

BAB IV

HASIL DAN PEMBAHASAN

4.1 Gambaran Umum

Pusat teknologi informasi dan pangkalan data (PUSTIPD) UIN Raden Fatah Palembang sebagai lembaga pusat teknologi informasi yang memiliki tanggung jawab *service*, pemantau, sekaligus pengembang sistem yang ada di UIN Raden Fatah Palembang. PUSTIPD UIN Raden Fatah Palembang dipimpin oleh kepala yang diangkat oleh dan bertanggung jawab kepada rektor.

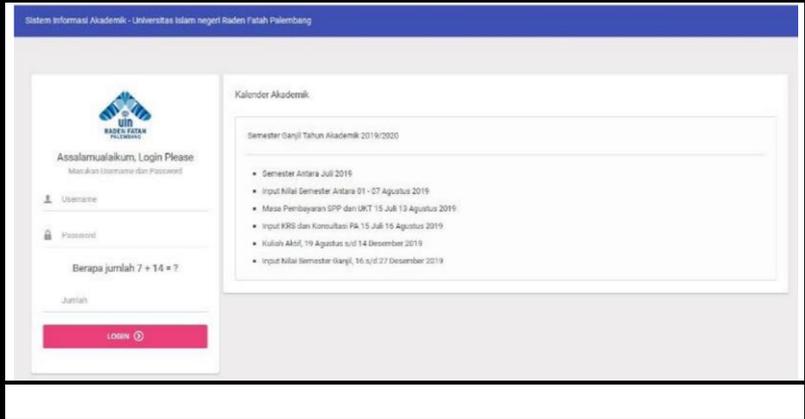
Sebagai lembaga yang bertanggung jawab dibidang teknologi, tentunya PUSTIPD berperan sangat penting bagi Universitas. Dibentuknya tujuan terbaik akan menentukan baik tidaknya kualitas dan kuantitas yang diharapkan, untuk itu PUSTIPD memiliki visi sebagai berikut: menjadikan teknologi informasi sebagai media transformasi keilmuan, dalam upaya mendukung pelaksanaan tri dharma perguruan tinggi, dan tanggap dengan kebutuhan civitas akademika uin raden fatah palembang. Serta misi sebagai berikut:

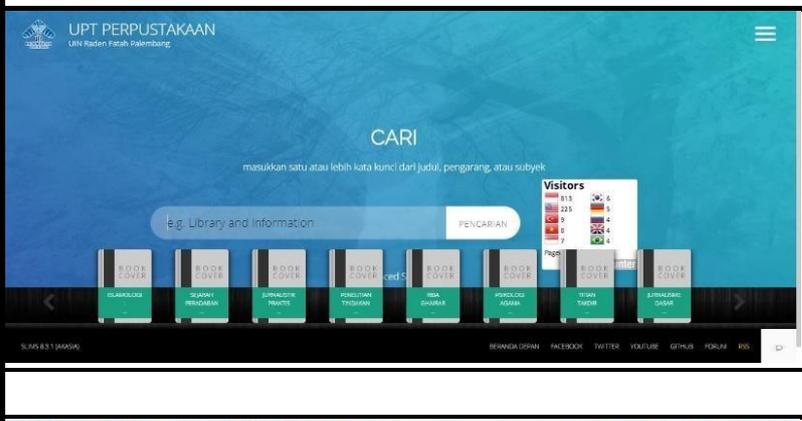
1. Meningkatkan kualitas pengelolaan data dan informasi secara profesional.
2. Mengembangkan dan meningkatkan kualitas layanan teknologi informasi yang informatif dan komunikatif.
3. Mengembangkan dan meningkatkan berbagai olahan data akademik, kepegawaian, dan keuangan yang siap saji dan dapat dipilih dan diakses secara terbatas (data keuangan) dan tak terbatas (data akademik dan kepegawaian) oleh pengguna kapan dan di mana saja.

4. Memberikan layanan TI yang prima kepada civitas akademika dan stakeholders secara bermatabat dan bersahabat.
5. Berperan aktif meningkatkan kemampuan dan keterampilan civitas akademika dalam bidang teknologi informasi.

PUSTIPD memiliki beberapa tanggung jawab terhadap beberapa sistem, akan tetapi fokus pada penelitian ini terdiri dari: SIMAK UIN Raden Fatah, E-lkp, Ejurnal, Slims, E-repository, dan Lpse UIN Raden Fatah. Persyaratan dari setiap sistem diputuskan dari kesepakatan oleh pihak PUSTIPD & BAAK, sedangkan untuk tanggungjawab pengembangan, *service*, serta keamanan dikendalikan oleh pihak PUSTIPD.

Tabel 4.1 Gambaran Sistem PUSTIPD UIN Raden Fatah Palembang

Sistem	Halaman Login/Beranda
SIMAK https://simak.ra.denfatah.ac.id/	 <p>Sistem Informasi Akademik - Universitas Islam negeri Raden Fatah Palembang</p> <p>Assalamualaikum, Login Please Masukkan Username dan Password</p> <p>Username</p> <p>Password</p> <p>Berapa jumlah 7 + 14 = ?</p> <p>Jumlah</p> <p>LOGIN</p> <p>Kalender Akademik</p> <p>Semester Ganjil Tahun Akademik 2019/2020</p> <ul style="list-style-type: none"> • Semester Antara Juli 2019 • Input Nilai Semester Antara 01 - 07 Agustus 2019 • Meas Pembayaran SPP dan UKT 15 Juli 13 Agustus 2019 • Input KRIS dan Konsultasi PA 15 Juli 16 Agustus 2019 • Kuliah Abad, 19 Agustus s.d 14 Desember 2019 • Input Nilai Semester Ganjil, 16 s.d 27 Desember 2019

Sistem	Halaman Login/Beranda
<p>E-Lkp https://elkp.radenfatah.ac.id/</p>	
<p>E-Journal http://jurnal.radenfatah.ac.id/</p>	
<p>SLIMS http://slims.radenfatah.ac.id/</p>	
<p>E-Repository/E-Prints http://eprints.radenfatah.ac.id/</p>	

LPSE
<http://lpse.rade.nfatah.ac.id/epr/oc4>



Berikut penjelasan dari beberapa sistem diatas:

1. SIMAK

SIMAK adalah sistem informasi yang dibuat untuk mempermudah kegiatan administrasi akademik di kampus yang diatur secara *online*. SIMAK UIN Raden Fatah berkembang menjadi 9 SIMAK yaitu SIMAK fakultas SAINTEK, fakultas dakwah dan komunikasi, fakultas syariah, fakultas ekonomi dan bisnis islam, fakultas adab dan humaniora, fakultas ushuluddin dan pemikiran islam, fakultas ilmu sosial dan politik, dan pascasarjana.

2. E-Lkp

Yaitu elektronik lembar kerja pegawai UIN Raden Fatah Palembang yang berfungsi untuk melaporkan hasil kerja pegawai.

3. E-journal

Sistem informasi penyedia atau wadah penerbitan artikel-artikel ilmiah dalam suatu jurnal ilmiah ber-ISSN yang dilakukan oleh suatu institusi melalui media elektronik dan disebarkan kepada atau bisa diakses seluruh audiens pembaca melalui portal internet yang tersedia.

4. Slims

Perangkat lunak pengelolaan perpustakaan yang pertama kali dikembangkan dan digunakan oleh Perpustakaan Kemendikbud.

5. E-repository

Perangkat lunak opensource yang dikembangkan oleh *School of Electronics and Computer Science*, University of Southampton, England United Kingdom.

Repository ini bisa berbentuk arsip, selain itu bisa digunakan untuk menyimpan gambar, data penelitian dan suara dalam bentuk digital.

6. LPSE

Sistem informasi sebagai layanan pengadaan secara elektronik barang/jasa pemerintah.

4.2 Elemen Manajemen Risiko

Elemen manajemen risiko terdiri dari prasarana manajemen risiko yaitu prasarana lunak (non-fisik) dan prasarana keras (fisik), dari hasil penelitian terdapat beberapa elemen manajemen risiko yang ada pada PUSTIPD:

4.2.1 Prasarana Lunak

1. Pertemuan seminggu sekali/sebulan sekali, membahas tentang penilaian kinerja.
2. Melakukan pemasangan *firewall*, anti DdoS dan antivirus untuk melindungi sistem dari serangan.
3. Menggunakan *software* yang berlisensi seperti: office dan windows.
4. Melakukan *backup* secara berkala (mingguan-bulanan).
5. Menerapkan konfirmasi hak akses untuk menjaga keamanan tiap pengguna.

4.2.2 Prasarana Keras

Terdapat penentuan dan pemilihan situs fisik, dengan membandingkan berbagai referensi serta menempatkan server pada posisi aman dan diluar keramaian.

4.3 Hasil Audit Teknologi Informasi

Sesuai dengan tujuan pertama dari penelitian, peneliti melakukan audit teknologi informasi untuk manajemen risiko pada PUSTIPD UIN Raden Fatah dengan teknik pengumpulan data untuk audit yaitu observasi dan wawancara *COBIT Control Assessment Questionnaire* untuk meendapatkan dan mengevaluasi secara objektif bukti yang berkaitan dengan penilaian mengenai berbagai kegiatan yang dilakukan, untuk memastikan tingkat kesesuaiannya dengan penilaian-penilaian tersebut. Kemudian membentuk kriteria yang akan disampaikan kepada pemangku kepentingan. Dari hasil audit nanti dibentuk laporan audit yang akan diberikan kepada pihak terkait penelitian. Berikut wawancara *COBIT Control Assessment Questionnaire*.

Responden: Head IT Administration

IT Process	Pertanyaan	Jawaban
PO4	1. Apakah PUSTIPD telah menetapkan struktur organisasi, termasuk komite dan hubungan TI dengan pemangku kepentingan?	Struktur organisasi sudah dibentuk, komite juga sudah secara umum dan untuk bagian TI dan pemangku kepentingan sudah dibentuk berdasarkan kebutuhan dan pemangku kepentingan.
	2. Apakah PUSTIPD telah merancang kerangka proses IT?	Ya sudah dirancang, terangnya proses TI ini dibentuknya untuk mendukung pelaksanaan rencana strategis di PUSTIPD.
	3. Apakah PUSTIPD menetapkan dan mengimplementasikan peran dan tanggung jawab TI, termasuk pengewasaan dan pemisahan tugas?	Ya ditetapkan dan diimplementasikan. Dengan pembagian job desk untuk tiap staf TI di PUSTIPD, sebagai kerangka peran, tanggung jawab terhadap TI, serta penguasaan dan pemisahan tugas.
PO 6	1. Apakah PUSTIPD mengembangkan dan memelihara kebijakan IT?	PUSTIPD memiliki kebijakan TI dengan penentuan kebijakan yang sesuai dengan manajemen perolehan, dikembangkan berdasarkan kebutuhan dan penguasaan perolehanan TI.
	2. Apakah PUSTIPD mengkomunikasikan kerangka kontrol TI dan tujuan TI	tersebut di komunikasikan, dengan cara melakukan sosialisasi dan pengujian pelatihan.

Gambar 4.1 Wawancara Audit RACI Head IT Administration

Wawancara audit tersebut dilakukan dengan melakukan wawancara dengan pihak terkait yang melaksanakan bidang terkait sesuai dengan pemetaan pada tabel RACI (dapat dilihat pada halaman 36) terdiri dari peran CEO, CIO, CFO, Chief Architect, Head IT Administration, Head Operation, Head Development, dan CAS. Masing-masing peran mendapat pertanyaan yang berbeda-beda sesuai dengan ketentuan COBIT 4.1. Lebih lengkapnya dapat dilihat pada lampiran halaman 120.

Internal Audit Department
COBIT Control Assessment Questionnaire

COBIT Kontrol Kuesioner Penilaian

COBIT
GOVERNANCE, CONTROL
& RELATED TECHNOLOGY

Prinsip untuk meningkatkan produktivitas bisnis organisasi melalui bentuk standar yang terintegrasi. Audit untuk memastikan kepatuhan terhadap standar yang ditetapkan. Standar untuk meningkatkan kinerja yang lebih baik. Audit yang baik untuk IT harus mencakup layanan yang digunakan oleh semua orang yang terlibat dengan organisasi IT, yaitu, pengalihan informasi antara 4 domain IT.
- IT Governance Institute

Informasi Audit:

Audit / Nama Proyek	Objekt	Tanggal Mulai Akhir Tanggal	Audit Pemimpin Tim
Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UN Raden Fatah Palembang	PUSTIPD UN Raden Fatah Palembang	13-17 Januari 2020	Syella Rohadani 'Ary

Informasi Klien:

Information For Clients Participating In The Joint Assessment			
Nama	Jabatan	Phone	Lokasi
F. Ardiyaningrum, M. Kom	Kepala PUSTIPD (CID)		PUSTIPD UN RADEN FATAH PALEMBANG
Kris. Jansariyasa, HM.S.Si.Pd.MPd	Direktur Operasional (Head of Operation)		PUSTIPD UN RADEN FATAH PALEMBANG
A. Arsyad, S. Kom	D. Pengembang Software (Chief Architect)		PUSTIPD UN RADEN FATAH PALEMBANG
M. Anand, S. Kom	D. Pengembang Software (Head of Operation)		PUSTIPD UN RADEN FATAH PALEMBANG

Informasi lain

Gambar 4.2 Informasi Audit dan Klien

Mendata informasi-informasi mengenai audit seperti nama proyek, objek audit, tanggal mulai dan akhir dilakukan audit, auditor serta informasi klien atau responden yang menyangkut nama, jabatan klien, nomor telpon, dan lokasi.

Internal Audit Department
COBIT Control Assessment Questionnaire

Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi: 4 (p0.2, p0.6, p0.8, p0.11, p0.10, p0.19)

COBIT Penilaian Tingkat Kematangan: POJ Menentukan Proses, Organisasi, dan Hubungan IT:

Rating	Deskripsi
0 - Non Existent	Organisasi TI tidak secara efektif ditirikan untuk fokus pada pencapaian tujuan bisnis.
1 - Initial Ad Hoc	Kegiatan dan fungsi TI bersifat reaktif dan tidak konsisten dilaksanakan. IT terlibat dalam proyek bisnis hanya di tahap selanjutnya. Fungsi TI dianggap sebagai fungsi pendukung, tetapi persepsi organisasi secara keseluruhan. Ada pemahaman implisit tentang perlunya organisasi TI. Nama, peran dan tanggung jawab tidak didefinisikan atau ditetapkan.
2 - Repeatable but Inconsistent	Fungsi TI diatur untuk merespons secara reaktif, tetapi tidak konsisten, terdapat kebutuhan pelanggan dan hubungan vendor. Keahlian untuk organisasi yang terstruktur dan manajemen vendor dikomunikasikan, tetapi kepatuhan masih bergantung pada pengetahuan dan keterampilan individu kunci. Ada masalahnya teknik umum untuk mengelola organisasi IT dan hubungan vendor.
3 - Defined	Peran dan tanggung jawab yang ditetapkan untuk organisasi TI dan pihak ketiga ada. Organisasi TI dikembangkan, dikoordinasikan, dikomunikasikan dan diarahkan dengan strategi TI. Lingkungan kontrol internal didefinisikan. Ada formalisasi hubungan dengan pihak lain, termasuk konsultasi, audit internal, dan manajemen vendor. Organisasi TI secara fungsional terintegrasi. Ada definisi fungsi yang harus dilakukan oleh personel TI dan yang harus dilakukan oleh pengguna. Perencanaan dan keahlian staf TI yang penting ditetapkan dan diawasi. Ada definisi formal tentang hubungan dengan pengguna dan pihak ketiga. Pembagian peran dan tanggung jawab tidak dimasukkan dan ditingkatkan.
4 - Managed and Measurable	Organisasi TI secara proaktif menanggapi perubahan dan mencakup semua peran yang diperlukan untuk memastikan penyelarasan bisnis. Manajemen TI, proses kepatuhan, akuntabilitas dan tanggung jawab didefinisikan dan diawasi. Praktik baik internal telah diterapkan dalam organisasi fungsi-fungsi TI. Manajemen TI memiliki keahlian dan keterampilan yang tepat untuk mendefinisikan, menerapkan, dan memantau organisasi dan hubungan yang dituntut. Mekanisme untuk mendeteksi risiko bisnis dan faktor keberhasilan kritis yang ditunjukkan pengguna (CSF) adalah standar. Inventaris keterampilan tersedia untuk mendukung staf proyek dan pengembangan profesional. Keseimbangan antara keterampilan dan sumber daya yang tersedia secara internal dan yang dibutuhkan dari organisasi eksternal didefinisikan dan ditetapkan. Swadaya organisasi TI secara tepat memverifikasi kebutuhan bisnis dengan menyediakan layanan yang selaras dengan proses bisnis strategis, daripada dengan teknologi terisolasi.
5 - Optimized	Struktur organisasi TI bersifat fleksibel dan adaptif. Praktik baik industri diterapkan. Ada banyak penggunaan teknologi untuk mendukung mematuhi kinerja organisasi dan proses TI. Teknologi ditinjau secara teratur untuk mendukung kompleksitas dan distribusi geografis organisasi. Ada proses perbaikan berkelanjutan di tempat.

Nilai Keseluruhan Tingkat Kematangan Terendah: 2 (p0.4)

Gambar 4.3 Nilai Kematangan Tiap Proses TI

Penilaian tingkat kematangan tiap proses TI disesuaikan dengan informasi hasil audit yang dilakukan. Tingkat kematangan proses TI tersebut berbeda-beda, sesuai dengan ketentuan pada COBIT 4.1

Detail Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klasifikasi Response & Assessment Hasil	
Detail Control Objective PO4: PO4.1 Bagaimana Proses, Organisasi, dan Hubungan IT terencana TI dilakukan dengan memperhatikan persyaratan untuk staf, keterampilan, fungsi, alokasi, sumber, peran dan tanggung jawab dan program? Organisasi ini terencana dalam kerangka kerja proses TI yang mencakup perencanaan dan keterkaitan, keterkaitan dengan unit dan organisasi lain, dan cara ini lebih lanjut pengingat di masa depan dan TI bagaimana memastikan pemenuhan rencana TI yang sesuai dengan kebutuhan bisnis. Proses, kebijakan dan prosedur administratif tersedia untuk proses, dengan perhatian khusus pada pengembangan, pemenuhan kriteria, manajemen risiko, komunikasi informasi, kepatuhan data dan sistem, dan pemeliharaan regu. Untuk memastikan alignment perencanaan bisnis yang tepat waktu, TI harus diintegrasikan dalam proses keputusan yang relevan.	3	PO4.1 1. Apakah PUSTIPD memastikan kerangka kerja teknologi informasi untuk melaksanakan rencana strategi teknologi informasi? 2. Bagaimana PUSTIPD mengorganisir kerangka kerja teknologi informasi? 3. Bagaimana PUSTIPD mengorganisir kerangka kerja informasi ke dalam sistem informasi manajemen?	1. Pula pertanyaan ini menjamin kerangka kerja teknologi informasi yang mendukung pelaksanaan rencana strategi teknologi informasi yang ada di bagian. 2. Bagaimana PUSTIPD memastikan kerangka kerja teknologi informasi yang akan dilaksanakan yang benar/benar?	
	4	PO4.2 4. Apakah PUSTIPD menyediakan strategi teknologi informasi? 5. Bagaimana PUSTIPD memastikan bahwa ada kerangka teknologi informasi untuk strategi?		3. Bagaimana PUSTIPD memastikan kerangka kerja informasi ke dalam sistem informasi manajemen? 4. Apakah PUSTIPD menyediakan strategi teknologi informasi? 5. Bagaimana PUSTIPD memastikan bahwa ada kerangka teknologi informasi untuk strategi?
	3	PO4.3 6. Apakah PUSTIPD telah menyediakan kerangka pengingat teknologi informasi? 7. Apakah PUSTIPD dapat memastikan pemenuhan persyaratan teknologi informasi secara teratur setiap tahun?		6. Apakah PUSTIPD telah menyediakan kerangka pengingat teknologi informasi? 7. Apakah PUSTIPD dapat memastikan pemenuhan persyaratan teknologi informasi secara teratur setiap tahun?
	2	PO4.4 8. Apakah PUSTIPD memverifikasi fungsi teknologi informasi dalam struktur organisasi secara keseluruhan?		8. Apakah PUSTIPD memverifikasi fungsi teknologi informasi dalam struktur organisasi secara keseluruhan?

Gambar 4.4 Penilaian Tiap Detail Control Objective

Memberikan pertanyaan sesuai dengan ketentuan detail control objective pada COBIT 4.1. Dengan mengajukan beberapa butir pertanyaan, informasi tersebut dapat berguna sebagai tolak ukur penentuan tingkat kematangan. Untuk lebih jelasnya bisa dilihat pada lampiran halaman 133. Hasil audit kemudian dikumpulkan dalam tabel 4.2 berikut:

Tabel 4.2 Rekapitulasi Audit Maturity Level Subdomain

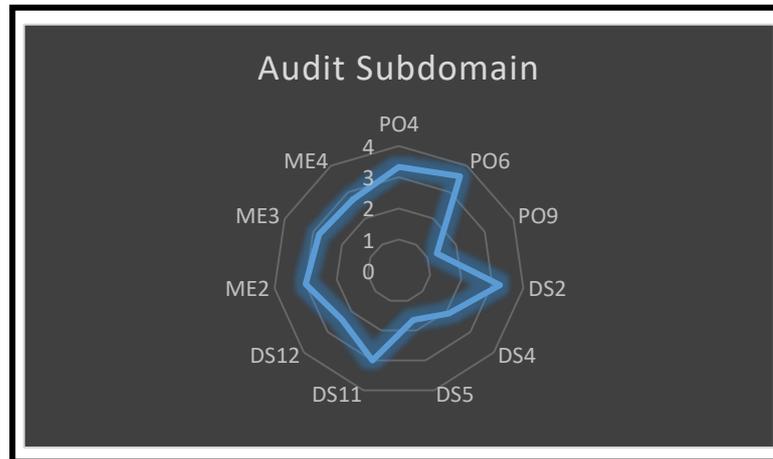
IT Process	Indeks Maturity	Maturity Level	Keterangan
PO4 Define the IT Processes, Organization and Relationships	3,33	3	Defined
PO6 Communicate Management Aims and Direction	3,6	4	Managed
PO9 Assess and Manage IT Risk	1,33	1	Initial/Ad-Hoc
DS2 Manage Third-party Services	3,25	3	Defined
DS4 Ensure Continuous Service	2,1	2	Repeatable
DS5 Ensure Systems Security	1,64	2	Repeatable
DS11 Manage Data	3	3	Defined
DS12 Manage the Physical Environment	2,4	2	Repeatable

IT Process		Indeks Maturity	Maturity Level	Keterangan
ME2	<i>Monitor and Evaluate Internal Control</i>	3	3	<i>Defined</i>
ME3	<i>Ensure Compliance With External Requirements</i>	2,8	3	<i>Defined</i>
ME4	<i>Provide IT Governance</i>	2,71	3	<i>Defined</i>

(Sumber: Data diolah dengan *MS Excel* 2013)

Berdasarkan hasil rekapitulasi audit *maturity level* subdomain didapat *control objective* yang mencapai tingkat 4 (*managed*) yaitu pada PO6 *Communicate Management Aims and Direction* yang berarti manajemen menerima tanggung jawab untuk mengkomunikasikan kebijakan pengendalian internal serta mendelegasikan tanggung jawab dan mengalokasikan sumber daya yang cukup untuk menjaga lingkungan sejalan dengan perubahan signifikan. Kemudian *control objective* yang memiliki kontrol informasi lengkap dan lingkungan manajemen mutu yang dikembangkan, didokumentasikan dan dikomunikasikan oleh manajemen dan mencakup kerangka kerja untuk kebijakan, rencana serta prosedur yaitu pada *control objective* PO4 *Define the IT Processes, Organization and Relationships*, DS2 *Manage Third-party Services*, DS11 *Manage Data*, ME2 *Monitor and Evaluate Internal Control*, ME3 *Ensure Compliance With External Requirements*, dan ME4 *Provide IT Governance*. Terdapat juga *control objective* yang prosesnya telah berkembang ke tahap dimana prosedur serupa diikuti oleh orang yang berbeda yang melakukan tugas yang sama, tidak ada pelatihan formal dan tanggung jawabnya diserahkan kepada individu berada pada DS4 *Ensure Continuous Service*, DS5 *Ensure Systems Security*, dan DS12 *Manage the Physical Environment*. Pada PO9 *Supplier Relationship Management* risiko TI dipertimbangkan secara ad hoc, penilaian informal terhadap risiko, terkadang

diidentifikasi dalam rencana proyek tetapi jarang ditugaskan untuk manajer. Lebih jelasnya dapat dilihat dari grafik radar hasil penilaian audit subdomain pada gambar 4.5 berikut:



Gambar 4.5 Grafik Radar (Spider Chart) Audit Subdomain

Untuk mendapatkan nilai indeks *maturity* dilakukan perhitungan indeks *maturity*, sebagai contoh perhitungan diambil subdomain secara acak pada subdomain DS5 *Ensure Systems Security* dengan jumlah jawaban 18, pertanyaan sebanyak 11 butir dan 1 auditor maka nilai indeks *maturity* adalah 1,64 lebih jelasnya sebagai berikut:

$$\text{Indeks maturity} = \frac{\sum(\text{jumlah jawaban})}{\sum(\text{jumlah pertanyaan} \times \text{jumlah responden})}$$

$$\text{Indeks} = \frac{18}{11 \times 1}$$

$$\text{Indeks} = \frac{18}{11} = 1,636364$$

Maka hasil perhitungan *maturity level* nilai dari subdomain *Ensure Systems Security* yaitu 1,64.

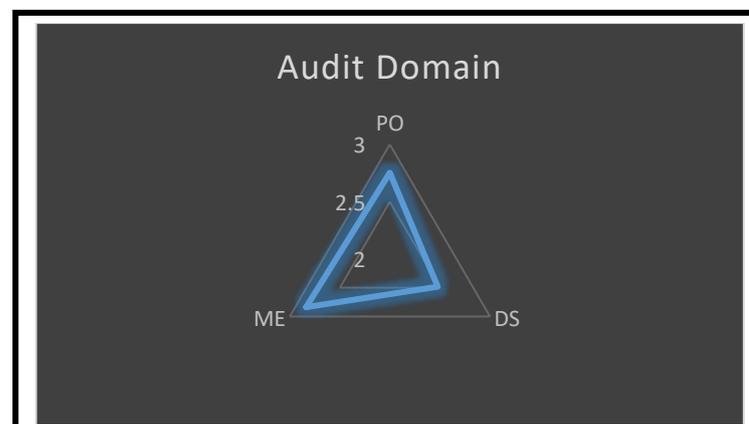
Untuk mendapatkan hasil audit keadaan saat ini, peneliti menggunakan alat bantu Microsoft Excel 2013 dengan mencari rata-rata dari keseluruhan perhitungan *maturity level* pada setiap *indicator* domain *Plan and Organise, Delivery and Support, Monitor and Evaluation*. Rata-rata perhitungan setiap domain dapat dilihat pada Tabel 4.3 sebagai berikut:

Tabel 4.3 Hasil Pengujian Audit Domain

No	Domain	Indeks Maturity	Maturity Level	Keterangan
1.	<i>Plan and Organize</i>	2,75	3	<i>Defined</i>
2.	<i>Delivery and Support</i>	2,48	2	<i>Repeatable</i>
3.	<i>Monitor and Evaluate</i>	2,84	3	<i>Defined</i>
Tingkat kematangan keseluruhan		2,69	3	<i>Defined</i>

(Sumber: Data diolah dengan *MS Excel* 2013)

Pada tabel diatas dapat dilihat bahwa hasil temuan audit pada TI untuk manajemen risiko pada PUSTIPD saat ini berada pada tingkat kematangan 3 yaitu *defined* yang artinya prosedur distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Kemudian diamanatkan bahwa proses-proses tersebut harus diikuti. Namun penyimpangan tidak mungkin dapat terdeteksi. Prosedur sendiri tidak lengkap namun sudah memformalkan praktek yang berjalan. Berikut gambaran *maturity level* domain hasil audit dalam grafik radar (*spider chart*):



Gambar 4.6 Grafik Radar (Spider Chart) Audit Domain

Dapat disimpulkan bahwa pada PUSTIPD UIN Raden Fatah Palembang terdapat proses-proses teknologi informasi untuk manajemen risiko yang belum memiliki prosedur yang distandarisasi dan didokumentasikan untuk dikomunikasikan melalui pelatihan yaitu pada PO9 *Supplier Relationship Management* (manajemen hubungan pemasok), DS4 *Ensure Continuous Service* (memastikan layanan berkelanjutan), DS5 *Ensure Systems Security* (memastikan keamanan sistem), dan DS12 *Manage the Physical Environment* (mengelola lingkungan fisik). Tetapi secara keseluruhan nilai *maturity level* saat ini untuk manajemen risiko pada PUSTIPD mencapai 3 yang artinya prosedur distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Kemudian diamanatkan bahwa proses-proses tersebut harus diikuti. Namun penyimpangan tidak mungkin dapat terdeteksi. Prosedur sendiri tidak lengkap namun sudah memformalkan praktek yang berjalan.

4.4 Analisis Data

4.4.1 Deskripsi Responden

Survey dilakukan dengan menyebarkan kuesioner sebanyak 11 responden yang telah dipetakan berdasarkan RACI. Terdapat 2 jenis kuesioner yaitu *maturity level* dan *management awareness*.

Metode penyebaran kuesioner dilakukan dengan memberi sedikit penjelasan kepada responden tentang masing-masing kuesioner, cara menjawab, dan menjelaskan setiap item keterangan. Semua responden berjenis kelamin laki-laki dengan latar belakang pendidikan dibidang ilmu komputer dan berpendidikan S1 dan S2.

4.4.2 Rekapitulasi Hasil dan Deskripsi Variabel Penelitian

Berdasarkan pengumpulan data dengan wawancara, observasi dan penyebaran kuesioner kepada responden mengenai teknologi informasi pada PUSTIPD UIN Raden Fatah Palembang. Peneliti melakukan rekap data terlebih dahulu sebelum data tersebut dikelola. Data yang akan direkap merupakan hasil dari jawaban responden berdasarkan pernyataan dari *framework* COBIT 4.1.

Pada kuesioner *management awareness* yang bertujuan untuk mendapatkan opini responden mengenai tingkat kesadaran terhadap manajemen risiko TI, menggunakan skala *likert* sebagai nilai tingkatan jawaban, yaitu 1 (sangat tidak penting), 2 (tidak penting), 3 (sedikit penting), 4 (penting) dan 5 (sangat penting).

Sedangkan untuk mengetahui tingkat kematangan menggunakan kuesioner *maturity level* dengan tingkatan 0-5 yaitu 0 (*non-existent*), 1 (*initial/ad-hoc*), 2 (*repeatable but intuitive*), 3(*defined*), 4(*manage and measurable*) dan 5 (*optimised*).

1. Rekapitulasi Perhitungan Tingkat *Management Awareness*

Pengukuran ini dilakukan dengan memberikan pernyataan tentang seberapa penting proses-proses yang ada dalam manajemen risiko. Dengan menggunakan skala *likert* sebagai alat ukur tingkat kepentingan yaitu skala 1-5 dengan ketentuan 1 (sangat tidak penting), 2 (tidak penting), 3 (sedikit penting), 4 (penting) dan 5 (sangat penting). Semakin tinggi skala yang diberikan, maka proses tersebut semakin tinggi nilai kepentingannya. Diberikan 81 pernyataan dari *framework* COBIT 4.1 sesuai dengan fokus area utama *risk management*. Berikut bentuk kuesioner *management awareness* pada gambar 4.3 berikut:

Kuisisioner 1 : Management Awareness

Kuisisioner ini bertujuan untuk mendapatkan informasi mengenai pendapat atau opini dari Saudara i tentang pengelolaan Teknologi Informasi (TI) pada PUUSTIPD Universitas Islam Negeri Raden Fatah Palembang, yang akan digunakan dalam rangka penelitian skripsi.

Kuisisioner *Management Awareness* ini dikembangkan untuk mengetahui tingkat pemenuhan terhadap *Detailed Control Objective* dan pencapaian indikator kinerja dalam proses TI.

Untuk mempermudah responden dalam menjawab, maka kuisisioner ini dirancang dalam bentuk pilihan ganda. Masing-masing pertanyaan mempunyai 5 pilihan jawaban yang menunjukkan tingkat kepentingan terhadap atribut tertentu pada proses TI. Pada kolom jawaban, responden dapat memilih salah satu jawaban yang dianggap paling bisa mewakili seberapa penting proses tersebut dengan memberikan tanda (✓) pada tempat yang tersedia.

Untuk itu mohon kiranya Saudara i dapat memberikan pendapatnya atas pernyataan-pernyataan dalam kuisisioner ini, untuk dapat diolah lebih lanjut

Nama Responden	
Jabatan Responden	
Unit Bidang/Subbid	

Penilaian menggunakan skala likert, yang mempunyai gradasi dari sangat tidak penting sampai sangat penting. Semakin tinggi kepentingan semakin besar pula nilai yang diperoleh. Acuan penilaian ialah sebagai berikut:

Penilaian	Deskripsi
1	Sangat Tidak Penting
2	Tidak Penting
3	Sedikit Penting
4	Penting
5	Sangat Penting

Kode	Proses	Seberapa penting tujuan tersebut bagi proses bisnis?				
		Sangat Tidak Penting	Tidak Penting	Sedikit Penting	Penting	Sangat Penting
		1	2	3	4	5
PO4	Menetapkan proses TI, organisasi, dan hubungan					
PO4.1	PUUSTIPD menentukan kerangka proses TI untuk menjalankan rencana strategis TI					
PO4.2	PUUSTIPD membentuk komite strategi TI di tingkat dewan direksi					

Gambar 4.7 Kuesioner Management Awareness

Kuesioner *management awareness* dilakukan untuk menilai tingkat kepentingan proses tersebut pada organisasi. Setelah dilakukan pengujian validitas dan reabilitas kemudian dilakukan pengukuran skala *likert*. Hasilnya dikumpulkan dalam rekapitulasi skala likert pada tabel 4.4 berikut:

Tabel 4.4 Rekapitulasi Skala Likert Subdomain

IT Process		Skala Likert					Hasil
		STP (1)	TP (2)	SDP (3)	P (4)	SP (5)	
PO4	Define the IT Processes, Organization and Relationships	2	4	20	79	60	165
PO6	Communicate Management Aims and Direction	0	1	6	33	15	55
PO9	Assess and Manage IT Risk	0	6	4	38	18	66
DS2	Manage Third-party Services	0	4	5	28	7	44
DS4	Ensure Continuous Service	0	9	7	65	29	110
DS5	Ensure Systems Security	0	0	15	52	54	121
DS11	Manage Data	0	0	8	38	20	66
DS12	Manage the Physical Environment	0	0	3	24	28	55

IT Process		Skala Likert					Hasil
		STP (1)	TP (2)	SDP (3)	P (4)	SP (5)	
ME2	Monitor and Evaluate Internal Control	0	0	3	24	28	55
ME3	Ensure Compliance With External Requirements	0	0	5	33	17	55
ME4	Provide IT Governance	0	0	5	33	17	55
Total		2	24	81	447	293	847

(Sumber: Data diolah dengan MS Excel 2013)

Berikut rekapitulasi keseluruhan kuesioner *management awareness* dengan menggunakan skala *likert* :

Tabel 4.5 Rekapitulasi Keseluruhan Kuesioner *Management Awareness* dengan Skala *Likert*

No	Jawaban	Skala Likert	Frekuensi (f)	Persentase $P = f/n \times 100\%$
1.	Sangat Tidak Penting	1	2	0,24%
2.	Tidak Penting	2	24	2,83%
3.	Sedikit Penting	3	81	9,56%
4.	Penting	4	447	52,77%
5.	Sangat Penting	5	293	34,59%
Total = $\sum f$			847	100%
Jumlah skor dari hasil penelitian = $\sum f \times skala$			3546	

(Sumber: Data diolah dengan MS Excel 2013)

Pada Tabel 4.5 dapat dilihat nilai persentase terbesar adalah 52,77% Artinya sebagian besar proses TI berdasarkan penilaian responden pada PUSTIPD dinyatakan penting. Untuk mencari nilai tingkat kepentingan, peneliti menggunakan *microsoft excel 2013* sebagai alat bantu menghitung rata-rata dari setiap proses TI.

2. Rekapitulasi Perhitungan Tingkat *Maturity Level*

Hasil pemetaan *IT process* pada COBIT 4.1 berdasarkan fokus area utama manajemen risiko menghasilkan 81 pertanyaan. Setiap tingkatan pertanyaan tersebut dihitung dengan *maturity model* pada COBIT 4.1.

Maturity model dimaksudkan untuk mengetahui keberadaan persoalan yang ada dan bagaimana menentukan prioritas peningkatan. *Maturity level* menggunakan 0 sampai 5 tingkatan yaitu 0 (*non-existent*), 1 (*initial/ad-hoc*), 2 (*repeatable but intuitive*), 3 (*defined*), 4 (*manage and measurable*) dan 5 (*optimised*). Semakin tinggi *maturity level* maka akan semakin baik proses pengelolaan teknologi informasi. Responden akan memilih tingkat pengelolaan dan pengendalian yang sesuai dengan kondisi saat ini. Hal ini berguna dalam mengetahui keberadaan persoalan yang ada dan bagaimana menentukan prioritas peningkatan sehingga organisasi dapat mengenali deskripsi kemungkinan keadaan saat ini.

Kuesioner II : *Maturity Level*

Kuesioner ini bertujuan untuk mendapatkan informasi mengenai pendapat atau opini dari Saudara/i tentang pengelolaan Teknologi Informasi (TI) pada PUSTIPD Universitas Islam Negeri Raden Fatah Palembang, yang akan digunakan dalam rangka penelitian skripsi.

Kuesioner *Maturity Level* ini dikembangkan untuk mengetahui tingkat kematangan pada proses TI untuk kondisi terkini. Adapun pendekatan dalam pengukuran dilakukan dengan mempertimbangkan 6 atribut *maturity level* yang didefinisikan dalam COBIT 4.1.

Untuk mempermudah responden dalam menjawab, maka kuesioner ini dirancang dalam bentuk pilihan ganda. Masing-masing pertanyaan mempunyai 6 pilihan jawaban yang menunjukkan tingkat kepentingan terhadap atribut tertentu pada proses TI. Pada kolom jawaban, responden dapat memilih salah satu jawaban yang dianggap paling bisa mewakili seberapa penting proses tersebut dengan memberikan tanda (✓) pada tempat yang tersedia.

Untuk itu mohon kiranya Saudara/i dapat memberikan pendapatnya atas pernyataan-pernyataan dalam kuesioner ini, untuk dapat diolah lebih lanjut.

Nama Responden	
Jabatan Responden	
Unit/Bidang Subbid	

Legenda Untuk Pedoman Umum COBIT Manajemen Penilaian Kematangan **:

Penilaian	Deskripsi
0 – Proses belum ada	Organisasi sama sekali belum memiliki kebijakan dan prosedur yang diperlukan untuk melaksanakan praktik-praktik pengendalian intern.
1 – Proses dirintis	Terdapat praktik pengendalian intern, namun pendekatan risiko dan pengendalian yang diperlukan masih bersifat <i>ad-hoc</i> dan tidak terorganisasi dengan baik.
2 – Pengulangan proses berdasarkan intuisi	Terdapat standar proses dalam hal tersebut, tetapi masih secara umum.
3 – Proses telah didefinisikan	Terdapat prosedur yang telah distandarisasi dan didokumentasikan.
4 – Proses dikelola dan terukur	Sudah terencana, terorganisasi dan terukur, sehubungan terdapat prosedur.
5 – Proses dioptimalkan	Proses yang distandarkan, selalu memonitor, dan melakukan perbaikan.

Kode	Proses	Jawaban					
		Proses belum ada	Proses dirintis	Pengulangan Proses berdasarkan intuisi	Proses telah didefinisikan	Proses dikelola dan terukur	Proses dioptimalkan
		0	1	2	3	4	5
PO4	Menetapkan proses TI, organisasi, dan hubungan						

Plan and Organize, mencakup proses perencanaan dan penyalarsan Teknologi Informasi (TI) dengan strategi perusahaan sehingga dapat berkontribusi dengan baik untuk organisasi?

Gambar 4.8 Kuesioner *Maturity Level*

Pada sub bab ini akan dijelaskan hasil dari jawaban responden berdasarkan pernyataan yang diberikan. Secara umum rata-rata jawaban responden untuk seluruh pernyataan domain *plan and organize* sebanyak 26 pernyataan, rincian pernyataan domain *plan and organize* tersebut ialah PO4 sebanyak 15 pernyataan, PO6 sebanyak 5 pernyataan dan PO9 sebanyak 6 pernyataan. Untuk domain *deliver*

and support yaitu sebanyak 36 pernyataan, masing-masing pernyataan domain *deliver and support* adalah DS2 sebanyak 4 pernyataan, DS4 sebanyak 10 pernyataan, DS5 sebanyak 11 pernyataan, DS11 sebanyak 6 pernyataan, dan DS12 sebanyak 5 pernyataan. Sedangkan domain *monitor and evaluate* sebanyak 19 pernyataan, terdiri dari ME2 sebanyak 7 pernyataan, ME3 sebanyak 5 pernyataan, dan ME4 sebanyak 7 pernyataan. Adapun rincian dari hasil pengujian tersebut dapat di lihat pada Table 4.6:

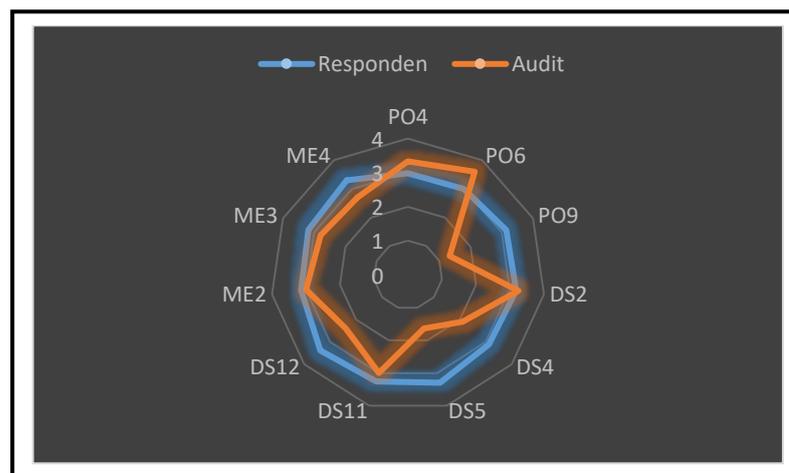
Tabel 4.6 Rekapitulasi *Maturity Level* Subdomain

<i>IT Process</i>		<i>Indeks Maturity</i>	<i>Maturity Level</i>	<i>Keterangan</i>
PO4	<i>Define the IT Processes, Organization and Relationships</i>	2,98	3	<i>Defined</i>
PO6	<i>Communicate Management Aims and Direction</i>	3	3	<i>Defined</i>
PO9	<i>Assess and Manage IT Risk</i>	3,15	3	<i>Defined</i>
DS2	<i>Manage Third-party Services</i>	3,18	3	<i>Defined</i>
DS4	<i>Ensure Continuous Service</i>	3,12	3	<i>Defined</i>
DS5	<i>Ensure Systems Security</i>	3,30	3	<i>Defined</i>
DS11	<i>Manage Data</i>	3,26	3	<i>Defined</i>
DS12	<i>Manage the Physical Environment</i>	3,38	3	<i>Defined</i>
ME2	<i>Monitor and Evaluate Internal Control</i>	3,14	3	<i>Defined</i>
ME3	<i>Ensure Compliance With External Requirements</i>	3,12	3	<i>Defined</i>
ME4	<i>Provide IT Governance</i>	3,29	3	<i>Defined</i>

(Sumber: Data diolah dengan *MS Excel* 2013)

Dari hasil jawaban responden untuk setiap pernyataan yang diberikan. Secara umum rata-rata jawaban responden untuk keseluruhan pernyataan pada domain nilai indeks *maturity level Plan and Organize* (PO) adalah antara 2,98 sampai 3,15 domain *Deliver and Support* (DS) adalah 3,12 sampai 3,30 dan *Monitor and*

Evaluate (ME) 3,12 sampai 3,29 atau berada pada *maturity level* 3 artinya prosedur distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Setelah dilakukan perhitungan rata-rata *maturity level* pada setiap subdomain, hasil penilaian tersebut digambarkan dalam sebuah grafik radar (*spider chart*) gambaran antara penilaian responden dan penilaian audit. Dapat dilihat pada Gambar 4.9 sebagai berikut :



Gambar 4.9 Grafik Radar (*Spider Chart*) Subdomain antara Responden dan Hasil Audit

Untuk memperjelas hasil yang lebih akurat maka peneliti memberi langkah-langkah proses perhitungan *maturity level* pada tabel 4.3, sebagai contoh perhitungan yang akan diambil secara acak yaitu pada domain *Plan and Organize* yaitu pada proses TI PO4 *Define the IT Processes, Organization and Relationships* dan ME2 *Monitor and Evaluate Internal Control* sebagai berikut:

Diketahui jumlah jawaban *Define the IT Processes, Organization and Relationships* 492, jumlah item pernyataan sebanyak 15 butir pernyataan dan 11 responden maka indeks *maturity level* sebagai berikut:

$$\text{Indeks maturity} = \frac{\Sigma(\text{jumlah jawaban})}{\Sigma(\text{jumlah pertanyaan} \times \text{jumlah responden})}$$

$$\text{Indeks} = \frac{492}{15 \times 11}$$

$$\text{Indeks} = \frac{492}{165} = 2,981818$$

Maka hasil perhitungan *maturity level* nilai dari subdomain *Define the IT Processes, Organization and Relationships* yaitu 2,98.

Diketahui jumlah jawaban *Monitor and Evaluate Internal Control* 242, jumlah item pernyataan sebanyak 7 butir pernyataan dan 11 responden maka indeks *maturity level* sebagai berikut:

$$\text{Indeks maturity} = \frac{\Sigma(\text{jumlah jawaban})}{\Sigma(\text{jumlah pertanyaan} \times \text{jumlah responden})}$$

$$\text{Indeks} = \frac{242}{7 \times 11}$$

$$\text{Indeks} = \frac{242}{77} = 3,1428701$$

Maka hasil perhitungan *maturity level* nilai dari subdomain *Monitor and Evaluate Internal Control* yaitu 3,14.

Berdasarkan grafik radar (*spider chart*), kondisi pada setiap subdomain keseluruhan *maturity level* berada pada level 3 dengan nilai tertinggi pada domain DS12 *Manage the Physical environment* sebesar 3,38 dan nilai terendah berada pada domain *Define the IT Processes, Organization and Relationships* sebesar 2,98.

Dalam mendapatkan hasil keadaan saat ini, peneliti menggunakan alat bantu Microsoft Excel 2013 dengan mencari rata-rata dari keseluruhan perhitungan *maturity level* pada setiap *indicator* domain *Plan and Organise, Delivery and Support*, *Monitor and Evaluation*. Rata-rata perhitungan setiap domain dapat dilihat pada Tabel 4.7 sebagai berikut:

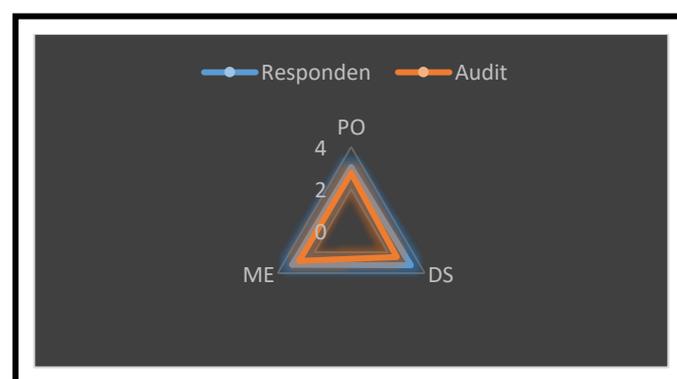
Tabel 4.7 Hasil Pengujian Domain

No	Domain	Indeks Maturity	Maturity Level	Keterangan
1.	<i>Plan and Organize</i>	3,04	3	<i>Defined</i>
2.	<i>Delivery and Support</i>	3,25	3	<i>Defined</i>
3.	<i>Monitor and Evaluate</i>	3,21	3	<i>Defined</i>
Tingkat kematangan keseluruhan		3,17	3	<i>Defined</i>

(Sumber: Data diolah dengan *MS Excel* 2013)

Hasil pengujian kuesioner *maturity level*, rata-rata tingkat *maturity level* yang diperoleh adalah 3,04 untuk domain *Plan and Organize*, 3,25 untuk domain *Deliver and Support*, 3,21 untuk domain *Monitor and Evaluate*. Nilai dari keseluruhan perhitungan *maturity level* saat ini pada PUSTIPD adalah 3,17. Berdasarkan tingkatan *maturity level* saat ini PUSTIPD berada di level 2,50 – 3,49 yaitu 3 (*defined*). Tingkat *maturity level* 3 (*defined*) secara umum menurut *framework* COBIT 4.1 artinya prosedur distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Kemudian diamanatkan bahwa proses-proses tersebut harus diikuti. Namun penyimpangan tidak mungkin dapat terdeteksi. Prosedur sendiri tidak lengkap namun sudah memformalkan praktek yang berjalan.

Setelah dilakukan perhitungan rata-rata *maturity level* pada setiap domain, perhitungan tersebut digambarkan dalam sebuah radar (*spider chart*) untuk menampilkan prioritas keadaan saat ini. Dapat dilihat pada gambar 4.4 sebagai berikut :



Gambar 4.4 Grafik Radar (*Spider Chart*) Domain antara Responden dan Hasil Audit

Dapat disimpulkan bahwa untuk proses-proses teknologi informasi untuk manajemen risiko pada PUSTIPD dari hasil penilaian responden tersebut untuk subdomain maupun domain berada pada *maturity level 3* (defined).

4.5 Hasil dan Pembahasan

Setelah peneliti melakukan audit teknologi informasi untuk manajemen risiko pada PUSTIPD, hasil temuan audit saat ini tingkat kematangannya berada pada level 3 (*defined*) dengan nilai 2,69 (dapat dilihat pada Tabel 4.4). Berdasarkan hasil jawaban kuesioner pada penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, tingkat kematangan TI untuk manajemen risiko menurut responden berada pada tingkat 3 (*defined*) dengan nilai 3,17 (dapat dilihat pada Tabel 4.7) artinya sesuai *maturity level* antara penilaian hasil audit dan responden.

Dari kesesuaian antara jawaban responden dengan bukti yang ada, dapat disimpulkan bahwa terdapat prosedur yang distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan, diamanatkan bahwa proses-proses tersebut harus diikuti. Namun penyimpangan mungkin tidak dapat terdeteksi. Prosedur sendiri tidak lengkap namun sudah memformalkan praktek yang telah dijalankan.

Setelah dilakukan pengukuran tingkat kematangan proses TI yang membantu manajemen melihat dimana letak kekurangan proses manajemen risiko TI. Maka diberikan rekomendasi guna membantu perusahaan mengambil keputusan, untuk menentukan perbaikan mekanisme, prosedur, dan proses TI yang digunakan.

1. Domain *Plan and Organize* (PO)

Pada domain *plan and organize*, mencakup strategi dan taktik dan menyangkut identifikasi teknologi informasi yang dapat memberikan kontribusi terbaik untuk pencapaian tujuan. Realisasi visi strategis perlu direncanakan, dikomunikasikan dan dikelola untuk perspektif yang berbeda. Organisasi yang tepat serta infrastruktur teknologi harus diberlakukan. Terdapat 3 proses TI pada domain *plan and organize* yaitu PO4, PO6, dan PO9 yang telah dihitung *maturity level* dari hasil audit tingkat kematangan berada pada tingkat 3 (*defined*) dengan nilai 2,75 (dapat dilihat pada Tabel 4.3) dan dari jawaban responden juga berada pada tingkat 3 (*defined*) dengan nilai 3,04 (dapat dilihat pada Tabel 4.7). Artinya sesuai antara penilaian audit dan responden, keadaan TI saat ini terdapat prosedur yang distandarisasi dan didokumentasikan serta dikomunikasikan melalui pelatihan.

1.1 PO4 *Define the IT Processes, Organization and Relationships*

Dari hasil tingkat kematangan pada proses TI *Define the IT Processes, Organization and Relationships* hasil temuan audit mengenai teknologi informasi untuk manajemen risiko saat ini pada organisasi berada pada tingkat kematangan 3 (*defined*) dengan nilai 3.33 (dapat dilihat pada Tabel 4.2), artinya peran dan tanggung jawab TI yang ditetapkan untuk organisasi dan pihak ketiga ada. Organisasi TI dikembangkan, didokumentasikan, dikomunikasikan dan diselaraskan dengan strategi TI. Lingkungan kontrol internal didefinisikan. Ada formalisasi hubungan dengan pihak lain, termasuk komite pengarah, audit internal, dan manajemen vendor. Organisasi TI secara fungsional lengkap. Ada definisi fungsi yang harus dilakukan oleh personel TI dan yang harus dilakukan oleh pengguna. Persyaratan dan keahlian staf TI yang penting ditetapkan dan dipenuhi.

Ada definisi formal tentang hubungan dengan pengguna dan pihak ketiga. Pembagian peran dan tanggung jawab didefinisikan dan diimplementasikan. Menurut penilaian responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 2,98 (dapat dilihat pada Tabel 4.6) artinya kesesuaian jawaban antara responden dan hasil audit sesuai.

Berikut penjelasan mengenai keadaan TI dari hasil audit pada PUSTIPD UIN Raden Fatah Palembang:

Tabel 4.8 Keadaan TI PO4 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
PO4.1	Terdapat penentuan kerangka proses teknologi informasi, namun pencapaian kerangka kerja teknologi informasi tidak seluruhnya telah dilakukan.	3	3	Sesuai
PO4.2	Terdapat strategi teknologi informasi, komite strategi teknologi informasi telah dibentuk secara umum untuk melaksanakan strategi teknologi informasi.	4	3	Sesuai
PO4.3	Terdapat komite pengarah teknologi informasi dari vendor	3	3	Sesuai
PO4.4	Terdapat penempatan fungsi teknologi informasi dalam struktur organisasi, namun belum secara keseluruhan.	2	3	Tidak sesuai
PO4.5	Terdapat penetapan struktur organisasi teknologi informasi dilihat dari analisis jabatan, penempatan proses teknologi informasi dilakukan secara akademik.	3	3	Sesuai
PO4.6	Terdapat pembentukan peran dan tanggung jawab teknologi informasi sesuai <i>job desk</i>	4	3	Sesuai
PO4.7	Terdapat tanggung jawab untuk jaminan kualitas teknologi informasi	3	3	Sesuai
PO4.8	Terdapat tanggung jawab untuk keamanan dilakukan <i>monitoring</i> secara berkala dan <i>maintenance</i> mendalam.	4	3	Sesuai
PO4.9	Terdapat kepemilikan data dengan membagi hak akses, namun pengklarifikasian dilakukan sesuai kebutuhan	3	3	Sesuai
PO4.10	Terdapat pengawasan teknologi informasi untuk memastikan peran dan tanggung jawab dilakukan	3	3	Sesuai
PO4.11	Terdapat pembagian peran dan tanggung jawab pada pemisahan tugas	4	3	Sesuai
PO4.12	Terdapat evaluasi kepegawaian secara berkala dengan laporan kerja karyawan didalam rapat internal.	4	3	Sesuai
PO4.13	Terdapat penentuan dan identifikasi staf teknologi informasi secara umum	3	3	Sesuai

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
PO4.14	Terdapat kebijakan dan prosedur staf yang terkontrak	4	3	Sesuai
PO4.15	Terdapat hubungan teknologi informasi dengan bisnis teknologi informasi.	4	3	Sesuai
Rata-rata		3,33	2,98	Sesuai

(Sumber: Data diolah dengan *MS Excel* 2013)

Dari hasil kesesuaian audit dan responden PO4 terdapat proses yang tidak sesuai atau tidak dijalankan sesuai dengan opini responden, yaitu pada PO4.4 responden menilai bahwa proses TI PO4.4 sudah didefinisikan dan didokumentasikan, namun setelah dilakukan audit hasilnya proses tersebut masih dilakukan secara taktis sesuai kebutuhan. Tetapi juga terdapat *maturity level* dari hasil audit diatas responden, berada pada tingkat 4 yaitu PO4.2, PO4.6, PO4.8, PO4.11, PO4.12, PO4.14, dan PO4.15 artinya proses tersebut telah memiliki pengawasan dan pengukuran mengenai proses TI, organisasi dan hubungan. Diperlukan rekomendasi untuk proses teknologi informasi yang mengacu pada COBIT.

Tabel 4.9 Rekomendasi PO4

Control Objective	Rekomendasi
PO4.1	Melakukan pengukuran kerangka kerja teknologi informasi secara keseluruhan, mulai dari struktur proses dan hubungan TI, kepemilikan, kedewasaan, pengukuran kinerja, peningkatan, kepatuhan, target kualitas dan rencana untuk mencapainya. Harus menyediakan integrasi antara proses TI, manajemen portofolio perusahaan, proses bisnis dan proses perubahan bisnis. Kerangka proses TI harus diintegrasikan ke dalam sistem manajemen mutu (SMM) dan kerangka kerja pengendalian internal.
PO4.2	Memastikan tata kelola TI, sebagai bagian tata kelola perusahaan, menangani secara memadai; memberi saran tentang arah strategis; dan meninjau investasi besar.
PO4.3	Membentuk komite pengarah TI yang terdiri dari eksekutif, bisnis dan manajemen TI

Control Objective	Rekomendasi
PO4.4	Menempatkan fungsi TI dalam struktur organisasi secara keseluruhan dengan model bisnis yang bergantung pada pentingnya TI dalam perusahaan, khususnya kekritisannya terhadap strategi bisnis dan tingkat ketergantungan operasional pada TI. Garis pelaporan CIO harus sepadan dengan pentingnya TI di dalam perusahaan.
PO4.5	Menetapkan struktur organisasi teknologi informasi eksternal dan internal, dan menempatkan proses teknologi informasi secara berkala dalam meninjau kebutuhan staf.
PO4.6	Mempertahankan peran dan tanggung jawab untuk kebutuhan organisasi. Serta menetapkan dan mengkomunikasikan pengguna akhir yang menggambarkan antara personil TI dan otoritas pengguna akhir, tanggung jawab dan akuntabilitas untuk memenuhi kebutuhan organisasi.
PO4.7	Mempertahankan tanggung jawab untuk jaminan kualitas teknologi informasi, dan memberikan kelompok penjamin kualitas dengan sistem. Pastikan bahwa penempatan organisasi dan tanggung jawab dan ukuran grup QA memenuhi persyaratan organisasi.
PO4.8	Menetapkan tanggung jawab manajemen risiko dan keamanan di tingkat perusahaan untuk menangani isu-isu organisasional.
PO4.9	Perusahaan harus membuat keputusan tentang mengklasifikasikan informasi dan sistem dan melindungi mereka sesuai dengan klasifikasi.
PO4.10	Menetapkan penilaian apakah semua personil memiliki kewenangan dan sumber daya yang memadai.
PO4.11	Mempertahankan pembagian peran dan tanggung jawab pada pemisahan tugas
PO4.12	Mempertahankan evaluasi kepegawaian secara berkala dengan laporan kerja karyawan didalam rapat internal.
PO4.13	Menentukan secara khusus dan identifikasi personil TI kunci (misalnya, penggantian / cadangan personel), dan kurangi ketergantungan pada satu individu yang melakukan fungsi pekerjaan penting.
PO4.14	Mempertahankan kebijakan dan prosedur staf yang terkontrak
PO4.15	Membentuk dan mempertahankan koordinasi optimal, komunikasi, dan struktur penghubung antara fungsi TI dan berbagai kepentingan lain di dalam dan di luar fungsi TI,

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa dalam kerangka proses TI harus melakukan pengukuran kerangka kerja teknologi informasi secara keseluruhan. Selain itu, PUSTIPD harus memastikan tata kelola TI sebagai bagian tata kelola perusahaan. Melakukan penempatan fungsi TI secara keseluruhan, tidak hanya pada bagian tertentu. PUSTIPD harus membuat keputusan tentang mengklarifikasikan informasi dan sistem dan melindungi sesuai dengan klarifikasi. Menentukan secara khusus dan identifikasi personil TI kunci (misalnya, penggantian / cadangan personel), dan kurangi ketergantungan pada satu individu yang melakukan fungsi pekerjaan penting. Kemudian Membentuk dan

mempertahankan koordinasi optimal, komunikasi, dan struktur penghubung antara fungsi TI dan berbagai kepentingan lain di dalam dan di luar fungsi TI.

1.2 PO6 *Communicate Management Aims and Direction*

Dari hasil tingkat kematangan pada proses TI *Communicate Management Aims and Direction* menurut hasil temuan audit mengenai teknologi informasi untuk manajemen risiko saat ini *maturity level* pada organisasi berada pada tingkat 4 (*managed and measurable*) dengan nilai 3,6 (dapat dilihat pada Tabel 4.2), artinya artinya manajemen menerima tanggung jawab untuk mengkomunikasikan kebijakan pengendalian internal dan mendelegasikan tanggung jawab dan mengalokasikan sumber daya yang cukup untuk menjaga lingkungan sejalan dengan perubahan signifikan. Lingkungan pengendalian informasi yang positif dan proaktif, termasuk komitmen terhadap kualitas dan kesadaran keamanan TI, ditetapkan. Seperangkat kebijakan, rencana dan prosedur yang lengkap dikembangkan, dipelihara dan dikomunikasikan dan merupakan gabungan dari praktik-praktik baik internal. Kerangka untuk peluncuran dan pemeriksaan kepatuhan berikutnya ditetapkan. Sedangkan berdasarkan penilaian responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3 (dapat dilihat pada Tabel 4.6) artinya kontrol informasi lengkap dan lingkungan manajemen mutu dikembangkan, didokumentasikan dan dikomunikasikan oleh manajemen dan mencakup kerangka kerja untuk kebijakan, rencana dan prosedur. Proses pengembangan kebijakan disusun, dipelihara dan diketahui oleh staf, dan kebijakan, rencana dan prosedur yang ada cukup masuk akal dan mencakup isu-isu kunci. Manajemen membahas pentingnya kesadaran keamanan TI dan memulai program kesadaran. Pelatihan formal tersedia untuk mendukung lingkungan

pengendalian informasi tetapi tidak diterapkan secara ketat. Meskipun ada kerangka kerja pengembangan menyeluruh untuk kebijakan dan prosedur pengendalian, ada pemantauan kepatuhan yang tidak konsisten terhadap kebijakan dan prosedur ini. Ada kerangka kerja pembangunan secara keseluruhan. Teknik untuk mempromosikan kesadaran keamanan telah distandarisasi dan diformalkan. Berikut penjelasan mengenai keadaan TI dari hasil audit:

Tabel 4.10 Keadaan TI PO6 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
PO6.1	Terdapat penentuan elemen lingkungan kontrol untuk teknologi informasi	4	3	Sesuai
PO6.2	Terdapat pengembangan dan pemeliharaan kerangka kerja dan selaras dengan kebijakan TI dan lingkungan pengendalian serta kerangka kerja risiko dan kontrol perusahaan.	3	3	Sesuai
PO6.3	Terdapat manajemen kebijakan teknologi informasi	4	3	Sesuai
PO6.4	Terdapat peluncuran dan penegakan kebijakan teknologi informasi semua staf secara umum	3	3	Sesuai
PO6.5	Terdapat komunikasi kesadaran dan pemahaman tentang tujuan dan arah TI	4	3	Sesuai
Rata-rata		3,6	3	Tidak Sesuai

(Sumber: Data diolah dengan *MS Excel* 2013)

Dari hasil audit terdapat *maturity level* yang nilainya lebih tinggi dari hasil responden. Artinya proses tersebut dilakukan manajemen untuk menerima tanggung jawab yaitu pada *control objective* PO6.1, PO6.3 dan PO6.5. Sedangkan *control objective* PO6.2 dan PO6.4 telah sesuai dengan nilai *maturity level* dari hasil audit. Untuk peningkatan proses teknologi informasi yang lebih baik diberikan rekomendasi yang mengacu pada COBIT.

Tabel 4.11 Rekomendasi PO6

Control Objective	Rekomendasi
PO6.1	Mempertahankan penentuan elemen lingkungan kontrol TI yang selaras dengan filosofi manajemen perusahaan dan operasi.
PO6.2	Pastikan kerangka kerja selaras dengan kebijakan TI dan lingkungan pengendalian serta kerangka kerja risiko dan kontrol perusahaan.
PO6.3	Mempertahankan pengembangan dan pelihara satu set kebijakan untuk mendukung strategi TI.
PO6.4	Tingkatkan proses peluncuran dan penegakkan kebijakan TI untuk semua staf yang relevan,
PO6.5	Mempertahankan pengkomunikasikan kesadaran dan pemahaman tentang tujuan dan arahan bisnis dan TI kepada pemangku kepentingan dan pengguna yang tepat di seluruh perusahaan.

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa dalam lingkungan pengendalian PUSTIPD harus memastikan kerangka kerja selaras dengan kebijakan TI dan lingkungan pengendalian serta kerangka kerja risiko dan kontrol perusahaan. Selain itu, perlunya pengembangan dan pemeliharaan satu kebijakan untuk mendukung strategi TI. Serta mengkomunikasikan kesadaran dan pemahaman tentang tujuan dan arahan bisnis dan TI kepada pemangku kepentingan perusahaan.

1.3 PO9 Assess and Manage IT Risk

Dari hasil tingkat kematangan pada proses *TI Assess and Manage IT Risk* hasil temuan audit mengenai teknologi informasi untuk manajemen risiko saat ini pada organisasi berada pada tingkat kematangan 1 (*initial/ad hoc*) dengan nilai 1,33 (dapat dilihat pada Tabel 4.2), artinya risiko TI dipertimbangkan secara ad-hoc. Penilaian informal terhadap risiko proyek terjadi sebagaimana ditentukan oleh masing-masing proyek. Penilaian risiko terkadang diidentifikasi dalam rencana proyek tetapi jarang ditugaskan untuk manajer tertentu. Risiko terkait TI tertentu, seperti keamanan, ketersediaan, dan integritas, kadang-kadang dipertimbangkan berdasarkan proyek per proyek. Risiko terkait TI yang mempengaruhi operasi sehari-hari jarang dibahas dalam rapat manajemen. Ketika risiko dipertimbangkan,

mitigasi tidak konsisten. Ada pemahaman yang muncul bahwa risiko TI penting dan perlu dipertimbangkan. Sedangkan menurut responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,15 (dapat dilihat pada Tabel 4.6) artinya kebijakan manajemen risiko seluruh organisasi mendefinisikan kapan dan bagaimana melakukan penilaian risiko. Manajemen risiko mengikuti proses yang ditentukan yang didokumentasikan. Pelatihan manajemen risiko tersedia untuk semua anggota staf. Keputusan untuk mengikuti proses manajemen risiko dan menerima pelatihan diserahkan kepada kebijaksanaan individu. Metodologi untuk penilaian risiko meyakinkan dan sehat dan memastikan bahwa risiko utama untuk bisnis diidentifikasi. Suatu proses untuk mengurangi risiko utama biasanya dilembagakan begitu risiko teridentifikasi. Deskripsi pekerjaan mempertimbangkan tanggung jawab manajemen risiko. Berikut penjelasan mengenai keadaan TI dari hasil audit pada PUSTIPD UIN Raden Fatah Palembang dapat dilihat pada Tabel 4.12:

Tabel 4.12 Keadaan PO9 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
PO9.1	Belum ada penetapan kerangka kerja manajemen risiko TI	0	3	Tidak sesuai
PO9.2	Belum ada penetapan konteks risiko	1	3	Tidak sesuai
PO9.3	Terdapat proses identifikasi risiko, namun proses pencatatan belum dilakukan	2	3	Tidak sesuai
PO9.4	Belum dilakukan penilaian risiko	1	3	Tidak sesuai
PO9.5	Belum ada pengembangan dan pertahanan proses respons risiko yang dirancang	1	3	Tidak sesuai
PO9.6	Terdapat prioritas dan perenanaan kegiatan pengendalian	3	3	Sesuai
Rata-rata		1	3,15	Tidak sesuai

(Sumber: Data diolah dengan *MS Excel* 2013)

Terdapat *control objective* pada PO9.1, PO9.2, PO9.3, PO9.4, dan PO4.5 yang tidak sesuai dengan hasil responden. PO9.1 belum melakukan penilaian risiko untuk proses dan keputusan bisnis, perusahaan belum memiliki kerangka manajemen risiko teknologi informasi. Untuk *control objective* PO9.2, PO9.4, PO9.5 proses disadari untuk diatasi namun dengan menggunakan pendekatan *ad-hoc*, dan *control objective* PO9.3 ditemukan pengembangan proses dan proses diikuti oleh pihak-pihak yang berbeda untuk pekerjaan yang sama. Dalam hal ini rekomendasi sangat diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT pada tabel 4.13 berikut ini:

Tabel 4.13 Rekomendasi PO9

Control Objective	Rekomendasi
PO9.1	Menetapkan kerangka kerja manajemen risiko TI yang selaras dengan kerangka manajemen risiko perusahaan (organisasi).
PO9.2	Menetapkan konteks di mana kerangka penilaian risiko diterapkan untuk memastikan hasil yang sesuai.
PO9.3	Meningkatkan proses identifikasi risiko, mencatat dan pertahankan risiko yang relevan dalam registri risiko.
PO9.4	Menilai secara berulang kemungkinan dan dampak dari semua risiko yang teridentifikasi, menggunakan metode kualitatif dan kuantitatif
PO9.5	Mengembangkan dan pertahankan proses respons risiko yang dirancang untuk memastikan bahwa pengendalian yang hemat biaya mengurangi paparan risiko secara berkelanjutan
PO9.6	Memprioritaskan dan merencanakan kegiatan pengendalian di semua tingkatan untuk menerapkan respons risiko yang diidentifikasi seperlunya

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa organisasi harus terlebih dahulu membentuk atau menetapkan kerangka kerja manajemen risiko TI terlebih dahulu yang di selaraskan dengan kerangka kerja manajemen risiko perusahaan. Kemudian, baru dibentuk konteks risiko untuk pengidentifikasian risiko dengan mencatat serta memperbaiki risiko yang terjadi. PUSTIPD juga harus mengadakan penilaian risiko berguna untuk pemeliharaan dan pemantauan rencana tindakan kedepan.

2. Domain *Deliver and Support* (DS)

Pada domain *deliver and support* berkaitan dengan pengiriman yang sebenarnya dari layanan yang dibutuhkan, yang meliputi pengiriman layanan, manajemen keamanan dan kontinuitas, dukungan layanan untuk pengguna, dan pengelolaan data dan fasilitas operasional. Terdapat 5 proses TI pada domain *delivery and support* yaitu DS2, DS4, DS5, DS11 dan DS12 yang telah dihitung *maturity level* dari hasil audit tingkat kematangannya berada pada tingkat 2 (*repeatable but intuitive*) dengan nilai 2,48 (dapat dilihat pada Tabel 4.3) sedangkan berdasarkan jawaban responden berada pada tingkat 3 (*defined*) dengan nilai 3,24 (dapat dilihat pada Tabel 4.7).

2.1 DS2 *Manage Third-party Services*

Dari hasil tingkat kematangan pada proses TI *Manage Third-party Services* hasil temuan audit mengenai teknologi informasi untuk manajemen risiko tingkat kematangan saat ini pada organisasi berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,25 (dapat dilihat pada Tabel 4.3). Sedangkan menurut responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,18 (dapat dilihat pada Tabel 4.6) artinya prosedur terdokumentasi dengan baik ada untuk mengatur layanan pihak ketiga, dengan proses yang jelas untuk memeriksa dan bernegosiasi dengan vendor. Ketika sebuah kesepakatan untuk penyediaan layanan dibuat, hubungan dengan pihak ketiga adalah murni kontrak. Sifat dari layanan yang akan diberikan terperinci dalam kontrak termasuk persyaratan hukum, operasional dan kontrol. Tanggung jawab untuk pengawasan layanan pihak ketiga ditetapkan. Ketentuan kontrak didasarkan pada *template* standar. Artinya kesesuaian antara penilaian hasil audit dan penilaian responden sesuai Berikut penjelasan mengenai keadaan TI dari hasil audit pada PUSTIPD UIN Raden Fatah Palembang.

Tabel 4.14 Keadaan DS2 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
DS2.1	Terdapat identifikasi layanan pemasok secara umum	2	3	Tidak sesuai
DS2.2	Terdapat formalitas proses manajemen hubungan pemasok, penyelesaian masalah dan pemastian kualitas berdasarkan SLA	4	3	Sesuai
DS2.3	Terdapat identifikasi dan mitigasi risiko pemasok	4	3	Sesuai
DS2.4	Terdapat pengawasan kinerja pemasok dengan evaluasi dan <i>monitoring</i>	3	3	Sesuai
Rata-rata		3,25	3,18	Sesuai

(Sumber: Data diolah dengan *MS Excel 2013*)

Terdapat nilai *maturity level* audit yang lebih rendah daripada responden berada pada DS2.1 artinya pada proses TI ini masih ada proses untuk pengawasan yang bersifat informal. Dan terdapat *maturity level* yang lebih tinggi yaitu pada DS2.2 dan DS2.3 artinya kriteria formal dan standar ditetapkan untuk mendefinisikan persyaratan. Untuk *control objective* DS2.4 sudah sesuai dengan hasil audit. Rekomendasi diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT.

Tabel 4.15 Rekomendasi DS2

Control Objective	Rekomendasi
DS2.1	Mengidentifikasi semua layanan pemasok, dan kategorikan sesuai dengan jenis pemasok, signifikansi dan kekritisan.
DS2.2	Mempertahankan manajemen hubungan pemasok
DS2.3	Mempertahankan identifikasi dan mitigasi risiko pemasok
DS2.4	Menetapkan proses untuk memantau penyampaian layanan untuk memastikan bahwa pemasok memenuhi persyaratan bisnis saat ini.

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa PUSTIPD harus mengidentifikasi semua layanan pemasok, dikategorikan sesuai

dengan jenis, signifikansi dan kekritisannya. Dokumen formal hubungan teknis dan organisasi serta manajemen hubungan pemasok dipertahankan. PUSTIPD juga harus memastikan kontrak sesuai dengan persyaratan hukum dan menetapkan proses untuk memantau penyampaian layanan untuk memastikan bahwa pemasok memenuhi persyaratan bisnis saat ini dan terus mematuhi perjanjian kontrak dan SLA.

2.2 DS4 *Ensure Continuous Service*

Dari hasil tingkat kematangan pada proses TI *Ensure Continuous Service* berdasarkan hasil temuan audit mengenai teknologi informasi untuk manajemen risiko tingkat saat ini pada organisasi berada pada tingkat kematangan 2 (*repeatable but intuitive*) dengan nilai 2,1 (dapat dilihat pada Tabel 4.2), artinya tanggung jawab untuk memastikan layanan berkelanjutan ditugaskan. Pendekatan untuk memastikan layanan berkelanjutan terpecah-pecah. Pelaporan ketersediaan sistem bersifat sporadis, mungkin tidak lengkap dan tidak memperhitungkan dampak bisnis. Tidak ada rencana kesinambungan TI yang didokumentasikan, meskipun ada komitmen untuk ketersediaan layanan berkelanjutan dan prinsip-prinsip utamanya diketahui. Inventarisasi sistem dan komponen penting ada, tetapi mungkin tidak dapat diandalkan. Praktek layanan berkelanjutan muncul, tetapi kesuksesan bergantung pada individu. Sedangkan dari hasil penilaian responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,12 (dapat dilihat pada Tabel 4.6) artinya akuntabilitas untuk pengelolaan layanan berkelanjutan tidak ambigu. Tanggung jawab untuk perencanaan dan pengujian layanan berkelanjutan ditetapkan dan ditetapkan dengan jelas. Rencana kesinambungan TI didokumentasikan dan berdasarkan pada kekritisannya sistem dan dampak bisnis. Ada

pelaporan berkala pengujian layanan berkelanjutan. Individu mengambil inisiatif untuk mengikuti standar dan menerima pelatihan untuk menghadapi insiden besar atau bencana. Manajemen mengkomunikasikan secara konsisten kebutuhan untuk merencanakan untuk memastikan layanan berkelanjutan. Komponen ketersediaan tinggi dan redundansi sistem sedang diterapkan. Inventarisasi sistem dan komponen penting dipertahankan. Berikut penjelasan mengenai keadaan TI dari hasil audit pada PUSTIPD:

Tabel 4.16 Keadaan DS4 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
DS4.1	Terdapat pengembangan kerangka kerja untuk kontinuitas TI	3	3	Sesuai
DS4.2	Terdapat pengembangan rencana kesinambungan TI diimplementasikan dengan menyesuaikan <i>workflow</i> dari renstra	4	3	Sesuai
DS4.3	Terdapat pemusatan perhatian pada item yang ditentukan sebagai yang paling penting dalam rencana kontinuitas TI	3	3	Sesuai
DS4.4	Terdapat pemeliharaan rencana kesinambungan TI	3	3	Sesuai
DS4.5	Terdapat pengujian rencana kesinambungan TI	3	3	Sesuai
DS4.6	Belum ada sesi pelatihan rencana kesinambungan TI	1	3	Tidak sesuai
DS4.7	Belum ada penentuan strategi distribusi yang dikelola dan diterapkan	0	3	Tidak sesuai
DS4.8	Belum ada perencanaan tindakan untuk pemulihan dan perbaikan layanan TI, masih dalam tahap proses pembuatan.	1	3	Tidak sesuai
DS4.9	Terdapat penyimpanan cadangan untuk pemulihan TI	2	3	Tidak sesuai
DS4.10	Belum ada prosedur pemusatan perhatian pada item yang ditentukan sebagai yang paling penting dalam rencana kontinuitas TI	1	3	Tidak sesuai
Rata-rata		2,1	3,12	Tidak sesuai

(Sumber: Data diolah dengan MS Excel 2013)

Terdapat *control objective* yang *maturity level* audit berada diatas responden, yaitu DS4.2 artinya tanggung jawab dan standar untuk layanan berkelanjutan ditegakkan. Kemudian terdapat proses yang tidak dijalankan pada DS4.7. Dan terdapat proses yang memiliki tanggung jawab untuk layanan berkelanjutan yang bersifat internal pada DS4.6, DS4.8, dan DS4.10. Untuk *control objective* DS4.9 proses memiliki pemberian tanggung jawab untuk memastikan layanan berkelanjutan. Rekomendasi sangat diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT pada Tabel 4.17 berikut:

Tabel 4.17 Rekomendasi DS4

Control Objective	Rekomendasi
DS4.1	Kerangka kerja kontinuitas harus membahas struktur organisasi untuk manajemen kontinuitas meliputi peran, tugas dan tanggung jawab penyedia layanan internal dan eksternal, manajemen dan pelanggan, dan proses perencanaan
DS4.2	Mempertahankan pengembangan rencana kesinambungan TI berdasarkan kerangka kerja dan pengurangan dampak gangguan
DS4.3	Mempertahankan pemusatan perhatian pada item yang ditentukan sebagai yang paling penting dalam rencana kontinuitas TI
DS4.4	Mengkomunikasikan perubahan dalam prosedur dan tanggung jawab dengan jelas dan tepat waktu
DS4.5	Melakukan pengujian dengan mempertimbangkan sejauh mana pengujian pemulihan aplikasi tunggal untuk terintegrasi skenario pengujian
DS4.6	Menyediakan semua pihak yang terlibat dengan sesi pelatihan reguler mengenai prosedur dan peran serta tanggung jawab mereka jika terjadi insiden atau bencana.
DS4.7	Menentukan bahwa strategi distribusi yang ditetapkan dan dikelola ada untuk memastikan bahwa rencana didistribusikan dengan benar dan aman
DS4.8	Merencanakan tindakan yang harus diambil untuk kondisi ketika TI sedang memulihkan dan melanjutkan layanan. Termasuk aktivasi situs cadangan, inisiasi pemrosesan alternatif, komunikasi pelanggan dan pemangku kepentingan, dan prosedur kembalinya.
DS4.9	Menentukan konten penyimpanan cadangan dalam kolaborasi antara pemilik proses bisnis dan personil TI.
DS4.10	Menentukan apakah manajemen TI telah menetapkan prosedur untuk menilai kecukupan rencana dalam kaitannya dengan kembalinya fungsi TI setelah bencana, dan perbarui rencana yang sesuai.

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa kerangka kerja kontinuitas harus membahas struktur organisasi untuk manajemen

kontinuitas, yang meliputi peran, tugas dan tanggung jawab penyedia layanan internal dan eksternal, manajemen dan pelanggan, dan proses perencanaan. Selain itu PUSTIPD harus mengadakan sesi pelatihan reguler kepada semua pihak terkait prosedur dan peran serta tanggung jawab ketika ada insiden atau bencana. Kemudian harus ditentukan strategi distribusi yang dikelola dan diterapkan untuk memastikan rencana didistribusikan, merencanakan tindakan yang diambil untuk memulihkan TI dan melanjutkan layanan serta menentukan pelaksanaan oleh manajemen TI dalam menetapkan prosedur untuk menilai kecukupan rencana setelah kembalinya fungsi TI.

2.3 DS5 *Ensure Systems Security*

Dari hasil tingkat kematangan pada proses TI *Ensure Systems Security* dari hasil temuan audit mengenai teknologi informasi untuk manajemen tingkat kematangan saat ini pada organisasi berada pada tingkat kematangan 2 (*repeatable but intuitive*) dengan nilai 2 (dapat dilihat pada Tabel 4.2) artinya tanggung jawab dan akuntabilitas untuk keamanan TI ditugaskan ke koordinator keamanan IT, meskipun otoritas manajemen koordinator terbatas. Kesadaran akan kebutuhan keamanan terfragmentasi dan terbatas. Meskipun informasi yang relevan dengan keamanan dihasilkan oleh sistem, itu tidak dianalisis. Layanan dari pihak ketiga tidak dapat memenuhi kebutuhan keamanan spesifik organisasi. Kebijakan keamanan sedang dikembangkan, tetapi keterampilan dan alat tidak memadai. Pelaporan keamanan TI tidak lengkap, menyesatkan atau tidak relevan. Pelatihan keamanan tersedia tetapi dilakukan terutama atas prakarsa individu. Keamanan TI dilihat terutama sebagai tanggung jawab dan domain TI dan bisnis tidak melihat keamanan TI dalam domainnya. Sedangkan dari penilaian responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,30 (dapat dilihat pada

Tabel 4.6) artinya kesadaran keamanan ada dan dipromosikan oleh manajemen. Prosedur keamanan TI didefinisikan dan selaras dengan kebijakan keamanan TI. Tanggung jawab untuk keamanan TI ditetapkan dan dipahami, tetapi tidak ditegakkan secara konsisten. Rencana keamanan dan solusi keamanan TI ada karena didorong oleh analisis risiko. Pelaporan keamanan tidak mengandung fokus bisnis yang jelas. Pengujian keamanan ad hoc (misalnya, pengujian intrusi) dilakukan. Pelatihan keamanan tersedia untuk TI dan bisnis, tetapi hanya dijadwalkan dan dikelola secara informal. Berikut penjelasan mengenai keadaan TI dari hasil audit:

Tabel 4.18 Keadaan DS5 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
DS5.1	Belum ada pengelola keamanan TI pada tingkat organisasi tertinggi yang sesuai.	0	3	Tidak sesuai
DS5.2	Terdapat penerjemahan persyaratan bisnis, risiko dan kepatuhan serta mengkomunikasikan kebijakan, namun belum ada pemastian rencana tersebut diimplementasikan	1	3	Tidak sesuai
DS5.3	Terdapat identifikasi pengguna dan aktivitas secara umum, ada proses konfirmasi pada hak akses	3	3	Sesuai
DS5.4	Terdapat proses pengelolaan akun, namun belum secara spesifik.	2	3	Tidak sesuai
DS5.5	Belum dapat menguji dan memantau implementasi keamanan TI secara proaktif	2	3	Tidak sesuai
DS5.6	Belum mendefinisikan dengan jelas dan komunikasikan karakteristik potensi insiden keamanan	1	3	Tidak sesuai
DS5.7	Belum membuat teknologi terkait keamanan tahan terhadap gangguan, dan jangan mengungkapkan dokumentasi keamanan secara tidak perlu.	1	3	Tidak sesuai
DS5.8	Terdapat kebijakan dan prosedur secara umum	1	3	Tidak sesuai

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
DS5.9	Terdapat pencegahan, deteksi, koreksi terhadap perangkat lunak berbahaya	3	3	Sesuai
DS5.10	Terdapat penggunaan teknik keamanan dan prosedur manajemen terkait	3	3	Sesuai
DS5.11	Belum bertukar data transaksi sensitif hanya melalui jalur atau media tepercaya	1	3	Tidak sesuai
Rata-rata		1,64	3,30	Tidak sesuai

(Sumber: Data diolah dengan MS Excel 2013)

Terdapat *control objective* yang belum terdapat atau belum dijalankan prosesnya yaitu pada *control objective* DS5.1. Untuk *control objective* DS5.2, DS5.6, DS5.7, DS5.8, dan DS5.11 proses keamanan TI ditangani secara reaktif. Dan *control objective* DS5.4 serta DS5.5 proses keamanannya terfragmentasi dan terbatas. Rekomendasi sangat diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT.

Tabel 4.19 Rekomendasi DS5

Control Objective	Rekomendasi
DS5.1	Kelola keamanan TI pada tingkat organisasi tertinggi yang sesuai, sehingga pengelolaan tindakan keamanan sesuai dengan persyaratan bisnis.
DS5.2	Pastikan bahwa rencana tersebut diterapkan dalam kebijakan dan prosedur keamanan bersama dengan investasi yang sesuai dalam layanan, personel, perangkat lunak, dan perangkat keras
DS5.3	Pastikan bahwa semua pengguna dan aktivitas mereka pada sistem TI dapat diidentifikasi secara unik.
DS5.4	Lakukan permintaan alamat, membuat, menerbitkan, menanggihkan, memodifikasi dan menutup akun pengguna dan hak istimewa pengguna terkait dengan satu set prosedur manajemen akun pengguna
DS5.5	Lakukan uji dan pantau implementasi keamanan TI secara proaktif. Keamanan TI harus direkreditasi secara tepat waktu untuk memastikan bahwa <i>baseline</i> keamanan informasi perusahaan yang disetujui dipertahankan.
DS5.6	Definisikan dengan jelas dan komunikasikan karakteristik potensi insiden keamanan sehingga dapat diklasifikasikan dan diperlakukan dengan baik oleh insiden dan proses manajemen masalah.
DS5.7	Buat teknologi terkait keamanan tahan terhadap gangguan, dan jangan mengungkapkan dokumentasi keamanan secara tidak perlu.

Control Objective	Rekomendasi
DS5.8	Tentukan bahwa kebijakan dan prosedur ada untuk mengatur pembuatan, perubahan, pencabutan, perusakan, distribusi, sertifikasi, penyimpanan, entri, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.
DS5.9	Letakkan tindakan pencegahan, detektif, dan korektif di tempat di seluruh organisasi
DS5.10	Pertahankan penggunaan teknik keamanan dan prosedur manajemen terkait (misalnya firewall, peralatan keamanan, segmentasi jaringan, deteksi intrusi)
DS5.11	Bertukar data transaksi sensitif hanya melalui jalur atau media tepercaya dengan kontrol untuk memberikan keaslian konten, bukti pengajuan, bukti tanda terima dan tidak menyangkal asal.

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa PUSTIPD harus mengelola keamanan TI pada tingkat organisasi tertinggi yang sesuai, melakukan penerjemahan persyaratan bisnis, risiko dan kepatuhan dalam keamanan TI dengan pertimbangan infrastruktur dan keamanan TI serta memastikan rencana tersebut diimplementasikan. Memberikan manajemen terkait akun pengguna. Melakukan proses pengujian dan pemantauan implementasi keamanan TI secara proaktif, mendefinisikan dan mengkomunikasikan karakteristik insiden secara jelas, membuat TI tahan terhadap gangguan, melakukan manajemen kunci kriptografis, dan melakukan proses menukar data transaksi sensitif melalui jalur atau media tepercaya.

2.4 DS11 Manage Data

Dari hasil tingkat kematangan pada proses TI *Manage Data* berdasarkan hasil temuan audit mengenai teknologi informasi untuk manajemen risiko tingkat kematangan saat ini pada organisasi berada pada tingkat kematangan 3 (*defined*) dengan nilai 3 (dapat dilihat pada Tabel 4.2) artinya kebutuhan untuk manajemen data dalam TI dan di seluruh organisasi dipahami dan diterima. Tanggung jawab untuk manajemen data ditetapkan. Kepemilikan data ditugaskan kepada pihak yang bertanggung jawab yang mengontrol integritas dan keamanan. Prosedur

manajemen data diformalkan dalam TI, dan beberapa alat untuk *backup*/restorasi dan pembuangan peralatan digunakan. Beberapa pemantauan atas manajemen data sudah ada. Metrik kinerja dasar ditetapkan. Pelatihan untuk anggota staf manajemen data sedang muncul. Menurut responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,26 (dapat dilihat pada Tabel 4.6) artinya kesesuaian antara penilaian hasil audit dengan hasil penilaian responden sesuai. Berikut penjelasan mengenai keadaan TI dari hasil audit dan penilaian responden:

Tabel 4.20 Keadaan DS11 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
DS11.1	Terdapat proses verifikasi data namun dilakukan sesuai dengan yang dibutuhkan	1	3	Tidak sesuai
DS11.2	Terdapat penentuan dan penerapan prosedur untuk penyimpanan dan pengarsipan data	4	3	Sesuai
DS11.3	Terdapat penentuan dan penerapan prosedur untuk memelihara inventaris	3	3	Sesuai
DS11.4	Terdapat penentuan dan penerapan prosedur untuk memastikan perlindungan data dan perangkat lunak terpenuhi	3	3	Sesuai
DS11.5	Terdapat pencadangan dan pemulihan data	3	3	Sesuai
DS11.6	Terdapat persyaratan keamanan untuk manajemen data	4	3	Sesuai
Rata-rata		3	3,26	Sesuai

(Sumber: Data diolah dengan *MS Excel* 2013)

Terdapat nilai *maturity level* audit yang lebih tinggi daripada responden yaitu DS11.2 dan DS11.6 artinya kebutuhan untuk manajemen data dipahami, dan tindakan yang diperlukan diterima. Dan terdapat penilaian menurut responden prosesnya manajemen datanya dipahami dan tindakannya dilakukan, tetapi setelah dilakukan audit hasilnya proses dilakukan dengan pendekatan *ad-hoc* dan tidak ada

prosedur komunikasi formal yaitu pada DS11.1. Rekomendasi diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT.

Tabel 4.21 Rekomendasi DS11

Control Objective	Rekomendasi
DS11.1	Verifikasi bahwa semua data yang diharapkan untuk diproses diterima dan diproses sepenuhnya, akurat dan tepat waktu, dan semua output dikirimkan sesuai dengan persyaratan bisnis.
DS11.2	Pertahankan penentuan dan penerapan prosedur untuk penyimpanan data
DS11.3	Pertahankan penentuan dan penerapan prosedur untuk memelihara inventaris media yang disimpan dan diarsipkan untuk memastikan kegunaan dan integritasnya.
DS11.4	Pertahankan penentuan dan penerapan prosedur untuk memastikan bahwa persyaratan bisnis untuk perlindungan data dan perangkat lunak yang sensitif terpenuhi ketika data dan perangkat keras dibuang atau dipindahkan.
DS11.5	Pertahankan penentuan dan penerapan prosedur untuk memastikan bahwa persyaratan bisnis untuk perlindungan data dan perangkat lunak yang sensitif terpenuhi ketika data dan perangkat keras dibuang atau dipindahkan.
DS11.6	Pertahankan persyaratan keamanan untuk manajemen data

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa PUSTIPD harus melakukan verifikasi bahwa semua data yang diharapkan untuk diproses diterima dan diproses sepenuhnya, akurat dan tepat waktu, dan semua output dikirimkan sesuai dengan persyaratan bisnis. Mendukung kebutuhan restart dan proses ulang. Menentukan dan menerapkan prosedur untuk memelihara inventaris media yang disimpan dan diarsipkan untuk memastikan kegunaan dan integritasnya. Kemudian, tentukan dan terapkan prosedur untuk memastikan bahwa persyaratan bisnis untuk perlindungan data dan perangkat lunak yang sensitif terpenuhi. Serta Menetapkan dan menerapkan prosedur untuk pencadangan dan pemulihan sistem, aplikasi, data dan dokumentasi yang sesuai dengan persyaratan bisnis dan rencana kesinambungan.

2.5 DS12 *Manage the Physical Environment*

Dari hasil tingkat kematangan pada proses TI *Manage the Physical Environment* dari hasil temuan audit mengenai teknologi informasi untuk manajemen risiko tingkat kematangan saat ini pada organisasi berada pada tingkat kematangan 2 (*repeatable but intuitive*) dengan nilai 2,4 (dapat dilihat pada Tabel 4.2) artinya kontrol lingkungan dilaksanakan dan dipantau oleh personel operasi. Keamanan fisik adalah proses informal, didorong oleh sekelompok kecil karyawan yang memiliki tingkat perhatian yang tinggi tentang mengamankan fasilitas fisik. Prosedur pemeliharaan fasilitas tidak didokumentasikan dengan baik dan bergantung pada praktik baik dari beberapa individu. Tujuan keamanan fisik tidak didasarkan pada standar formal, dan manajemen tidak memastikan bahwa tujuan keamanan tercapai. Sedangkan dari hasil penilaian menurut responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,38 (dapat dilihat pada Tabel 4.6) artinya kebutuhan untuk mempertahankan lingkungan komputasi terkontrol dipahami dan diterima di dalam organisasi. Pengendalian lingkungan, pemeliharaan preventif dan keamanan fisik adalah item anggaran yang disetujui dan dilacak oleh manajemen. Pembatasan akses diterapkan, dengan hanya personel yang disetujui yang diizinkan mengakses fasilitas komputasi. Pengunjung login dan dikawal, tergantung pada individu. Fasilitas fisik rendah profil dan tidak mudah diidentifikasi. Otoritas sipil memantau kepatuhan dengan peraturan kesehatan dan keselamatan. Risiko diasuransikan dengan upaya minimal untuk mengoptimalkan biaya asuransi. Berikut penjelasan mengenai keadaan TI dari hasil audit:

Tabel 4.22 Keadaan DS12 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
DS12.1	Terdapat penentuan dan pemilihan situs fisik	3	3	Sesuai
DS12.2	Belum ada penetapan dan penerapan langkah keamanan fisik sesuai persyaratan bisnis	1	3	Tidak sesuai
DS12.3	Terdapat penetapan dan penerapan prosedur akses fisik	3	3	Sesuai
DS12.4	Belum terdapat perancangan perlindungan faktor lingkungan	2	4	Tidak sesuai
DS12.5	Terdapat manajemen fasilitas fisik	3	3	Sesuai
Rata-rata		2,4	3,38	Tidak sesuai

(Sumber: Data diolah dengan *MS Excel* 2013)

Terdapat proses mengelola lingkungan fisik yang dilakukan dengan pendekatan *ad-hoc* organisasi mengakui persyaratan bisnis untuk menyediakan lingkungan fisik yang sesuai yang melindungi sumber daya dan personel terhadap bahaya buatan manusia dan alam. Namun, manajemen fasilitas dan peralatan tergantung pada keterampilan dan kemampuan individu, proses tersebut berada pada *control objective* DS12.2 yang menurut penilaian responden sudah memahami dan menerima kontrol lingkungan fisik. Dan terdapat proses yang dikembangkan namun belum terdapat pelatihan pada *control objective* DS12.4. Rekomendasi sangat diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT.

Tabel 4.23 Rekomendasi DS12

Control Objective	Rekomendasi
DS12.1	Pemilihan dan desain tata letak situs harus mempertimbangkan risiko yang terkait dengan bencana alam dan buatan manusia, mempertimbangkan hukum dan peraturan yang relevan, seperti peraturan kesehatan dan keselamatan kerja.
DS12.2	Tetapkan dan terapkan langkah-langkah keamanan fisik harus mampu secara efektif mencegah, mendeteksi dan mengurangi risiko yang berkaitan dengan pencurian, suhu, api, asap, air, getaran, teror, vandalisme, pemadaman listrik, bahan kimia atau bahan peledak.

Control Objective	Rekomendasi
DS12.3	Akses ke tempat, bangunan dan area harus dibenarkan, diotorisasi, dicatat dan dimonitor.
DS12.4	Merancang dan menerapkan langkah-langkah untuk perlindungan terhadap faktor lingkungan. Instal peralatan dan perangkat khusus untuk memantau dan mengendalikan lingkungan
DS12.5	Kelola fasilitas, termasuk peralatan listrik dan komunikasi, sesuai dengan undangundang dan peraturan, persyaratan teknis dan bisnis, spesifikasi vendor, dan pedoman kesehatan dan keselamatan.

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa pemilihan dan desain tata letak harus mempertimbangkan dari risiko yang terkait dengan bencana alam dan buatan manusia, serta pertimbangan hukum dan peraturan. Menetapkan dan menerapkan langkah-langkah keamanan fisik harus efektif, penerapan prosedur akses fisik dilakukan, perancangan dan penerapan perlindungan terhadap faktor lingkungan, dan penerapan manajemen fasilitas fisik dilakukan.

3. Monitor and Evaluate (ME)

Pada domain *monitor and evaluate* berkaitan dengan semua proses TI harus secara teratur dinilai dari waktu ke waktu untuk kualitas dan kepatuhan mereka dengan persyaratan kontrol. Domain ini membahas manajemen kinerja, pemantauan pengendalian internal, kepatuhan terhadap peraturan dan tata kelola. Terdapat 3 proses TI pada domain *monitor and evaluate* yaitu ME2, ME3, dan ME4 yang telah dihitung *maturity level* dari hasil audit tingkat kematangannya berada pada tingkat 3 (*defined*) dengan nilai 2,84 (dapat dilihat pada Tabel 4.3). Dan penilaian responden juga berada pada tingkat 3 (*defined*) dengan nilai 3,21 (dapat dilihat pada Tabel 4.7).

3.1 ME2 Monitor and Evaluate Internal Control

Dari hasil tingkat kematangan pada proses TI *Monitor and Evaluate Internal Control* berdasarkan hasil temuan audit mengenai teknologi informasi untuk manajemen risiko tingkat kematangan saat ini pada organisasi berada pada tingkat kematangan 3 (*defined*) dengan nilai 3 (dapat dilihat pada Tabel 4.3). Menurut responden saat ini *control objective* juga berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,14 (dapat dilihat pada Tabel 4.6) artinya kesesuaian penilaian responden dengan hasil audit sesuai. *Maturity level 3* pada *control objective* ME2 berarti manajemen mendukung dan melembagakan pemantauan pengendalian internal. Kebijakan dan prosedur dikembangkan untuk menilai dan melaporkan kegiatan pemantauan pengendalian internal. Program pendidikan dan pelatihan untuk pemantauan pengendalian internal didefinisikan. Proses didefinisikan untuk penilaian diri dan tinjauan jaminan pengendalian internal, dengan peran untuk bisnis yang bertanggung jawab dan manajer TI. Alat sedang digunakan tetapi tidak perlu diintegrasikan ke dalam semua proses. Kebijakan penilaian risiko proses TI sedang digunakan dalam kerangka kerja kontrol yang dikembangkan khusus untuk organisasi TI. Risiko spesifik proses dan kebijakan mitigasi didefinisikan. Berikut penjelasan mengenai keadaan TI dari hasil audit:

Tabel 4.24 Keadaan ME2 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audir	Maturity Level Responden	Keterangan
ME2.1	Terdapat pemantauan dan kerangka kontrol internal	3	3	Sesuai
ME2.2	Terdapat pemantau dan pengevaluasi efisiensi dan efektivitas pengendalian tinjauan manajerial internal.	3	3	Sesuai

Control Objective	Keadaan TI saat ini	Maturity Level Audir	Maturity Level Responden	Keterangan
ME2.3	Terdapat identifikasi pengecualian kontrol, dan analisis dan identifikasi akar penyebabnya	3	3	Sesuai
ME2.4	Terdapat evaluasi kelengkapan dan efektivitas pengendalian manajemen atas proses, kebijakan, dan kontrak TI	3	3	Sesuai
ME2.5	Terdapat jaminan kontrol internal	3	3	Sesuai
ME2.6	Terdapat pengendalian internal di pihak ketiga	3	3	Sesuai
ME2.7	Terdapat tindakan perbaikan	3	3	Sesuai
Rata-rata		3	3,14	Sesuai

(Sumber: Data diolah dengan *MS Excel* 2013)

Berdasarkan hasil audit dan penilaian responden, hasil *maturity level* tiap *control objective* sudah sesuai yaitu berada pada *maturity level 3* artinya manajemen mendukung dan melembagakan pemantauan pengendalian internal. Kebijakan dan prosedur dikembangkan untuk menilai dan melaporkan kegiatan pemantauan pengendalian internal. Rekomendasi diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT.

Tabel 4.25 Rekomendasi ME2

Control Objective	Rekomendasi
ME2.1	Terus pantau, patokan dan tingkatkan lingkungan pengendalian TI dan kerangka kontrol untuk memenuhi tujuan organisasi
ME2.2	Pertahankan pemantauan dan pengevaluasi efisiensi dan efektivitas pengendalian tinjauan manajerial internal.
ME2.3	Identifikasi pengecualian kontrol, dan analisis dan identifikasi akar penyebabnya. Tingkatkan pengecualian kontrol dan laporkan kepada pemangku kepentingan secara tepat.
ME2.4	Pertahankan evaluasi kelengkapan dan efektivitas pengendalian manajemen atas proses, kebijakan, dan kontrak TI melalui program penilaian mandiri yang berkelanjutan
ME2.5	Dapatkan, sesuai kebutuhan, jaminan lebih lanjut atas kelengkapan dan efektivitas pengendalian internal melalui ulasan pihak ketiga.
ME2.6	Konfirmasikan bahwa penyedia layanan eksternal mematuhi persyaratan hukum dan peraturan serta kewajiban kontraktual.
ME2.7	Mengidentifikasi, inisiasi, lacak dan laksanakan tindakan perbaikan yang timbul dari penilaian dan pelaporan pengendalian.

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa PUSTIPD harus terus memantau, patokan dan tingkatkan lingkungan pengendalian TI dan kerangka kontrol untuk memenuhi tujuan organisasi. Kemudian pertahankan, pantau dan evaluasi efisiensi dan efektivitas pengendalian tinjauan manajerial internal. Untuk kontrol pengecualian, tingkatkan kontrol pengecualian dan laporkan kepada pemangku kepentingan secara tepat. Pertahankan kontrol penilaian diri dan jaminan kontrol internal. Konfirmasikan bahawa penyedia layanan eksternal mematuhi persyaratan hukum dan peraturan serta kewajiban kontraktual. Tingkatkan tindakan perbaikan mulai dari identifikasi, mulai, melacak dan menerapkan tindakan perbaikan.

3.2 ME3 *Ensure Compliance With External Requirements*

Dari hasil tingkat kematangan pada proses TI *Ensure Compliance With External Requirements* hasil temuan audit mengenai teknologi informasi untuk manajemen risiko tingkat kematangan saat ini pada organisasi berada pada tingkat kematangan 3 (*defined*) dengan nilai 2,8 (dapat dilihat pada Tabel 4.2) artinya kebijakan, rencana dan prosedur dikembangkan, didokumentasikan dan dikomunikasikan untuk memastikan kepatuhan terhadap peraturan dan kewajiban kontrak dan hukum, tetapi beberapa mungkin tidak selalu diikuti, dan beberapa mungkin sudah ketinggalan zaman atau tidak praktis untuk dilaksanakan. Ada sedikit pemantauan yang dilakukan dan ada persyaratan kepatuhan yang belum ditangani. Pelatihan diberikan dalam persyaratan hukum dan peraturan eksternal yang mempengaruhi organisasi dan proses kepatuhan yang ditentukan. Kontrak pro forma standar dan proses hukum ada untuk meminimalkan risiko yang terkait dengan kewajiban kontraktual. Sedangkan dari penilaian menurut responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,18 (dapat dilihat pada

Tabel 4.6) artinya kesesuaian penilaian responden dengan hasil audit sesuai.

Berikut penjelasan mengenai keadaan TI dari hasil audit:

Tabel 4.26 Keadaan ME3 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
ME3.1	Terdapat identifikasi persyaratan hukum, peraturan dan kontrak eksternal dengan penyesuaian	3	3	Sesuai
ME3.2	Terdapat peninjauan dan penyesuaian kebijakan, standar, prosedur dan metodologi TI	3	3	Sesuai
ME3.3	Terdapat evaluasi kepatuhan	3	3	Sesuai
ME3.4	Terdapat jaminan kepatuhan yang diperoleh dari survei kebutuhan	3	3	Sesuai
ME3.5	Terdapat langkah penintegrasian	2	3	Tidak sesuai
Rata-rata		2,8	3,18	Sesuai

(Sumber: Data diolah dengan *MS Excel* 2013)

Berdasarkan tabel diatas kesesuaian antara penilaian hasil audit dan responden telah sesuai. Kecuali pada ME3.5 masih terdapat pemahaman perlunya persyaratan eksternal, namun tidak ada pendekatan standar. Dimana kepatuhan merupakan persyaratan yang berulang, seperti didalam peraturan keuangan atau undang-undang privasi, prosedur kepatuhan individu telah dikembangkan dan diikuti berdasarkan tahun ke tahun. Namun demikian, tidak ada pendekatan standar. Rekomendasi diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT.

Tabel 4.27 Rekomendasi ME3

Control Objective	Rekomendasi
ME3.1	Pertahankan proses identifikasi dan ditingkatkan menurut hukum internasional

Control Objective	Rekomendasi
ME3.2	Tinjau dan sesuaikan kebijakan, standar, prosedur, dan metodologi TI untuk memastikan bahwa persyaratan hukum, peraturan dan kontrak ditangani dan dikomunikasikan.
ME3.3	Komunikasikan kepatuhan terhadap kebijakan, standar, prosedur, dan metodologi TI dengan persyaratan hukum dan peraturan
ME3.4	Dapatkan dan laporkan kepastian kepatuhan dan kepatuhan terhadap semua kebijakan internal yang berasal dari arahan internal atau persyaratan hukum.
ME3.5	Mengintegrasikan pelaporan TI pada persyaratan hukum, peraturan dan kontrak dengan output serupa dari fungsi bisnis lainnya

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa proses identifikasi hukum nasional dan internasional, peraturan, dan persyaratan eksternal dilakukan secara terus menerus. Kemudian PUSTIPD harus meningkatkan optimalisasi respon terhadap persyaratan eksternal dan evaluasi kepatuhan dengan persyaratan eksternal. Proses memperoleh dan melaporkan jaminan kepatuhan dan kepatuhan kebijakan internal, dilakukan dari arahan internal atau persyaratan peraturan. Dan lakukan pengintegrasian pelaporan TI dengan output serupa dari fungsi bisnis yang lain.

3.3 ME4 Provide IT Governance

Berdasarkan hasil tingkat kematangan pada proses TI *Provide IT Governance* dari hasil temuan audit mengenai teknologi informasi untuk manajemen risiko tingkat kematangan *Provide IT Governance* saat ini pada organisasi berada pada tingkat kematangan 3 (*defined*) dengan nilai 2,71 (dapat dilihat pada Tabel 4.2) artinya pentingnya kebutuhan untuk tata kelola TI dipahami oleh manajemen dan dikomunikasikan kepada organisasi. Satu set dasar indikator tata kelola TI dikembangkan di mana hubungan antara ukuran hasil dan indikator kinerja didefinisikan dan didokumentasikan. Prosedur distandarisasi dan didokumentasikan. Manajemen mengomunikasikan prosedur standar, dan pelatihan ditetapkan. Alat diidentifikasi untuk membantu mengawasi tata kelola TI.

Dasbor didefinisikan sebagai bagian dari scorecard bisnis seimbang TI. Namun, diserahkan kepada individu untuk mendapatkan pelatihan, mengikuti standar dan menerapkannya. Proses dapat dipantau, tetapi penyimpangan, sementara sebagian besar ditindaklanjuti oleh inisiatif individu, tidak mungkin terdeteksi oleh manajemen. Berdasarkan penilaian menurut responden saat ini berada pada tingkat kematangan 3 (*defined*) dengan nilai 3,30 (dapat dilihat pada Tabel 4.6) artinya kesesuaian penilaian responden dengan hasil audit sesuai. Berikut penjelasan mengenai keadaan TI dari hasil audit:

Tabel 4.28 Keadaan ME4 Saat Ini

Control Objective	Keadaan TI saat ini	Maturity Level Audit	Maturity Level Responden	Keterangan
ME4.1	Terdapat penetapan dan penyesuaian tata kelola TI dengan mempertimbangkan kebutuhan	3	4	Tidak sesuai
ME4.2	Terdapat proses penyesuaian strategi	3	3	Sesuai
ME4.3	Terdapat pengolahan program investasi, layanan, dan aset TI	3	3	Sesuai
ME4.4	Terdapat pengawasan sumber daya dengan melakukan <i>monitoring</i>	3	3	Sesuai
ME4.5	Belum ada penentuan manajemen risiko namun keamanan dilakukan	1	3	Tidak sesuai
ME4.6	Terdapat pengukuran kinerja	3	3	Sesuai
ME4.7	Terdapat jaminan independen	3	3	Sesuai
Rata-rata		2,71	3,30	Sesuai

(Sumber: Data diolah dengan *MS Excel* 2013)

Pada ME4.1 hasil auditnya nilai *maturity level* lebih rendah daripada hasil responden, *control objective* tersebut prosesnya dipahami dan dikomunikasikan, namun belum ditentukan dan dipantau melalui SLA. Untuk *control objective* ME4.5 prosesnya diakui perlu ditangani tetapi pendekatannya hanya dengan komunikasi sporadis dan tidak konsisten. Rekomendasi diperlukan organisasi untuk proses teknologi informasi yang mengacu pada COBIT.

Tabel 4.29 Rekomendasi ME4

Control Objective	Rekomendasi
ME4.1	Mendasarkan kerangka kerja pada proses TI dan model kontrol yang sesuai dan memberikan akuntabilitas dan praktik.
ME4.2	Memungkinkan pengurus dan pemahaman eksekutif atas isu-isu TI strategis, seperti peran TI, wawasan teknologi, dan kemampuan.
ME4.3	Pastikan bahwa hasil bisnis yang diharapkan dari investasi yang didukung IT dan lingkup upaya penuh yan diperlukan.
ME4.4	Lakukan pengawasan melalui penilaian rutin atas inisiatif dan operasi TI untuk memastikan sumber daya dan penyesuaian yang sesuai dengan sasaran strategis dan bisnis saat ini dan di masa mendatang.
ME4.5	Bekerja dengan dewan untuk menentukan keinginan perusahaan untuk risiko TI, dan memperoleh jaminan yang menjamin bahwa praktik manajemen risiko TI sesuai, untuk memastikan bahwa risiko TI sebenarnya tidak melebihi risiko yang ditetapkan dewan. Tanamkan tanggung jawab manajemen risiko ke dalam organisasi, memastikan bahwa bisnis dan TI secara teratur menilai dan melaporkan risiko terkait TI dan dampaknya dan bahwa posisi risiko TI perusahaan transparan bagi semua pemangku kepentingan.
ME4.6	Melakukan pengukuran kinerja teknolog informasi secara intensif
ME4.7	Melakukan langkah pemastian jaminan sesuai dengan kebijakan dan prosedur

Dilihat dari tabel rekomendasi di atas maka dapat disimpulkan bahwa PUSTIPD harus mendasarkan kerangka kerjanya dengan model kontrol yang sesuai untuk pemberian akuntabilitas dan praktik. Menambah pemahaman pada penyesuaian strategi dan memastikan hasil bisnis sesuai. Untuk manajemen sumber daya TI dilakukan pengawasan secara berkala melalui penilaian rutin atas inisiatif dan operasi TI. Membuat kerangka manajemen risiko yang jelas dan pastikan implementasinya. Melakukan pengukuran kinerja secara intensif serta melakukan pemastian jaminan independen.