

BAB IV

HASIL DAN PEMBAHASAN

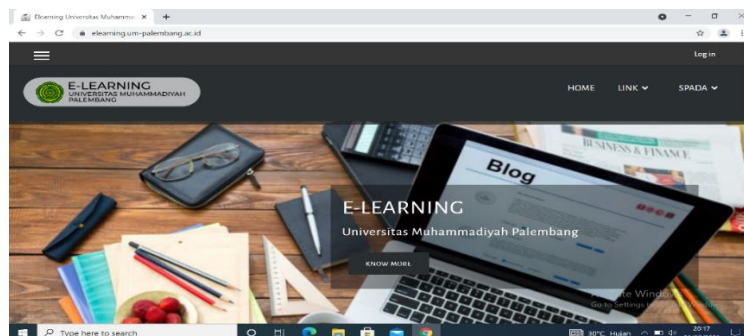
4.1 Gambaran Umum

4.1.1 Sejarah *E-Learning* Universitas Muhammadiyah Palembang

Universitas Muhammadiyah Palembang sebagai salah satu penyelenggara kegiatan akademik dan sekaligus institusi pendidikan, tentu menginginkan kegiatan akademik dengan baik dan lancar yang nantinya mampu mencetak generasi muda yang berprestasi dan dapat diandalkan. Upaya meningkatkan mutu pendidikan dilakukan dengan memberdayakan seluruh potensi yang mendukung proses pembelajaran yang efektif dan efisien guna terciptanya generasi penerus bangsa yang kompetitif. Sejak tahun 2017 Universitas Muhammadiyah Palembang mengimplementasikan *E-Learning*. *E-Learning* merupakan sarana pendukung layanan pendidikan berbasis web yang digunakan dalam proses pembelajaran yang digunakan oleh dosen dan mahasiswa. *E-Learning* Universitas Muhammadiyah Palembang dikelola oleh UPT-IT UMP dan dapat diakses melalui *website* <https://elearning.um-palembang.ac.id>.

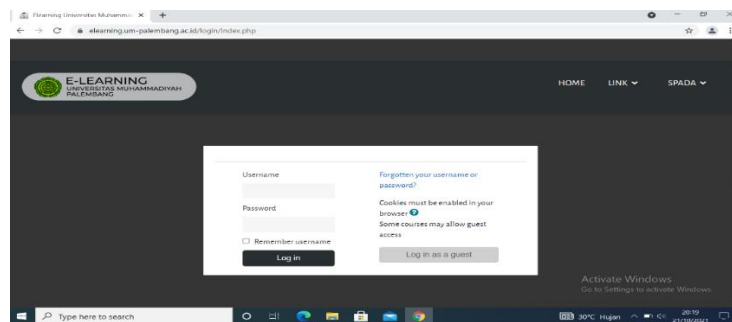
Berikut adalah tampilan *E-Learning* Universitas Muhammadiyah Palembang:

a. Halaman depan *E-Learning* UMP:



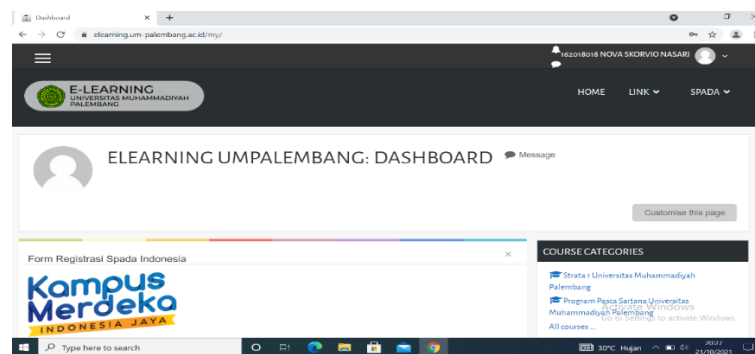
Gambar 4.1 Halaman depan *E-Learning* UMP

b. Halaman *login E-Learning UMP*:



Gambar 4.2 Halaman *login E-Learning UMP*

c. Halaman *dashboard E-Learning UMP*:



Gambar 4.3 Halaman *dashboard E-Learning UMP*

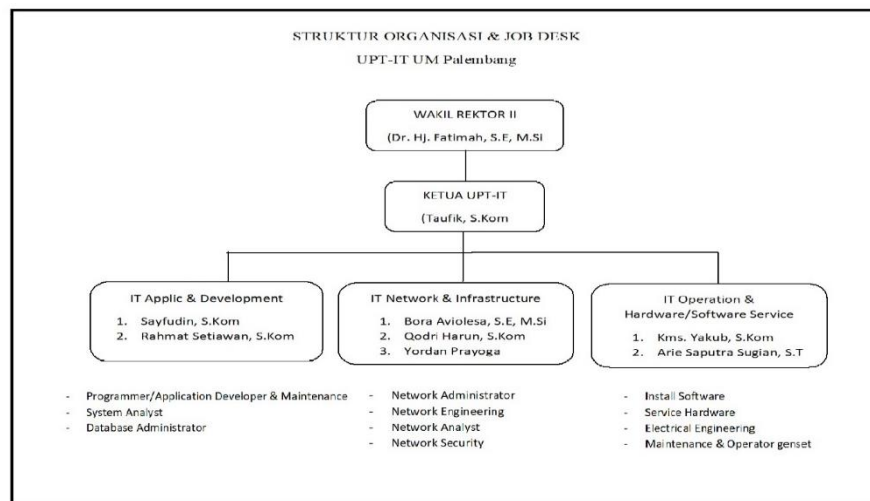
4.2 Pemeriksaan Pendahuluan

Pada tahapan pemeriksaan pendahuluan, auditor melakukan identifikasi terhadap infrastruktur TI yang digunakan, memahami struktur organisasi, serta profil responden yang akan menjadi *auditee* pada audit sistem informasi ini.

4.2.1 Struktur Organisasi

Struktur organisasi yang menunjukkan kerangka dan susunan perwujudan pola hubungan diantara setiap fungsi bahwa ada pembagian kerja dan bagaimana fungsi atau kegiatan-kegiatan berbeda yang di koodinasikan. Struktur organisasi pada UPT-IT UMP dipimpin oleh Ibu Dr. Hj. Fatimah, S. E, M. Si dan beberapa

staf lainnya yang kegiatannya berbeda-beda. Berikut Gambar 4.3 struktur organisasi pada UPT-IT UMP:



Gambar 4.4 Struktur Organisasi

4.2.2 Profil Responden

Survey dilakukan dengan kuesioner 4 orang anggota UPT-IT UMP sebagai orang yang bertanggung jawab untuk *capability level*. Metode penyebaran kuesioner dilakukan dengan mendampingi tiap-tiap responden dalam menjawab pernyataan pada kuesioner. Semua responden berjenis laki-laki dan berlatar belakang pendidikan D3, S1 dan S2 rentang usia 25-55 tahun.

4.2.3 Infrastruktur dalam Pemrosesan E-Learning UMP

Teknologi dan fasilitas (*hardware, operating systems, database management system, networking, multimedia* dan lingkungan pendukung lainnya) yang dapat memproses aplikasi meliputi *Hardware* pada UMP yakni *Harddisk* 500 GB, *Ram* 2 GB, *Corei* 3, *CPU*, *Mouse*. *Software* pada UMP yakni *Windows* 7, *Chrome*, *Xampp*. *Basis data* pada UMP yakni *My SQL*. Jaringan komputer pada UMP yakni *Telkom* Kecepatan 300 Mbps.

4.3 Pemeriksaan Terperinci

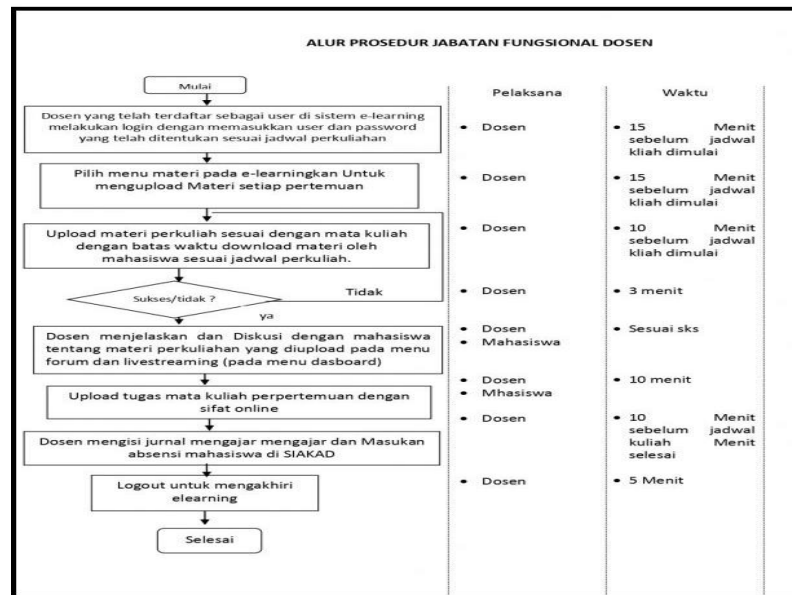
Pemeriksaan terperinci adalah di mana peneliti memutuskan untuk melanjutkan audit terhadap sistem informasi *E-Learning* UMP. Tahap ini dilakukan setelah tahap pemeriksaan pendahuluan.

Dalam tahap ini peneliti berupaya mendapatkan informasi secara lebih mendalam untuk memahami pengendalian yang diterapkan dalam sistem *E-Learning* UMP. Informasi yang didapat dari tahap ini adalah standar operasional prosedur pelaksanaan pembelajaran pada *E-Learning* UMP antara lain:

1. Urutan prosedur pelaksanaan pembelajaran Dosen
 - a. Dosen yang telah mendaftar sebagai user di sistem *e-learning* melakukan login dengan memasukkan *user* dan *password* yang telah ditentukan sesuai jadwal perkuliahan
 - b. Pilih menu materi pada *e-learning* untuk mengupload materi setiap pertemuan
 - c. Upload materi perkuliahan sesuai dengan mata kuliah dengan batas waktu download materi oleh mahasiswa sesuai jadwal perkuliahan
 - d. Cek materi apa bisa didownload atau tidak dengan cara mendownload materi tersebut
 - e. Dosen menjelaskan dan melakukan diskusi dengan mahasiswa tentang materi perkuliahan yang diupload pada menu forum dan *livestreaming* (pada menu *dashboard*)
 - f. Upload tugas mata kuliah pertemuan dengan sifat *online*
 - g. Dosen mengisi jurnal mengajar dan memasukan absensi mahasiswa di SIMAKAD

h. *Log out* untuk mengakhiri *e-learning*

2. Bagan alir proses pembelajaran *e-learning* dosen

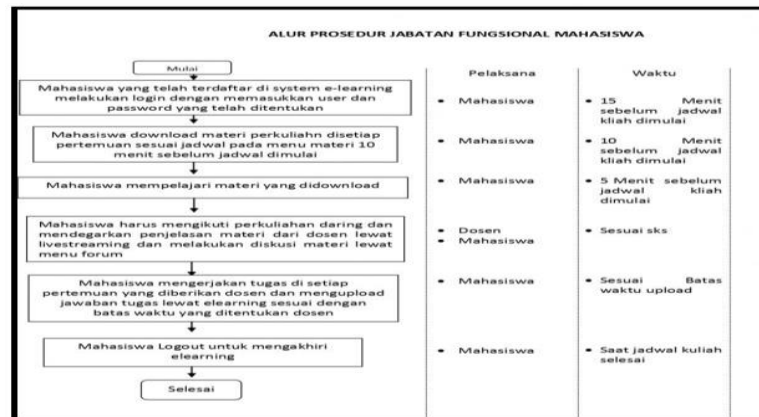


Gambar 4.5 Diagram alir proses pembelajaran *E-Learning* dosen

3. Urutan prosedur pembelajaran mahasiswa

- Mahasiswa yang telah mendaftar di sistem *e-learning* melakukan login dengan memasukkan *user* dan *password* yang telah ditentukan
- Mahasiswa *download* materi perkuliahan disetiap pertemuan sesuai jadwal pada menu materi 10 menit sebelum jadwal dimulai
- Mahasiswa mempelajari materi yang didownload
- Mahasiswa harus mengikuti perkuliahan daring dan mendengarkan penjelasan materi dari dosen lewat *livestreaming* dan melakukan diskusi materi melalui menu forum
- Mahasiswa mengerjakan tugas di setiap pertemuan yang diberikan dosen dan mengupload jawaban melalui *e-learning* sesuai dengan batas waktu yang ditentukan dosen
- Log out* untuk mengakhiri *e-learning*

4. Bagan alir proses pembelajaran mahasiswa



Gambar 4.6 Bagan alir proses pembelajaran *E-Learning* mahasiswa

Selanjutnya dari tahap ini peneliti mendapatkan informasi mengenai pengguna sistem informasi *E-Learning* UMP yaitu seluruh mahasiswa yang berjumlah 8.660 dan dosen yang berjumlah 446. Berdasarkan hasil pemeriksaan terperinci, maka peneliti memutuskan untuk melanjutkan audit terhadap sistem informasi *E-Learning* UMP.

4.4 Pengujian Kesesuaian

Pengujian kesesuaian adalah tahapan dimana peneliti melakukan wawancara untuk mengetahui apakah proses-proses teknologi informasi yang terdapat pada COBIT 5 telah diterapkan atau sebaliknya pada tatakelola *E-Learning* UMP.

Berikut adalah hasil kesesuaian pada *E-Learning* UMP berdasarkan Domain DSS, dapat dilihat pada Tabel 4.1 berikut:

Tabel 4.1 Hasil Kesuaian pada *E-Learning* UMP berdasarkan Domian DSS COBIT 5

Subdomain DSS	Detailed Control Objectives	Pernyataan	Penerapan <i>E-Learning</i> UMP	Sesuai atau Tidak Sesuai
DSS01 (<i>Manage Operations</i>)	DSS01.02	Mengelola layanan TI yang dialihdayakan	Penegelolaan keamanan pemrosesan layanan TI sudah sesuai dengan kontrak SLA dan dilakukan pemantauan agar tidak terjadi pelanggaran, serta pengintegrasian proses manajemen TI juga telah dilakukan sesuai kebutuhan system.	Sesuai
	DSS01.04	Mengelola lingkungan	Telah dilakukan pengelolaan lingkungan untuk mengurangi dampak ancaman lingkungan pada fasilitas TI, serta telah dilakukan pemantauan dan pemeliharaan secara proaktif	Sesuai
	DSS01.05	Mengelola Fasilitas	Pengelolaan, pemeriksaan dan perindungan fasilitas TI telah dilakukan sesuai dengan prosedur SOP yang ada	Sesuai
DSS02 (<i>Manage Service Requests and Incidents</i>)	DSS02.01	Menentukan insiden dan layanan permintaan masalah	Dilakukan penetapan klasifikasi masalah dan permintaan layanan serta melakukan penanganan masalah sesuai dengan jenis insiden	Sesuai
	DSS02.02	Merekam, mengklasifikasikan dan memprioritaskan permintaan dan insiden	Pengklasifikasian dan pemrioritasan permintaan layanan dan masalah dilakukan berdasarkan memo/log dari sistem	Sesuai
	DSS02.03	Memverifikasi, menyetujui dan memenuhi permintaan layanan	Memverifikasi, meyetujui dan memenuhi permintaan layanan, maka dilakukan rapat umum yang dilakukan oleh bagian IT	Sesuai
	DSS02.04	Menyelidiki, mendiagnosa dan mengalokasikan insiden	Dalam menyelidiki, mendiagnosa, mengalokasikan masalah dapat dideteksi dari log	Sesuai

Tabel 4.1 Hasil Kesesuaian pada e-Learning UMP berdasarkan Domain DSS COBIT 5 Lanjutan

Subdomain DSS	Detailed Control Objectives	Pernyataan	Penerapan E-Learning UMP	Sesuai atau Tidak Sesuai
	DSS02.05	Menyelesaikan dan memulihkan insiden	Resolusi yang diterapkan berdasarkan jenis masalah	Sesuai
	DSS02.06	Menutup permintaan layanan dan insiden	Jika permintaan layanan telah terpenuhi serta dilakukan monitoring bagaimana tindakan terhadap insiden yang ada maka dilakukan penutupan	Sesuai
	DSS02.07	Melacak status dan menghasilkan laporan	Dilakukan pemantauan sampai sistem kembali normal.	Sesuai
DSS03 (<i>Manage Problems</i>)	DSS03.01	Mengidentifikasi dan mengklasifikasi masalah	Identifikasi masalah dilakukan melalui log dan dilakukan pengklasifikasian masalah oleh kelompok berdasarkan job desk	Sesuai
	DSS03.02	Menyelidiki dan mendiagnosis masalah	Menyelidiki dan mendiagnosis masalah dengan dilakukan perbandingan data masalah dengan log	Sesuai
	DSS03.03	Meningkatkan kesalahan yang diketahui	Penyelesaian masalah yang diketahui dan diberikan solusi dengan mempertimbangkan biaya dan manfaat	Sesuai
	DSS03.04	Menyelesaikan dan menutup masalah	Jika masalah telah diketahui maka secepatnya dilakukan perbaikan dan penutupan masalah, serta dilakukan penginformasian kepada pihak pengelola bagian yang bersangkutan	Sesuai
	DSS03.05	Melakukan proaktif manajemen masalah	Diadakan pertemuan untuk mengkomunikasikan terkait perubahan jika masalah yang terjadi signifikan, namun jika tidak maka penginformasian hanya dilakukan via <i>online</i>	Sesuai
DSS04 (<i>Manage Continuity</i>)	DSS04.01	Menentukan keberlangsungan kebijakan bisnis, tujuan dan ruang lingkup	Mengidentifikasi proses bisnis, aktivitas layanan berdasarkan sistem, dan adanya kebijakan yang dispakati untuk keberlangsungan dan pencapaian tujuan bisnis	Sesuai
	DSS04.02	Mempertahankan strategi kontinuitas	Memasang alat pencadangan data untuk mempertahankan kontinuitas proses bisnis	Sesuai

Tabel 4.1 Hasil Kesesuaian pada e-Learning UMP berdasarkan Domain DSS COBIT 5 Lanjutan

Subdomain DSS	Detailed Control Objectives	Pernyataan	Penerapan E-Learning UMP	Sesuai atau Tidak Sesuai
	DSS04.03	Mengembangkan dan mengimplementasikan respon keberlangsungan bisnis	Adanya tindak tanggap insiden dan dilakukan pemantauan secara berkala terhadap proses bisnis dan selalau menjaga integritas informasi	Sesuai
	DSS04.04	Latihan, tes dan ulasan BCP	Belum ada latihan, tes dan ulasan BCP	Tidak sesuai
	DSS04.05	Meninjau, mempertahankan dan meningkatkan rencana yang berkesinambungan	Belum dilakukan	Tidak sesuai
	DSS04.06	Melakukan pelatihan perencanaan berkesinambungan	Belum ada pelatihan	Tidak sesuai
	DSS04.07	Mengelola pengaturan cadangan	Dilakukan <i>backup</i> sistem dan data secara berkala	Sesuai
	DSS04.08	Melakukan peninjauan pasca dimulainya kembali	Dilakukan pengecekan dan <i>maintenance</i> masalah dan dijadikan bahan acuan agar masalah yang sama tidak terjadi lagi	Sesuai
DSS05 (<i>Manage Security Services</i>)	DSS05.01	Melindungi dari <i>malware</i>	Mengaktifkan alat perlindungan <i>malware</i> , melakukan filter lalu lintas jaringan, dan pengkomukasian bahaya <i>malware</i> kepada pengguna	Sesuai
	DSS05.02	Mengelola jaringan dan keamanan konektifitas	Hak akses hanya diberikan izin kepada perangkat resmi yang memiliki akses kata sandi dan menrapakan alat pemfilter jaringan seperti firewall untuk mengontrol lalu lintas jaringan	Sesuai
	DSS05.03	Megelola keamanan titik akhir	Belum dilakukan pengelolaan keamanan titik akhir	Tidak sesuai
	DSS05.04	Mengelola identitas pengguna dan akses logis	Hak akses user diberikan secara unik dan dilakukan penginformasian kepada user untuk menjaga hak akses masing-masing agar tidak disalahgunakan.	Sesuai

Tabel 4.1 Hasil Kesesuaian pada e-Learning UMP berdasarkan Domain DSS COBIT 5 Lanjutan

Subdomain DSS	Detailed Control Objectives	Pernyataan	Penerapan E-Learning UMP	Sesuai atau Tidak Sesuai
	DSS05.05	Mengelola akses fisik untuk asset TI	Dilakukan pengawasan terhadap pemberian akses fasilitas komputasi	Sesuai
	DSS05.06	Mengelola dokumen sensitif dan perangkat keluaran	Ada prosedur dalam pengelolaan dokumen sensitif dan perangkat keluaran	Sesuai
	DSS05.07	Memantau infrastruktur untuk peristiwa yang berhubungan dengan keamanan	Memasang alat pemantauan berupa mikrotik	Sesuai
DSS06 (<i>Manage Business Process Controls</i>)	DSS06.01	Sejajarkan aktivitas kontrol yang disematkan dalam proses bisnis dengan tujuan perusahaan	Aktivitas kontrol proses bisnis seperti identifikasi, dokumentasi dilakukan melalui alat pencadangan data dan pemantauan kegiatan pengendalian proses bisnis melalui log	Sesuai
	DSS06.02	Kontrol pemrosesan informasi	Memastikan bahwa pemrosesan layanan informasi valid, lengkap, akurat, tepat waktu dan aman. Dan dilakukan pengiriman ulang data jika salah input data tanpa mengurangi otorisasi data asli	Sesuai
	DSS06.03	Mengelola peran, tanggung jawab, hak akses dan level otoritas	Mengalokasikan peran tanggung jawab, dan wewenang berdasarkan job desk. Serta mengalokasikan hak akses dan hak istimewa berdasarkan peran dan tanggung jawab	Sesuai
	DSS06.04	Kelola kesalahan dan pengecualian	Mengelola kesalahan informasi dengan melakukan tindakan perbaikan secara tanggap dan dilakukan koordinasi dengan ketua IT untuk segera menganalisis penyebab masalah dan menentukan solusi	Sesuai

Dari tabel di atas dapat dilihat hasil tingkat kesesuaian proses TI yang terdapat pada setiap subdomain DSS yaitu sesuai dan tidak sesuai. Setiap proses TI yang terdapat pada setiap subdomain dapat dikatakan sesuai apabila proses TI E-

Learning yang ada pada UMP sudah sesuai dengan proses TI yang ada pada subdomain DSS yang ada pada COBIT 5. Begitupun sebaliknya dikatakan tidak sesuai apabila proses TI *E-Learning* yang ada pada UMP belum sesuai dengan proses TI yang ada pada subdomain DSS yang ada pada COBIT 5.

4.5 Pengujian Kebenaran

Pada tahap pengujian kebenaran, auditor melakukan penilaian secara umum atas hasil pengujian atau hasil temuan audit yang telah dilakukan. Pada tahap ini peneneliti melakukan perhitungan *Capability Level*.

4.5.1 Deskripsi Hasil Perhitungan *Capability Level*

Hasil audit yang telah dilakukan oleh peneliti terhadap COBIT 5 berdasarkan hasil jawaban kuesioner yang telah diberikan oleh responden menggunakan *capability level* sebagai parameter pengukuran untuk menentukan suatu nilai terhadap level yang mampu dicapai oleh suatu organisasi. *Capability level* untuk pengelolaan dan pengendalian pada proses teknologi informasi didasarkan pada metode evaluasi organisasi sehingga dapat mengevaluasi sendiri dari tingkat 0 (*Incomplete Process*), tingkat 1 (*Performed Process*), tingkat 2 (*Manage Process*), tingkat 3 (*Established Process*), tingkat 4 (*Predictable Process*), dan tingkat 5 (*Optimising Process*). Penilaian tingkat kapabilitas dilakukan mencari nilai rata-rata dari hasil kuesioner pada setiap subdomain yang ada pada domain DSS yaitu DSS01 (*Manage Operation*), DSS02 (*Manage Service Requests and Incidents*), DSS03 (*Manage Problems*), DSS04 (*Manage Continuity*), DSS05 (*Manage Security Services*), dan DSS06 (*Manage Business Process Controls*).

Berikut merupakan contoh perhitungan yang diambil pada subdomain *manage operations* dengan jumlah responden 3 orang yang bertanggung jawab dan rekapitulasi jumlah level yang ada pada *manage operations* sebagai berikut:

Tabel 4.2 Rekapitulasi Manage Operations

Manage Operations		
Level Capability	Proses TI	Responden
0	0	- Ketua UPT-IT - IT Applic & Development - IT Operation Hardware - Software Service
1	0	
2	1	
3	1	
4	1	
5	0	

Dari table diatas diketahui *Manage Operations* jumlah proses yang berada pada level 2 yaitu 1 (DSS01.02), level 3 yaitu 1 (DSS01.04), dan level 4 yaitu 1 (DSS01.05). Adapun jumlah pertanyaan yang ada pada *manage operations* yaitu berjumlah 3 pertanyaan. Maka indeks *capability level* dapat dilihat dipenjelasan berikut:

$$\text{Indeks Capability} = \frac{(0 * y_0) + (1 * y_1) + (2 * y_2) + \dots (5 * y_5)}{z}$$

$$\text{Indeks} = \frac{(2*1)+(3*1)+(4*1)}{3}$$

$$\text{Indeks} = \frac{2+3+4}{3} = 3$$

Maka hasil perhitungan capability level nilai dari subdomain *Manage Operation* yaitu 3 (*Established*).

Semakin tinggi *capability level* maka semakin baik proses pengelolaan dan pengendalian pada proses teknologi informasi dalam mengetahui keberadaan persoalan yang ada dan bagaimana menentukan prioritas peningkatan sehingga organisasi akan dapat mengenali sebagai deskripsi kemungkinan keadaan saat ini.

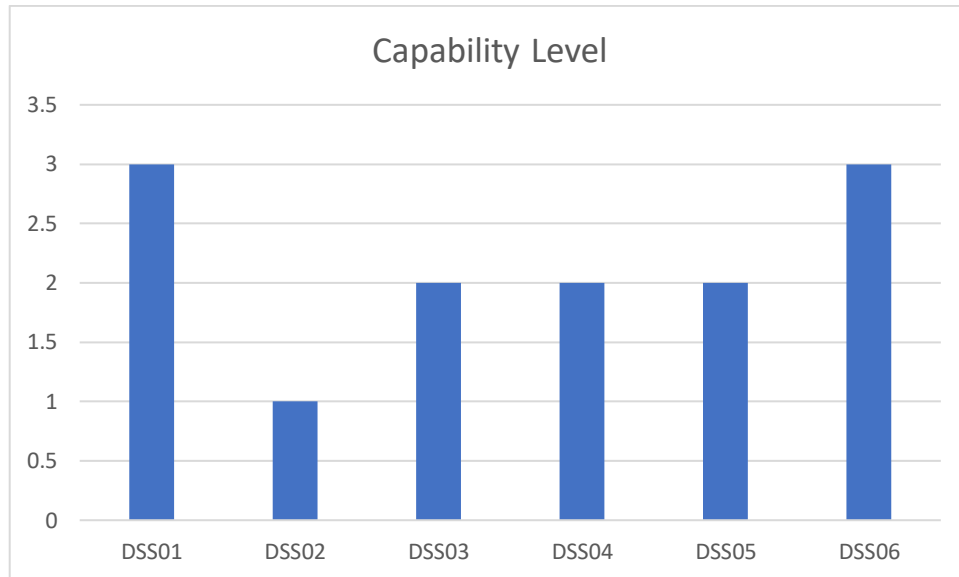
Cara perhitungan diatas berlaku sama pada setiap subdomain yang ada pada domain DSS dalam menentukan nilai kapabilitas. Untuk melihat rekapitulasi hasil perhitungan subdomain dari DSS dapat dilihat pada Tabel 4.3 berikut:

Tabel 4.3 Rekapitulasi Hasil Perhitungan *Subdomain*

No	Sub Domain	<i>IT Proses</i>	Hasil Perhitungan	Tingkat <i>Capability Level</i>	Keterangan
1	DSS01	<i>Manage Operations</i>	3	3	<i>Established</i>
2	DSS02	<i>Manage Service Requests and Incidents</i>	1,28	1	<i>Performed</i>
3	DSS03	<i>Manage Problems</i>	2,4	2	<i>Managed</i>
4	DSS04	<i>Manage Continuity</i>	2	2	<i>Managed</i>
5	DSS05	<i>Manage Security Services</i>	1,57	2	<i>Managed</i>
6	DSS06	<i>Manage Business Process Controls</i>	3,25	3	<i>Established</i>

Dari hasil perhitungan yang didapat pada tabel di atas, maka dilakukan pembulatan untuk memudahkan mencari kondisi terkini berdasarkan *Capability Level* yang telah ditetapkan dan telah dijelaskan pada bab sebelumnya. Berdasarkan jawaban responden setiap pernyataan yang diberikan. Secara umum rata-rata jawaban responden untuk keseluruhan pernyataan dengan domain *Deliver Service and Support* adalah antara 1,28 sampai 3,25 atau Level 1 sampai 3.

Setelah dilakukan perhitungan *capability level* pada setiap sub domain tersebut digambarkan dalam sebuah grafik. Dapat dilihat pada Gambar 4.7 sebagai berikut:



Gambar 4.7 Grafik Subdomain Responden

Dari grafik diatas dapat dilihat bahwa kondisi *subdomain* dengan nilai tertinggi berada pada level 3 yaitu domain *Manage Business Process Controls* dan dengan nilai terendah pada level 1 yaitu *Manage Service Request and Incidents*. Hal ini menunjukkan bahwa proses-proses tersebut telah diimplementasikan dengan baik meski tetap harus dijaga dan ditingkatkan lagi.

Dari Gambar 4.7 diketahui pada domain DSS terdapat 6 subdomain dengan nilai pada masing-masing subdomain yan berada pada level 1 yaitu 1, level 2 yaitu 3, dan level 3 yaitu 2. Maka indeks *capability level* dapat dilihat dipenjelasan berikut:

$$Capability\ level = \frac{(1*1)+(2*3)+(3*2)}{6} = 2,16$$

Dari hasil perhitungan diatas maka dapat ditarik kesimpulan bahwa *capability level* yang diperoleh *E-Learning* UMP yaitu 2,16 atau berada pada level 2 (*Manage*).

4.6 Rekomendasi

Pemberian rekomendasi merupakan hal yang penting dalam proses menentukan sebuah keputusan. Rekomendasi diimplementasikan dengan menggunakan bahasa yang mudah dipahami. Dengan adanya rekomendasi dalam audit siste informasi ini, bertujuan untuk memperbaiki mekanisme sistem dari aspek proses teknologi informasi menuju tercapainya tujuan, sasaran, strategi organisasi berdasarkan tingkat keabilitas.

4.6.1 *Deliver Service and Support*

Berdasarkan pengumpulan data dengan cara menyebarkan kuesioner, wawancara, dan observasi yang telah dilakukan penulis, maka dilakukan perhitungan *capability level* tata kelola teknologi informasi pada *E-Learning* UMP saat ini pada domain DSS berada pada tingkat keabilitas 2 (*managed*) dengan nilai 2,16. Hal ini menunjukkan bahwa proses yang diimplementasikan mencapai tujuan prosesnya, adanya sebuah pengukuran mengenai pencapaian tujuan dari suatu proses yang berhasil dicapai dan tidak terdapat bukti yang dapat dipertanggungjawabkan. Untuk itu penulis melihat kesesuaian antara jawaban responden dengan data dan bukti yang ada, setelah melakukan kesesuaian tersebut maka diperoleh hasil dari audit yang menyatakan bahwa proses pelayanan TI, dukungan pelayanan TI termasuk pemberian layanan, pengelolaan keamanan dan keberlangsungan proses bisnis, dukungan layanan terhadap pengguna, serta pengelolaan data dan fasilitas operasional TI sudah diimplementasikan dan mencapai tujuan prosesnya dan telah dikelola berdasarkan peran dan tanggungjawab. Namun belum adanya kesadaran akan pentingnya laporan atau bukti terhadap pengelolaan layanan dan insiden, serta belum adanya kesadaran akan

pelatihan personal untuk meningkatkan dan mengembangkan potensi kerja guna untuk meningkatkan kemampuan personal dan dapat meningkatkan pengelolaan TI. Oleh karena itu peneliti memberikan rekomendasi sebagai acuan perbaikan dan peningkatan kualitas sistem. Pada domain DSS ini terdapat 6 *IT Process* yaitu DSS01, DSS02, DSS03, DSS04, DSS05, DSS05.

4.6.1.1 DSS01 *Manage Operation*

Dari hasil *capability level* subdomain *Manage Operation* berada pada level 3 (*Established*) yaitu proses pengelolaan yang telah dijelaskan sebelumnya sekarang diimplementasikan dengan menggunakan proses yang didefinisikan yang mampu mencapai hasil prosesnya. Pada UMP kegiatan pengelolaan layanan TI, pengelolaan lingkungan dan fasilitas TI telah dilakukan sesuai dengan prosedur operasi standar yang telah ditentukan sebelumnya, dilakukan pemantauan serta pemeliharaan. Namun belum adanya perencanaan audit independent terhadap penyedia layanan *outsourcing* dan belum adanya fasilitas pelatihan terhadap personel pengelolaan fasilitas TI.

Berikut Tabel 4.4 dapat dilihat keadaan tata kelola subdomain DSS01 *Manage Operation*:

Tabel 4.4 Keadaan Tata Kelola Saat ini DSS01

Control Objectives	Keadaan Tata Kelola Saat Ini
DSS01.02	Sudah ada kerjasama dengan pihak ketiga, penyedia layanan layanan TI dan sudah mematuhi kontrak sesuai dengan prosedur yang disepakati dengan pihak ketiga, serta pengintegrasiaan proses manajemen telah sesuai dengan kebutuhan sistem. Namun belum ada perencanaan audit independent.
DSS01.04	Untuk bentuk pemantauan sudah terdapat cctv disetiap ruangan dan untuk meminimalkan dampak yang terjadi dari ancaman lingkungan yang dapat menyebabkan kehilangan data, maka UMP bekerjasama dengan pihak layanan penyimpanan data. namun belum ada alat pendeteksi ancaman lingkungan dan alarm lingkungan.
DSS01.05	Dalam pengelolaan fasilitas TI terdapat alat pencegah kebakaran berupa racun api, dan untuk mendukung keberlangsungan bisnis pada saat pemadaman listrik terdapat genset dan UPS. Memastikan

	keamanan dan keselamatan pegawai dan fasilitas ti yang digunakan telah sesuai aturan, namun belum ada pelatihan K3.
--	---

Pada hasil temuan audit keadaan tata kelola teknologi informasi terhadap setiap variabel pada tingkat kapabilitas *Manage Opreation* saat ini pada organisasi berada pada tingkat kematangan 3 (*Established*) dengan nilai 3 dapat dilihat pada Tabel 4.3 dan sangat perlu untuk rekomendasi. Untuk rekomendasi pada domain *manage operation* ini mengacu pada proses teknologi informasi yang terdapat pada pedoman COBIT 5 *Enabling Processes* (ISACA, 2012, p. 174). Adapun proses pada domain *manage operation* ini yaitu mengkoordinasikan dan melaksanakan kegiatan dan prosedur operasional diperlukan dalam memberikan layanan TI internal dan *outsourcing*, termasuk pelaksanaan prosedur operasi standar yang telah ditentukan dan kegiatan pemantauan yang diperlukan. Sehingga rekomendasi pada domain *manage operation* ini dapat dilihat pada tabel 4.5 berikut:

Tabel 4.5 Rekomendasi DSS01

Control Objectives	Rekomendasi
DSS01.02	Perlu dilakukannya pengukuran secara independent dengan pihak ketiga penyedia layanan, agar dapat memaksimalkan proses operasi sistem dan mencapai hasil proses yang maksimal
DSS01.04	Perlu adanya alat yang dapat mendeteksi ancaman dan perlu dipasangnya alam lingkungan untuk meminimalisir dampak yang bisa merugikan organisasi
DSS01.05	Mencari ilmu pengetahuan dan informasi mengenai K3 memang bisa dilakukan dimana saja baik melalui individu ataupun media internet. Namun, untuk meningkatkan performa pengetahuan dan keterampilan keselamatan kerja karyawan maka perlu dilakukannya pelatihan k3.

Berdasarkan tabel rekomendasi di atas maka dapat disimpulkan bahwa UMP secara keseluruhan dapat berkembang lebih baik lagi dengan meningkatkan pelayanan TI yang dialihdayakan, memasang alat pendeteksi ancaman lingkungan untuk memaksimalkan dalam pengelolaan lingkungan, dan perlu diadakanya pelatihan K3 untuk lebih membekali karyawan dalam mengelola lingkungan TI.

4.4.1.2 DSS02 *Manage Service Request and Incidents*

Dari hasil *capability level* subdomain *Manage Service Request and Incident* berada pada level 1 (*Performed*) yaitu proses yang diimplementasikan mencapai tujuan prosesnya, adanya sebuah pengukuran mengenai pencapaian tujuan dari suatu proses yang berhasil dicapai dan tidak terdapat bukti yang dapat dipertanggungjawabkan. Pada UMP kegiatan menanggapi insiden dan permintaan layanan, serta menangani secara tepat waktu. Namun belum dilakukan pencatatan permintaan insiden dan laporan terhadap penanganan insiden.

Berikut Tabel 4.6 dapat dilihat keadaan tata kelola subdomain DSS02 *Manage Service Request and Incidents*:

Tabel 4.6 Keadaan Tata Kelola Saat ini DSS02

Control Objectives	Keadaan Tata Kelola Saat Ini
DSS01.01	Proses menentukan skema klasifikasi layanan permintaan dan insiden dan kriteria pendaftaran masalah dikomunikasikan kepada pengguna pada rapat berkala
DSS02.02	Pengklasifikasian dan pemrioritasan permintaan layanan dan insiden hanya dilakukan berdasarkan log aktifitas yang didapat dari pengguna sistem.
DSS02.03	Adanya rapat umum yang dilakukan bagian TI untuk membahas mengenai permintaan layanan dan insiden yang diajukan oleh user.
DSS02.04	Penyelidikan dan pendiagnosian masalah dilakukan dengan melihat log aktifitas untuk menentukan penyebab dari insiden. Namun belum ada ahli khusus yang dilibatkan dalam mengelola insiden.
DSS02.05	Insiden yang diterima kemudia diberi resolusi sesuai denga jenis masalah yang terjadi. Namun belum ada dokumentasi resolusi insiden.
DSS02.06	Ada bagian yang memonitoring bagaimana tindakan terhadap insiden yang ada
DSS02.07	Dilakukannya pemantauan dari resolusi insiden. Namun belum ada bukti laporan terkait insiden yang ada

Pada hasil temuan audit keadaan tata kelola teknologi informasi terhadap setiap variabel pada tingkat kapabilitas *Manage Service Request and Incidents* saat

ini pada organisasi berada pada tingkat kematangan 1 (*Performed*) dengan nilai 1,28 dapat dilihat pada Tabel 4.3. Untuk rekomendasi pada domain *Manage Service Request and Incidents* ini mengacu pada proses teknologi informasi yang terdapat pada pedoman COBIT 5 *Enabling Processes* (ISACA, 2012, p. 179). Adapun proses pada domain *Manage Service Request and Incidents* ini yaitu memberikan respons yang tepat waktu dan efektif terhadap permintaan pengguna dan resolusi semua jenis insiden, memulihkan layanan normal, merekam dan memenuhi permintaan pengguna, dan menyelesaikan insiden. Sehingga rekomendasi pada domain *Manage Service Request and Incidents* ini dapat dilihat pada tabel 4.7 berikut:

Tabel 4.7 Rekomendasi DSS02

Control Objectives	Rekomendasi
DSS02.01	Membuat klasifikasi terhadap jenis-jenis layanan dan insiden yang dilayani, sehingga mudah untuk dipetakan ke bagian yang akan langsung menyelesaikan layanan atau insiden tersebut.
DSS02.02	Menetapkan aturan-aturan mengenai penanganan insiden, serta membuat strategi-strategi dalam permintaan layanan dan pemecahan insiden baik dalam bentuk kebijakan atau tindakan penanganan langsung.
DSS02.03	Memberikan wadah untuk kritik dan saran kepada pengguna untuk menilai pelayanan, kepuasan pengguna dan pemngembangannya.
DSS02.04	Perlu adanya ahli khusus yang dilibatkan dalam pelayanan insiden, sehingga dapat menangani insiden dengan maksimal
DSS02.05	Membuat dokumentasi terhadap resolusi atau solusi alternative terhadap pemecahan insiden dan mengevaluasinya.
DSS02.06	Mengembangkan sistem yang dapat melaporkan kecenderungan masalah atau insiden yang dihadapi sehingga pihak pengembang sistem informasi dapat mengetahui ksalahan-kesalahan yang didapatkan.
DSS02.07	Perlu dilakukannya pelaporan dan rapat secara berkala terhadap insiden yang ada.

Berdasarkan tabel rekomendasi di atas maka dapat disimpulkan bahwa adanya permintaan layanan dan insiden yang diketahui dan dipandang sebagai persoalan yang perlu ditangani. Hanya saja pengelolaannya belum terorganisir dan belum adanya proses standar dan cenderung dilakukan perorangan pada kasus yang

ada. Proses pengembangannya pun tidak dapat dipresiksi dan tidak stabil, karena proses masih selalu berubah dan dimodifikasi selama pengerjaan berjalan dari satu perminttan ke permintaan lainnya, dan perlu dibuat laporan secara tertulis dan dilakukan rapat secara berkala untuk menimalkan insiden.

4.4.1.3 DSS03 *Manage Problems*

Dari hasil *capability level* subdomain *Manage Problems* berada pada level 2 (*Manage*) yaitu pengelolaan proses yang telah dijelaskan sebelumnya sekarang dilaksanakan dengan cara dikelola (direncanakan, dipantau dan disesuaikan) dan produk kerjanya ditetapkan, dikontrol, dipelihara dengan tepat. Pada UMP kegiatan mengidentifikasi dan mengklasifikais masalah dan akar penyebab masalahnya, serta memberikan resolusi perbaikan secara tepat waktu. Namun belum ada laporan secara berkala terkait masalah dan manajemen perubahan yang terjadi.

Berikut Tabel 4.8 dapat dilihat keadaan tata kelola subdomain DSS03 *Manage Problems*:

Tabel 4.8 Keadaan Tata Kelola Saat ini DSS03

Control Objectives	Keadaan Tata Kelola Saat Ini
DSS03.01	Identikasi masalah dilakukan melalui log aktivitas dan dilakukan oleh kelompok pendukung berdasarkan <i>job description</i>
DSS03.02	Menyelidiki dan mendiagnosis masalah dengan membandingkan dengan log. Namun belum ada laporan yang dibuat untuk dikomunikasikan dalam kemanjuan menyelesaikan masalah dan memantau dampak berkelanjutan dari masalah
DSS03.03	Memberikan solusi dari masalah yang diketahui dengan memperhatikan manfaat dan biaya
DSS03.04	Penyelesaian dan penutupan masalah dilakukan secepatnya jika masalah telah diketahui dan dilakukan penginformasian kepada pihak pengelola. Namun belum ada laporan terkait mananajemen perubahan yang ada
DSS03.05	Penginformasian terkait manajemen perubahan dilakukan namun dalam bentuk daring, belum dibuat secara tertulis.

Pada hasil temuan audit keadaan tata kelola teknologi informasi terhadap setiap variabel pada tingkat kapabilitas *Manage Problems* saat ini pada organisasi berada pada tingkat kematangan 2 (*Manage*) dengan nilai 2,4 dapat dilihat pada Tabel 4.3. Untuk rekomendasi pada domain *Manage Problems* ini mengacu pada proses teknologi informasi yang terdapat pada pedoman COBIT 5 *Enabling Processes* (ISACA, 2012, p. 182). Adapun proses pada domain *Manage Problems* ini yaitu mengidentifikasi dan mengklasifikasikan masalah dan akar penyebabnya dan memberikan resolusi tepat waktu untuk mencegah insiden berulang, serta memberikan rekomendasi untuk perbaikan. Sehingga rekomendasi pada domain *Manage Problems* ini dapat dilihat pada tabel 4.9 berikut:

Tabel 4.9 Rekomendasi DSS03

Control Objectives	Rekomendasi
DSS03.01	Dilakukan pemeliharaan dan pengembangan log untuk terus meningkatkan kinerja dan proses dalam memenuhi tujuan bisnis disama yang akan datang
DSS03.02	Perlu adanya laporan yang dibuat sebagai acuan dalam menyelesaikan masalah dan sebagai acuan untuk memantau dampak berkelanjutan dari masalah
DSS03.03	Solusi yang didapatkan diharapkan dapat menjadi inovasi kedepannya untuk meningkatkan efisiensi dan efektivitas sistem dimasa yang akan datang dengan terus memperhatikan manfaat dan biaya
DSS03.04	Perlu dibuat laporan terkait manajemen perubahan sebagai acuan perbaikan sistem dan pengembangan system
DSS03.05	Penginformasian terkait manajemen perubahan sebaiknya dibuat dalam bentuk tertulis

Berdasarkan tabel rekomendasi di atas maka dapat disimpulkan bahwa untuk meningkatkan proses identifikasi dan penyelesaian masalah perlu dilakukannya pemeliharaan dan pengembangan log, dan adanya laporan yang diuat secara tertulis sebagai panduan dan acuan dalam penyelesaian masalah yang akan berdampak terhadap perkembangan sistem kedepannya.

4.4.1.4 DSS04 *Manage Continuity*

Dari hasil *capability level* subdomain *Manage Continuity* berada pada level 2 (*Manage*) yaitu pengelolaan proses yang telah dijelaskan sebelumnya sekarang dilaksanakan dengan cara dikelola (direncanakan, dipantau dan disesuaikan) dan produk kerjanya ditetapkan, dikontrol, dipelihara dengan tepat. Pada UMP kegiatan penetapan dan pemeliharaan rencana dalam merespon insiden dan gangguan dalam melanjutkan keberlangsungan proses bisnis telah dilaksanakan dan dikelola. Namun belum ada pengujian dan peninjauan rencana manajemen terhadap keberlangsungan operasional dan strategi bisnis.

Berikut Tabel 4.10 dapat dilihat keadaan tata kelola subdomain DSS04 *Manage Continuity*:

Tabel 4.10 Keadaan Tata Kelola Saat ini DSS04

Control Objectives	Keadaan Tata Kelola Saat Ini
DSS04.01	Mengidentifikasi proses bisnis dan aktivitas layanan sesuai dengan fungsi dan tujuan system dan terus memastikan peran dan tanggung jawab pemangku kepentingan sesuai dengan job description yang telah disetujui dan tetap memantau kebijakan yang telah disepakati demi keberlangsungan proses bisnis
DSS04.02	Mempertahankan strategi kontinuitas dengan memasang alat yang berfungsi untuk mengcover data agar sistem tetap dapat berjalan ketika terjadi insiden demi keberlangsungan proses bisnis
DSS04.03	Melakukan tindakan tanggap insiden, melakukan pemantauan kapasitas RAM dan internet untuk mendukung keberlangsungan bisnis, dan tetap menjaga integritas informasi pasca insiden agar tetap maksimal
DSS04.04	Belum adanya kelengkapan BCP
DSS04.05	Belum adanya peninjauan rencana manajemen terhadap keberlangsungan tujuan operasional dan strategi bisnis
DSS04.06	Belum ada pelatihan yang ditujukan kepada karyawan dalam mengelola TI
DSS04.07	<i>Back up</i> data dan pengujian pembaharuan data dilakukan secara berkala
DSS04.08	Pengecekan dan <i>maintenance</i> dilakukan pasca terjadi insiden dengan tujuan agar masalah tidak terulang lagi

Pada hasil temuan audit keadaan tata kelola teknologi informasi terhadap setiap variabel pada tingkat kapabilitas *Managge Continuity* saat ini pada organisasi berada pada tingkat kematangan 2 (*Manage*) dengan nilai 2 dapat dilihat pada Tabel 4.3. Untuk rekomendasi pada domain *Manage Continuity* ini mengacu pada proses teknologi informasi yang terdapat pada pedoman COBIT 5 *Enabling Processes* (ISACA, 2012, p. 186). Adapun proses pada domain *Manage Continuity* ini yaitu membuat dan memelihara rencana untuk memungkinkan bisnis dan TI merespons insiden dan gangguan untuk melanjutkan operasi proses bisnis penting dan layanan TI yang diperlukan dan menjaga ketersediaan informasi pada tingkat yang dapat diterima oleh instansi. Sehingga rekomendasi pada domain *Manage Continuity* ini dapat dilihat pada tabel 4.11 berikut:

Tabel 4.11 Rekomendasi DSS04

Control Objectives	Rekomendasi
DSS04.01	Pengimplementasian proses bisnis dan layanan TI terus ditingkatkan baik dari segi sistem maupun pengelola sistem agar mampu mencapai hasil proses yang maksimal
DSS04.02	Dilakukan pengujian secara berkala terhadap alat pengcover data agar dapat terus ditingkatkan dan beroperasi dengan menghasilkan kinerja yang diinginkan
DSS04.03	Kapasitas RAM dan internet terus ditingkatkan agar tetap menjaga dan meningkatkan keberlangsungan bisnis
DSS04.04	Perlu dilakukan pengujian sistem bisnis untuk memverifikasi kelengkapan BCP oleh renstra
DSS04.05	Perlu dilakukannya peninjauan rencana manajemen terhadap keberlangsungan tujuan operasional dan strategi bisnis
DSS04.06	Perlu diladakannya pelatihan kepada karyawan untuk terus meningkatkan pengelolaan TI demi keberlangsungan proses bisnis
DSS04.07	Terus ditingkatkan dalam proses pengelolaan data untuk mencapai hasil yang diinginkan sesuai dengan tujuan system
DSS04.08	Peninjauan pasca insiden terus ditingkatkan dan harus dilakukan optimaliasasi agar tidak terjadi insiden yang sama dimasa yang akan datang

Berdasarkan tabel rekomendasi di atas maka dapat disimpulkan bahwa pemeliharaan rencana keberlangsungan bisnis telah diimplemtasikan namun belum ada kelengkapan BCP, serta perlu diadakan pelatihan terhadap pihak pengelola.

4.4.1.5 DSS05 *Manage Security Services*

Dari hasil *capability level* subdomain *Manage Security Services* berada pada level 2 (*Manage*) yaitu pengelolaan proses yang telah dijelaskan sebelumnya sekarang dilaksanakan dengan cara dikelola (direncanakan, dipantau dan disesuaikan) dan produk kerjanya ditetapkan, dikontrol, dipelihara dengan tepat. Pada UMP kegiatan melakukan perlindungan terhadap informasi telah dilakukan namun belum ada pengelolaan hak akses dan peninjauan terhadap semua akun, belum dilakukan pembatasan hak akses, belum dilakukan pemantauan semua pengunjung yang masuk ke situs serta belum ada pencatatan dalam bentuk laporan kejadian terkait keamanan sistem, dan belum ada keamanan titik akhir.

Berikut Tabel 4.12 dapat dilihat keadaan tata kelola subdomain DSS05 *Manage Security Services*:

Tabel 4.12 Keadaan Tata Kelola Saat ini DSS05

Control Objectives	Keadaan Tata Kelola Saat Ini
DSS05.01	Mengkomunikasikan kepada pengguna akan bahaya <i>malware</i> , Mengaktifkan alat perlindungan <i>malware</i> berupa <i>Malwarebytes</i> , dan melakukan filterlalu lintas jaringan. Namun belum ada pelatihan terkait bahaya <i>malware</i>
DSS05.02	Menerapkan mekanisme filter jaringan berupa <i>firewall</i> , hanya megizinkan perangkat resmi yang memiliki katasandi untuk masuk ke jaringan sistem, dan dilakukan pengujian sistem pada saat terjadiinsiden saja
DSS05.03	Belum ada pemantauan kemananan dan penyaringan lalu lintas titik akhir
DSS05.04	Mengelola hak akses dengan memberikan kata sandi yang berbeda-beda agar tidak terjadi akses pihak luar. Kegiatan aktivitas pebgguna masih tetap dipantau namun belum ada pengelolaan hak akses baik dalam pembuatan, modifikasi maupun penghapusan
DSS05.05	Pemberian permintaan dan pemberian hak akses dilakukan jika keadaan mendesak saja. Namun saat ini belum dilakukan pencatatan terhadap semua pengunjung yang masuk ke situs TI dan belum ada pembatasan akses kesitus TI serta alarm jika terjadi akses yang tidak sah

DSS05.06	Penerimaan, penggunaan, pemindahan dan pembuangan dokumen sensitive telah sesuai dengan prosedur. Dan sudah ada pembatasan akses dokumen sensitive
DSS05.07	Alat pemantau keamanan TI berupa mikrotik. Namun belum ada pencatatan kejadian terkait keamanan.

Pada hasil temuan audit keadaan tata kelola teknologi informasi terhadap setiap variabel pada tingkat kapabilitas *Manage Security Services* saat ini pada organisasi berada pada tingkat kematangan 2 (*Manage*) dengan nilai 1,57 dapat dilihat pada Tabel 4.3. Untuk rekomendasi pada domain *Manage Security Services* ini mengacu pada proses teknologi informasi yang terdapat pada pedoman COBIT 5 *Enabling Processes* (ISACA, 2012, p. 192). Adapun proses pada domain *Manage Security Services* ini yaitu melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan, menetapkan dan memelihara peran keamanan informasi dan hak akses, dan melakukan pemantauan keamanan. Sehingga rekomendasi pada domain *Manage Security Services* ini dan sangat perlu untuk rekomendasi pada proses teknologi informasi yang mengacu pada COBIT yang terdapat pada pedoman COBIT 5 *Enabling Processes*, dapat dilihat pada tabel 4.13 berikut:

Tabel 4.13 Rekomendasi DSS05

Control Objectives	Rekomendasi
DSS05.01	Perlu diadakanya pelatihan terkait bahaya <i>malware</i> baik untuk pengguna maupun pengeola. Agar lebih bijak dalam menggunakan sistem informasi
DSS05.02	Pengujian sistem sebaiknya dilakukan secara berkala agar jaringan dapat selalu terjaga keamanannya
DSS05.03	Pemantauan keamanan dan penyaringan lalu Intas titik akhir perlu dilakukan agar dapat terhindar dari ancaman <i>malware</i>
DSS05.04	Perlu adanya pengelolaan hak akses baik dalam pembuatan, modifikasi maupun penghapusan. Agar tidak terjadi penyalahgunaan hak akses dimasa yang akan datang
DSS05.05	Perlu dilakukan pencatatan dan pembatasan hak akses yang masuk ke situs TI. Dan perlu dipasang alarm jika terjadi akses yang tidak sah
DSS05.06	Pengawasan terhadap akses dokumen sensitif perlu ditingkatkan, dan dibuat aturan secara tertulis tentang permintaan dan pemberian dokumen sensitif.

DSS05.07	Perlu dilakukan pencatatan kejadian terkait keamanan
----------	--

Berdasarkan tabel rekomendasi di atas maka dapat disimpulkan bahwa perlu diadakannya pelatihan terkait bahaya *malware*, dilakukan pengujian sistem secara berkala, pengelolaan dan pengawasan hak akses, dan melakukan pencatatan terkait kejadian keamanan.

4.4.1.6 DSS06 *Manage Business Process Controls*

Dari hasil *capability level* subdomain *Manage Security Services* berada pada level 3 (*Established*) yaitu proses pengelolaan yang telah dijelaskan sebelumnya sekarang diimplemetasikan dengan menggunakan proses yang didefinisikan dan mampu mencapai hasil prosesnya. Pada UMP mempertahankan control proses bisnis dengan cara mengidentifikasi dan mendokumentasikan aktivitas proses bisnis pada alat pengcover data, mengontrol layanan informasi, mengalokasikan peran dan tanggung jawab berdasarkan job description dan melakukan pengelolaan informasi.

Berikut Tabel 4.14 dapat dilihat keadaan tata kelola subdomain DSS06 *Manage Business Process Controls*:

Tabel 4.14 Keadaan Tata Kelola Saat ini DSS06

Control Objectives	Keadaan Tata Kelola Saat Ini
DSS06.01	Melakukan indentifikasi dan dokumentasi aktivitas pengendalian proses bisnis mealalui alat pengcover data arau DRC. Melakukan pemantauan kegiatan proses bisnis melalui log
DSS06.02	Memastikan kelengkapan layanan informasi dan mampu memperbaiki kesalahan dalam pengiriman data
DSS06.03	Mengaloksikan peran dan tanggung jawab berdasarkan <i>job description</i>
DSS06.04	Mengelola kesalahan informasi dengan melakukan perbaikan secara cepat dan mengkoordinasikan nya dengan Ketua IT untuk melakuka analisis penyebab dan solusi.

Pada hasil temuan audit keadaan tata kelola teknologi informasi terhadap setiap variabel pada tingkat kapabilitas *Manage Business Process Controls* saat ini pada organisasi berada pada tingkat kematangan 3 (*Establishes*) dengan nilai 3,25 dapat dilihat pada Tabel 4.3. Untuk rekomendasi pada domain *Manage Business Process Controls* ini mengacu pada proses teknologi informasi yang terdapat pada pedoman COBIT 5 *Enabling Processes* (ISACA, 2012, p. 192). Adapun proses pada domain *Manage Business Process Controls* ini yaitu mendefinisikan dan memelihara kontrol proses bisnis yang tepat untuk memastikan bahwa informasi yang terkait dan diproses oleh proses bisnis internal atau outsourcing untuk memenuhi semua persyaratan kontrol informasi yang relevan, mengidentifikasi persyaratan pengendalian informasi yang relevan dan mengelola serta mengoperasikan pengendalian yang memadai untuk memastikan bahwa informasi dan pemrosesan informasi memenuhi persyaratan. Sehingga rekomendasi pada domain *Manage Business Process Controls* ini dapat dilihat pada tabel 4.15 berikut:

Tabel 4.15 Rekomendasi DSS06

Control Objectives	Rekomendasi
DSS06.01	Perlu dilakukan pengukuran terhadap DRC dan log agar lebih maksimal pengoperasiannya untuk mencapai hasil proses yang maksimal juga
DSS06.02	Selalu melakukan pemantauan dan peningkatan dalam layanan informasi agar tidak terjadi penginformasian yang tidak valid kebenarannya
DSS06.03	Perlu adanya peningkatan efisiensi akan kesadaran peran dan tanggungjawab asing-masing personel sesuai dengan peran dan tanggungjawab yang telah ditetapkan
DSS06.04	Terus ditingkatkan kemampuan dalam mengelola kesalahan informasi agar informasinya yang diberikan dapat diterima baik oleh pengguna

Berdasarkan tabel rekomendasi di atas maka dapat disimpulkan bahwa perlu dilakukan pengukuran, pemantauan dalam meningkatkan layanan informasi, serta meningkatkan kemampuan dalam pengelolaan informasi.

