem serta pemanfaatan umpan balik dari pengguna sebagai dasar perbaikan. Namun demikian, dokumentasi alur kerja belum disusun dalam bentuk diagram proses yang terstruktur, sehingga alur aktivitas belum sepenuhnya terdokumentasi secara visual dan sistematis. Pemantauan terhadap pelaksanaan proses masih terbatas pada aspek teknis melalui alat bantu seperti Grafana, dan belum mencakup keseluruhan proses bisnis yang berjalan di sistem. Selain itu, belum tersedia mekanisme audit internal yang dilaksanakan secara formal dan berkala untuk menilai efektivitas pengendalian proses. Berdasarkan hasil evaluasi, hanya satu aktivitas yang berada pada kategori *Fully Achieved*, sementara dua aktivitas dinilai *Partially Achieved* dan satu aktivitas *Not Achieved*. Dengan kondisi tersebut, *capability level* saat ini ditetapkan pada Level 0, dan target pengembangan diarahkan pada Level 2, mengacu pada pentingnya dokumentasi yang terstruktur, pemantauan menyeluruh, serta pelaksanaan evaluasi berkelanjutan dalam menjaga efisiensi dan kesinambungan layanan.

Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.23 (Lampiran 7, halaman 182 - 183).

Domain MEA (Monitor, Evaluate, and Assess)

1. MEA01.01 - Memantau Kinerja Sistem (*Monitor System Performance*)

Proses MEA01.01 memperlihatkan bahwa pemantauan terhadap kinerja sistem JB Class telah dilakukan secara teknis, terutama oleh tim IT. Beberapa indikator performa telah digunakan dalam praktik, dan masukan dari pengguna turut dijadikan dasar untuk perbaikan layanan. Namun, proses ini belum sepenuhnya didukung oleh dokumentasi formal maupun standar operasional tertulis. Penetapan indikator kinerja belum berdasarkan pada standar internal atau kebijakan resmi, dan evaluasi dampak performa terhadap kenyamanan pengguna masih belum berbasis metode survei yang terstruktur. Selain itu, penanganan terhadap penurunan performa sistem belum dilandasi oleh prosedur tertulis atau pelaporan formal. Berdasarkan hasil evaluasi, hanya satu aktivitas yang berada pada kategori *Fully Achieved*, sementara dua aktivitas lainnya *Partially Achieved* dan satu *Not Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 3, sesuai dengan pentingnya monitoring performa sistem secara rutin, berbasis indikator yang terstandarisasi, serta dilengkapi dokumentasi yang mendukung pengambilan keputusan dan peningkatan layanan. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.24 (Lampiran 7, halaman 183).

2. MEA01.02 - Memantau Efektivitas Kontrol (*Monitor Control Effectiveness*)

Proses MEA01.02 menunjukkan bahwa pemantauan terhadap efektivitas kontrol pada sistem JB Class telah dilaksanakan, namun masih bersifat teknis dan belum didukung oleh dokumentasi formal yang memadai. Evaluasi dilakukan oleh tim teknis dalam operasional harian, tetapi belum tersedia laporan tertulis atau sistem yang merekam hasil evaluasi secara konsisten. Selain itu, tidak terdapat metrik formal atau indikator kuantitatif yang dapat digunakan sebagai dasar penilaian objektif terhadap efektivitas kontrol yang

diterapkan. Meskipun hasil evaluasi teknis dimanfaatkan untuk pengambilan keputusan, pemanfaatan tersebut belum didukung oleh sistem pelaporan atau dokumentasi yang terstruktur. Siklus evaluasi juga belum dirancang secara formal, sehingga pemantauan cenderung dilakukan secara reaktif, bukan sebagai bagian dari proses berkala yang terstandarisasi. Berdasarkan hasil evaluasi, seluruh aktivitas masih berada pada kategori *Largely Achieved* dan *Not Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 3, dengan menekankan pentingnya dokumentasi hasil evaluasi, penggunaan indikator pengukuran yang jelas, serta pelaksanaan pemantauan secara rutin dan terdokumentasi untuk menjamin efektivitas kontrol dalam jangka panjang. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.25 (Lampiran 7, halaman 184).

3. MEA01.03 - Memantau Kepatuhan terhadap Regulasi Eksternal (*Monitor Compliance with External Requirements*)

Proses MEA01.03 menunjukkan bahwa penerapan prinsip dasar keamanan informasi serta pemenuhan terhadap kebijakan dari instansi pemerintah telah mulai diimplementasikan dalam sistem JB Class. Penyesuaian sistem terhadap regulasi eksternal, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), belum dirumuskan secara eksplisit maupun terdokumentasi dalam kebijakan teknis sistem. Mekanisme pemantauan terhadap perubahan regulasi belum disusun secara sistematis, dan audit kepatuhan oleh pihak eksternal juga belum pernah dilaksanakan. Selain itu, belum terdapat dokumentasi formal yang mencatat penyesuaian sistem terhadap pembaruan regulasi yang berlaku. Berdasarkan hasil evaluasi, tidak terdapat aktivitas yang berada pada kategori *Fully Achieved*, dengan dua aktivitas memperoleh *Largely Achieved* dan dua lainnya *Not Achieved*. Dengan demikian, *capability level* saat ini ditetapkan pada Level 0, sedangkan target pengembangan diarahkan pada Level 3. Peningkatan difokuskan pada penyusunan sistem pemantauan regulasi yang terstruktur, pelaksanaan audit eksternal secara berkala, serta dokumentasi formal atas seluruh penyesuaian sebagai bentuk pemenuhan terhadap

kepatuhan hukum dan perlindungan data pengguna. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.26 (Lampiran 7, halaman 184 - 185).

4. MEA02 - Mengevaluasi Sistem Pengendalian Internal (*Assess the System of Internal Control*)

Proses MEA02 menunjukkan bahwa pelaksanaan sistem pengendalian internal pada sistem JB Class belum berjalan secara optimal. Aktivitas pengendalian sebagian besar belum tercapai, terutama pada aspek dokumentasi prosedur, pelaksanaan audit internal, serta tindak lanjut terhadap hasil evaluasi. Pemantauan aktivitas pengguna masih dilakukan secara manual dan belum dilengkapi dengan sistem pelacakan yang terdokumentasi. Evaluasi efektivitas pengendalian hanya dilakukan berdasarkan pengalaman teknis, tanpa dukungan indikator atau metrik formal. Selain itu, belum tersedia prosedur resmi dalam menangani pelanggaran, maupun panduan atau SOP yang mengatur mekanisme pengendalian internal secara sistematis. Audit internal juga belum pernah dilakukan, sehingga tidak terdapat dokumentasi hasil audit maupun langkah perbaikan yang ditindaklanjuti secara formal. Seluruh aktivitas dalam proses ini belum menunjukkan pencapaian optimal, dengan sebagian besar berada pada kategori *Not Achieved*. Oleh karena itu, *capability level* saat ini berada pada Level 0, dan target pengembangan diarahkan pada Level 3, dengan menekankan pentingnya dokumentasi kebijakan, pemantauan rutin, serta penguatan evaluasi berbasis indikator yang jelas dalam mendukung efektivitas pengendalian internal. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.27 (Lampiran 7, halaman 185 - 186).

5. MEA03 - Kepatuhan terhadap Persyaratan Eksternal (*Compliance with External Requirements*)

Proses MEA03 mengindikasikan bahwa kepatuhan terhadap regulasi eksternal belum diimplementasikan secara formal dan menyeluruh dalam sistem JB Class. Prinsip-prinsip dasar keamanan informasi telah diterapkan, namun sistem belum memiliki daftar regulasi resmi sebagai acuan dalam

operasionalnya. Pemantauan terhadap kepatuhan dilakukan secara informal dan belum didukung oleh prosedur verifikasi maupun audit eksternal. Selain itu, dokumentasi perubahan yang dilakukan berdasarkan regulasi belum tersedia, dan tidak terdapat informasi terbuka mengenai kebijakan privasi atau perlindungan data pengguna. Seluruh aktivitas dalam proses ini belum menunjukkan capaian optimal, dengan sebagian besar berada pada kategori *Not Achieved* dan tidak satu pun yang mencapai *Fully Achieved*, sehingga *capability level* saat ini berada pada Level 0**.** Target pengembangan diarahkan pada Level 3**,** dengan menekankan pentingnya dokumentasi regulasi yang digunakan, pelaksanaan audit eksternal secara berkala, serta penyediaan informasi kebijakan secara terbuka kepada pengguna sebagai bentuk akuntabilitas tata kelola. Rincian hasil evaluasi proses ini disajikan dalam Tabel Lampiran 7.28 (Lampiran 7, halaman 186).

6. MEA04 - Memberikan Jaminan (*Provide Assurance*)

Proses MEA04 menunjukkan bahwa kegiatan *assurance* terhadap sistem JB Class belum dilaksanakan dan belum terdokumentasi secara formal. Tidak ditemukan prosedur atau SOP yang mengatur pelaksanaan *assurance*, baik oleh pihak internal maupun eksternal. Selain itu, tidak terdapat bukti pelaksanaan pengujian sistem secara terstruktur yang mencakup aspek keamanan, akses, maupun fungsionalitas fitur. Penjadwalan maupun pembaruan hasil evaluasi juga belum dilakukan karena kegiatan assurance belum pernah diimplementasikan. Berdasarkan hasil penilaian, seluruh aktivitas pada proses ini berada pada kategori *Not Achieved*, sehingga *capability level* saat ini ditetapkan pada Level 0. Target pengembangan diarahkan pada Level 2, dengan fokus pada penyusunan prosedur formal, pelaksanaan evaluasi secara berkala, serta dokumentasi hasil assurance guna menjamin keandalan sistem dan memenuhi ekspektasi pemangku kepentingan. Rincian penilaian aktivitas ditampilkan dalam Tabel Lampiran 7.29 (Lampiran 7, halaman 186 - 187).

B. Hasil Audit dan Rekomendasi

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 per proses disajikan pada Tabel 4.30 dan Tabel 4.31.

Tabel 4.30 Hasil Audit dan Rekomendasi Domain DSS

Proses	*Gap*	Hasil	Keterangan	Rekomendasi
DSS01.01	2	Tidak Sesuai Standar	Perlu penguatan SOP, dokumentasi, dan pelaksanaan yang konsisten	1. Menyusun SOP formal yang mencakup seluruh prosedur operasional sistem JB Class, termasuk pengecekan rutin, *backup*, dan manajemen kelas. 2. Menerapkan pencatatan harian terhadap aktivitas operasional (seperti monitoring, pembaruan data, atau laporan error ringan) dalam bentuk log digital/manual. 3. Menerapkan sistem pembaruan versi pada dokumen panduan operasional agar setiap revisi terdokumentasi dan terverifikasi.
DSS01.02	3	Tidak Sesuai Standar	Proses belum memenuhi standar dokumentasi dan kontrol performa yang diharuskan pada layanan pihak ketiga. Evaluasi belum sistematis dan belum terdokumentasi.	1. Menyusun SLA formal dan rinci, yang mencantumkan *uptime*, *downtime* maksimum, serta *response & recovery time.* 2. Menerapkan mekanisme evaluasi dan pelaporan berkala terhadap performa layanan oleh pihak Kominfo. 3. Mencantumkan ketentuan pemenuhan standar keamanan informasi (seperti ISO 27001 atau kebijakan perlindungan data pribadi) dalam dokumen perjanjian kerja sama.
DSS01.03	3	Tidak Sesuai Standar	Infrastruktur telah dimonitor, tetapi tidak didokumentasikan dan belum ada evaluasi formal.	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.

Proses	*Gap*	Hasil	Keterangan	Rekomendasi
				3. Membuat laporan hasil monitoring harian atau mingguan untuk disimpan sebagai dokumentasi formal.
DSS01.04	2	Tidak Sesuai Standar	Belum memenuhi syarat minimum pengelolaan lingkungan fisik secara formal.	1. Menyusun SOP formal terkait mitigasi risiko lingkungan fisik, mencakup prosedur tang*gap* darurat terhadap potensi ancaman seperti panas berlebih, kebocoran air, kebakaran, dan gangguan listrik. 2. Menetapkan mekanisme pelaporan berkala dari Dinas Kominfo kepada Balai Tekkomdik terkait kondisi keamanan fisik server, termasuk status sistem pendingin, CCTV, alarm, dan akses ruang server. 3. Melengkapi dokumen kerja sama dengan ketentuan tentang tanggung jawab pemantauan dan pemeliharaan infrastruktur fisik, sehingga peran dan kewajiban masing-masing pihak terdokumentasi dengan jelas.
DSS01.05	2	Tidak Sesuai Standar	Belum memenuhi syarat minimum dokumentasi dan pengendalian operasional formal. Sehingga perbaikan diarahkan pada peningkatan dokumentasi dan penyusunan SOP formal untuk operasional harian.	1. Menyusun SOP operasi TI harian, termasuk prosedur *backup*, monitoring, dan pemeliharaan rutin. 2. Membuat sistem pencatatan log aktivitas pengguna dan admin, minimal untuk pelacakan perubahan data atau akses tidak wajar. 3. Menyusun prosedur pengelolaan akun pengguna, mulai dari pembuatan, perubahan hak akses, hingga penonaktifan.
DSS02.01	2	Tidak Sesuai Standar	Proses belum memiliki prosedur formal maupun pencatatan digital yang terstandar.	1. Menyusun SOP pengelolaan permintaan layanan, mulai dari penerimaan hingga penyelesaian. 2. Mengembangkan atau mengadopsi sistem pelaporan permintaan layanan, seperti formulir online atau sistem ticketing sederhana. 3. Mencatat dan memantau setiap permintaan dari pengguna secara teratur.
DSS02.02	2	Tidak Sesuai Standar	Proses belum terdokumentasi, tidak diklasifikasi, dan tidak memiliki mekanisme evaluasi insiden.	1. Membuat sistem pencatatan insiden, bisa berbasis Excel yang terstandar, atau sistem digital jika memungkinkan. 2. Menyusun klasifikasi insiden berdasarkan kategori, prioritas dan dampak. 3. Menyusun SOP penanganan insiden, termasuk pencatatan, penanganan, eskalasi, dan pelaporan.

Proses	*Gap*	Hasil	Keterangan	Rekomendasi
DSS02.03	2	Tidak Sesuai Standar	Proses berjalan, namun tidak terdokumentasi dan belum memenuhi kontrol minimum dalam penanganan insiden.	1. Menyusun SOP teknis untuk eskalasi insiden, agar proses pelimpahan dari tim internal ke pihak rekanan berjalan lebih sistematis dan dapat dipertanggungjawabkan. 2. Menetapkan SLA berdasarkan kategori tingkat keparahan insiden untuk memperjelas ekspektasi penyelesaian waktu dan prioritas teknis. 3. Mengembangkan sistem dokumentasi penyelesaian insiden, agar langkah penanganan tercatat dan bisa dijadikan rujukan untuk kasus serupa.
DSS02.04	2	Tidak Sesuai Standar	Proses belum terdokumentasi secara formal, belum ada prosedur penutupan dan evaluasi terstruktur.	1. Menyusun SOP resmi penutupan insiden, termasuk format laporan dan penentuan status penyelesaian secara tertulis. 2. Menetapkan prosedur validasi penyelesaian insiden, agar penyelesaian insiden tidak hanya bersifat teknis tapi juga terdokumentasi dan dapat diverifikasi. 3. Menyusun laporan evaluasi terhadap insiden berdampak besar, sehingga organisasi dapat belajar dari kejadian tersebut dan mencegah berulang.
DSS03.01	2	Tidak Sesuai Standar	Proses klasifikasi dan identifikasi belum terdokumentasi dan belum dilengkapi sistem formal.	1. Menyusun sistem klasifikasi masalah berdasarkan penyebab (kesalahan pengguna vs masalah sistem), termasuk kategorisasi berdasarkan dampak dan frekuensi. 2. Mengembangkan prosedur dokumentasi masalah agar setiap masalah teknis tercatat sebagai bahan evaluasi dan rujukan penanganan berikutnya. 3. Melakukan evaluasi berkala terhadap log server untuk mendeteksi potensi masalah tersembunyi dan pola gangguan yang berulang.
DSS03.02	2	Tidak Sesuai Standar	Belum memenuhi standar minimal dokumentasi dan struktur investigasi masalah secara formal.	1. Menyusun SOP identifikasi akar penyebab masalah, termasuk metode RCA atau sejenisnya. 2. Membangun sistem dokumentasi hasil investigasi masalah, agar hasil analisis tidak hanya disimpan dalam chat/ingatan, tapi dapat diakses sebagai rujukan resmi. 3. Menggunakan alat bantu tambahan, seperti log analyzer atau error tracking tools, untuk mempercepat identifikasi dan diagnosis masalah.

Proses	*Gap*	Hasil	Keterangan	Rekomendasi
DSS03.03	2	Tidak Sesuai Standar	Proses belum terdokumentasi, tidak memiliki sistem pencatatan, dan solusi bersifat reaktif.	1. Membangun basis data atau daftar *known errors* secara formal, sebagai referensi tim untuk mencegah pengulangan masalah. 2. Menyusun kebijakan dan dokumentasi solusi jangka panjang (*permanent fix*) terhadap known errors. 3. Membuat prosedur pemanfaatan histori kesalahan untuk peningkatan efisiensi penanganan masalah teknis ke depan.
DSS04.01	2	Tidak Sesuai Standar	Proses belum terdokumentasi secara formal dan belum ada kebijakan toleransi downtime atau sistem pemantauan yang terstandar.	1. Menyusun dokumen analisis risiko dan *business continuity requirement*, yang memuat identifikasi risiko utama serta prioritas keberlangsungan sistem. 2. Menetapkan SLA atau kebijakan resmi terkait toleransi *downtime* layanan. 3. Menyusun prosedur pemantauan sistem secara tertulis, yang melengkapi penggunaan Grafana dengan panduan teknis, tanggung jawab, dan sistem pelaporan.
DSS04.02	3	Tidak Sesuai Standar	Proses belum terdokumentasi secara formal dan belum memiliki rencana pemulihan bencana yang memadai.	1. Menyusun dokumen formal *disaster recovery plan* (DRP) yang mencakup skenario gangguan dan rencana pemulihan layanan JB Class. 2. Mengembangkan dan menstandarkan SOP *backup* data secara menyeluruh, baik untuk database maupun file konfigurasi penting. 3. Mengotomatisasi proses *backup* secara penuh agar tidak hanya bergantung pada proses manual dan memastikan semua komponen sistem dicadangkan.
DSS04.03	3	Tidak Sesuai Standar	Tidak ada simulasi, tidak ada dokumentasi formal, dan belum tersedia siklus evaluasi.	1. Melakukan simulasi dan uji coba formal terhadap rencana pemulihan layanan, untuk memastikan kesiapan teknis dan prosedural dalam menghadapi gangguan. 2. Menyusun dokumentasi rencana pemulihan yang dapat diakses oleh seluruh tim teknis, termasuk langkah-langkah pemulihan, penanggung jawab, serta prosedur alternatif. 3. Menetapkan jadwal evaluasi berkala terhadap rencana kontinuitas, agar tetap relevan dengan kondisi sistem dan potensi risiko terkini.

Proses	*Gap*	Hasil	Keterangan	Rekomendasi
DSS05.01	3	Tidak Sesuai Standar	Proses perlindungan terhadap malware belum dilakukan secara sistematis dan formal. Belum tersedia mekanisme yang melibatkan proteksi aplikasi langsung maupun pemindaian unggahan.	1. Menyusun kebijakan formal perlindungan terhadap malware, termasuk peran dan tanggung jawab tim dalam menjaga keamanan sistem JB Class. 2. Mengimplementasikan fitur pemindaian otomatis terhadap file yang diunggah pengguna untuk mencegah penyebaran malware melalui unggahan. 3. Menyusun prosedur pembaruan keamanan sistem yang terdokumentasi, termasuk jadwal rutin dan mekanisme koordinasi internal oleh tim IT Balai Tekkomdik sebagai pengelola sistem, untuk mengatasi potensi kerentanan keamanan pada platform JB Class.
DSS05.02	1	Sesuai Standar	Sistem telah memenuhi standar minimum untuk keamanan jaringan, meskipun masih bisa ditingkatkan pada sisi monitoring otomatis dan dokumentasi pelengkap.	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.
DSS05.03	2	Tidak Sesuai Standar	Keamanan endpoint belum dijalankan secara formal. Tidak ada enkripsi, pembatasan perangkat, atau deteksi terhadap perangkat yang tidak dikenal.	1. Menyusun kebijakan pengamanan perangkat kerja staf (endpoint), termasuk penggunaan antivirus, pembaruan sistem, dan kontrol akses fisik. 2. Menerapkan sistem enkripsi pada perangkat kerja yang digunakan untuk mengakses sistem JB Class guna melindungi data dari kebocoran atau akses tidak sah. 3. Mengembangkan sistem verifikasi perangkat agar hanya perangkat yang terdaftar atau dikenal yang dapat mengakses akun, demi mencegah akses ilegal.
DSS05.04	2	Tidak Sesuai Standar	Proses belum dilengkapi sistem verifikasi dan autentikasi tambahan, sehingga belum memenuhi standar pengelolaan identitas yang aman.	1. Mengaktifkan autentikasi dua faktor (2FA) untuk akun dengan akses sensitif guna menambah lapisan keamanan dalam sistem login. 2. Menambahkan mekanisme validasi akun, seperti verifikasi email atau OTP, untuk memastikan bahwa pendaftaran dilakukan oleh pihak yang sah.

Proses	*Gap*	Hasil	Keterangan	Rekomendasi
				3. Menyusun SOP pengelolaan akun pengguna, termasuk prosedur aktivasi, pencabutan akses, dan pengelolaan akun siswa yang sudah tidak aktif, prosedur penonaktifan dan penghapusan akses secara terstruktur.
DSS05.05	3	Tidak Sesuai Standar	Sistem belum mencatat insiden secara otomatis, belum ada SOP pelaporan dan tindak lanjut. Hanya struktur tanggung jawab yang sudah berjalan. Tanpa prosedur pelaporan dan pencatatan insiden yang terdokumentasi, organisasi menghadapi risiko keterlambatan dalam mendeteksi dan merespons ancaman yang dapat mengganggu operasional layanan.	1. Menyusun SOP pelaporan dan eskalasi insiden keamanan, termasuk alur pencatatan dan penanganan insiden oleh tim yang bertanggung jawab. 2. Mengembangkan sistem pencatatan insiden keamanan secara otomatis di dalam sistem JB Class untuk mendeteksi login mencurigakan atau aktivitas tidak sah. 3. Menyusun format laporan dan evaluasi pasca-insiden sebagai bagian dari upaya peningkatan keamanan berkelanjutan dan dokumentasi pembelajaran atas insiden sebelumnya.
DSS06.01	3	Tidak Sesuai Standar	Evaluasi menunjukkan bahwa sebagian besar kontrol dan penyesuaian fitur telah dilakukan secara teknis dan praktis, namun belum tertuang dalam dokumentasi formal yang menjadi acuan pengembangan dan pengendalian sistem.	1. Menyusun SOP kontrol proses bisnis utama (seperti input nilai, akses materi, pengiriman tugas) yang menjelaskan alur kerja dan pengaturan hak akses berbasis peran. 2. Menetapkan standar pengujian fitur sebelum rilis, termasuk dokumentasi uji coba dan validasi dari perwakilan pengguna untuk mencegah gangguan fungsi. 3. Mengembangkan mekanisme pencatatan aktivitas pengguna (audit log) untuk memantau perubahan data atau aktivitas penting dalam sistem secara otomatis.
DSS06.02	3	Tidak Sesuai Standar	Sistem belum menerapkan kontrol pemrosesan informasi secara menyeluruh. Belum tersedia audit trail, rollback, atau validasi lanjutan lintas data. Validasi input yang diterapkan saat ini masih bersifat teknis dasar dan belum	1. Mengembangkan fitur audit trail untuk mencatat seluruh perubahan data penting oleh pengguna, termasuk waktu, nilai lama/baru, dan pelaku perubahan. 2. Meningkatkan validasi input dengan menambahkan validasi lintas data atau berbasis logika bisnis, tidak hanya validasi teknis dasar.

Proses	*Gap*	Hasil	Keterangan	Rekomendasi
			mencakup kemampuan mendeteksi kesalahan kontekstual maupun perubahan tidak sah secara otomatis.	3. Menambahkan fitur rollback atau mekanisme koreksi otomatis agar kesalahan input dapat diperbaiki tanpa harus dilakukan secara manual oleh admin.
DSS06.03	2	Tidak Sesuai Standar	Dokumentasi proses sudah tersedia namun belum dalam bentuk formal seperti SOP atau diagram alur proses. Pemantauan masih terbatas pada aspek teknis. Belum ada audit internal dan sistem pengelolaan feedback yang terstruktur.	1. Menyusun dokumentasi alur proses bisnis formal, dalam bentuk SOP atau diagram alur, agar proses operasional memiliki standar yang dapat dievaluasi. 2. Membentuk mekanisme audit internal proses bisnis, minimal secara berkala untuk meninjau kesesuaian pelaksanaan proses dengan ketentuan sistem. 3. Membangun sistem pengumpulan dan pengelolaan umpan balik pengguna, agar masukan dapat terdokumentasi, ditindaklanjuti, dan dijadikan dasar perbaikan.

Tabel 4.31 Hasil Audit dan Rekomendasi Domain MEA

Proses	*Gap*	Hasil	Keterangan	Rekomendasi
MEA01.01	3	Tidak Sesuai Standar	Penetapan indikator dan penanganan performa belum didukung SOP atau kebijakan formal. Evaluasi masih bersifat teknis dan reaktif, belum didukung sistem pemantauan dan laporan terstruktur.	1. Menetapkan indikator sederhana untuk mengukur kinerja sistem, seperti kecepatan akses dan stabilitas layanan, agar penilaian terhadap performa sistem memiliki dasar yang jelas. 2. Mengoptimalkan penggunaan alat monitoring yang sudah tersedia seperti Grafana, agar pemantauan performa sistem dapat dilakukan secara teratur dan data yang dihasilkan lebih mudah dianalisis. 3. Menyusun prosedur penanganan jika terjadi gangguan performa, termasuk langkah-langkah respons dan dokumentasi sederhana agar setiap insiden dapat ditindaklanjuti dengan lebih terarah.
MEA01.02	3	Tidak Sesuai Standar	Proses evaluasi kontrol sudah berjalan secara teknis namun belum terdokumentasi secara formal. Belum tersedia metrik pengukuran, siklus evaluasi berkala, maupun pelaporan	1. Menyusun dokumen formal yang menjelaskan prosedur evaluasi efektivitas kontrol sistem, termasuk tanggung jawab dan alur pelaksanaan evaluasi. 2. Menetapkan metrik evaluasi kontrol yang terukur (kuantitatif) untuk menilai efektivitas kontrol secara objektif dan konsis

			sistematis. Perlu penguatan dokumentasi, penetapan metrik, dan prosedur audit untuk mencapai efektivitas pengendalian yang berkelanjutan.	3. Membuat siklus evaluasi kontrol secara berkala (bulanan atau triwulanan), serta mendokumentasikan hasilnya sebagai dasar untuk perbaikan dan peningkatan sistem secara berkelanjutan.
MEA01.03	3	Tidak Sesuai Standar	Proses pemantauan kepatuhan regulasi eksternal belum terdokumentasi dan belum sistematis. Belum ada audit eksternal maupun dokumentasi perubahan sistem berbasis regulasi. Perlu peningkatan dalam bentuk penyusunan kebijakan eksplisit, pemantauan berkala, audit regulasi, dan prosedur dokumentasi perubahan berbasis regulasi.	1. Menyusun kebijakan dan SOP internal untuk menyesuaikan sistem JB Class terhadap regulasi eksternal seperti UU PDP dan kebijakan dari Dinas Pendidikan. 2. Mendorong pelaksanaan audit kepatuhan secara berkala sesuai arahan atau permintaan dari instansi terkait, serta menyusun dokumentasi hasil audit sebagai bahan evaluasi dan tindak lanjut. 3. Menyusun log perubahan sistem yang terdorong oleh regulasi baru, mencakup waktu perubahan, alasan perubahan, dan dampak terhadap layanan, agar tercipta jejak dokumentasi yang rapi dan dapat diaudit.
MEA02	3	Tidak Sesuai Standar	Proses pengendalian internal belum dijalankan secara sistematis. Tidak tersedia dokumentasi prosedur, pemantauan log aktivitas, ataupun siklus audit dan evaluasi formal. Dibutuhkan kebijakan resmi dan sistem pelaporan untuk menjamin integritas kontrol serta perbaikan berkelanjutan.	1. Menyusun SOP pengendalian internal yang mencakup pemantauan aktivitas pengguna, pelaporan pelanggaran, serta tindak lanjut perbaikan. 2. Mengembangkan fitur audit log yang dapat mencatat aktivitas pengguna secara otomatis untuk meningkatkan transparansi dan deteksi dini terhadap aktivitas mencurigakan. 3. Menyusun dan menjadwalkan audit internal secara berkala guna mengevaluasi efektivitas kontrol sistem dan mendukung perbaikan berkelanjutan berdasarkan hasil audit.
MEA03	3	Tidak Sesuai Standar	Proses kepatuhan terhadap persyaratan eksternal belum berjalan secara formal dan terdokumentasi. Meskipun terdapat pemenuhan prinsip	1. Menyusun daftar regulasi dan kebijakan eksternal yang relevan, seperti ISO 27001, UU ITE, dan kebijakan dari Dinas Pendidikan, sebagai acuan formal untuk pengembangan dan evaluasi sistem. 2. Menyusun mekanisme verifikasi internal untuk memastikan bahwa sistem telah menyesuaikan diri terhadap regulasi yang berlaku, serta

			keamanan dasar, sistem belum memiliki sertifikasi atau audit resmi, tidak tersedia daftar regulasi formal, verifikasi regulasi tidak terdokumentasi, serta belum ada kebijakan privasi yang ditampilkan kepada pengguna.	mencatat setiap perubahan sistem yang dilakukan sebagai bagian dari proses kepatuhan.
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.	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.

Berdasarkan Tabel 4.30, pada domain DSS terdapat 13 proses yang dievaluasi, dengan hasil 1 proses dinyatakan sesuai standar dengan level 1 dan 12 proses belum memenuhi standar. Sementara itu, pada Tabel 4.31 domain MEA, dari total 6 proses yang dievaluasi, seluruhnya belum memenuhi standar. Hasil temuan ini mencerminkan bahwa sistem JB Class masih menghadapi banyak kekurangan, baik dalam hal pelaksanaan prosedur operasional, pengelolaan layanan, dokumentasi aktivitas, maupun aspek monitoring dan pengendalian yang seharusnya dilakukan secara berkala dan terdokumentasi. Secara keseluruhan, sistem belum berjalan secara optimal dan belum sepenuhnya memenuhi prinsip tata kelola teknologi informasi berdasarkan kerangka kerja COBIT 2019. Oleh karena itu, diperlukan langkah perbaikan yang mencakup penyusunan kebijakan formal, penguatan dokumentasi, serta pelaksanaan evaluasi dan audit berkala untuk meningkatkan kapabilitas sistem secara menyeluruh.