BAB V

PENUTUP

5.1 Simpulan

Berdasarkan uraian pada bab yang dibahas sebelumnya, dapai ditarik kesimpulan sebagai berikut:

1. Hasil implementasi *framework* COBIT 4.1 dalam melakukan proses penilaian *maturity level* TI pada saat ini, dari penilaian responden dan hasil audit diperoleh hasil nilai rata-rata domain PO, DS dan ME berada pada tingkat 3 (*defined)* dengan nilai rata-rata hasil responden 3,17 dan hasil audit 2,65.
2. Domain *plan and organize* dari hasil audit dan responden berada pada tingkat 3 (*defined*). Sebagian besar proses sudah dijalankan dan mencapai tujuan, namun pada kenyataanya untuk penilaian dan pengelolaan risiko masih terdapat proses yang belum terpenuhi. Rekomendasi yang diberikan mengusulkan langkah yang perlu dilakukan untuk mencapai tingkat *maturity level* 3 sesuai yang diharapkan responden.
3. Domain *deliver and support* dari hasil audit berada pada tingkat 2 (*repeatable but intuitive)* sedangkan penilaian responden berada pada tingkat 3. Pemastian layanan berkelanjutan dan sistem keamanan penugasannya pada koordinator keamanan TI meskipun otoritasnya terbatas. Rekomendasi yang diberikan mengusulkan tindakan yang perlu dilakukan untuk mencapai tingkat 3 sesuai dengan harapan dari penilaian responden.
4. Domain *monitor and evaluate* dari hasil audit dan penilaian responden berada pada tingkat 3 (*defined*). Namun untuk manajemen risiko belum terdapat

penentuan manajemen risiko serta penjamin praktiknya telah sesuai. Rekomendasi diberikan untuk mengusulkan tindakan yang harus dilakukan organisasi dalam mencapai tingkat yang sesuai dengan harapan dari penilaian responden.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, maka ada beberapa saran untuk memperbaiki dan meningkatkan teknologi informasi untuk manajemen risiko pada PUSTIPD UIN Raden Fatah Palembang yaitu:

1. PUSTIPD perlu melakukan audit tindak lanjut untuk mengetahui apakah manajemen telah melaksanakan rekomendasi audit yang telah diberikan.
2. Pelaksanaan audit harus memiliki waktu yang terjadwal, bisa dilakukan setiap bulan, perkuartal, dua kali setahun atau satu kali setahun sesuai dengan ketetapan dari organisasi.
3. PUSTIPD perlu mengolah bagian perencanaan dan pengorganisasian dalam penempatan fungsi TI pada organisasi secara keseluruhan, dengan menyiapkan dokumentasi kerangka kontrol dan risiko TI serta kerangka kerja manajemen risiko pada perusahaan untuk penentuan respon risiko ketika terjadi bencana.
4. Mengadakan dukungan untuk layanan TI dimasa yang akan datang. Dengan memastikan keamanan sistem, pengolah data, dan pengolah lingkungan fisik yang dibutuhkan untuk menjaga integritas informasi dan melindungi aset TI.
5. Melakukan pengawasan pengelolaan TI pada PUSTIPD, melalui peningkatan pelaporan yang terintegrasi dan manajemen risiko sebagai jaminan untuk tata kelola yang lebih baik.

DAFTAR PUSTAKA

Akmal, D., & Hadi, M. (2010). *EDP AUDIT Praktek Teknik Audit Berbantuan Komputer dengan Aplikasi MS Excel dan ACL*. Jakarta: Erlangga.

Andry, J. F. (2016). *Audit Sistem Informasi Sumber Daya Manusia Pada Training Center Di Jakarta Menggunakan Framework COBIT 4.1*. JURNAL ILMIAH FIFO, 42.

Andry, Johanes Fernandes dan Kevin Christianto. (2017). *Audit Menggunakan COBIT 4.1 dan COBIT 5 dengan Case Study*. Jakarta: Teknosains.

Ege, Prof. Dr., dan Dr., Yasar. (2017). *SWOT Analysis: A Theoritical Review*. The Journal of International Social Research, Volume:10, Issue: 51, Agustus 2017. ISSN: 1307-9581.

Firdaus, Nurfitri Zukhrufatul dan Suprapto. (2017). *Evaluasi Manajemen RIsiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus: PT. Petrokimia Gresik)*. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. Vol. 1, No.1, Juni 2017, e-ISSN: 2548-964X.

Gondodiyoto, S. (2007). *Audit Sistem Informasi + Pendekatan CobIT*. Jakarta: Mitra Wacana Media.

Hall, J. A. (2017). *AUDIT TEKNOLOGI INFORMASI DAN ASSURANCE*. Terjemahan: Dewi Fitriasari. Singapore: South-Western.

Institute, I. G. (2007). *COBIT 4.1 Framework Control Objectives, Management Guidelines, Maturity Models.* Amerika: ITGI.

ITGI. (2007). *COBIT 4.1*. Amerika Serikat: ISACA.

ITGI. (2015, September 26). *Audit IT - IT Governance Indonesia | ITGID | Audit IT*. Retrieved from https://itgid.org: https://itgid.org/audit-ti/

ITGI. (2016, September 26). *Framework COBIT Sebagai Pengendali Perusahaan | ITGID*. Retrieved from https://itgid.org/: https://itgid.org/framework-cobit/

Kosasi, Sandy dan Vedyanto. (2015). *The Maturity Level of Information Technology Governance of Online Cosmetics Business.* International Conference on New Media (CONMEDIA), ISBN 978-602-95532-9-1.

Megawati dan Mimi Kazmaini. (2018). *Analisa Manajemen Resiko Sistem Informasi Perpustakaan Menggunakan COBIT 4.1 Pada Domain PO9* Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi. Vol.4, No.1, Februari 2018, Hal. 73-76. e-ISSN 2520-8995, p-ISSN 2460-8181.

Nugroho, Heru. (2012). *Analisis Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 4.1*.Konferensi Nasional ICT-M Politeknik Telkom (KNIP). ISSN:2302-1896.

Pangestuti, Dewi Cahyani, SE.MM. (2019). *Manajemen Risiko Bisnis*. Jakarta. Universitas Pembangunan Nasional Veteran Jakarta.

Siregar, Syofian. 2013. *Metode penelitian kuantitatif dilengkapi dengan perbandingan perhitungan manual & SPSS.* Jakarta : Prenadamedia Group.

Sugiyono, P. D. (2017). *METODE PENELITIAN KUANTITATIF, KUALITATIF, DAN R&d.* Bandung: Alfabeta.

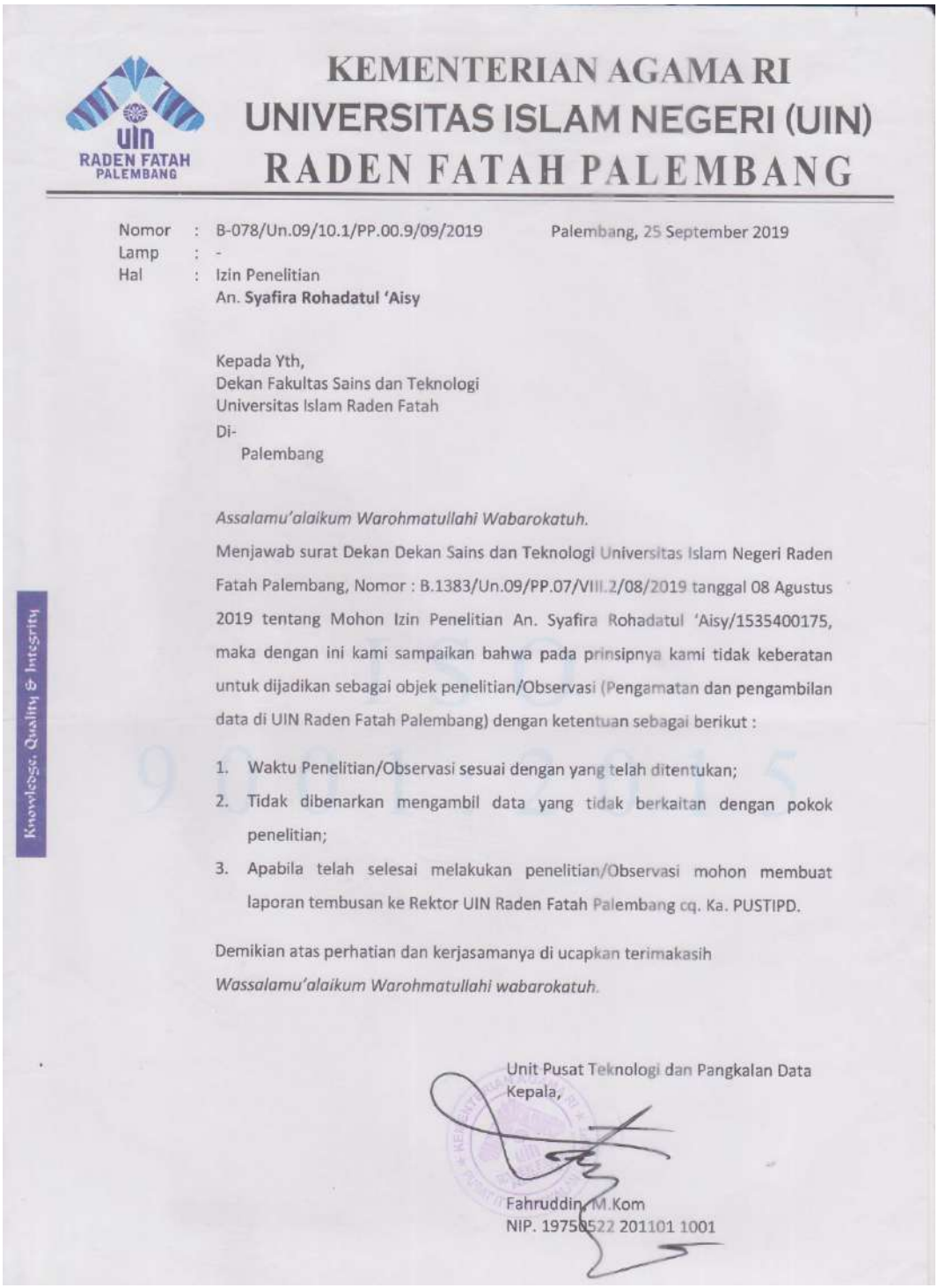
Sutabri, T. (2012). *Konsep Sistem Informasi.* Yogyakarta: CV. ANDI OFFSET.

Swastika, I. P. (2016). *AUDIT SISTEM INFORMASI DAN TATA KELOLA TEKNOLOGI INFORMASI IMPLEMENTASI DAN STUDI KASUS.* Yogyakarta: CV. ANDI OFFSET.

Wardani Setia dan Mita Puspitasari.2014. *Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT Dengan Model Maturity Level (Studi Kasus Fakultas ABC)*. Jurnal Teknologi. Volume 7, Nomor 1.

LAMPIRAN

Surat Balasan Izin Penelitian



KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG

Nomor : B-078/Un.09/10.1/PP.00.9/09/2019 Palembang, 25 September 2019
Lamp : -
Hal : Izin Penelitian
An. **Syafira Rohadatul 'Aisy**

Kepada Yth,
Dekan Fakultas Sains dan Teknologi
Universitas Islam Raden Fatah
Di-
Palembang

Assalamu'alaikum Warohmatullahi Wabarokatuh.

Menjawab surat Dekan Dekan Sains dan Teknologi Universitas Islam Negeri Raden Fatah Palembang, Nomor : B.1383/Un.09/PP.07/VIII.2/08/2019 tanggal 08 Agustus 2019 tentang Mohon Izin Penelitian An. Syafira Rohadatul 'Aisy/1535400175, maka dengan ini kami sampaikan bahwa pada prinsipnya kami tidak keberatan untuk dijadikan sebagai objek penelitian/Observasi (Pengamatan dan pengambilan data di UIN Raden Fatah Palembang) dengan ketentuan sebagai berikut :

1. Waktu Penelitian/Observasi sesuai dengan yang telah ditentukan;
2. Tidak dibenarkan mengambil data yang tidak berkaitan dengan pokok penelitian;
3. Apabila telah selesai melakukan penelitian/Observasi mohon membuat laporan tembusan ke Rektor UIN Raden Fatah Palembang cq. Ka. PUSTIPD.

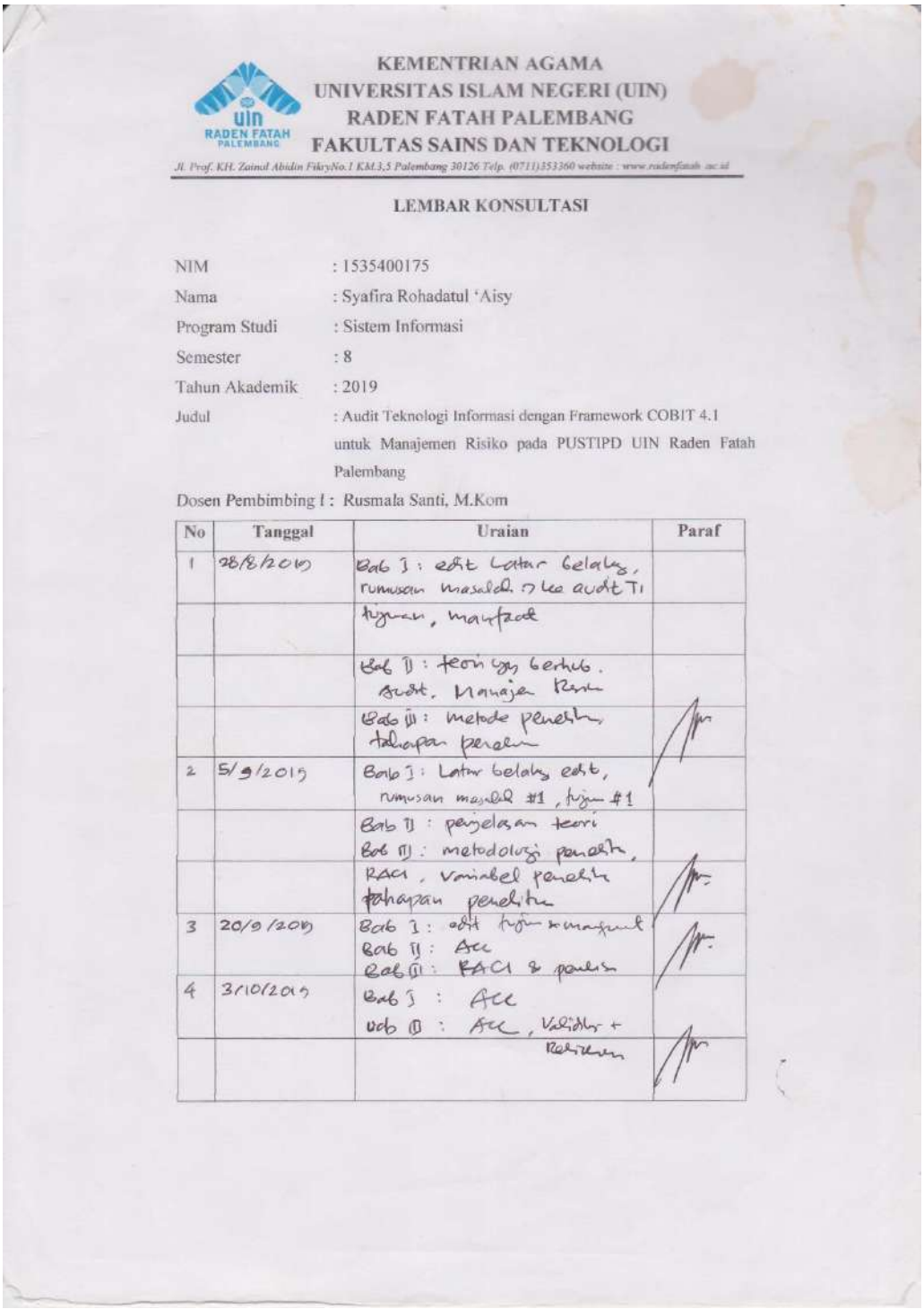
Demikian atas perhatian dan kerjasamanya di ucapkan terimakasih
Wassalamu'alaikum Warohmatullahi wabarokatuh.

Unit Pusat Teknologi dan Pangkalan Data
Kepala,

Fahruddin, M.Kom
NIP. 19758522 201101 1001

Knowledge, Quality & Integrity

Lembar Konsultasi Pembimbing I



KEMENTRIAN AGAMA
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

Jl. Prof. KH. Zainal Abidin Fikry No.1 KM.3,5 Palembang 30126 Telp. (0711)353360 website : www.radenfatah.ac.id

LEMBAR KONSULTASI

NIM : 1535400175
Nama : Syafira Rohadatul 'Aisy
Program Studi : Sistem Informasi
Semester : 8
Tahun Akademik : 2019
Judul : Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UIN Raden Fatah Palembang

Dosen Pembimbing I : Rusmala Santi, M.Kom

No	Tanggal	Uraian	Paraf
1	28/8/2019	Bab I : edit Latar belakang, rumusan masalah, tkp audit TI	
		tujuan, manfaat	
		Bab II : teori yg berhub. Audit, Manajen Risiko	
		Bab III : metode penelitian, tahapan penelitian	
2	5/9/2019	Bab I : Latar belakang edit, rumusan masalah #1, tujuan #1	
		Bab II : penjelasan teori	
		Bab III : metodologi penelitian, RACI, variabel penelitian tahapan penelitian	
3	20/9/2019	Bab I : edit tujuan manajemen	
		Bab II : Acc	
		Bab III : RACI & paparan	
4	3/10/2019	Bab I : Acc	
		Bab II : Acc, Validasi + Rekomendasi	

KEMENTRIAN AGAMA
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Prof. KH. Zainal Abidin FikryNo.1 KM.3,5 Palembang 30126 Telp. (0711)353360 website : www.radenfatah .ac.id

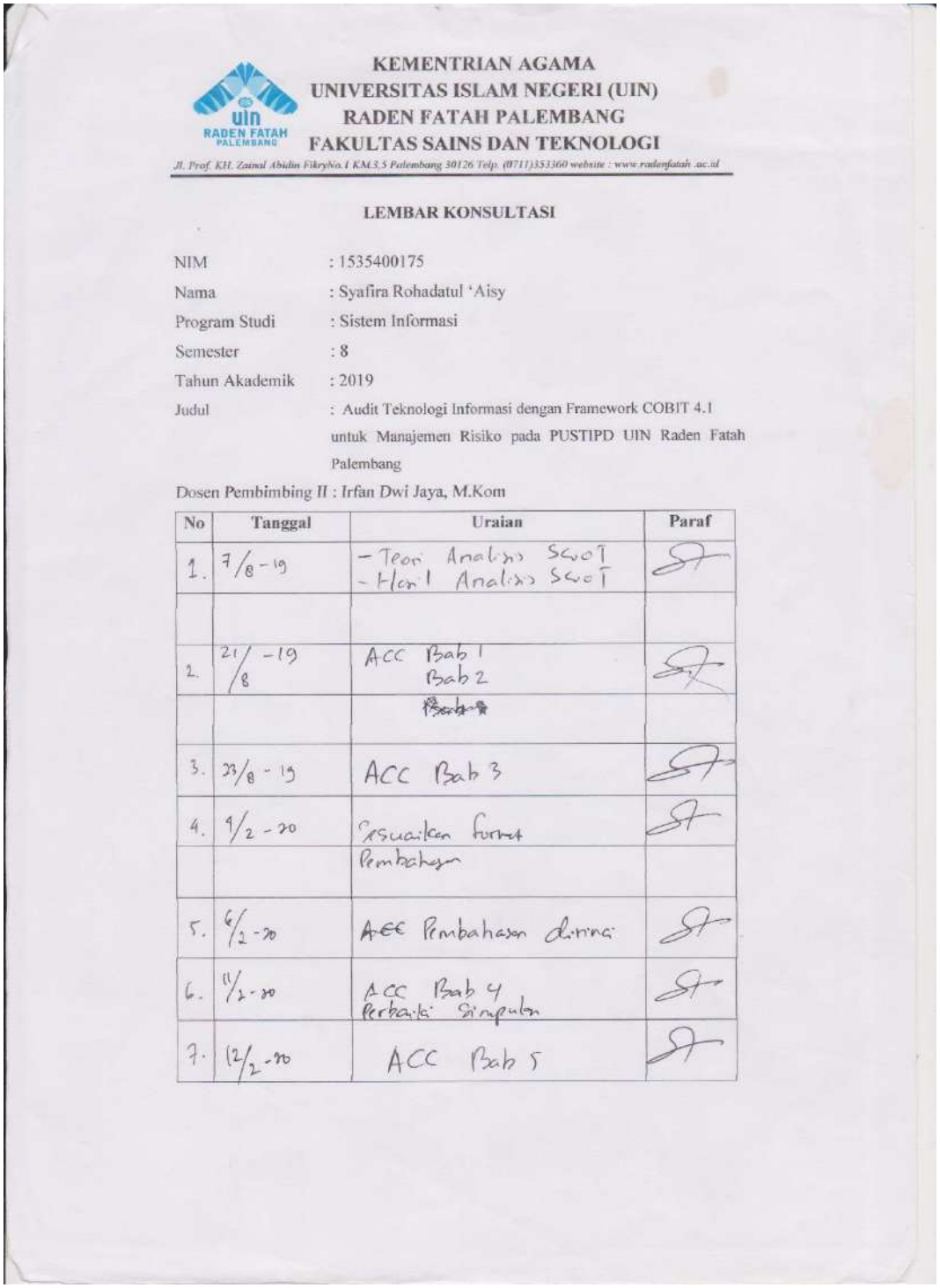
LEMBAR KONSULTASI

NIM : 1535400175
Nama : Syafira Rohadatul 'Aisy
Program Studi : Sistem Informasi
Semester : 8
Tahun Akademik : 2020
Judul : Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UIN Raden Fatah Palembang

Dosen Pembimbing I : Rusmala Santi, M.Kom

No	Tanggal	Uraian	Paraf
5	14/2/2020	Bab IV : dahulukan audit + manajemen risiko → matriks	
		pembahasan → teori + relevansi Bab V : Simpulan + saran & ell	
6	19/2/2020	Bab IV : Acc Bab V : perbaiki saran	
7	20/2/2020	Bab V : Acc	

Lembar Konsultasi Pembimbing II



KEMENTRIAN AGAMA
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

Jl. Prof. KH. Zainal Abidin FikryNo.1 KM.3.5 Palembang 30126 Telp. (0711)353360 website : www.radenfatah .ac.id

LEMBAR KONSULTASI

NIM : 1535400175
Nama : Syafira Rohadatul 'Aisy
Program Studi : Sistem Informasi
Semester : 8
Tahun Akademik : 2019
Judul : Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UIN Raden Fatah Palembang

Dosen Pembimbing II : Irfan Dwi Jaya, M.Kom

No	Tanggal	Uraian	Paraf
1.	7/8-19	- Teori Analisis SWOT - Hasil Analisis SWOT	
2.	21/8-19	ACC Bab 1 Bab 2	
		Bab 3	
3.	23/8-19	ACC Bab 3	
4.	9/2-20	Sesuaikan format Pembahasan	
5.	6/2-20	ACC Pembahasan dilanj	
6.	11/2-20	ACC Bab 4 Perbaiki Simpulan	
7.	12/2-20	ACC Bab 5	

SK Pembimbing

KEPUTUSAN DEKAN FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG
NOMOR : 72 TAHUN 2019

TENTANG

PENUNJUKAN PEMBIMBING SKRIPSI STRATA SATU (S.1)
BAGI MAHASISWA TINGKAT AKHIR FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG

DEKAN FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG

Menimbang :
1. Bahwa untuk mengakhiri Program sarjana (S1) bagi Mahasiswa, maka perlu ditunjuk Tenaga ahli sebagai Pembimbing Utama dan Pembimbing kedua yang bertanggung jawab dalam rangka penyelesaian Skripsi Mahasiswa;
2. Bahwa untuk lancarnya tugas pokok itu, maka perlu dikeluarkan Surat Keputusan Dekan (SKD) tersendiri. Dosen yang ditunjuk dan tercantum dalam SKD ini memenuhi syarat untuk melaksanakan tugas tersebut.

Mengingat :
1. Undang-Undang No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
2. Undang-Undang No. 14 Tahun 2005 tentang Guru dan Dosen;
3. Undang-Undang No.12 Tahun 2012 tentang Pendidikan Tinggi;
4. Peraturan Pemerintah Nomor 9 Tahun 2003 tentang Wewenang Pengangkatan, Pemindahan dan Pemberhentian Pegawai Negeri Sipil;
5. Peraturan Pemerintah No. 19 Tahun 2005 tentang Standar Nasional Pendidikan;
6. Peraturan Menteri Agama RI No. 53 Tahun 2015 tentang Organisasi dan tata kerja Institut Agama Islam Negeri Raden Fatah Palembang;
7. Peraturan Menteri Keuangan Nomor 53/PMK.02.2014 tentang Standar Biaya Masukan;
8. Peraturan Menteri Pendidikan dan Kebudayaan No.154/2014 tentang Rumpun Ilmu pengetahuan dan Teknologi serta Gelar Lulusan Perguruan Tinggi;
9. Peraturan Menteri Agama No.62 tahun 2015 tentang Statuta Universitas Islam Negeri (UIN) Raden Fatah Palembang;
10. Peraturan Menteri Agama No.33 tahun 2016 tentang Gelar Akademik Perguruan Tinggi Keagamaan;
11. Keputusan Menteri Agama No.394 tahun 2003 tentang Pedoman Pendirian Perguruan Tinggi Agama;
12. DIPA Universitas Islam Negeri Raden Fatah Palembang Tahun 2017;
13. Keputusan Rektor Universitas Islam Negeri Raden Fatah Nomor 669B Tahun 2014 tentang Standar Biaya Honorarium dilingkungan Universitas Islam Negeri Raden Fatah Palembang Tahun 2015;
14. Peraturan Presiden Nomor 129 Tahun 2014 tentang Alih Status IAIN menjadi Universitas Islam Negeri.

M E M U T U S K A N

MENETAPKAN

Pertama : Menunjuk sdr. :
1. Rusmala Santi, M.Kom — NIP : 197911252014032002
2. Irfan Dwi Jaya, M.Kom — NIDN : 0208018701

Dosen Fakultas Sains dan Teknologi Universitas Islam Negeri (UIN) Raden Fatah Palembang masing-masing sebagai Pembimbing Utama dan Pembimbing Kedua Skripsi Mahasiswa :

Nama	:	**SYAFIRA ROHADATUL 'AISY**
NIM/Jurusan	:	1535400175/Sistem Informasi
Semester/Tahun	:	Genap / 2018 - 2019
Judul Skripsi	:	Audit Teknologi Informasi Dengan Framework Cobit 4.1 Untuk Manajemen Risiko Pada Pustipd UIN Raden Fatah Palembang

Kedua : Kepada Pembimbing Utama dan Pembimbing Kedua tersebut diberi hak sepenuhnya untuk merevisi judul/ kerangka dengan sepengetahuan Fakultas.

Ketiga : Masa berlakunya Surat Keputusan Dekan ini Terhitung Mulai Tanggal di tetapkannya sampai dengan Tanggal 30 Juli 2020.

Keempat : Keputusan ini mulai berlaku satu tahun sejak tanggal ditetapkan dan akan ditinjau kembali apabila dikemudian hari ternyata terdapat kekeliruan dalam penetapan ini.

DITETAPKAN DI : PALEMBANG
PADA TANGGAL : 30 - 07 - 2019
A.n. REKTOR
DEKAN,

FAKULTAS SAINS DAN TEKNOLOGI

ERLINA

TEMBUSAN :

Berita Acara Penyebaran Kuesioner

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: PUSTIPD
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019
Kepala PUSTIPD

Fahruddin, M.Kom

Peneliti

Syafira Rohadatul 'Aisy

Divisi Jaringan

Naenggolan, MTCA., MTCRE

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: PUSTIPD
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang akan dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019
Kepala PUSTIPD

Fahruddin, M.Kom

Peneliti

Syafira Rohadatul 'Aisy

Divisi Pengembangan Software

M. Aswadi, S.Kom

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat : Universitas Islam Negeri Raden Fatah Palembang

Responden : PUSTIPD

Peneliti : Syafira Rohadatul 'Aisy

Jurusan/Fakultas : Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019
Kepala PUSTIPD

Fahruddin, M.Kom

Peneliti	Divisi Diklat
Syafira Rohadatul 'Aisy	Awang Sugiarto, S.Kom.,IT-IL.MTA

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: PUSTIPD
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019
Kepala PUSTIPD

Fahruddin, M.Kom

Peneliti	Divisi Jaringan
Syafira Rohadatul 'Aisy	Insan Mustofa N.A., S.Pd.I.MTCNA., MTCRE

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: PUSTIPD
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019
Kepala PUSTIPD

Fahruddin, M.Kom

Peneliti	Divisi Pengembangan Software
Syafira Rohadatul 'Aisy	A. Arroyan Rasyid, S.Kom

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: PUSTIPD
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019
Kepala PUSTIPD

Peneliti

Syafira Rohadatul 'Aisy

Fahruddin, M.Kom

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: PUSTIPD
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019
Kepala PUSTIPD

Fahruddin, M.Kom

Peneliti

Syafira Rohadatul 'Aisy

Divisi Pengembangan Software

Jawasi, S.Pd.I

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: PUSTIPD
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019
Kepala PUSTIPD

Fahruddin, M.Kom

Peneliti	Divisi Pengembangan Software
Syafira Rohadatul 'Aisy	KMS. Jumansyah, HM.S.SI.IT-IL.MTA

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: PUSTIPD
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019

Peneliti

Syafira Rohadatul 'Aisy

Kepala Bagian Perencanaan dan Keuangan

Musli Darosan. S.Ag.M.SI

BERITA ACARA PENYEBARAN KUESIONER

Pada tanggal 30 Oktober 2019 dilaksanakan penyebaran kuesioner yang berkaitan dengan penelitian yang dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat	: Universitas Islam Negeri Raden Fatah Palembang
Responden	: Lembaga Penjamin Mutu (LPM)
Peneliti	: Syafira Rohadatul 'Aisy
Jurusan/Fakultas	: Sistem Informasi/ Sains dan Teknologi

Peneliti melakukan penyebaran kuesioner dengan pihak responden melalui cara offline, yang berkaitan dengan penelitian yang akan dilakukan di PUSTIPD UIN Raden Fatah Palembang, kemudian responden menjawab setiap butir pertanyaan terkait yang dibutuhkan peneliti. Adapun kuesioner yang disebar peneliti terlampir.

Mengetahui,
Palembang, 30 Oktober 2019

Peneliti

Syafira Rohadatul 'Aisy

Kepala Lembaga Penjamin Mutu (LPM)

Dr.H. Fajri Ismail, M.Pd.I

Lampiran foto

Lampiran Wawancara

1. PUSTIPD memiliki beberapa sistem, yaitu simak, e-kinerja, e-jurnal, slims, e-repository, lpse UIN Raden Fatah dari masing-masing sistem itu siapa penggunanya dan siapa yang mengoperasikannya?
2. Siapa pembuat keputusan investasi dari masing-masing sistem?
3. Siapa yang memutuskan persyaratan?
4. Siapa yang mengembangkan kemampuan sistem?
5. Siapa yang bertanggung jawab akan keamanan, privasi dan tanggung jawab terhadap risiko?
6. Siapa yang membutuhkan/menyediakan jasa asuransi?
7. Apa saja infrastruktur yang tersedia pada masing-masing sistem dan yang tidak tersedia? Kategori infrastruktur: hardware, software, sumber daya, sistem manajemen database, jaringan, multimedia, lingkungan.
8. Selama ini risiko apa yang sudah terjadi di masing-masing sistem baik dari segi data/informasi, infrastruktur, dll?
9. Siapa yang menanganinya serta bagaimana cara penanganan?
10. Apakah ada jadwal pemantauan khusus untuk pencegahan terjadinya risiko?

1. PUSTIPD sebagi pengembang, pemantau, maintenance dll. Untuk pengolah sistem kembali pada unit/pusat sistem masing-masing. Yang mengoperasikannya, seperti:
   -simak: fakultas (sebagai unit) penggunanya admin dan mahasiswa
   -slims, e-jurnal, e-repository: perpustakaan (sebagai unit) penggunanya admin dan mahasiswa
   -e-kinerja/elkp: Dosen -LPSE: PPK(unit) sistem pengadaan barang
2. Keputusan investasi kembali pada unit masing-masing
3. Kesepakatan antara PUSTIPD & BAK
4. PUSTIPD
5. Untuk privasi data (unit masing-masing), keamanan (PUSTIPD), tanggung jawab (PUSTIPD)
6. Belum ada jasa asuransi terhadap sistem
7. Infrastruktur yang ada sudah memenuhi namun belum dikatakan ideal. Backup data masih sentral sehingga kemungkinan kehilangan data cukup besar, untuk duplikasi belum ada. Server hanya ada pada PUSTIPD
8. Pernah terjadi pada simak UIN Raden Fatah: korupt database yang disebabkan karena mati lampu. Karena pada saat data dieksekusi kemudian lampu mati, eksekusi yang belum selesai menyebabkan data ada sebagian yang tidak terproses. Waktu perbaikan selama ½ hari dampak yang ditimbulkannya tidak bisa diaksesnya simak.
9. Ada, berdasarkan firewall

Wawancara Audit I

Responden: CEO

IT Process	Pertanyaan	Jawaban
ME4	1. Apakah pada PUSTIPD telah menetapkan pengawasan dan fasilitas eksekutif dan dewan terhadap kegiatan TI?	Iya PUSTIPD sudah memberikan pengawasan dan fasilitas eksekutif dan dewan kegiatan TI. Dengan diterbentuk divisi/ bidang yang mengatur tiap kegiatan TI, bagaimana pada bidang masing-masing.
	2. Apakah PUSTIPD meninjau, mendukung, menyelaraskna dan mengkomunikasikan kinerja TI, strategi TI, dan manajemen sumberdaya dan risiko dengan strategi bisnis?	Untuk kinerja TI, strategi TI dan manajemen sumberdaya ditinjau, didukung, diselaraskan serta dikomunikasikan dengan strategi bisnis, namun untuk manajemen risiko belum ada power penjajaran dan pengkaitan dengan strategi bisnis.
	3. Apakah PUSTIPD mendapatkan penilaian independent berkala atas kinerja dan kepatuhan terhadap kebijakan rencana dan prosedur?	Iya kinerja dan kepatuhan dinilai secara independent berkala terhadap kebijakan dan prosedur yang diatur dalam pustipd
	4. Apakah PUSTIPD menyelesaikan temuan penilaian indapenden, dan memastikan implementasi manajemen atas rekomendasi yang didapati?	Iya diadakannya tenaga pustipd independennya, cara dipantaunya juga rekomendasi diimplementasikan

Responden: Chief Architect

IT Process	Pertanyaan	Jawaban
PO4	1. Apakah PUSTIPD mengidentifikasi pemilik data?	Iya mengidentifikasi pemilik data serta dibagi tiap unitnya
PO9	2. Apakah PUSTIPD mengidentifikasi peristiwa/kejadian yang terkait dengan tujuan bisnis?	Iya mengidentifikasi peristiwa/kejadian yang terkait dengan tujuan bisnis
	3. Apakah PUSTIPD menilai risiko yang terkait dengan peristiwa/kejadian?	Saat ini pada pustipd belum dilakukan penilaian risiko terkait peristiwa/kejadian
	4. Apakah PUSTIPD mengevaluasi dan memilih respon risiko?	Iya pustipd mengatasi risiko terkait, setelah diketahui akan dapat ditentukan penanganan risiko.

DS4	1.	Apakah PUSTIPD mengembangkan kerangka kerja kontinuitas TI?	Iya pustipd mengembangkan kerangka kerja kontinuitas TI untuk mendukung manajemen kontinuitas bisnis.

esponden: Chief Architect

DS5	1.	Apakah PUSTIPD telah menetapkan, membuat, dan mengoperasikan identitas(akun) prosee manajemen?	Untuk secara detailnya belum, terkait identitas akun akun secara umum.
	2.	Apakah PUSTIPD menerapkan dan memelihara kontrol teknis dan prosedural untuk melindungi arus informasi di seluruh jaringan?	Saat ini belum menggunakan teknis kemanan dan prosedur manajemen.
DS11	1.	Apakah PUSTIPD menerjemahkan penyimpanan data dan persyaratan penyimpanan ke dalam prosedur?	Iya penyimpanan datanya disesuaikan waktu prosedur yang diterapkan

ME3	1. Apakah PUSTIPD mengevaluasi kepatuhan kebijakan TI dengan kebijakan, rencana, dan prosedur TI?	Iya pustipo mengevaluasi kepatuhan kebijakan TI dengan kebijakan, rencana, dan prosedur TI

Responden: Chief Architect

IT Process	Pertanyaan	Jawaban
PO4	1. Apakah PUSTIPD mengidentifikasi pemilik data?	Iya mengidentifikasi pemilik data serta hak aksesnya
PO9	2. Apakah PUSTIPD mengidentifikasi peristiwa/kejadian yang terkait dengan tujuan bisnis?	Iya mengidentifikasi peristiwa/kejadian yang terkait dengan tujuan bisnis
	3. Apakah PUSTIPD menilai risiko yang terkait dengan peristiwa/kejadian?	Saat ini pada pustipo belum dilakukan penilaian risiko terkait peristiwa/kejadian
	4. Apakah PUSTIPD mengevaluasi dan memilih respon risiko?	Iya pustipo mengelola risiko terkait, setelah dievaluasi akan dapat ditentukan penanganan risiko.

DS4	1. Apakah PUSTIPD mengembangkan kerangka kerja kontinuitas TI?	Iya pustipo mengembangkan kerangka kerja kontinuitas TI untuk mendukung manajemen kontinuitas bisnis.

Responden: Chief Architect

DS5	1. Apakah PUSTIPD telah menetapkan, membuat, dan mengoperasikan identitas(akun) proses manajemen?	Untuk secara detailnya belum, terkait identitas akun akun secara umum.
	2. Apakah PUSTIPD menerapkan dan memelihara kontrol teknis dan prosedural untuk melindungi arus informasi di seluruh jaringan?	Saat ini belum menggunakan teknis komunikasi dan prosedur manajemen.
DS11	1. Apakah PUSTIPD menerjemahkan penyimpanan data dan persyaratan penyimpanan ke dalam prosedur?	Iya penyimpanan datanya diterapkan sesuai prosedur yang disepakati

Responden: Head Operations

IT Process	Pertanyaan	Jawaban
PO4	1. Bagaimana PUSTIPD menetapkan dan mengimplementasikan peran dan tanggung jawab TI, termasuk pengawasan dan pemisahan tugas?	Dengan membagi job desc tanggung jawab TI untuk tiap dep yang ada di pustipd
PO9	1. Apakah PUSTIPD telah memahami tujuan proses bisnis yang relevan?	Tujuan proses bisnis dipahami, namun mungkin belum relevan
	2. Apakah PUSTIPD mengidentifikasi peristiwa/kejadian yang terkait dengan tujuan bisnis?	Iya pustipd mengidentifikasi peristiwa / kejadian terkait dengan tujuan bisnis
	3. Apakah PUSTIPD menilai risiko yang terkait dengan peristiwa/kejadian?	Saat ini belum dilakukan penilaian risiko setiap kejadian.

Responden: Head Operations

PO9	4. Apakah PUSTIPD mengevaluasi dan memilih respon risiko?	Ada evaluasi dan pemilihan respon risiko dilakukan, namun belum ada prosedur resmi yang diikuti terkait evaluasi dan pemilihan respon risiko.
	5. Apakah PUSTIPD menyetujui dan memastikan pendanaan untuk rencana tindakan berisiko?	Untuk skrng belum diterapkan, pendanaan dilakukan tergantung situasi yg dihadapi
DS2	1. Apakah PUSTIPD mengidentifikasi dan mengkategorikan hubungan layanan dengan pihak ketiga?	Diidentifikasi secara umum
	2. Apakah PUSTIPD telah menetapkan dan mendokumentasikan proses manajemen pemasok?	Iya telah ditetapkan dan didokumentasikan oleh pustipd mengenai proses manajemen pemasok

Responden: Head IT Operations

DS2	3. Apakah PUSTIPD telah mengidentifikasi, menilai, dan mitigasi risiko pemasok?	Iya sudah dilakukan proses identifikasi, penilaian dan mitigasi risiko pemasok
	4. Apakah PUSTIPD memantau pengiriman dari pemasok?	Iya dilakukan evaluasi dan monitoring
DS4	1. Apakah PUSTIPD mengembangkan kerangka kerja kontinuitas TI?	Iya dilakukan pengembangan kerangka kerja kontinuitas TI untuk mendukung manajemen kontinuitas bisnis
	2. Apakah PUSTIPD melakukan analisis dampak bisnis dan penilaian risiko?	Belum dilakukan untuk saat ini

\

Respondem Head Operations

	DS4	3. Apakah PUSTIPD mengembangkan dan memelihara rencana kesinambungan TI?	Iya dilakukan pengembangan dan pemeliharaan rencana kesinambungan TI
		4. Apakah PUSTIPD mengidentifikasi dan mengkategorikan sumber daya TI berdasarkan tujuan pemulihan?	Iya untuk saat ini dilakukan secara dengan ketersediaan / utilisasi dari sumber daya IT untuk pemulihan.
		5. Apakah PUSTIPD menetapkan dan menjalankan prosedur kontrol perubahan untuk memastikan bahwa rancana kesinambungan TI pada saat ini?	Saat ini belum dilakukan
		6. Apakah PUSTIPD menguji rencana kesinambungan TI secara teratur?	Iya dilakukan pengujian rencana kesinambungan TI dengan menguji prosedur, secara dengan cop

Respondem Head Operations

	DS4	11. Apakah PUSTIPD menetapkan prosedur untuk melakukan tinjauan paska pengulasan.	Saat ini pustipd belum melakukan penetapan prosedur untuk tinjauan pasca pengulasan.
	DS5	1. Apakah PUSTIPD telah menetapkan, membuat, dan mengoperasikan identitas(akun) proses manajemen?	Telah diidentifikasi, namun hanya secara umum belum spesifik.
		2. Apakah PUSTIPD memantau potensi dan insiden keamanan aktual?	Belum dilakukan pengamatan pemantauan potensi dan insiden keamanan secara aktual
		3. Apakah PUSTIPD menetapkan dan memelihara prosedur untuk memelihara dan menjaga kunci kriptografi?	Belum ada prosedur pendistribusian dan penjagaan kunci enkripsi

Iponden Head Operations

	DS11	1. Apakah PUSTIPD telah menetapkan, memperbaharukan dan menerapkan prosedur untuk mengelola media perpustakaan?	Iya sudah ditetapkan prosedur pengelolaannya
		2. Apakah PUSTIPD telah menentukan, memelihara, dan menerapkan prosedur untuk penggantian media dari peralatan secara aman?	Biasanya untuk penggunaan media dan perbaikan tergantung situasi dan kondisi dari pertimbangan kalau memang harus ganti, ya diganti. Untuk prosedur dilakukan secara otomatis
		3. Apakah PUSTIPD telah mencadangkan data sesuai skema?	Iya dilakukan rutin setiapnya, biasanya berupa per minggu / bulan
		4. Apakah PUSTIPD menentukan, memelihara dan menerapkan prosedur untuk pemulihan data?	Pemulihan data belum ada prosedur, dilakukan tergantung individu

Responden: Head Operations

	DS12	1. Apakah PUSTIPD telah menetukan tingkat perlindungan fisik yang diperlukan?	Telah dilakukan untuk saat ini
		2. Apakah PUSTIPD memilih dan mengkomisikan situs (pusat data, kantor, dll)?	Iya, dengan membandingkan berbagai referensi dan brand.
		3. Apakah PUSTIPD telah menerapkan langkah-langkah lingkungan fisik?	Dengan melakukan penempatan server/peralatan ditempat yang aman, diluar keramaian.
		4. Apakah PUSTIPD telah mengelolah lingkungan fisik (termasuk pemeliharaan, pemantauan, dan pelaporan)?	Iya, pemeliharaan sama seperti tadi ditempatkan ditempat yang aman, jauh dari keramaian, dipantau dengan cctv ada pengembangan menyesuaikan dengan perkembangan zaman.

Responden: Head Operations

	DS12	5. Apakah PUSTIPD telah menetapkan dan menerapkan prosedur untuk otorisasi dan pemeliharaan akses fisik?	Untuk prosedur sedang diajukan dan dirancang
	ME2	1. Apakah PUSTIPD memantau dan mengendalikan kegiatan internal TI	Iya dilakukan proses pemantauan dan pengendalian kegiatan internal TI
		2. Apakah PUSTIIPD memantau proses penilaian diri?	Iya memantau proses penilaian diri
		3. Apakah PUSTIPD memantau kinerja dari rinjauan independent, audit, dan ujian?	Pemantauan kinerja dari hasil laporan rapat rutin setiap minggu/bulan

Responden: Head Operations

	ME2	4. Apakah PUSTIPD memantau proses untuk mendapatkan jaminan atas kontrol yang dioperasikan oleh pihak ketiga?	Iya dilakukan pemantauan proses, untuk mendapatkan jaminan atas kontrol yang dioperasikan pihak ketiga
		5. Apakah PUSTIPD memantau proses untuk mengidentifikasi dan menilai pengecualian kontrol?	Iya PUSTIPD memantau proses untuk mengidentifikasi dan menilai pengecualian kontrol
		6. Apakah PUSTIPD memantau proses untuk mengidentifikasi dan memulihkan pengecualian kontrol?	Iya PUSTIPD memantau proses untuk mengidentifikasi dan memulihkan pengecualian kontrol
	ME3	1. Apakah PUSTIPD mengevaluasi kepatuhan kebijakan TI dengan kebijakan, rencana, dan prosedur TI	Iya dilakukan proses evaluasinya.

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 diberitau, komite juga sudah secara general dan untuk hubungan TI dg pemangku kepentingan sudah dijelaskan berdasarkan kebutuhan dan pemangku kepentingan.
	2. Apakah PUSTIPD telah merancang kerangka proses TI?	Iya sudah dirancang, tetapi proses TI ini ditujukan untuk mendukung pelaksanaan rencana strategis di pustipd.
	3. Apakah PUSTIPD menetapkan dan mengimplementasikan peran dan tanggung jawab TI, termasuk pengawasan dan pemisahan tugas?	Iya ditetapkan dan diimplementasikan. Dengan pembagian job desk untuk tiap staf TI di pustipd, sehingga terbentuk peran, tanggung jawab terhadap TI, serta pengawasan dan pemisahan tugas.
PO 6	1. Apakah PUSTIPD mengembangkan dan memelihara kebijakan TI?	pustipd mendukung kebijakan TI dengan peraturan kebijakan yang selaras dengan manajemen perubahan, dikembangkan berdasarkan kebutuhan dan penyesuaian perkembangan TI.
	2. Apakah PUSTIPD mengkomunikasikan kerangka kontrol TI dan tujuan TI	tentunya dikomunikasikan, dengan cara melakukan sosialisasi dan pengadaan pelatihan

Responden: Head IT Administration

PO9	1.	Apakah PUSTIPD mengidentifikasi peristiwa/kejadian yang terkait dengan tujuan bisnis?	Iya pustipd mengidentifikasi peristiwa-peristiwa yang terkait dengan tujuan bisnis, pengaruhnya sebagai bahan analisis dan evaluasi untuk pelayanan dimasa mendatang.
	2.	Apakah PUSTIPD menilai risiko yang terkait dengan peristiwa/kejadian?	Belum untuk menilai risiko belum.
	3.	Apakah PUSTIPD mengevaluasi dan memilih respon risiko?	Iya, biasanya risiko tersebut dievaluasi kemudian ditentukan yang memerlukan untuk respon risiko.
DS2	1.	Apakah PUSTIPD mengidentifikasi dan mengkategorikan hubungan layanan dengan pihak ketiga?	Diidentifikasi secara umum, belum secara mendetail

Responden: Head IT Administration

DS2	2.	Apakah PUSTIPD telah menetapkan dan mendokumentasikan proses manajemen pemasok?	Iya sudah ditetapkan dan didokumentasikan proses manajemen pemasoknya secara formal pada pustipd
	3.	Apakah PUSTIPD telah menetapkan kebijakan dan prosedur evaluasi dan seleksi pemasok?	Iya telah ditetapkan kebijakan dan prosedur untuk evaluasi dan seleksi pemasok
	4.	Apakah PUSTIPD telah mengidentifikasi, menilai, dan mitigasi risiko pemasok?	Iya pada pemasok adalah risiko yang berasitan, didengarkan, dinilai, dan mitigasi
	5.	Apakah PUSTIPD memantau penginiman dari pemasok?	Iya ~~Apakah~~ dipantau

Responden: Head IT Administration

DS2	6.	Apakah PUSTIPD mengetahui tujuan jangka panjang dan hubungan layanan untuk semua pemangku kepentingan?	Untuk memberikan solusi, yang berkaitan dengan pustipd saja
DS4	1.	Apakah PUSTIPD menetapkan dan menjalankan prosedur kontrol perubahan untuk memastikan bahwa rencana kesinambungan TI pada saat ini?	iya ditetapkan dan dijalankan disesuaikan dengan work flow rencana strategis pustipd
	2.	Apakah PUSTIPD mengembangkan rencana tindak lanjut dari hasil tes?	Rencana kesinambungan TI disesuaikan dengan kondisinya beranjak kerja
	3.	Apakah PUSTIPD merencanakan dan melakukan pelatihan kesinambungan TI?	Belum ada perencanaan dan pelaksanaan pelatihan terkait kesinambungan TI di pustipd

Responden: Head IT Administration

DS4	4.	Apakah PUSTIPD merencanakan pemulihan layanan TI dan pemulihan kembali?	Untuk perencanaan pemulihan layanan TI dan pemulihan kembali sedang dalam tahap proses
ME2	1.	Apakah PUSTIPD memantau dan mengendalikan kegiatan internal TI	iya selalu, karena sistem tidak dipantau dan dikendalikan oleh subbagian.
	2.	Apakah PUSTIPD memantau proses penilaian diri?	iya pendapatnya didapat dianalisa dari hasil kontrol internal melalui aduan pihak ketiga dan review pihak ketiga
	3.	Apakah PUSTIPD memantau kinerja dari tinjauan independent, audit, dan ujian?	Biasanya dilihat dari hasil rapat untuk peningkatan/ perbaikan untuk evaluasi kinerja

Responden: Head IT Administration

ME2	4.	Apakah PUSTIPD memantau proses untuk mendapatkan jaminan atas kontrol yang dioperasikan oleh pihak ketiga?	iya pustipd memiliki sistem kontrol internal untuk layanan pihak ketiga, sesuaikan dengan prosedur di instansi pemerintah dan harus patuh dengan kontrak
	5.	Apakah PUSTIPD memantau proses untuk mengidentifikasi dan menilai pengecualian kontrol?	iya dipantau, dilaporkan analisa dan saran penyelesaiannya. pustipd juga melakukan peninjauan pengecualian kontrol dan ~~[illegible]~~ melaporkan ke pemangku kepentingan.
	6.	Apakah PUSTIPD memantau proses untuk mengidentifikasi dan memulihkan pengecualian kontrol?	iya pustipd mengidentifikasi saran penyelesaian dan memulihkan pengecualian kontrol
ME3	1.	Apakah PUSTIPD mengevaluasi kepatuhan kebijakan TI dengan kebijakan, rencana, dan prosedur TI	iya mengevaluasi kepatuhan kebijakan TI dengan kebijakan, rencana dan prosedur TI

Responden CIO

IT Process	Pertanyaan	Jawaban
PO8	1. Apakah PUSTIPD telah membangun dan memelihara lingkungan pengendalian dan kerangka TI?	Iya lingkungan pengendalian dan kerangka TI dibangun dan dipelihara, terkait dengan SDM, sarana yang berbasis, komputer serta pengembangan
	2. Apakah PUSTIPD mengembangkan dan memelihara kebijakan TI?	Iya dikembangkan dan juga dilakukan pemeliharaan terhadap kebijakan TI
	3. Apakah PUSTIPD mengkomunikasikan kerangka kontrol TI dan tujuan TI	Iya dikomunikasikan, dengan cara melakukan sosialisasi dan pelatihan.
PO9	1. Apakah PUSTIPD telah memahami strategis tujuan bisnis yang relevan?	Sudah memahami tujuan bisnis, namun belum bisa dikatakan relevan.

Responden CIO

PO9	2.	Bagaimanan PUSTIPD memelihara dan memantau rencana tidakan berlaku?	Dengan memantaunya kegiatan pengadaan, dan ada dilakukan monitoring
DS2	1.	Apakah PUSTIPD memantau pengiriman dari pemasok?	Iya pustipd memantau pengiriman dari pemasok
	2.	Apakah PUSTIPD mengetahui tujuan jangka panjang dan hubungan layanan untuk semua pemangku kepentingan?	pustipd mengetahui tujuan dan layanan jangka panjang untuk pemangku kepentingan yang berkaitan dengan pustipd, untuk melakukan bidang kerja yang tetap dengan pustipd saja.
ME2	1.	Apakah PUSTIPD melaporkan kepada pemangku kepentingan utama?	Iya dilaporkan kepada pemangku kepentingan utama

Responden CIO

ME3	1.	Apakah PUSTIPD menetapkan dan laksanakan proses untuk mengidentifikasikan persyaratan hukum, kontrak, kebijakan dan peraturan?	Iya dilakukan, dilaksanakan dengan standar/prosedur yang berlaku.
	2.	Apakah PUSTIPD mengevaluasi kepatuhan kebijakan TI dengan kebijakan, rencana, dan prosedur TI	Iya dilakukan evaluasi kebijakan TI dengan kebijakan, rencana dan prosedur TI, untuk perbaikan kebijakan TI yang lebih baik, serta mengurangi kelemahannya
	3.	Apakah PUSTIPD melaporkan jaminan positif kepatuhan kegiatan TI dengan kebijakan, rencana dan prosedur TI?	Iya dilakukan untuk jaminan kepatuhan kegiatan TI dengan kebijakan, rencana dan prosedur TI
	4.	Apakah PUSTIPD telah memberikan masukan untuk menyelaraskan kebijakan, rencana, dan prosedur TI dalam menanggapi persyaratan kepatuhan?	Iya memerlukan diperoleh dari hasil rapat, dalam [illegible] tinjauan review pihak ketiga atau pihak terkait

Responden: CIO

ME3	5. Apakah PUSTIPD mengintegrasikan pelaporan TI pada persyaratan peraturan dengan output serupa dari fungsi bisnis lainnya?	Iya pustipd bekerja sama mengintegrasikan laporan TI pada pengelola.
ME4	1. Apakah PUSTIPD membuat laporan tata kelola TI?	Untuk laporannya belum

Responden: CAS

ME4	2. Apakah PUSTIPD menyelesaikan temuan penilaian independen, dan memastikan implementasi manajemen atas rekomendasi yang didapati?	Iya pustipd mengetahui dan menginplementasikan rekomendasi yang telah diberikan.

Responden : Head Development

No	Process	Pertanyaan	Jawaban
	PO9	1. Apakah PUSTIPD mengidentifikasi peristiwa/kejadian yang terkait dengan tujuan bisnis?	Iya mengidentifikasi peristiwa/kejadian yang terkait dengan tujuan bisnis, yang memiliki fungsi sebagai bidang evaluasi
		2. Apakah PUSTIPD menilai risiko yang terkait dengan peristiwa/kejadian?	Saat ini pustipd belum melakukan penilaian risiko terkait peristiwa
		3. Apakah PUSTIPD mengevaluasi dan memilih respon risiko?	Iya dievaluasi untuk menentukan penanganan terhadap risiko yang dihadapi
	DS2	1. Apakah PUSTIPD mengidentifikasi dan mengkategorikan hubungan layanan dengan pihak ketiga?	Saat ini sudah diidentifikasi dan dikategorikan

Responden : CFO

No	Process	Pertanyaan	Jawaban
	PO9	1. Apakah pada PUSTIPD telah ditentukan keselarasan manajemen risiko (misalnya menilai risiko)?	Karena baru terangkan risiko pustipd belum dibentuk, sehingga belum bisa mengidentifikasi proses - proses berisiko.

Responden : Head Development

No	Process	Pertanyaan	Jawaban
	DS2	2. Apakah PUSTIPD telah menetapkan dan mendokumentasikan proses manajemen pemasok?	Iya sudah ada penetapan dan pendokumentasian proses manajemen pemasok
		3. Apakah PUSTIPD telah mengidentifikasi, menilai, dan mitigasi risiko pemasok?	Iya sudah dilakukan identifikasi, menilai, dan meminimasi risiko pemasok
		4. Apakah PUSTIPD memantau pengiriman dari pemasok?	Iya dilakukan pemantauan pengiriman dari pemasok
	DS4	1. Apakah PUSTIPD mengembangkan kerangka kerja kontinuitas TI?	Iya pustipd mengembangkan kerangka kerja kontinuitas TI, seperti bidang manajemen TI, konsep/prosedur dasar, dan pengembangan

Responden : Head Development

	DS4	2. Apakah PUSTIPD menetapkan dan menjalankan prosedur kontrol perubahan untuk memastikan bahwa rencana kesinambungan TI pada saat ini?	Iya saat ini sudah ditetapkan dan menjalankan prosedur kontrol perubahan
		3. Apakah PUSTIPD mengembangkan rencana tindak lanjut dari hasil tes?	Iya untuk mengembangkan rencana tindak lanjut disesuaikan berdasarkan kerangka kerja
		4. Apakah PUSTIPD merencanakan pemulihan layanan TI dan pemulian kembali?	Saat ini masih dalam tahapan perancangan
	DS5	5. Apakah PUSTIPD menerapkan dan memelihara kontrol teknis dan prosedural untuk melindungi arus informasi di seluruh jaringan?	Saat ini belum menerapkan dan memelihara kontrol teknis dan prosedural untuk melindungi arus informasi tiap jaringan

Responden : Head Development

	ME2	1. Apakah PUSTIPD memantau dan mengendalikan kegiatan internal TI	Iya memantau dan mengendalikan kegiatan internal TI
		2. Apakah PUSTIIPD memantau proses penilaian diri?	Iya dilakukan pemantauan pendiri diri, dengan mengevaluasi efektivitas proses TI, kebijakan tata kerbera
		3. Apakah PUSTIPD memantau kinerja dari tinjauan independent, audit, dan ujian?	Dalam pemantauan kinerja didapat dari laporan hasil kerja di rapat yang dilakukan setiap minggu / bulan.
		4. Apakah PUSTIPD memantau proses untuk mendapatkan jaminan atas kontrol yg dioperasikan oleh pihak ketiga?	Iya memantau proses untuk mendapat jaminan atas kontrol yg dioperasikan pihak ketiga

Responden : Head Development

	ME2	5. Apakah PUSTIPD memantau proses untuk mengidentifikasi dan menilai pengecualian kontrol?	Iya PUSTIPD memantau proses untuk identifikasi dan penilaian pengecualian kontrol
		6. Apakah PUSTIPD memantau proses untuk mengidentifikasi dan memulihkan pengecualian kontrol?	Iya, pertama didentifikasi kemudian dilakukan evaluasi untuk langkah penanganan penanganan dan penyelesaian
	ME3	1. Apakah PUSTIPD mengevaluasi kepatuhan kebijakan TI dengan kebijakan, rencana, dan prosedur TI	Iya dilakukan evaluasi kepatuhan kebijakan TI dengan kebijakan, rencana dan prosedur TI

Responden: CAS

IT Process	Pertanyaan	Jawaban
PO9	1. Bagaimanan PUSTIPD memelihara dan memantau rencana tidakan berisiko?	Dengan memprioritaskan dan merencanakan kegiatan pengendalian diikuti lanjutan.
DS4	2. Apakah PUSTIPD mengembangkan kerangka kerja kontinuitas TI?	Iya dikembangkan oleh pustipd
DS5	1. Apakah pada PUSTIPD telah menetapkan dan mempertahankan rencana keamanan TI?	Penetapan keamanan TI dilakukan secara kondisional ketika ada bencana/resiko diperbaiki dan dipulihkan. Untuk pendokumentasian formal belum ada
	2. Apakah PUSTIPD memantau potensi dan insiden keamanan aktual?	Belum dilaksanakan secara aktual

Responden: CAS

IT Process	Pertanyaan	Jawaban
DS5	3. Apakah pada PUSTIPD meninjau dan validasikan hak akses dan hak pengguna secara berkala?	Validasi tidak hanya dilakukan sekali, namun kurun waktu validasi tidak ditetapkan
	4. Apakah pada PUSTIPD telah dilakukan penilaian kerentanan secara berkala?	Iya dilakukan monitoring dengan berkala, dari waktu ke waktu sesuai dengan yang ditetapkan
ME3	1. Apakah PUSTIPD menetapkan dan laksanakan proses untuk mengidentifikasikan persyaratan hukum, kontrak, kebijakan dan peraturan?	Iya ditetapkan dan dilaksanakan, sesuai dengan standar nasional.
	2. Apakah PUSTIPD mengevaluasi kepatuhan kebijakan TI dengan kebijakan, rencana, dan prosedur TI	Iya dievaluasi kepatuhan kebijakan TI-nya dengan kebijakan, rencana dan prosedur TI

Responden: CAS

IT Process	Pertanyaan	Jawaban
ME3	3. Apakah PUSTIPD melaporkan jaminan positif kepatuhan kegiatan TI dengan kebijakan, rencana dan prosedur TI?	Iya dilaporkan jaminan positif kepatuhan kegiatan TI dengan kebijakan, rencana dan prosedur TI
	4. Apakah PUSTIPD telah memberikan masukan untuk menyelaraskan kebijakan, rencana, dan prosedur TI dalam menanggapi persyaratan kepatuhan?	Iya telah dilakukan oleh pustipd, ~~ajuan masukan~~ ajuan masukan untuk menyelaraskan kebijakan, rencana, dan prosedur TI dalam menanggapi persyaratan kepatuhan
	5. Apakah PUSTIPD mengintegrasikan pelaporan TI pada persyaratan peraturan dengan output serupa dari fungsi bisnis lainnya?	Saat ini pustipd masih mengupayakan untuk mengintegrasikan pelaporan TI pada persyaratan peraturan dengan output dari fungsi bisnis
ME4	1. Apakah PUSTIPD mendapatkan penilaian independent berkala atas kinerja dan kepatuhan terhadap kebijakan rencana dan prosedur?	Iya PUSTIPD dinilai secara berkala atas kinerja dan kepatuhan terhadap rencana dan prosedur

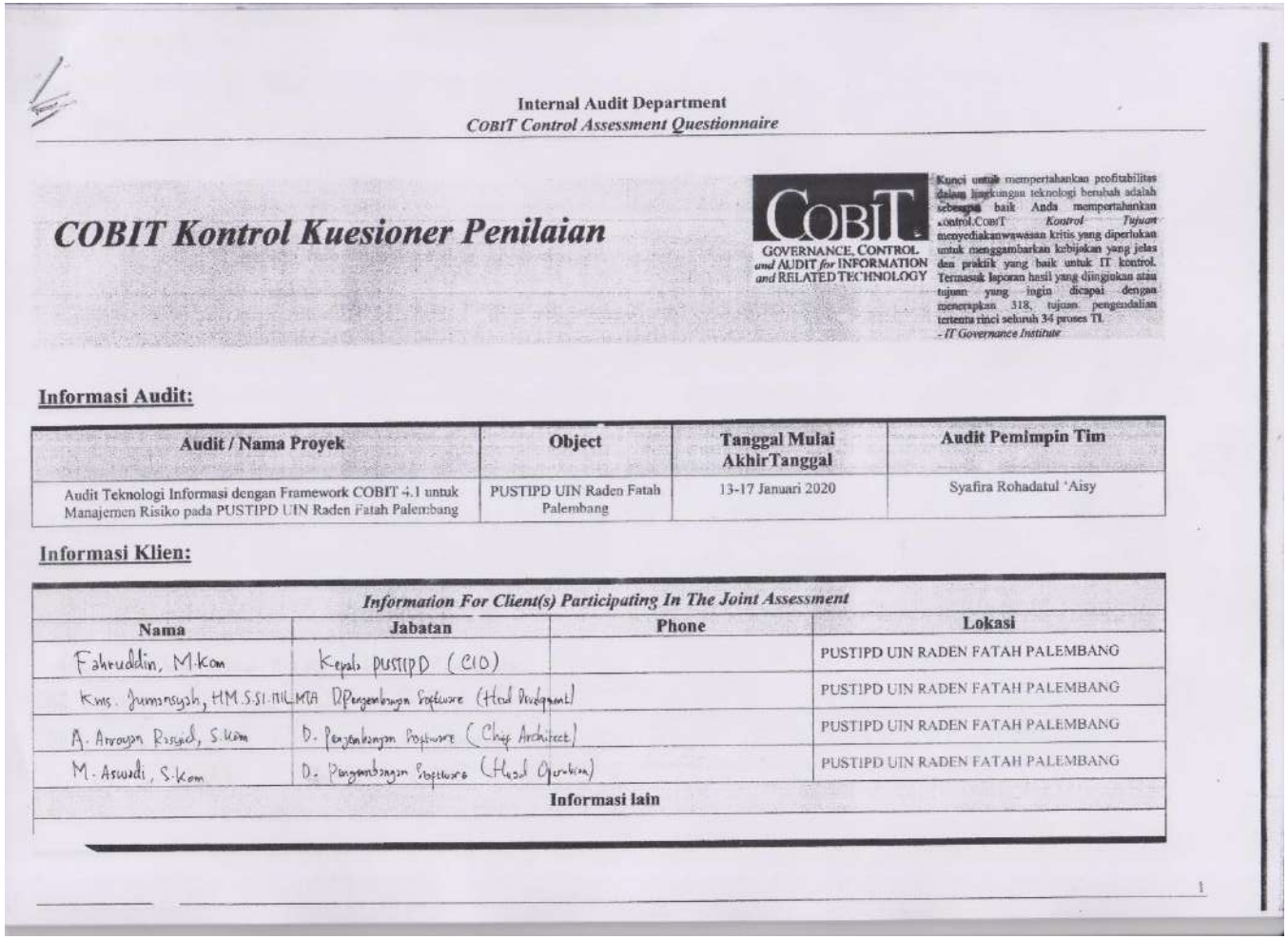
Responden: CFO

IT Process	Pertanyaan	Jawaban
PO9	1. Apakah pada PUSTIPD telah ditentukan keselarasan manajemen risiko (misalnya menilai risiko)?	Karena kerja manajemen risiko pustipd belum diterapkan, sehingga belum bisa menyelaraskan proses - proses terkait.

Responden: CAS

ME4	2. Apakah PUSTIPD menyelesaikan temuan penilaian independen, dan memastikan implementasi manajemen atas rekomendasi yang didapat?	Iya pustipd menyelesaikan dan menginplementasikan rekomendasi yang sudah diberikan.

Wawancara Audit II



Internal Audit Department
COBIT Control Assessment Questionnaire

COBIT Kontrol Kuesioner Penilaian

COBIT
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

Kunci untuk mempertahankan profitabilitas dalam lingkungan teknologi berubah adalah sebagian baik Anda mempertahankan control.COBIT *Kontrol Tujuan* menyediakanwawasan kritis yang diperlukan untuk menggambarkan kebijakan yang jelas dan praktik yang baik untuk IT kontrol. Termasuk laporan hasil yang diinginkan atau tujuan yang ingin dicapai dengan menerapkan 318, tujuan pengendalian tertentu rinci seluruh 34 proses TI.
- IT Governance Institute

Informasi Audit:

Audit / Nama Proyek	Object	Tanggal Mulai AkhirTanggal	Audit Pemimpin Tim
Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UIN Raden Fatah Palembang	PUSTIPD UIN Raden Fatah Palembang	13-17 Januari 2020	Syafira Rohadatul 'Aisy

Informasi Klien:

Information For Client(s) Participating In The Joint Assessment			
Nama	**Jabatan**	**Phone**	**Lokasi**
Fahruddin, M.Kom	Kepala PUSTIPD (CIO)		PUSTIPD UIN RADEN FATAH PALEMBANG
Kms. Jumnasyah, HM.S.SI.MIL.MTA	DPengembangan Software (Head Program)		PUSTIPD UIN RADEN FATAH PALEMBANG
A. Arrozan Rasyid, S.Kom	D. Pengembangan Software (Chief Architect)		PUSTIPD UIN RADEN FATAH PALEMBANG
M. Aswadi, S.Kom	D. Pengembangan Software (Head Operation)		PUSTIPD UIN RADEN FATAH PALEMBANG
Informasi lain			

1

Internal Audit Department
COBIT Control Assessment Questionnaire

COBIT Kontrol Kuesioner Penilaian

COBIT
GOVERNANCE, CONTROL *and* AUDIT *for* INFORMATION *and* RELATED TECHNOLOGY

Kunci untuk mempertahankan profitabilitas dalam lingkungan teknologi berubah adalah sebaiknya baik Anda mempertahankan kontrol.COBIT *Kontrol Tujuan* menyediakanwawasan kritis yang diperlukan untuk menggambarkan kebijakan yang jelas dan praktik yang baik untuk IT kontrol. Termasuk laporan hasil yang diinginkan atau tujuan yang ingin dicapai dengan menerapkan 318, tujuan pengendalian tertentu rinci seluruh 34 proses TI.
- IT Governance Institute

Informasi Audit:

Audit / Nama Proyek	Object	Tanggal Mulai AkhirTanggal	Audit Pemimpin Tim
Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UIN Raden Fatah Palembang	PUSTIPD UIN Raden Fatah Palembang	13-17 Januari 2020	Syafira Rohadatul 'Aisy

Informasi Klien:

Information For Client(s) Perticipating In The Joint Assessment			
Nama	**Jabatan**	**Phone**	**Lokasi**
Akbar Awing Sugiarto, S.Kom, M-I	LMA Head M Administration		PUSTIPD UIN RADEN FATAH PALEMBANG
Prof. DRS. H.M. Sirozi. M.A. ph.D	Rector (CEO)		PUSTIPD UIN RADEN FATAH PALEMBANG
Musli Dasuan. S. Ag. M.Si	Kabag Perencanaan dan Keuangan (CFO)		PUSTIPD UIN RADEN FATAH PALEMBANG
Dr. H. Fajri Ismail, M.Pd.I	Kepala LPM (CAE)		PUSTIPD UIN RADEN FATAH PALEMBANG
Informasi lain			

Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	4 (PO4.2, PO4.6, PO4.8, PO4.11, PO4.12, PO4.19)

COBIT Penilaian Tingkat Kematangan: *PO4* Menentukan Proses, Organisasi, dan Hubungan IT:

Rating	Deskripsi
0 - *Non Existent*	Organisasi TI tidak secara efektif didirikan untuk fokus pada pencapaian tujuan bisnis.
1 - *Initial/ Ad Hoc*	Kegiatan dan fungsi IT bersifat reaktif dan tidak konsisten dilaksanakan. IT terlibat dalam proyek bisnis hanya di tahap selanjutnya. Fungsi TI dianggap sebagai fungsi pendukung, tanpa perspektif organisasi secara keseluruhan. Ada pemahaman implisit tentang perlunya organisasi TI; Namun, peran dan tanggung jawab tidak diformalkan atau ditegakkan.
2 - *Repeatable but Intuitive*	Fungsi TI diatur untuk merespons secara taktis, tetapi tidak konsisten, terhadap kebutuhan pelanggan dan hubungan vendor. Kebutuhan untuk organisasi yang terstruktur dan manajemen vendor dikomunikasikan, tetapi keputusan masih bergantung pada pengetahuan dan keterampilan individu kunci. Ada munculnya 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, 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.
4 - *Managed and Measurable*	Organisasi TI secara proaktif menanggapi perubahan dan mencakup semua peran yang diperlukan untuk memenuhi persyaratan bisnis. Manajemen TI, proses kepemilikan, akuntabilitas dan tanggung jawab didefinisikan dan seimbang. 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 disukai. Metrik terukur untuk mendukung tujuan bisnis dan faktor keberhasilan kritis yang ditentukan 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 ditegakkan. Struktur organisasi TI secara tepat mencerminkan kebutuhan bisnis dengan menyediakan layanan yang selaras dengan proses bisnis strategis, daripada dengan teknologi terisolasi.
5 - *Optimised*	Struktur organisasi TI bersifat fleksibel dan adaptif. Praktik baik industri diterapkan. Ada banyak penggunaan teknologi untuk membantu memantau kinerja organisasi dan proses TI. Teknologi ditingkatkan sejalan untuk mendukung kompleksitas dan distribusi geografis organisasi. Ada proses perbaikan berkelanjutan di tempat.

Nilai Keseluruhan Tingkat Kematangan Terendah:	2 (PO4.9)

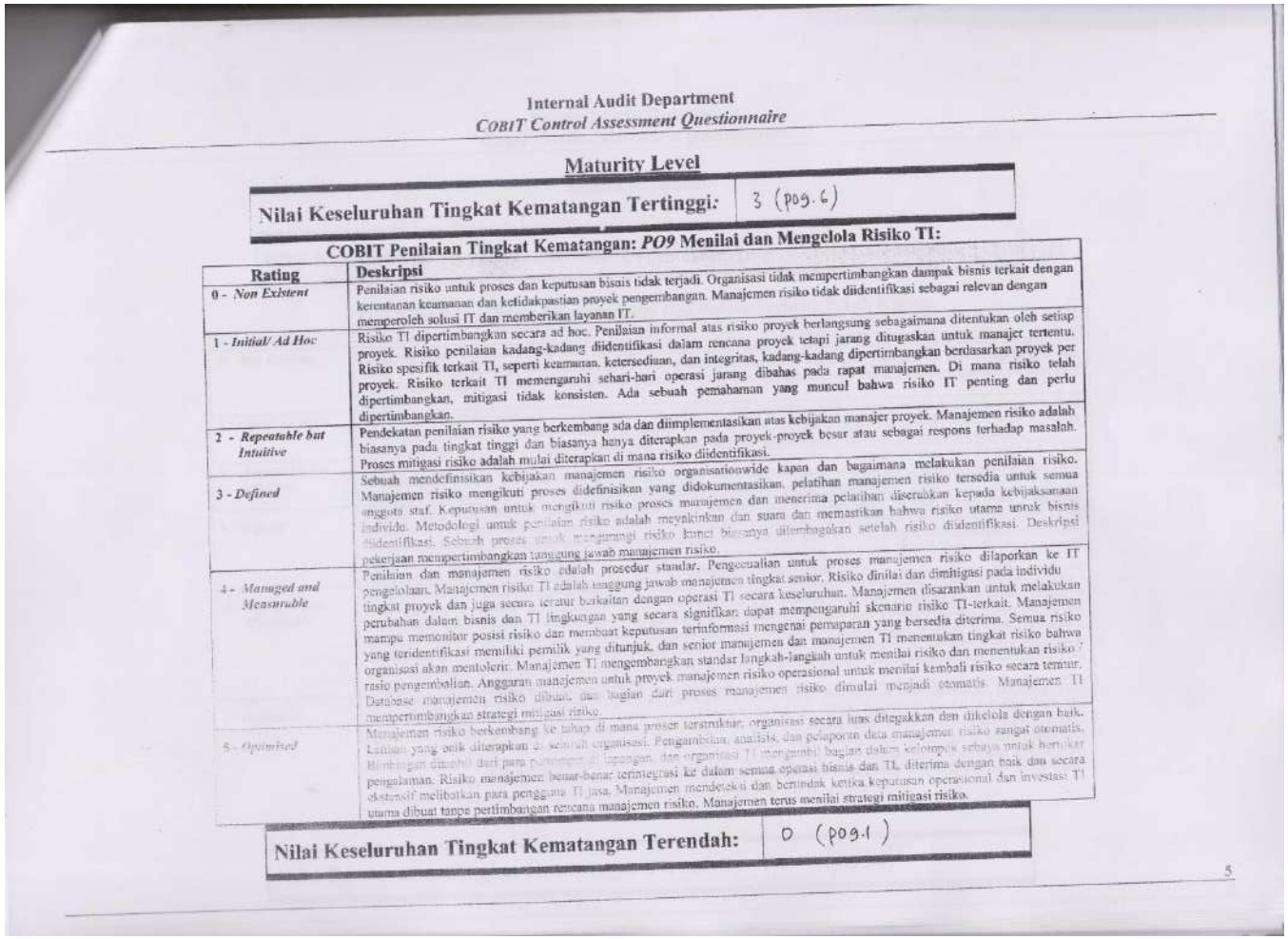
Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	4 (PO6.1, PO6.3, PO6.5)

COBIT Penilaian Tingkat Kematangan: *PO6* Komunikasikan Tujuan Manajemen dan Pengarahan:

Rating	Deskripsi
0 - *Non Existent*	Manajemen belum membentuk lingkungan kendali TI yang positif. Tidak ada pengakuan akan perlunya menetapkan seperangkat kebijakan, rencana dan prosedur, dan proses kepatuhan.
1 - *Initial/ Ad Hoc*	Manajemen reaktif dalam menangani persyaratan lingkungan kontrol informasi. Kebijakan, prosedur dan standar dikembangkan dan dikomunikasikan secara ad hoc karena didorong oleh masalah. Pengembangan, komunikasi, dan kepatuhan prosesnya informal dan tidak konsisten.
2 - *Repeatable but Intuitive*	Kebutuhan dan persyaratan lingkungan kontrol informasi yang efektif secara implisit dipahami oleh manajemen, tetapi praktik sebagian besar informal. Kebutuhan akan kebijakan, rencana, dan prosedur pengendalian dikomunikasikan oleh manajemen, tetapi pengembangan masih tertinggal untuk kebijaksanaan manajer individu dan bidang bisnis. Kualitas diakui sebagai filosofi yang diinginkan untuk diikuti, tetapi praktik diserahkan pada kebijaksanaan masing-masing manajer. Pelatihan dilakukan atas dasar individu, sesuai kebutuhan.
3 - *Defined*	Kontrol informasi yang lengkap dan lingkungan manajemen mutu dikembangkan, didokumentasikan dan dikomunikasikan oleh manajemen dan termasuk kerangka kerja untuk kebijakan, rencana dan prosedur. Proses pengembangan kebijakan terstruktur, dipelihara dan dikenal kepada staf, dan kebijakan, rencana, dan prosedur yang ada cukup masuk akal dan mencakup masalah-masalah utama. Manajemen membahas pentingnya kesadaran keamanan TI dan memulai program kesadaran. Pelatihan formal tersedia untuk mendukung informasi mengendalikan lingkungan tetapi tidak diterapkan dengan ketat. Sementara ada kerangka pengembangan keseluruhan untuk kebijakan kontrol dan prosedur, ada pemantauan kepatuhan yang tidak konsisten dengan kebijakan dan prosedur ini. Ada perkembangan menyeluruh kerangka. Teknik untuk meningkatkan kesadaran keamanan telah distandarisasi dan diformalkan.
4 - *Managed and Measurable*	Manajemen menerima tanggung jawab untuk mengkomunikasikan kebijakan pengendalian internal dan mendelegasikan tanggung jawab dan mengalokasikan cukup sumber daya untuk menjaga lingkungan sejalan dengan perubahan signifikan. Lingkungan kontrol informasi yang positif dan proaktif, termasuk komitmen terhadap kualitas dan kesadaran keamanan TI, didirikan. Satu set lengkap kebijakan, rencana dan prosedur adalah dikembangkan, dipelihara dan dikomunikasikan dan merupakan gabungan dari praktik baik internal. Kerangka kerja untuk peluncuran dan selanjutnya pemeriksaan kepatuhan telah ditetapkan
5 - *Optimised*	Lingkungan kontrol informasi selaras dengan kerangka kerja strategis dan visi dan sering ditinjau, diperbarui dan terus ditingkatkan. Para ahli internal dan eksternal ditugaskan untuk memastikan bahwa praktik-praktik baik industri sedang dilaksanakan diadopsi sehubungan dengan mengontrol pedoman dan teknik komunikasi. Monitoring, penilaian diri dan pengecekan kepatuhan adalah meresap dalam organisasi. Teknologi digunakan untuk memelihara basis pengetahuan kebijakan dan kesadaran dan untuk mengoptimalkan komunikasi, menggunakan otomatisasi kantor dan alat pelatihan berbasis komputer.

Nilai Keseluruhan Tingkat Kematangan Terendah:	3 (PO6.2, PO6.4)



Internal Audit Department
COBIT Control Assessment Questionnaire

Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	3 (PO9.6)

COBIT Penilaian Tingkat Kematangan: *PO9* Menilai dan Mengelola Risiko TI:

Rating	Deskripsi
0 - *Non Existent*	Penilaian risiko untuk proses dan keputusan bisnis tidak terjadi. Organisasi tidak mempertimbangkan dampak bisnis terkait dengan kerentanan keamanan dan ketidakpastian proyek pengembangan. Manajemen risiko tidak diidentifikasi sebagai relevan dengan memperoleh solusi IT dan memberikan layanan IT.
1 - *Initial/ Ad Hoc*	Risiko TI dipertimbangkan secara ad hoc. Penilaian informal atas risiko proyek berlangsung sebagaimana ditentukan oleh setiap proyek. Risiko penilaian kadang-kadang diidentifikasi dalam rencana proyek tetapi jarang ditugaskan untuk manajer tertentu. Risiko spesifik terkait TI, seperti keamanan, ketersediaan, dan integritas, kadang-kadang dipertimbangkan berdasarkan proyek per proyek. Risiko terkait TI memengaruhi sehari-hari operasi jarang dibahas pada rapat manajemen. Di mana risiko telah dipertimbangkan, mitigasi tidak konsisten. Ada sebuah pemahaman yang muncul bahwa risiko IT penting dan perlu dipertimbangkan.
2 - *Repeatable but Intuitive*	Pendekatan penilaian risiko yang berkembang ada dan diimplementasikan atas kebijakan manajer proyek. Manajemen risiko adalah biasanya pada tingkat tinggi dan biasanya hanya diterapkan pada proyek-proyek besar atau sebagai respons terhadap masalah. Proses mitigasi risiko adalah mulai diterapkan di mana risiko diidentifikasi.
3 - *Defined*	Sebuah mendefinisikan kebijakan manajemen risiko organisationwide kapan dan bagaimana melakukan penilaian risiko. Manajemen risiko mengikuti proses didefinisikan yang didokumentasikan, pelatihan manajemen risiko tersedia untuk semua anggota staf. Keputusan untuk mengikuti risiko proses manajemen dan menerima pelatihan diserahkan kepada kebijaksanaan individu. Metodologi untuk penilaian risiko adalah meyakinkan dan suara dan memastikan bahwa risiko utama untuk bisnis diidentifikasi. Sebuah proses untuk mengurangi risiko kunci biasanya ditembagukan setelah risiko diidentifikasi. Deskripsi pekerjaan mempertimbangkan tanggung jawab manajemen risiko.
4 - *Managed and Measurable*	Penilaian dan manajemen risiko adalah prosedur standar. Pengecualian untuk proses manajemen risiko dilaporkan ke IT pengelolaan. Manajemen risiko TI adalah tanggung jawab manajemen tingkat senior. Risiko dinilai dan dimitigasi pada individu tingkat proyek dan juga secara teratur berkaitan dengan operasi TI secara keseluruhan. Manajemen disarankan untuk melakukan perubahan dalam bisnis dan TI lingkungan yang secara signifikan dapat mempengaruhi skenario risiko TI-terkait. Manajemen mampu memonitor posisi risiko dan membuat keputusan terinformasi mengenai pemaparan yang bersedia diterima. Semua risiko yang teridentifikasi memiliki pemilik yang ditunjuk, dan senior manajemen dan manajemen TI menentukan tingkat risiko bahwa organisasi akan mentolerir. Manajemen TI mengembangkan standar langkah-langkah untuk menilai risiko dan menentukan risiko / rasio pengembalian. Anggaran manajemen untuk proyek manajemen risiko operasional untuk menilai kembali risiko secara teratur. Database manajemen risiko dibuat, dan bagian dari proses manajemen risiko dimulai menjadi otomatis. Manajemen TI mempertimbangkan strategi mitigasi risiko.
5 - *Optimized*	Manajemen risiko berkembang ke tahap di mana proses terstruktur, organisasi secara luas ditegakkan dan dikelola dengan baik. Latihan yang baik diterapkan di seluruh organisasi. Pengambilan, analisis, dan pelaporan data manajemen risiko sangat otomatis. Berkolaborasi dimotori dari para pemimpin di lapangan, dan organisasi TI mengambil bagian dalam kelompok sebaya untuk bertukar pengalaman. Risiko manajemen benar-benar terintegrasi ke dalam semua operasi bisnis dan TI, diterima dengan baik dan secara ekstensif melibatkan para pengguna TI jasa. Manajemen mendeteksi dan bertindak ketika keputusan operasional dan investasi TI utama dibuat tanpa pertimbangan rencana manajemen risiko. Manajemen terus menilai strategi mitigasi risiko.

Nilai Keseluruhan Tingkat Kematangan Terendah:	0 (PO9.1)

5

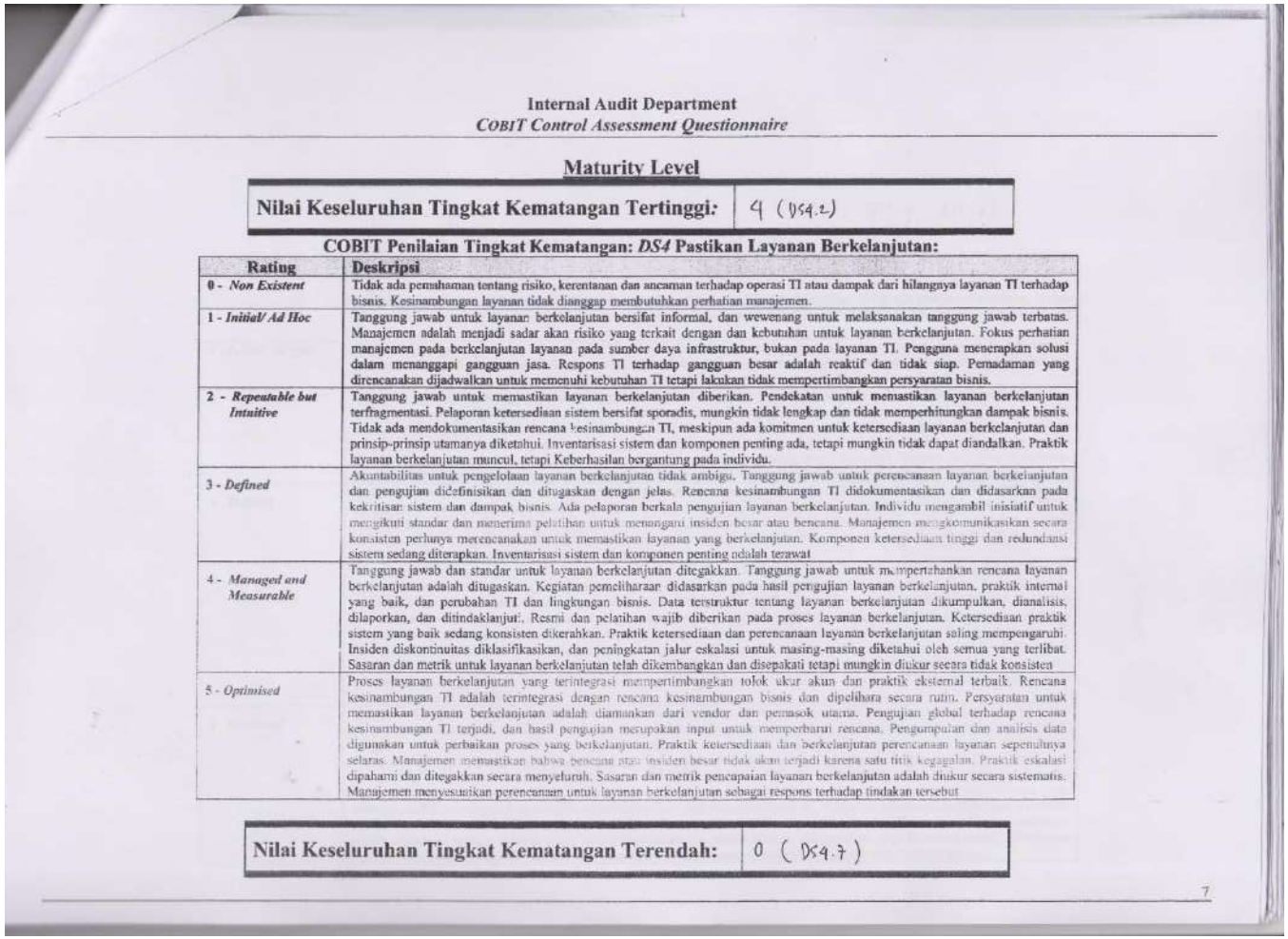
Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	4 (DS2.2, DS2.3)

COBIT Penilaian Tingkat Kematangan: *DS2* Kelola Layanan Pihak Ketiga:

Rating	Deskripsi
0 - *Non Existent*	Tanggung jawab dan akuntabilitas tidak ditentukan. Tidak ada kebijakan dan prosedur formal mengenai kontrak dengan pihak ketiga. Layanan pihak ketiga tidak disetujui atau ditinjau oleh manajemen. Tidak ada kegiatan pengukuran dan tidak pelaporan oleh pihak ketiga. Dengan tidak adanya kewajiban kontrak untuk pelaporan, manajemen senior tidak menyadari kualitas layanan yang diberikan.
1 - *Initial/ Ad Hoc*	Manajemen menyadari perlunya mendokumentasikan kebijakan dan prosedur untuk manajemen pihak ketiga, termasuk yang ditandatangani kontrak. Tidak ada ketentuan perjanjian standar dengan penyedia layanan. Pengukuran layanan yang diberikan bersifat informal dan reaktif. Praktik bergantung pada pengalaman (mis., Berdasarkan permintaan) individu dan pemasok.
2 - *Repeatable but Intuitive*	Proses untuk mengawasi penyedia layanan pihak ketiga, risiko yang terkait, dan pemberian layanan bersifat informal. Yang ditandatangani, kontrak pro forma digunakan dengan syarat dan ketentuan vendor standar (mis., deskripsi layanan yang akan diberikan). Laporan aktif layanan yang disediakan tersedia, tetapi tidak mendukung tujuan bisnis.
3 - *Defined*	Prosedur yang terdokumentasi dengan baik tersedia untuk mengatur layanan pihak ketiga, dengan proses yang jelas untuk pemeriksaan dan negosiasi dengan vendor. Ketika perjanjian untuk penyediaan layanan dibuat, hubungan dengan pihak ketiga adalah murni kontrak. Sifat layanan yang akan diberikan dirinci dalam kontrak dan mencakup persyaratan hukum, operasional, dan kontrol. Itu tanggung jawab untuk mengawasi layanan pihak ketiga ditugaskan. Ketentuan kontrak didasarkan pada templat terstandarisasi. Bisnis risiko yang terkait dengan layanan pihak ketiga dinilai dan dilaporkan
4 - *Managed and Measurable*	Kriteria formal dan standar ditetapkan untuk mendefinisikan persyaratan keterlibatan, termasuk ruang lingkup pekerjaan, layanan / hasil yang harus disediakan, asumsi, jadwal, biaya, pengaturan dan tanggung jawab penagihan. Tanggung jawab untuk manajemen kontrak dan vendor ditugaskan. Kualifikasi, risiko, dan kemampuan vendor diverifikasi secara berkelanjutan. Layanan persyaratan didefinisikan dan dikaitkan dengan tujuan bisnis. Ada proses untuk meninjau kinerja layanan terhadap kontrak persyaratan, memberikan input untuk menilai layanan pihak ketiga saat ini dan masa depan. Model penentuan harga transfer digunakan dalam proses pengadaan. Semua pihak yang terlibat mengetahui layanan, biaya, dan harapan pencapaian. Sasaran dan metrik yang disepakati untuk pengawasan penyedia layanan ada.
5 - *Optimised*	Kontrak yang ditandatangani dengan pihak ketiga ditinjau secara berkala dengan interval yang telah ditentukan. Tanggung jawab untuk mengelola pemasok dan kualitas layanan yang diberikan ditetapkan. Bukti kepatuhan kontrak terhadap ketentuan operasional, hukum, dan kontrol adalah dipantau, dan tindakan korektif ditegakkan. Pihak ketiga tunduk pada tinjauan berkala independen, dan umpan balik tentang kinerja disediakan dan digunakan untuk meningkatkan pemberian layanan. Pengukuran bervariasi dalam menanggapi perubahan kondisi bisnis. Tindakan mendukung deteksi dini masalah potensial dengan layanan pihak ketiga. Pelaporan pencapaian tingkat layanan yang komprehensif dan didefinisikan adalahterkait dengan kompensasi pihak ketiga. Manajemen menyesuaikan proses perolehan dan pemantauan layanan pihak ketiga berdasarkan pengukur.

Nilai Keseluruhan Tingkat Kematangan Terendah:	2 (DS2.1)



Internal Audit Department
COBIT Control Assessment Questionnaire

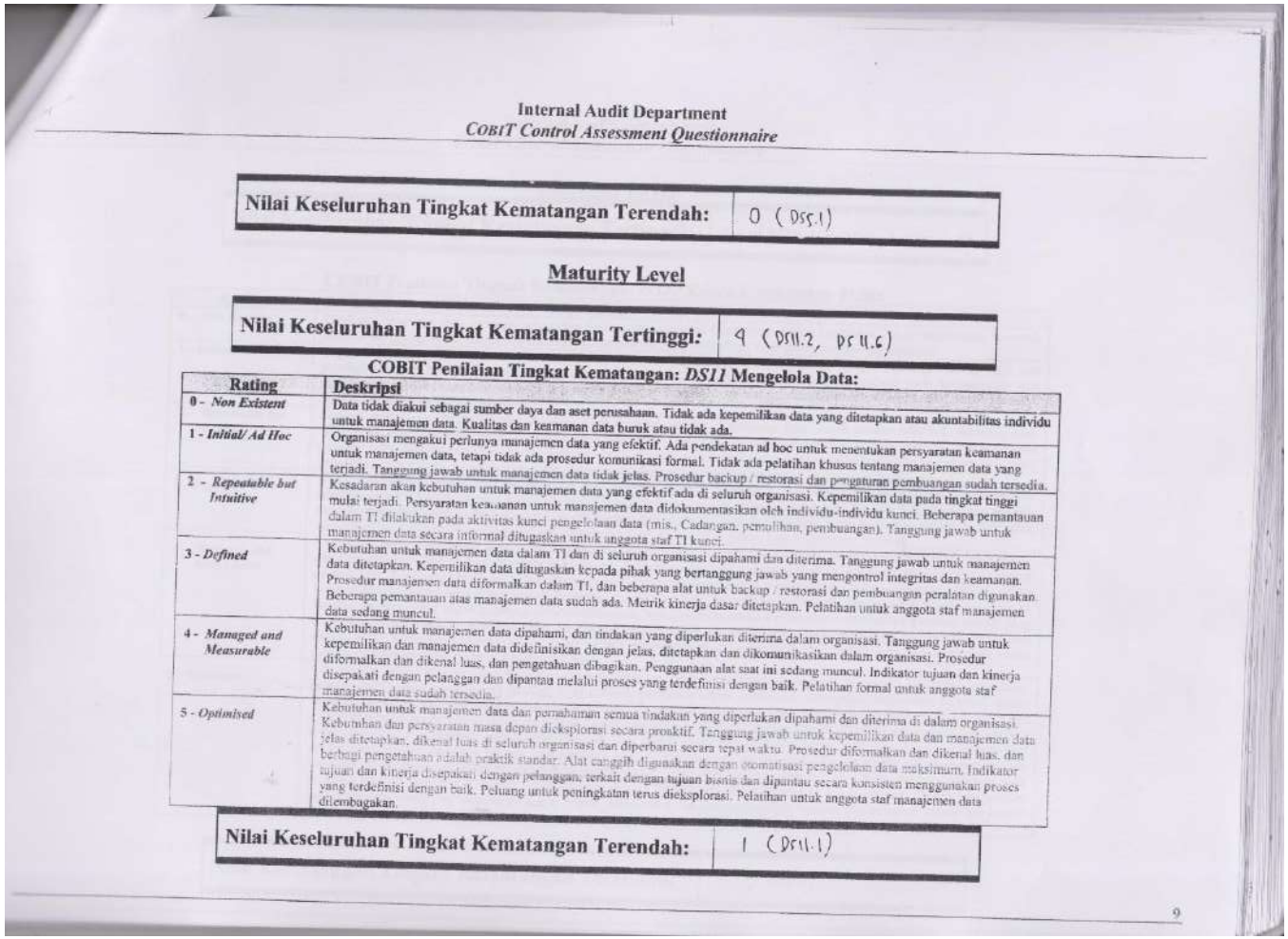
Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	4 (DS4.2)

COBIT Penilaian Tingkat Kematangan: *DS4* Pastikan Layanan Berkelanjutan:

Rating	Deskripsi
0 - *Non Existent*	Tidak ada pemahaman tentang risiko, kerentanan dan ancaman terhadap operasi TI atau dampak dari hilangnya layanan TI terhadap bisnis. Kesinambungan layanan tidak dianggap membutuhkan perhatian manajemen.
1 - *Initial/ Ad Hoc*	Tanggung jawab untuk layanan berkelanjutan bersifat informal, dan wewenang untuk melaksanakan tanggung jawab terbatas. Manajemen adalah menjadi sadar akan risiko yang terkait dengan dan kebutuhan untuk layanan berkelanjutan. Fokus perhatian manajemen pada berkelanjutan layanan pada sumber daya infrastruktur, bukan pada layanan TI. Pengguna menerapkan solusi dalam menanggapi gangguan jasa. Respons TI terhadap gangguan besar adalah reaktif dan tidak siap. Pemadaman yang direncanakan dijadwalkan untuk memenuhi kebutuhan TI tetapi lakukan tidak mempertimbangkan persyaratan bisnis.
2 - *Repeatable but Intuitive*	Tanggung jawab untuk memastikan layanan berkelanjutan diberikan. Pendekatan untuk memastikan layanan berkelanjutan terfragmentasi. Pelaporan ketersediaan sistem bersifat sporadis, mungkin tidak lengkap dan tidak memperhitungkan dampak bisnis. Tidak ada mendokumentasikan rencana kesinambungan TI, meskipun ada komitmen untuk ketersediaan layanan berkelanjutan dan prinsip-prinsip utamanya diketahui. Inventarisasi sistem dan komponen penting ada, tetapi mungkin tidak dapat diandalkan. Praktik layanan berkelanjutan muncul, tetapi Keberhasilan bergantung pada individu.
3 - *Defined*	Akuntabilitas untuk pengelolaan layanan berkelanjutan tidak ambigu. Tanggung jawab untuk perencanaan layanan berkelanjutan dan pengujian didefinisikan dan ditugaskan dengan jelas. Rencana kesinambungan TI didokumentasikan dan didasarkan pada kekritisan sistem dan dampak bisnis. Ada pelaporan berkala pengujian layanan berkelanjutan. Individu mengambil inisiatif untuk mengikuti standar dan menerima pelatihan untuk menangani insiden besar atau bencana. Manajemen mengkomunikasikan secara konsisten perlunya merencanakan untuk memastikan layanan yang berkelanjutan. Komponen ketersediaan tinggi dan redundansi sistem sedang diterapkan. Inventarisasi sistem dan komponen penting adalah terawat
4 - *Managed and Measurable*	Tanggung jawab dan standar untuk layanan berkelanjutan ditegakkan. Tanggung jawab untuk mempertahankan rencana layanan berkelanjutan adalah ditugaskan. Kegiatan pemeliharaan didasarkan pada hasil pengujian layanan berkelanjutan, praktik internal yang baik, dan perubahan TI dan lingkungan bisnis. Data terstruktur tentang layanan berkelanjutan dikumpulkan, dianalisis, dilaporkan, dan ditindaklanjuti. Resmi dan pelatihan wajib diberikan pada proses layanan berkelanjutan. Ketersediaan praktik sistem yang baik sedang konsisten dikerahkan. Praktik ketersediaan dan perencanaan layanan berkelanjutan saling mempengaruhi. Insiden diskontinuitas diklasifikasikan, dan peningkatan jalur eskalasi untuk masing-masing diketahui oleh semua yang terlibat. Sasaran dan metrik untuk layanan berkelanjutan telah dikembangkan dan disepakati tetapi mungkin diukur secara tidak konsisten
5 - *Optimised*	Proses layanan berkelanjutan yang terintegrasi mempertimbangkan tolok ukur akun dan praktik eksternal terbaik. Rencana kesinambungan TI adalah terintegrasi dengan rencana kesinambungan bisnis dan dipelihara secara rutin. Persyaratan untuk memastikan layanan berkelanjutan adalah diamankan dari vendor dan pemasok utama. Pengujian global terhadap rencana kesinambungan TI terjadi, dan hasil pengujian merupakan input untuk memperbarui rencana. Pengumpulan dan analisis data digunakan untuk perbaikan proses yang berkelanjutan. Praktik ketersediaan dan berkelanjutan perencanaan layanan sepenuhnya selaras. Manajemen memastikan bahwa rencana atau insiden besar tidak akan terjadi karena satu titik kegagalan. Praktik eskalasi dipahami dan ditegakkan secara menyeluruh. Sasaran dan metrik pencapaian layanan berkelanjutan adalah diukur secara sistematis. Manajemen menyesuaikan perencanaan untuk layanan berkelanjutan sebagai respons terhadap tindakan tersebut

Nilai Keseluruhan Tingkat Kematangan Terendah:	0 (DS4.7)



Internal Audit Department
COBIT Control Assessment Questionnaire

Nilai Keseluruhan Tingkat Kematangan Terendah:	0 (DS5.1)

Maturity Level

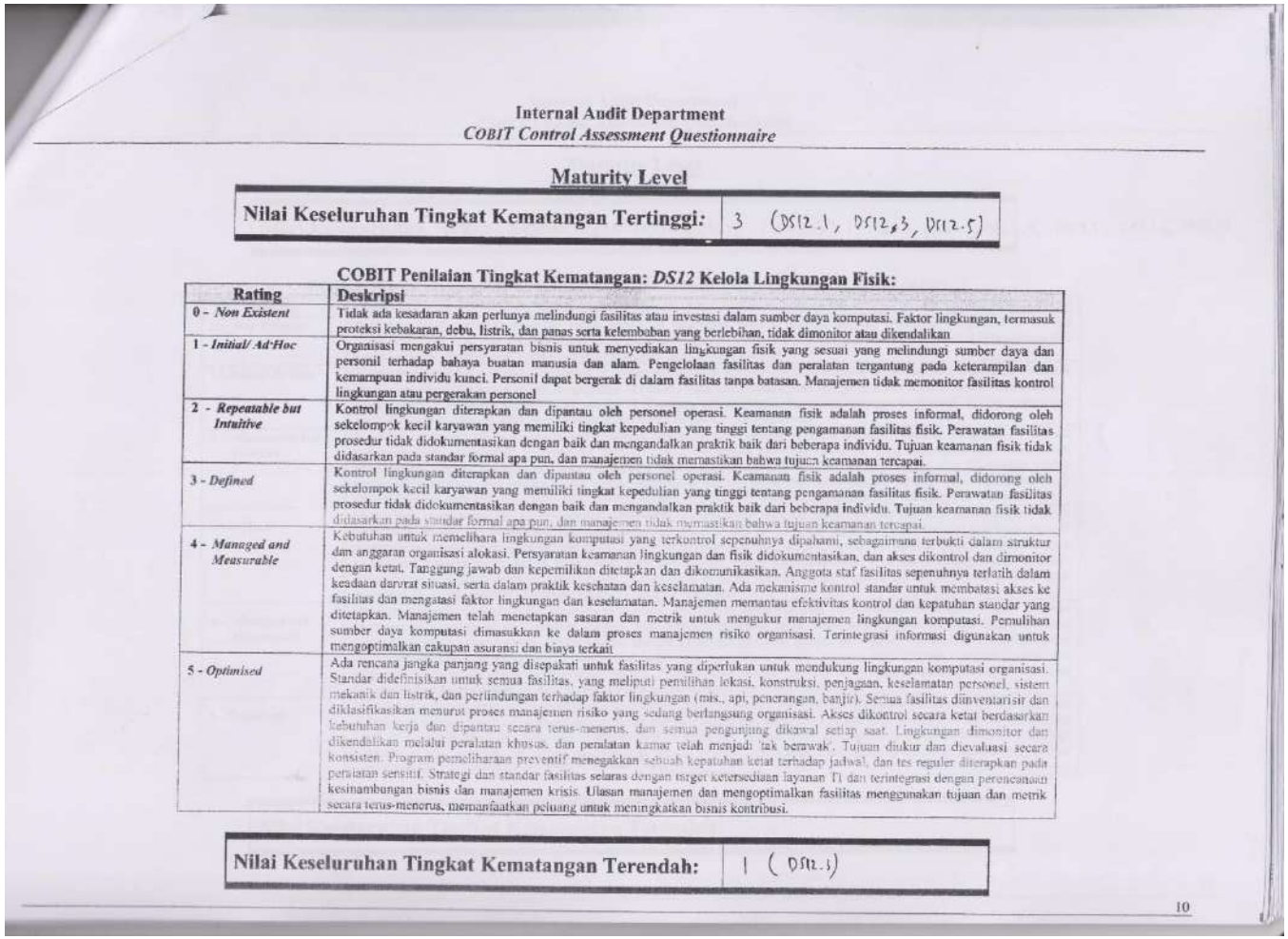
Nilai Keseluruhan Tingkat Kematangan Tertinggi:	9 (DS11.2, DS11.6)

COBIT Penilaian Tingkat Kematangan: *DS11* Mengelola Data:

Rating	Deskripsi
0 - *Non Existent*	Data tidak diakui sebagai sumber daya dan aset perusahaan. Tidak ada kepemilikan data yang ditetapkan atau akuntabilitas individu untuk manajemen data. Kualitas dan keamanan data buruk atau tidak ada.
1 - *Initial/ Ad Hoc*	Organisasi mengakui perlunya manajemen data yang efektif. Ada pendekatan ad hoc untuk menentukan persyaratan keamanan untuk manajemen data, tetapi tidak ada prosedur komunikasi formal. Tidak ada pelatihan khusus tentang manajemen data yang terjadi. Tanggung jawab untuk manajemen data tidak jelas. Prosedur backup / restorasi dan pengaturan pembuangan sudah tersedia.
2 - *Repeatable but Intuitive*	Kesadaran akan kebutuhan untuk manajemen data yang efektif ada di seluruh organisasi. Kepemilikan data pada tingkat tinggi mulai terjadi. Persyaratan keamanan untuk manajemen data didokumentasikan oleh individu-individu kunci. Beberapa pemantauan dalam TI dilakukan pada aktivitas kunci pengelolaan data (mis., Cadangan, pemulihan, pembuangan). Tanggung jawab untuk manajemen data secara informal ditugaskan untuk anggota staf TI kunci.
3 - *Defined*	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.
4 - *Managed and Measurable*	Kebutuhan untuk manajemen data dipahami, dan tindakan yang diperlukan diterima dalam organisasi. Tanggung jawab untuk kepemilikan dan manajemen data didefinisikan dengan jelas, ditetapkan dan dikomunikasikan dalam organisasi. Prosedur diformalkan dan dikenal luas, dan pengetahuan dibagikan. Penggunaan alat saat ini sedang muncul. Indikator tujuan dan kinerja disepakati dengan pelanggan dan dipantau melalui proses yang terdefinisi dengan baik. Pelatihan formal untuk anggota staf manajemen data sudah tersedia.
5 - *Optimized*	Kebutuhan untuk manajemen data dan pemahaman semua tindakan yang diperlukan dipahami dan diterima di dalam organisasi. Kebutuhan dan persyaratan masa depan dieksplorasi secara proaktif. Tanggung jawab untuk kepemilikan data dan manajemen data jelas ditetapkan, dikenal luas di seluruh organisasi dan diperbarui secara tepat waktu. Prosedur diformalkan dan dikenal luas, dan berbagi pengetahuan adalah praktik standar. Alat canggih digunakan dengan otomatisasi pengelolaan data maksimum. Indikator tujuan dan kinerja disepakati dengan pelanggan, terkait dengan tujuan bisnis dan dipantau secara konsisten menggunakan proses yang terdefinisi dengan baik. Peluang untuk peningkatan terus dieksplorasi. Pelatihan untuk anggota staf manajemen data dilembagakan.

Nilai Keseluruhan Tingkat Kematangan Terendah:	1 (DS11.1)

9



Internal Audit Department
COBIT Control Assessment Questionnaire

Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	3 (DS12.1, DS12.3, DS12.5)

COBIT Penilaian Tingkat Kematangan: *DS12* Kelola Lingkungan Fisik:

Rating	Deskripsi
0 - *Non Existent*	Tidak ada kesadaran akan perlunya melindungi fasilitas atau investasi dalam sumber daya komputasi. Faktor lingkungan, termasuk proteksi kebakaran, debu, listrik, dan panas serta kelembaban yang berlebihan, tidak dimonitor atau dikendalikan
1 - *Initial/ Ad Hoc*	Organisasi mengakui persyaratan bisnis untuk menyediakan lingkungan fisik yang sesuai yang melindungi sumber daya dan personil terhadap bahaya buatan manusia dan alam. Pengelolaan fasilitas dan peralatan tergantung pada keterampilan dan kemampuan individu kunci. Personil dapat bergerak di dalam fasilitas tanpa batasan. Manajemen tidak memonitor fasilitas kontrol lingkungan atau pergerakan personel
2 - *Repeatable but Intuitive*	Kontrol lingkungan diterapkan dan dipantau oleh personel operasi. Keamanan fisik adalah proses informal, didorong oleh sekelompok kecil karyawan yang memiliki tingkat kepedulian yang tinggi tentang pengamanan fasilitas fisik. Perawatan fasilitas prosedur tidak didokumentasikan dengan baik dan mengandalkan praktik baik dari beberapa individu. Tujuan keamanan fisik tidak didasarkan pada standar formal apa pun, dan manajemen tidak memastikan bahwa tujuan keamanan tercapai.
3 - *Defined*	Kontrol lingkungan diterapkan dan dipantau oleh personel operasi. Keamanan fisik adalah proses informal, didorong oleh sekelompok kecil karyawan yang memiliki tingkat kepedulian yang tinggi tentang pengamanan fasilitas fisik. Perawatan fasilitas prosedur tidak didokumentasikan dengan baik dan mengandalkan praktik baik dari beberapa individu. Tujuan keamanan fisik tidak didasarkan pada standar formal apa pun, dan manajemen tidak memastikan bahwa tujuan keamanan tercapai.
4 - *Managed and Measurable*	Kebutuhan untuk memelihara lingkungan komputasi yang terkontrol sepenuhnya dipahami, sebagaimana terbukti dalam struktur dan anggaran organisasi alokasi. Persyaratan keamanan lingkungan dan fisik didokumentasikan, dan akses dikontrol dan dimonitor dengan ketat. Tanggung jawab dan kepemilikan ditetapkan dan dikomunikasikan. Anggota staf fasilitas sepenuhnya terlatih dalam keadaan darurat situasi, serta dalam praktik kesehatan dan keselamatan. Ada mekanisme kontrol standar untuk membatasi akses ke fasilitas dan mengatasi faktor lingkungan dan keselamatan. Manajemen memantau efektivitas kontrol dan kepatuhan standar yang ditetapkan. Manajemen telah menetapkan sasaran dan metrik untuk mengukur manajemen lingkungan komputasi. Pemulihan sumber daya komputasi dimasukkan ke dalam proses manajemen risiko organisasi. Terintegrasi informasi digunakan untuk mengoptimalkan cakupan asuransi dan biaya terkait
5 - *Optimised*	Ada rencana jangka panjang yang disepakati untuk fasilitas yang diperlukan untuk mendukung lingkungan komputasi organisasi. Standar didefinisikan untuk semua fasilitas, yang meliputi pemilihan lokasi, konstruksi, penjagaan, keselamatan personel, sistem mekanik dan listrik, dan perlindungan terhadap faktor lingkungan (mis., api, penerangan, banjir). Semua fasilitas diinventarisir dan diklasifikasikan menurut proses manajemen risiko yang sedang berlangsung organisasi. Akses dikontrol secara ketat berdasarkan kebutuhan kerja dan dipantau secara terus-menerus, dan semua pengunjung dikawal setiap saat. Lingkungan dimonitor dan dikendalikan melalui peralatan khusus, dan peralatan kamar telah menjadi 'tak berawak'. Tujuan diukur dan dievaluasi secara konsisten. Program pemeliharaan preventif menegakkan sebuah kepatuhan ketat terhadap jadwal, dan tes reguler diterapkan pada peralatan sensitif. Strategi dan standar fasilitas selaras dengan target ketersediaan layanan TI dan terintegrasi dengan perencanaan kesinambungan bisnis dan manajemen krisis. Ulasan manajemen dan mengoptimalkan fasilitas menggunakan tujuan dan metrik secara terus-menerus, memanfaatkan peluang untuk meningkatkan bisnis kontribusi.

Nilai Keseluruhan Tingkat Kematangan Terendah:	1 (DS12.3)

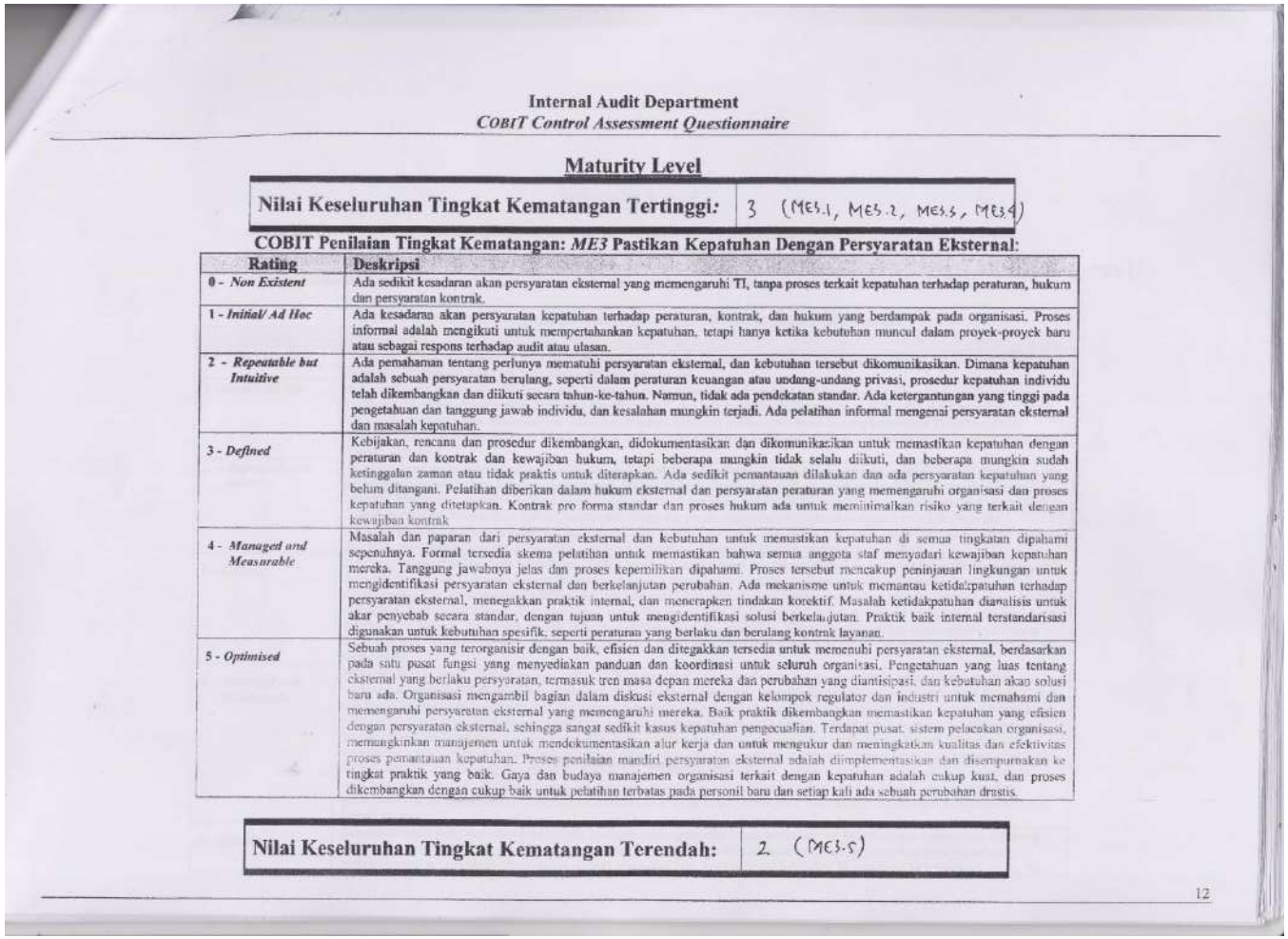
Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	3 (ME2.1, ME2.2, ME2.3, ME2.4, ME2.5, ME2.6, ME2.7)

COBIT Penilaian Tingkat Kematangan: *ME2* Monitor dan Evaluasi Kontrol Internal:

Rating	Deskripsi
0 - *Non Existent*	Organisasi tidak memiliki prosedur untuk memantau efektivitas kontrol internal. Metode pelaporan pengendalian internal manajemen tidak ada. Ada ketidaksadaran umum tentang keamanan operasional TI dan jaminan kontrol internal. Manajemen dan karyawan secara keseluruhan kurang memiliki kesadaran akan kontrol internal.
1 - *Initial/ Ad Hoc*	Manajemen mengakui perlunya manajemen TI reguler dan jaminan kontrol. Keahlian individu dalam menilai pengendalian internal kecukupan diterapkan secara ad hoc. Manajemen TI belum secara resmi menetapkan tanggung jawab untuk memantau keefektifan kontrol internal. Penilaian pengendalian internal TI dilakukan sebagai bagian dari audit keuangan tradisional, dengan metodologi dan keterampilan set yang tidak mencerminkan kebutuhan fungsi layanan informasi.
2 - *Repeatable but Intuitive*	Rumah sakit menggunakan laporan kontrol informal untuk memulai insiatif tindakan korektif. Penilaian pengendalian internal tergantung pada seperangkat keterampilan individu kunci. Organisasi memiliki kesadaran yang meningkat akan pemantauan pengendalian internal. Layanan informasi manajemen melakukan pemantauan atas keefektifan dari apa yang diyakininya adalah pengendalian internal yang penting secara teratur. Metodologi dan alat untuk memonitor kontrol internal mulai digunakan, tetapi tidak didasarkan pada rencana. Faktor risiko khusus untuk Lingkungan TI diidentifikasi berdasarkan keterampilan individu.
3 - *Defined*	Manajemen mendukung dan melembagakan pengawasan pengendalian internal. Kebijakan dan prosedur dikembangkan untuk menilai dan melaporkan tentang kegiatan pemantauan pengendalian internal. Program pendidikan dan pelatihan untuk pemantauan pengendalian internal ditentukan. Sebuah proses didefinisikan untuk penilaian sendiri dan tinjauan jaminan kontrol internal, dengan peran untuk manajer bisnis dan TI yang bertanggung jawab. Alat sedang digunakan tetapi tidak harus diintegrasikan ke dalam semua proses. Kebijakan penilaian risiko proses TI digunakan di dalam kerangka kerja kontrol yang dikembangkan khusus untuk organisasi TI. Risiko spesifik proses dan kebijakan mitigasi ditentukan.
4 - *Managed and Measurable*	Manajemen mengimplementasikan kerangka kerja untuk pemantauan kontrol internal TI. Organisasi menetapkan tingkat toleransi untuk proses pemantauan pengendalian internal. Alat diimplementasikan untuk menstandarkan penilaian dan secara otomatis mendeteksi pengecualian kontrol. Fungsi kontrol internal TI formal dibentuk, dengan profesional khusus dan bersertifikat yang memanfaatkan kerangka kerja kontrol formal didukung oleh manajemen senior. Anggota staf TI yang terampil secara rutin berpartisipasi dalam penilaian pengendalian internal. Metrik basis pengetahuan untuk informasi historis tentang pemantauan pengendalian internal ditetapkan. Peer review untuk pemantauan kontrol internal didirikan.
5 - *Optimized*	Manajemen menetapkan program peningkatan berkesinambungan organisasi yang memperhitungkan pelajaran yang dipelajari dan praktik baik industri untuk pemantauan pengendalian internal. Organisasi menggunakan alat yang terintegrasi dan diperbarui, jika perlu, itu memungkinkan penilaian efektif dari kontrol TI kritis dan deteksi cepat dari insiden pemantauan kontrol TI. Berbagi pengetahuan khusus untuk fungsi layanan informasi secara formal dilaksanakan. Benchmarking terhadap standar industri dan praktik yang baik diformalkan.

Nilai Keseluruhan Tingkat Kematangan Terendah:	–



Internal Audit Department
COBIT Control Assessment Questionnaire

Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	3 (ME5.1, ME5.2, ME5.3, ME5.4)

COBIT Penilaian Tingkat Kematangan: *ME3* Pastikan Kepatuhan Dengan Persyaratan Eksternal:

Rating	Deskripsi
0 - *Non Existent*	Ada sedikit kesadaran akan persyaratan eksternal yang memengaruhi TI, tanpa proses terkait kepatuhan terhadap peraturan, hukum dan persyaratan kontrak.
1 - *Initial/ Ad Hoc*	Ada kesadaran akan persyaratan kepatuhan terhadap peraturan, kontrak, dan hukum yang berdampak pada organisasi. Proses informal adalah mengikuti untuk mempertahankan kepatuhan, tetapi hanya ketika kebutuhan muncul dalam proyek-proyek baru atau sebagai respons terhadap audit atau ulasan.
2 - *Repeatable but Intuitive*	Ada pemahaman tentang perlunya mematuhi persyaratan eksternal, dan kebutuhan tersebut dikomunikasikan. Dimana kepatuhan adalah sebuah persyaratan berulang, seperti dalam peraturan keuangan atau undang-undang privasi, prosedur kepatuhan individu telah dikembangkan dan diikuti secara tahun-ke-tahun. Namun, tidak ada pendekatan standar. Ada ketergantungan yang tinggi pada pengetahuan dan tanggung jawab individu, dan kesalahan mungkin terjadi. Ada pelatihan informal mengenai persyaratan eksternal dan masalah kepatuhan.
3 - *Defined*	Kebijakan, rencana dan prosedur dikembangkan, didokumentasikan dan dikomunikasikan untuk memastikan kepatuhan dengan peraturan dan kontrak dan kewajiban hukum, tetapi beberapa mungkin tidak selalu diikuti, dan beberapa mungkin sudah ketinggalan zaman atau tidak praktis untuk diterapkan. Ada sedikit pemantauan dilakukan dan ada persyaratan kepatuhan yang belum ditangani. Pelatihan diberikan dalam hukum eksternal dan persyaratan peraturan yang memengaruhi organisasi dan proses kepatuhan yang ditetapkan. Kontrak pro forma standar dan proses hukum ada untuk meminimalkan risiko yang terkait dengan kewajiban kontrak
4 - *Managed and Measurable*	Masalah dan paparan dari persyaratan eksternal dan kebutuhan untuk memastikan kepatuhan di semua tingkatan dipahami sepenuhnya. Formal tersedia skema pelatihan untuk memastikan bahwa semua anggota staf menyadari kewajiban kepatuhan mereka. Tanggung jawabnya jelas dan proses kepemilikan dipahami. Proses tersebut mencakup peninjauan lingkungan untuk mengidentifikasi persyaratan eksternal dan berkelanjutan perubahan. Ada mekanisme untuk memantau ketidakpatuhan terhadap persyaratan eksternal, menegakkan praktik internal, dan menerapkan tindakan korektif. Masalah ketidakpatuhan dianalisis untuk akar penyebab secara standar, dengan tujuan untuk mengidentifikasi solusi berkelanjutan. Praktik baik internal terstandarisasi digunakan untuk kebutuhan spesifik, seperti peraturan yang berlaku dan berulang kontrak layanan.
5 - *Optimised*	Sebuah proses yang terorganisir dengan baik, efisien dan ditegakkan tersedia untuk memenuhi persyaratan eksternal, berdasarkan pada satu pusat fungsi yang menyediakan panduan dan koordinasi untuk seluruh organisasi. Pengetahuan yang luas tentang eksternal yang berlaku persyaratan, termasuk tren masa depan mereka dan perubahan yang diantisipasi, dan kebutuhan akan solusi baru ada. Organisasi mengambil bagian dalam diskusi eksternal dengan kelompok regulator dan industri untuk memahami dan memengaruhi persyaratan eksternal yang memengaruhi mereka. Baik praktik dikembangkan memastikan kepatuhan yang efisien dengan persyaratan eksternal, sehingga sangat sedikit kasus kepatuhan pengecualian. Terdapat pusat, sistem pelacakan organisasi, memungkinkan manajemen untuk mendokumentasikan alur kerja dan untuk mengukur dan meningkatkan kualitas dan efektivitas proses pemantauan kepatuhan. Proses penilaian mandiri persyaratan eksternal adalah diimplementasikan dan disempurnakan ke tingkat praktik yang baik. Gaya dan budaya manajemen organisasi terkait dengan kepatuhan adalah cukup kuat, dan proses dikembangkan dengan cukup baik untuk pelatihan terbatas pada personil baru dan setiap kali ada sebuah perubahan drastis.

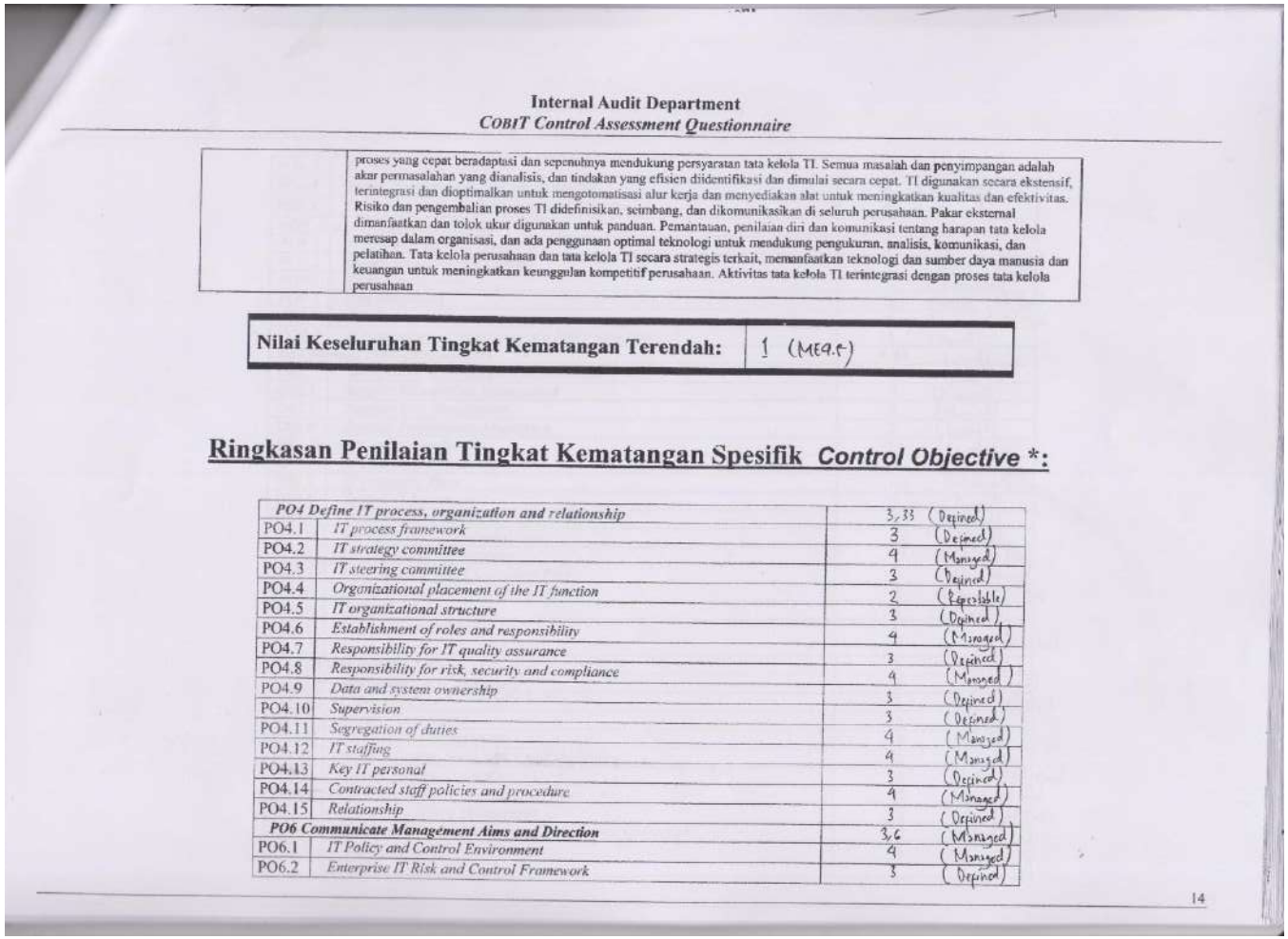
Nilai Keseluruhan Tingkat Kematangan Terendah:	2 (ME3.5)

Maturity Level

Nilai Keseluruhan Tingkat Kematangan Tertinggi:	3 (ME9.1, ME9.2, ME9.3, ME9.4, ME9.6, ME9.7)

COBIT Penilaian Tingkat Kematangan: *ME4* Menentukan Tata Kelola :

Rating	Deskripsi
0 - *Non Existent*	Tidak ada proses tata kelola TI yang dapat dikenali sepenuhnya. Organisasi bahkan tidak mengakui bahwa ada masalah yang harus ditangani; karenanya, tidak ada komunikasi tentang masalah ini.
1 - *Initial/ Ad Hoc*	Ada pengakuan bahwa masalah tata kelola TI ada dan perlu ditangani. Ada pendekatan ad hoc yang diterapkan secara individu atau per kasus per kasus. Pendekatan manajemen bersifat reaktif, dan hanya ada komunikasi yang sporadis dan tidak konsisten tentang isu dan pendekatan untuk mengatasinya. Manajemen hanya memiliki indikasi perkiraan tentang bagaimana TI berkontribusi terhadap kinerja bisnis.Manajemen hanya bereaksi secara reaktif terhadap insiden yang telah menyebabkan kerugian atau rasa malu kepada organisasi.
2 - *Repeatable but Intuitive*	Ada kesadaran masalah tata kelola TI. Aktivitas tata kelola TI dan indikator kinerja, yang meliputi perencanaan TI, pengiriman dan proses pemantauan, sedang dalam pengembangan. Proses TI yang dipilih diidentifikasi untuk peningkatan berdasarkan keputusan individu. Manajemen mengidentifikasi pengukuran dan teknik penilaian tata kelola TI dasar. Namun, prosesnya tidak diadopsi di seluruh organisasi. Komunikasi tentang standar dan tanggung jawab pemerintahan diserahkan kepada individu. Individu mendorong proses tata kelola dalam berbagai proyek dan proses TI. Proses, alat, dan metrik untuk mengukur tata kelola TI terbatas dan tidak dapat digunakan untuk kapasitas penuh mereka karena kurangnya keahlian dalam fungsi mereka.
3 - *Defined*	Pentingnya dan 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.
4 - *Managed and Measurable*	Ada pemahaman penuh tentang isu tata kelola TI di semua level. Ada pemahaman yang jelas tentang siapa pelanggan, dan tanggung jawab ditentukan dan dipantau melalui SLA. Tanggung jawabnya jelas dan kepemilikan proses ditetapkan. Proses TI dan tata kelola TI diselaraskan dengan dan diintegrasikan ke dalam bisnis dan strategi TI. Peningkatan proses TI terutama didasarkan pada pemahaman kuantitatif, dan dimungkinkan untuk memantau dan mengukur kepatuhan dengan prosedur dan metrik proses. Semua pemangku kepentingan proses sadar akan risiko, pentingnya TI dan peluang yang dapat ditawarkannya. Manajemen mendefinisikan toleransi di mana proses harus beroperasi. Ada terbatas, terutama taktis, penggunaan teknologi, berdasarkan teknik matang dan alat standar yang diberlakukan. Tata kelola TI telah diintegrasikan ke dalam perencanaan strategis dan operasional serta proses pemantauan. Indikator kinerja atas semua kegiatan tata kelola TI sedang direkam dan dilacak, yang mengarah ke peningkatan perbaikan di awal. Akuntabilitas keseluruhan kinerja proses kunci jelas, dan manajemen dihargai berdasarkan ukuran kinerja utama.
5 - *Optimised*	Ada pemahaman yang maju dan berwawasan ke depan tentang isu dan solusi tata kelola TI. Pelatihan dan komunikasi didukung oleh konsep dan teknik terdepan. Proses disempurnakan ke tingkat praktik industri yang baik, berdasarkan hasil perbaikan berkelanjutan dan pemodelan kematangan dengan organisasi lain. Implementasi kebijakan TI mengarah ke organisasi, orang, dan



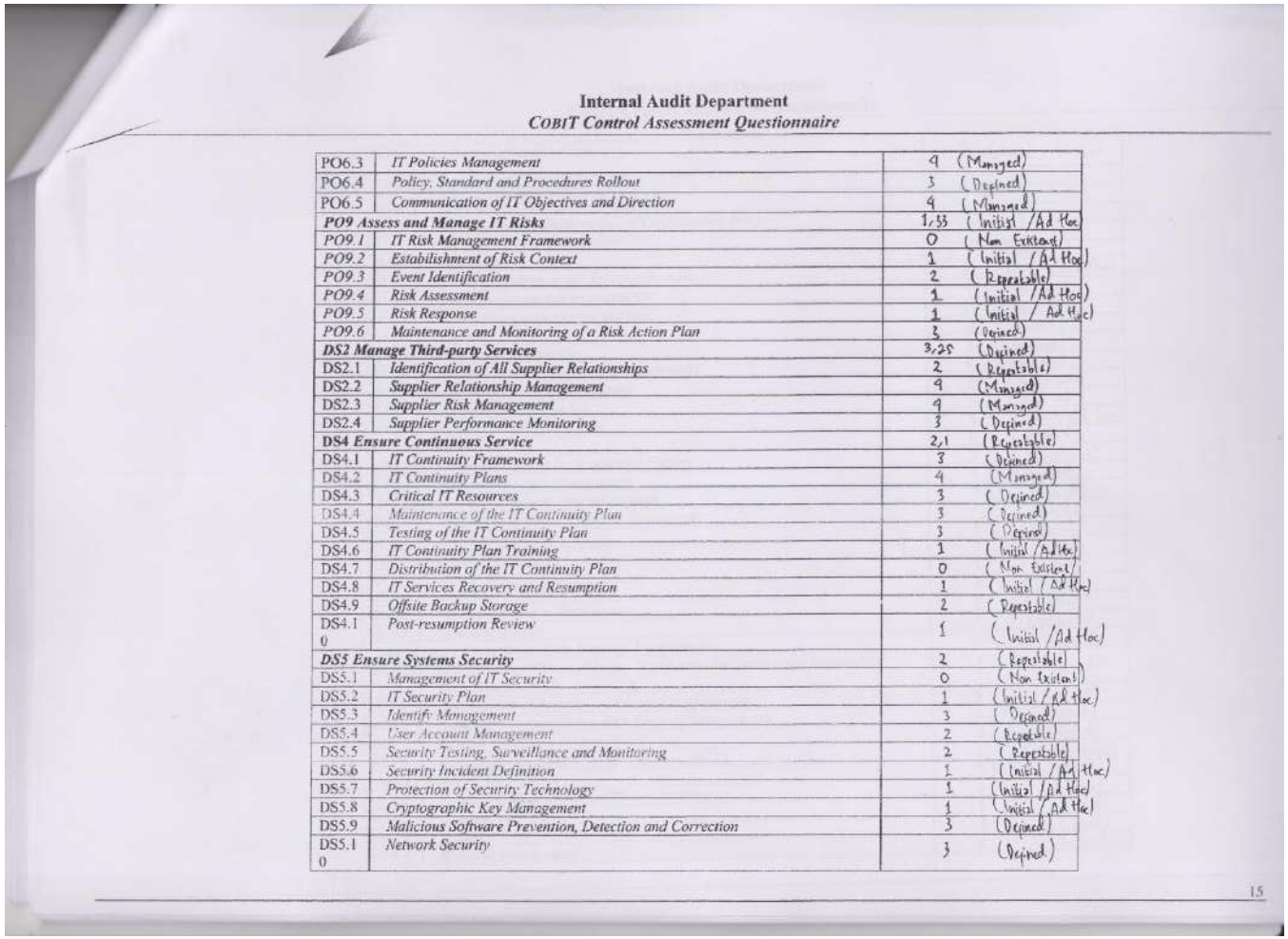
Internal Audit Department
COBIT Control Assessment Questionnaire

	proses yang cepat beradaptasi dan sepenuhnya mendukung persyaratan tata kelola TI. Semua masalah dan penyimpangan adalah akar permasalahan yang dianalisis, dan tindakan yang efisien diidentifikasi dan dimulai secara cepat. TI digunakan secara ekstensif, terintegrasi dan dioptimalkan untuk mengotomatisasi alur kerja dan menyediakan alat untuk meningkatkan kualitas dan efektivitas. Risiko dan pengembalian proses TI didefinisikan, scimbang, dan dikomunikasikan di seluruh perusahaan. Pakar eksternal dimanfaatkan dan tolok ukur digunakan untuk panduan. Pemantauan, penilaian diri dan komunikasi tentang harapan tata kelola meresap dalam organisasi, dan ada penggunaan optimal teknologi untuk mendukung pengukuran, analisis, komunikasi, dan pelatihan. Tata kelola perusahaan dan tata kelola TI secara strategis terkait, memanfaatkan teknologi dan sumber daya manusia dan keuangan untuk meningkatkan keunggulan kompetitif perusahaan. Aktivitas tata kelola TI terintegrasi dengan proses tata kelola perusahaan

Nilai Keseluruhan Tingkat Kematangan Terendah:	1 (ME9.5)

Ringkasan Penilaian Tingkat Kematangan Spesifik *Control Objective* *:

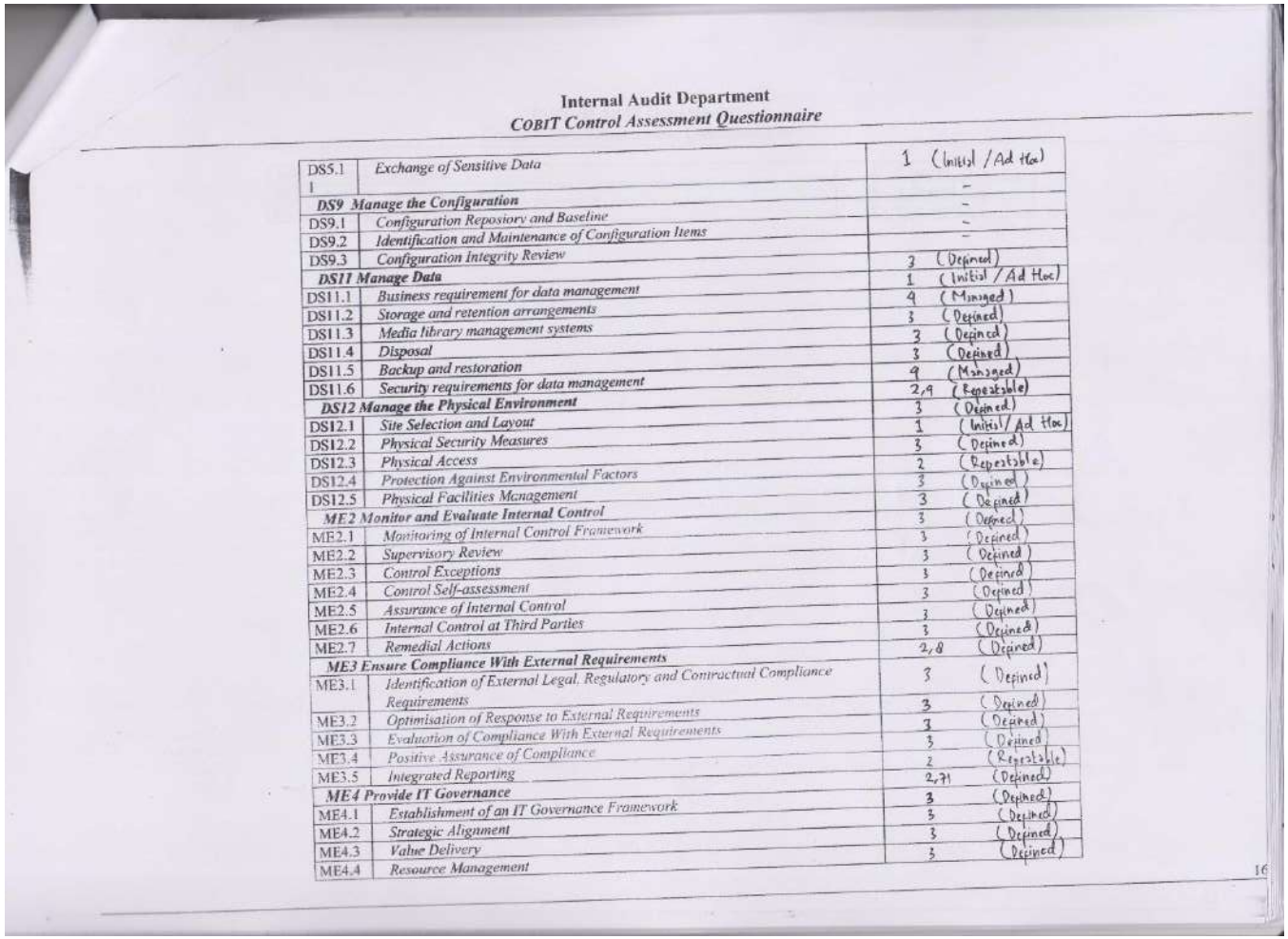
PO4 Define IT process, organization and relationship		3,33 (Defined)
PO4.1	*IT process framework*	3 (Defined)
PO4.2	*IT strategy committee*	4 (Managed)
PO4.3	*IT steering committee*	3 (Defined)
PO4.4	*Organizational placement of the IT function*	2 (Repeatable)
PO4.5	*IT organizational structure*	3 (Defined)
PO4.6	*Establishment of roles and responsibility*	4 (Managed)
PO4.7	*Responsibility for IT quality assurance*	3 (Defined)
PO4.8	*Responsibility for risk, security and compliance*	4 (Managed)
PO4.9	*Data and system ownership*	3 (Defined)
PO4.10	*Supervision*	3 (Defined)
PO4.11	*Segregation of duties*	4 (Managed)
PO4.12	*IT staffing*	4 (Managed)
PO4.13	*Key IT personal*	3 (Defined)
PO4.14	*Contracted staff policies and procedure*	4 (Managed)
PO4.15	*Relationship*	3 (Defined)
PO6 Communicate Management Aims and Direction		3,6 (Managed)
PO6.1	*IT Policy and Control Environment*	4 (Managed)
PO6.2	*Enterprise IT Risk and Control Framework*	3 (Defined)



Internal Audit Department

COBIT Control Assessment Questionnaire

PO6.3	*IT Policies Management*	4 (Managed)
PO6.4	*Policy, Standard and Procedures Rollout*	3 (Defined)
PO6.5	*Communication of IT Objectives and Direction*	4 (Managed)
PO9 Assess and Manage IT Risks		1,33 (Initial / Ad Hoc)
PO9.1	*IT Risk Management Framework*	0 (Non Existant)
PO9.2	*Establishment of Risk Context*	1 (Initial / Ad Hoc)
PO9.3	*Event Identification*	2 (Repeatable)
PO9.4	*Risk Assessment*	1 (Initial / Ad Hoc)
PO9.5	*Risk Response*	1 (Initial / Ad Hoc)
PO9.6	*Maintenance and Monitoring of a Risk Action Plan*	3 (Defined)
DS2 Manage Third-party Services		3,25 (Defined)
DS2.1	*Identification of All Supplier Relationships*	2 (Repeatable)
DS2.2	*Supplier Relationship Management*	4 (Managed)
DS2.3	*Supplier Risk Management*	4 (Managed)
DS2.4	*Supplier Performance Monitoring*	3 (Defined)
DS4 Ensure Continuous Service		2,1 (Repeatable)
DS4.1	*IT Continuity Framework*	3 (Defined)
DS4.2	*IT Continuity Plans*	4 (Managed)
DS4.3	*Critical IT Resources*	3 (Defined)
DS4.4	*Maintenance of the IT Continuity Plan*	3 (Defined)
DS4.5	*Testing of the IT Continuity Plan*	3 (Defined)
DS4.6	*IT Continuity Plan Training*	1 (Initial / Ad Hoc)
DS4.7	*Distribution of the IT Continuity Plan*	0 (Non Existant)
DS4.8	*IT Services Recovery and Resumption*	1 (Initial / Ad Hoc)
DS4.9	*Offsite Backup Storage*	2 (Repeatable)
DS4.10	*Post-resumption Review*	1 (Initial / Ad Hoc)
DS5 Ensure Systems Security		2 (Repeatable)
DS5.1	*Management of IT Security*	0 (Non Existant)
DS5.2	*IT Security Plan*	1 (Initial / Ad Hoc)
DS5.3	*Identity Management*	3 (Defined)
DS5.4	*User Account Management*	2 (Repeatable)
DS5.5	*Security Testing, Surveillance and Monitoring*	2 (Repeatable)
DS5.6	*Security Incident Definition*	1 (Initial / Ad Hoc)
DS5.7	*Protection of Security Technology*	1 (Initial / Ad Hoc)
DS5.8	*Cryptographic Key Management*	1 (Initial / Ad Hoc)
DS5.9	*Malicious Software Prevention, Detection and Correction*	3 (Defined)
DS5.10	*Network Security*	3 (Defined)

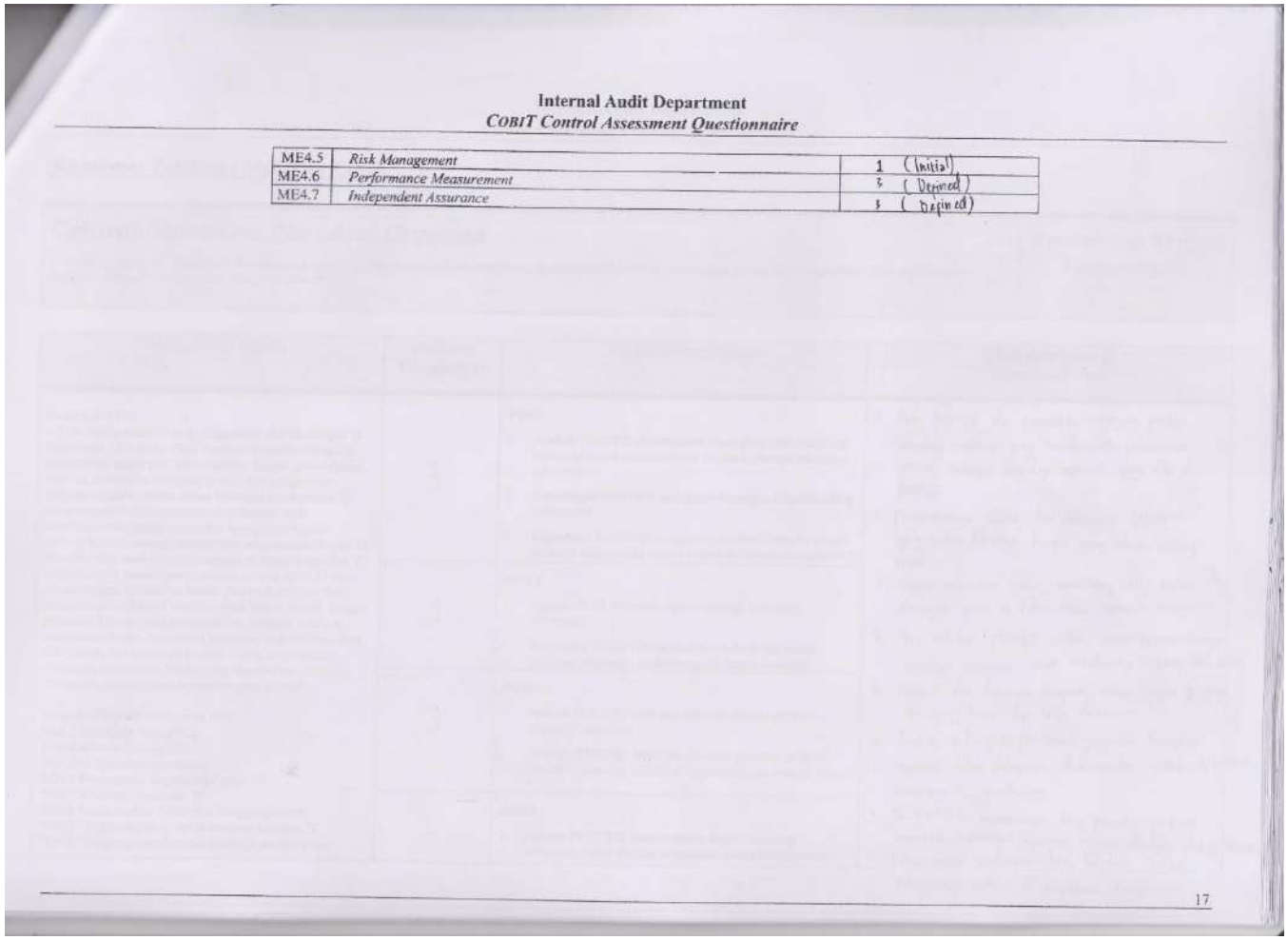


Internal Audit Department

COBIT Control Assessment Questionnaire

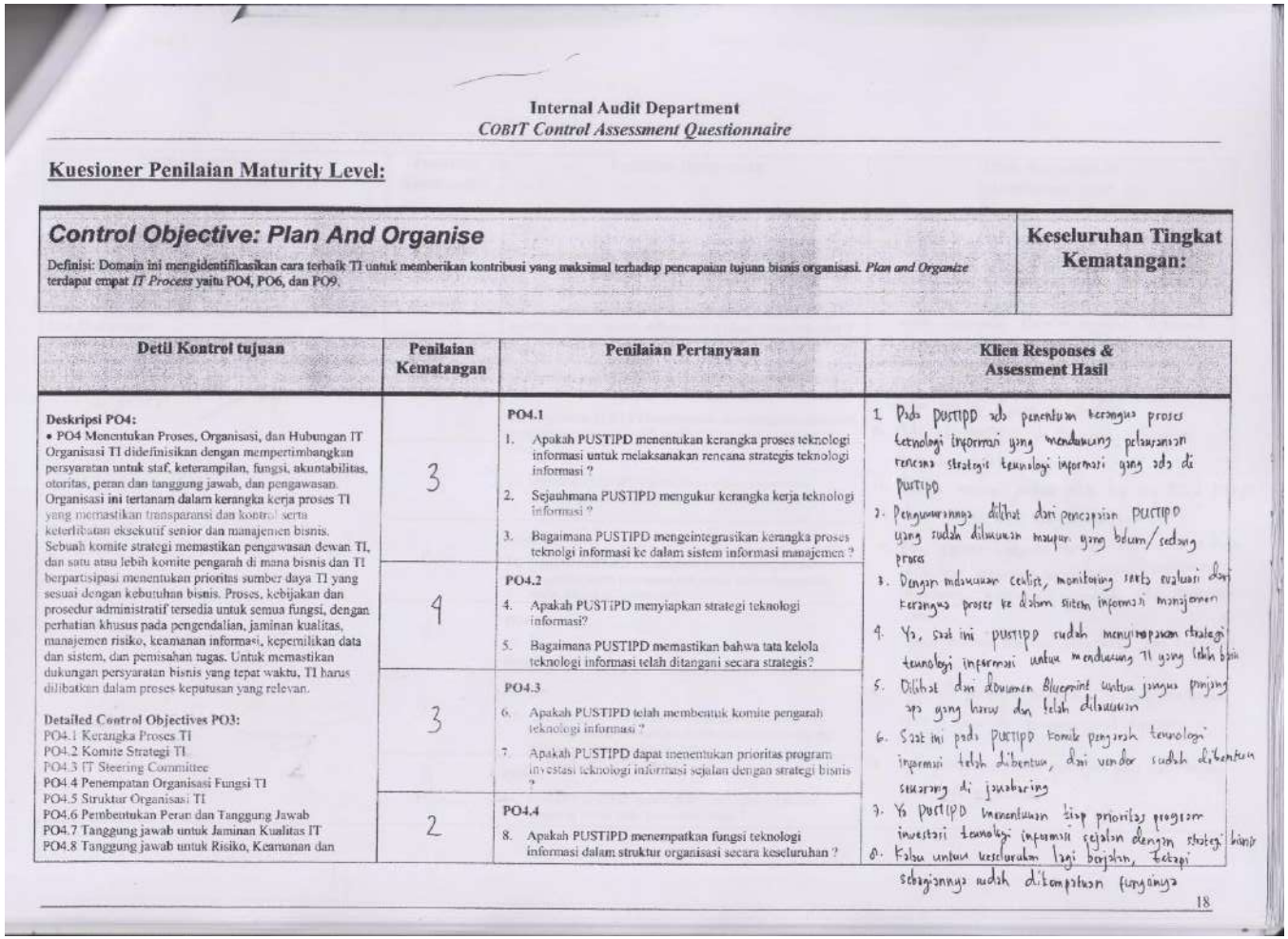
DS5.1	*Exchange of Sensitive Data*	1 (Initial / Ad Hoc)
	DS9 Manage the Configuration	-
DS9.1	*Configuration Repository and Baseline*	-
DS9.2	*Identification and Maintenance of Configuration Items*	-
DS9.3	*Configuration Integrity Review*	-
	DS11 Manage Data	3 (Defined)
DS11.1	*Business requirement for data management*	1 (Initial / Ad Hoc)
DS11.2	*Storage and retention arrangements*	4 (Managed)
DS11.3	*Media library management systems*	3 (Defined)
DS11.4	*Disposal*	3 (Defined)
DS11.5	*Backup and restoration*	3 (Defined)
DS11.6	*Security requirements for data management*	4 (Managed)
	DS12 Manage the Physical Environment	2,9 (Repeatable)
DS12.1	*Site Selection and Layout*	3 (Defined)
DS12.2	*Physical Security Measures*	1 (Initial / Ad Hoc)
DS12.3	*Physical Access*	3 (Defined)
DS12.4	*Protection Against Environmental Factors*	2 (Repeatable)
DS12.5	*Physical Facilities Management*	3 (Defined)
	ME2 Monitor and Evaluate Internal Control	3 (Defined)
ME2.1	*Monitoring of Internal Control Framework*	3 (Defined)
ME2.2	*Supervisory Review*	3 (Defined)
ME2.3	*Control Exceptions*	3 (Defined)
ME2.4	*Control Self-assessment*	3 (Defined)
ME2.5	*Assurance of Internal Control*	3 (Defined)
ME2.6	*Internal Control at Third Parties*	3 (Defined)
ME2.7	*Remedial Actions*	2,8 (Defined)
	ME3 Ensure Compliance With External Requirements	3 (Defined)
ME3.1	*Identification of External Legal, Regulatory and Contractual Compliance Requirements*	3 (Defined)
ME3.2	*Optimisation of Response to External Requirements*	3 (Defined)
ME3.3	*Evaluation of Compliance With External Requirements*	3 (Defined)
ME3.4	*Positive Assurance of Compliance*	2 (Repeatable)
ME3.5	*Integrated Reporting*	2,71 (Defined)
	ME4 Provide IT Governance	3 (Defined)
ME4.1	*Establishment of an IT Governance Framework*	3 (Defined)
ME4.2	*Strategic Alignment*	3 (Defined)
ME4.3	*Value Delivery*	3 (Defined)
ME4.4	*Resource Management*	

16



Internal Audit Department
COBiT Control Assessment Questionnaire

ME4.5	*Risk Management*	1 (Initial)
ME4.6	*Performance Measurement*	3 (Defined)
ME4.7	*Independent Assurance*	3 (Defined)



Internal Audit Department
COBIT Control Assessment Questionnaire

Kuesioner Penilaian Maturity Level:

Control Objective: Plan And Organise	**Keseluruhan Tingkat Kematangan:**
Definisi: Domain ini mengidentifikasikan cara terbaik TI untuk memberikan kontribusi yang maksimal terhadap pencapaian tujuan bisnis organisasi. *Plan and Organize* terdapat empat *IT Process* yaitu PO4, PO6, dan PO9.	

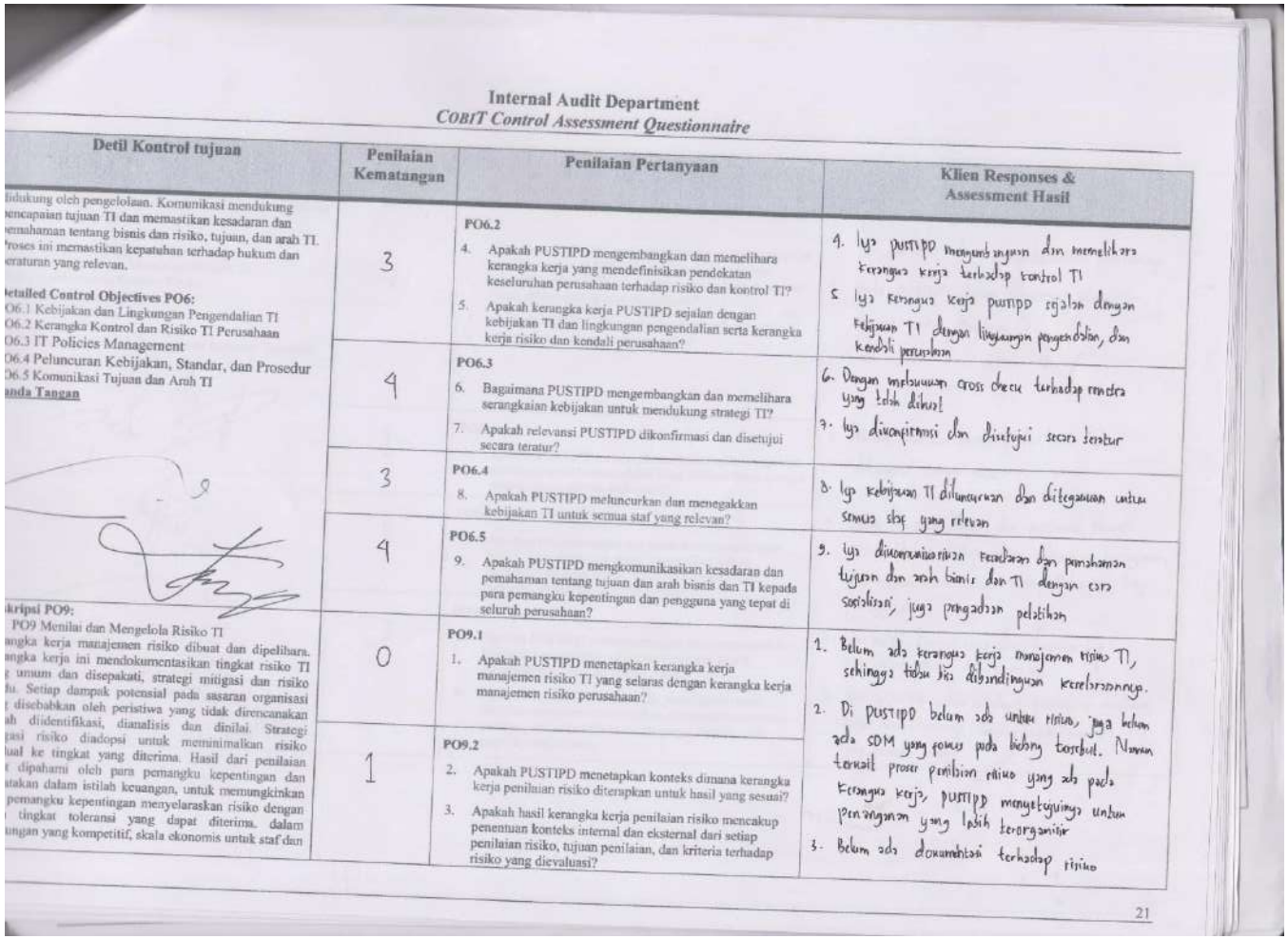
Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
Deskripsi PO4: • PO4 Menentukan Proses, Organisasi, dan Hubungan IT Organisasi TI didefinisikan dengan mempertimbangkan persyaratan untuk staf, keterampilan, fungsi, akuntabilitas, otoritas, peran dan tanggung jawab, dan pengawasan. Organisasi ini tertanam dalam kerangka kerja proses TI yang memastikan transparansi dan kontrol serta keterlibatan eksekutif senior dan manajemen bisnis. Sebuah komite strategi memastikan pengawasan dewan TI, dan satu atau lebih komite pengarah di mana bisnis dan TI berpartisipasi menentukan prioritas sumber daya TI yang sesuai dengan kebutuhan bisnis. Proses, kebijakan dan prosedur administratif tersedia untuk semua fungsi, dengan perhatian khusus pada pengendalian, jaminan kualitas, manajemen risiko, keamanan informasi, kepemilikan data dan sistem, dan pemisahan tugas. Untuk memastikan dukungan persyaratan bisnis yang tepat waktu, TI harus dilibatkan dalam proses keputusan yang relevan. **Detailed Control Objectives PO3:** PO4.1 Kerangka Proses TI PO4.2 Komite Strategi TI PO4.3 IT Steering Committee PO4.4 Penempatan Organisasi Fungsi TI PO4.5 Struktur Organisasi TI PO4.6 Pembentukan Peran dan Tanggung Jawab PO4.7 Tanggung jawab untuk Jaminan Kualitas IT PO4.8 Tanggung jawab untuk Risiko, Keamanan dan	3	**PO4.1** 1. Apakah PUSTIPD menentukan kerangka proses teknologi informasi untuk melaksanakan rencana strategis teknologi informasi ? 2. Sejauhmana PUSTIPD mengukur kerangka kerja teknologi informasi ? 3. Bagaimana PUSTIPD mengeintegrasikan kerangka proses teknolgi informasi ke dalam sistem informasi manajemen ?	1. Pada PUSTIPD ada penentuan kerangka proses teknologi informasi yang mendukung pelaksanaan rencana strategis teknologi informasi yang ada di pustipd 2. Pengukurannya dilihat dari perencanaan PUSTIPD yang sudah dilakukan maupun yang belum/sedang proses 3. Dengan melakukan control, monitoring serta evaluasi dari kerangka proses ke dalam sistem informasi manajemen 4. Ya, saat ini pustipd sudah menyiapkan strategi teknologi informasi untuk mendukung TI yang lebih baik 5. Dilihat dari dokumen Blueprint untuk jangka panjang yg yang harus dan telah dilakukan 6. Saat ini pada PUSTIPD komite pengarah teknologi informasi telah dibentuk, dari vendor sudah dibentuk struktur di jaringan 7. Ya PUSTIPD menentukan skip prioritas program investasi teknologi informasi sejalan dengan strategi bisnis 8. Fokus untuk kesseluruhan lagi berjalan, tetapi sebagiannya sudah ditempatkan fungsinya
	4	**PO4.2** 4. Apakah PUSTIPD menyiapkan strategi teknologi informasi? 5. Bagaimana PUSTIPD memastikan bahwa tata kelola teknologi informasi telah ditangani secara strategis?	
	3	**PO4.3** 6. Apakah PUSTIPD telah membentuk komite pengarah teknologi informasi ? 7. Apakah PUSTIPD dapat menentukan prioritas program investasi teknologi informasi sejalan dengan strategi bisnis ?	
	2	**PO4.4** 8. Apakah PUSTIPD menempatkan fungsi teknologi informasi dalam struktur organisasi secara keseluruhan ?	

Internal Audit Department
COBIT Control Assessment Questionnaire

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
Kepatuhan PO4.9 Kepemilikan Data dan Sistem PO4.10 Pengawasan PO4.11 Pemisahan Tugas PO4.12 Staffing IT PO4.13 Karyawan TI Kunci PO4.14 Kebijakan dan Prosedur Para Staf yang Terkontrak PO4.15 Hubungan **Tanda Tangan**	3	**PO4.5** 9. Bagaimana PUSTIPD Menetapkan struktur organisasi TI internal dan eksternal untuk memenuhi tujuan bisnis yang diharapkan dan mengubah keadaan ? 10. Apakah PUSTIPD dapat menempatkan proses teknologi informasi secara berkala dalam meninjaukan kebutuhan staff ?	9. Penempatannya dilihat dari analisis jabatan dan beban kerja, sesuai dengan beban kerjanya, semakin kompleks beban kerja maka struktur organisasi dapat berubah dan juga dilihat dari anggarannya untuk pemenuhan struktur organisasi TI internal dan external yang memenuhi kebutuhan bisnis. 10. Sedang diproses, sebagian ada yang sudah. Untuk yang telah ditetapkan dari sk yayasan dan untuk yang lagi diproses non sudah.
	4	**PO4.6** 11. Apakah staff PUSTIPD memiliki tanggung jawab untuk memenuhi kebutuhan organisasi ? 12. Bagaimana PUSTIPD membentuk dan mengkomunikasikan peran serta tanggung jawab untuk stef teknologi informasi ?	11. Jelas pada PUSTIPD ada tanggung jawab untuk memenuhi kebutuhan organisasi 12. Dengan membagi jobdesk untuk tiap staf TI di pustipd
	3	**PO4.7** 13. Dapatkah PUSTIPD memastikan bahwa organisasi tanggung jawab untuk jaminan kualitas teknologi informasi?	13. Iya, pustipd dapat menjamin kualitas TI
	4	**PO4.8** 14. Apakah PUSTIPD menetapkan peran penting untuk tanggung jawab keamanan informasi dalam mengelola risiko teknologi informasi?	14. Iya, pustipd menjamin keamanan dan risiko TI dengan dilakukan pengecekan secara berkala, melakukan monitoring, maintenance mendalam untuk pengamanan risiko
	3	**PO4.9** 15. Sejauhmana organisasi melindungi data sesuai dengan tanggung jawab ?	15. Dengan membagi hak akses penggunaan, yang berpentingan kebutuhan
	3	**PO4.10** 16. Apakah PUSTIPD menerapkan pengawasan teknologi informasi untuk memastikan bahwa peran dan tanggung jawab itu dilakukan dengan benar ?	16. Iya, ada penerapan pengawasan TI yang diberlakukan sehingga peran dan tanggung jawab dipertimbangkan
	4	**PO4.11** 17. Apakah PUSTIPD menerapkan pembagian peran dan tanggung jawab pada Pemisahan tugas ?	17. Iya, pustipd menerapkan pembagian peran dan tanggung jawab pada pemisahan

Internal Audit Department
COBIT Control Assessment Questionnaire

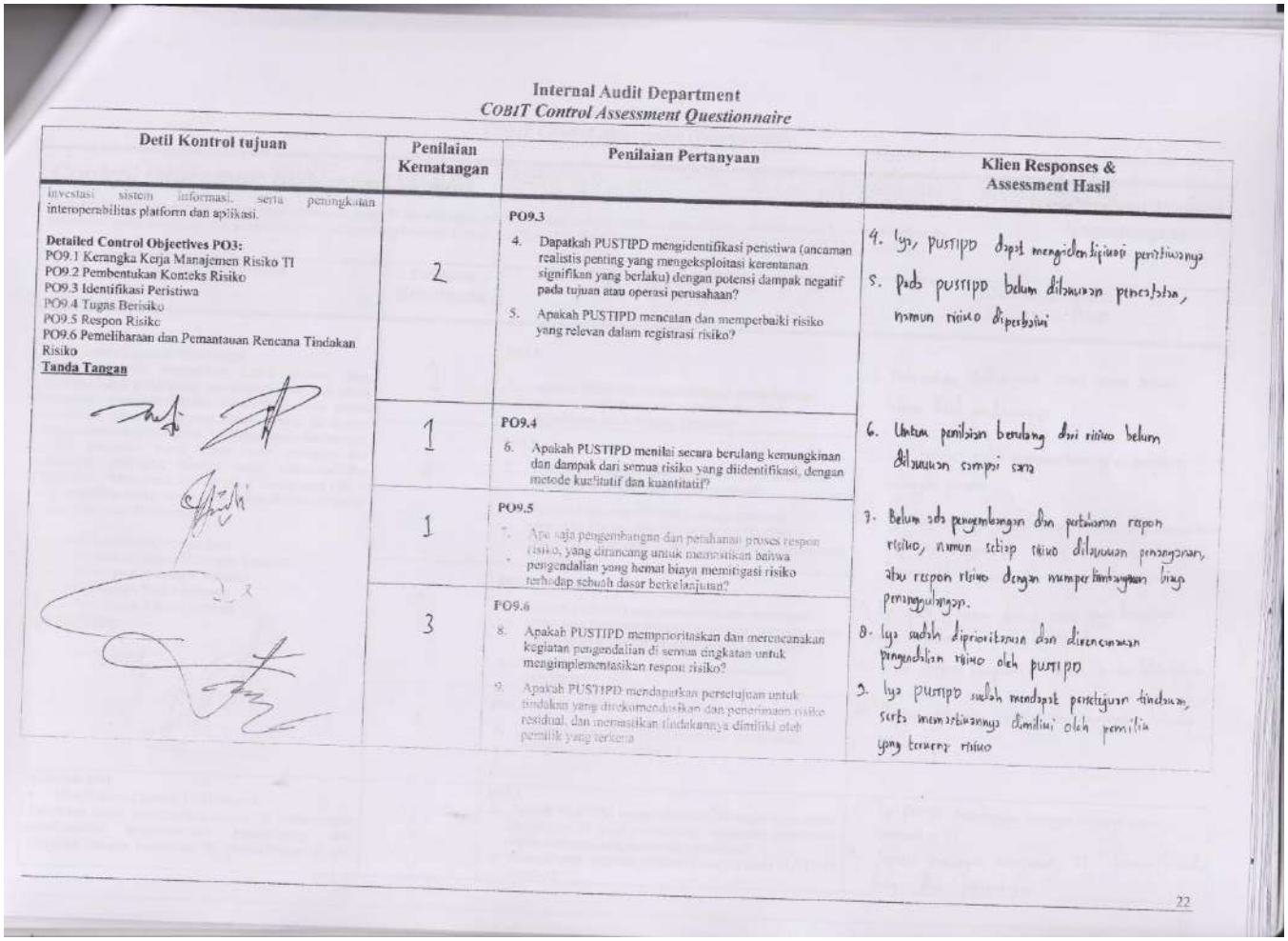
Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
	4	**PO4.12** 18. Bagaimana PUSTIPD mengevaluasi staff teknologi informasi secara berkala atau atas perubahan pada lingkungan bisnis, operasional atau teknologi informasi 19. Bagaiamana PUSTIPD memastikan bahwa fungsi teknologi informasi memiliki sumber daya yang cukup untuk mendukung tujuan dan sasaran bisnis secara memadai dan tepat ?	18. Dengan melihat laporan kerja karyawan, didalam rapat kerja internal yang dilakukan 1 minggu sekali 19. Dengan melakukan monitoring evaluasi, monitoring terhadap beban kerja
	3	**PO4.13** 20. Dapatkah PUSTIPD menentukan dan identifikasi staff TI (misalnya, penggantian / cadangan personil), dan kurangi ketergantungan pada satu individu yang melakukan fungsi pekerjaan penting ?	20. Iya ditentukan dan diidentifikasi, tetapi terkadang ada personil yang diminta bantuan untuk mengerjakan pekerjaan lain.
	4	**PO4.14** 21. Apakah PUSTIPD memastikan bahwa konsultan dan karyawan kontrak yang mendukung fungsi TI mengetahui dan mematuhi kebijakan organisasi ?	21. Iya diprioritaskan, pemantauannya ditentukan dari kecepatan kontrak yang telah dibuat dengan konsultan dan karyawan kontrak yang bersangkutan
	3	**PO4.15** 22. Bagaimana PUSTIPD membentuk dan mempertahankan koordinasi optimal, komunikasi, dan struktur penghubung untara fungsi teknologi informasi tentang berbagai kepentingan lain ?	22. Cara pustipd membentuk dan mempertahankan koordinasi optimal, komunikasi dan strukturnya dengan melakukan komunikasi efektif serta kolaborasi
Deskripsi PO6: • **Komunikasikan Tujuan dan Arahan Manajemen** Manajemen mengembangkan kerangka kerja kontrol TI perusahaan dan menetapkan serta mengkomunikasikan kebijakan. Komunikasi yang berkelanjutan program diimplementasikan untuk mengartikulasikan misi, tujuan layanan, kebijakan dan prosedur, dll, disetujui dan	4	**PO6.1** 1. Apakah PUSTIPD menentukan elemen lingkungan kontrol untuk TI, selaras dengan filosofi manajemen perusahaan dan gaya operasi? 2. Apa saja elemen yang terkait dengan TI tersebut? 3. Bagaimana lingkungan kontrol yang dibentuk pada PUSTIPD?	1. Iya, pustipd menentukan selaras dengan filosofi manajemen perusahaan dan gaya operasi 2. Elemen terkait TI tersebut adalah integritas nilai, kompetensi staf dan tanggung jawab 3. Dengan melakukan monitoring dan evaluasi secara berkala.



Internal Audit Department
COBIT Control Assessment Questionnaire

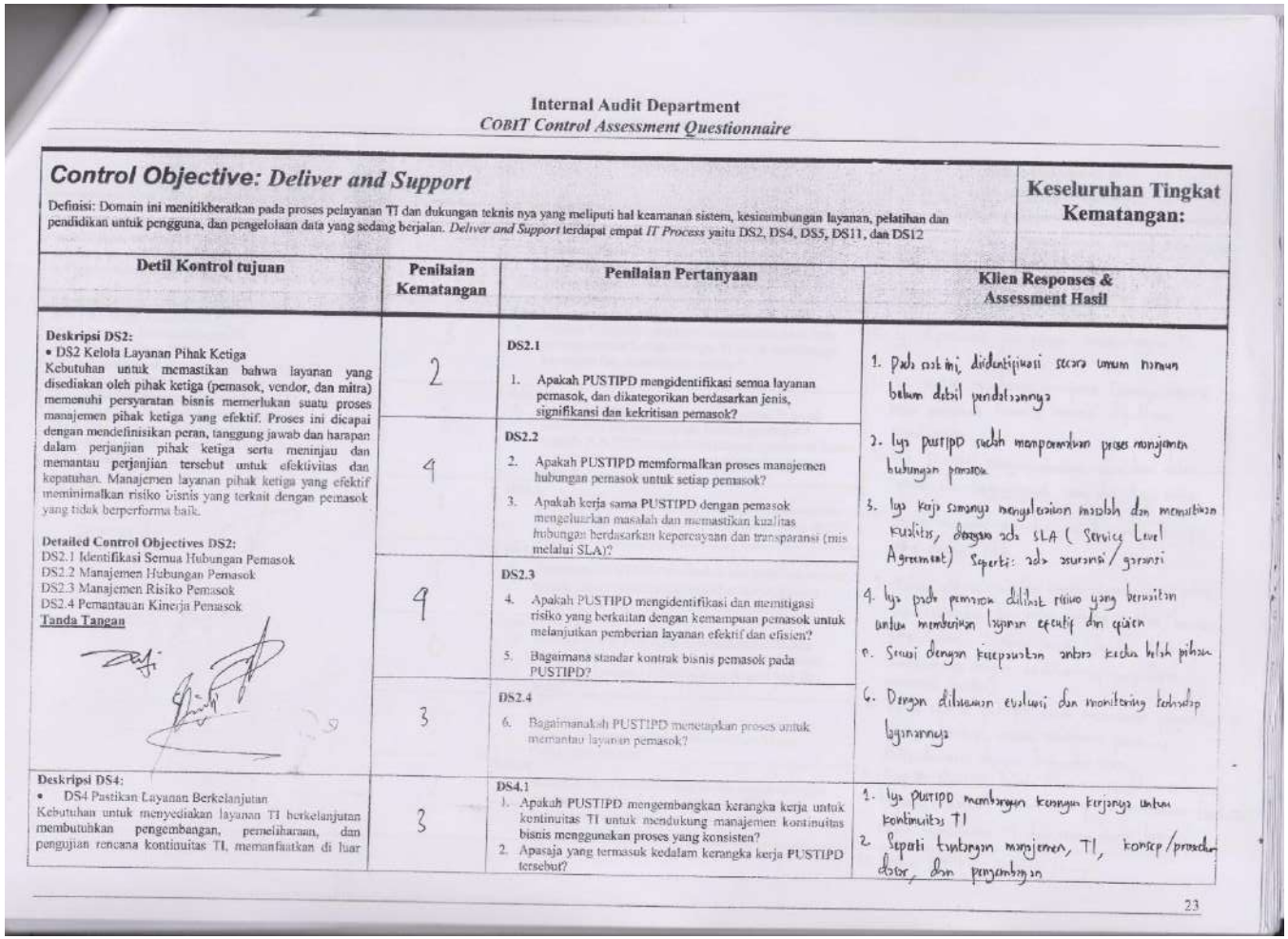
Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
lidukung oleh pengelolaan. Komunikasi mendukung encapaian tujuan TI dan memastikan kesadaran dan emahaman tentang bisnis dan risiko, tujuan, dan arah TI. roses ini memastikan kepatuhan terhadap hukum dan eraturan yang relevan. **etailed Control Objectives PO6:** O6.1 Kebijakan dan Lingkungan Pengendalian TI O6.2 Kerangka Kontrol dan Risiko TI Perusahaan O6.3 IT Policies Management O6.4 Peluncuran Kebijakan, Standar, dan Prosedur O6.5 Komunikasi Tujuan dan Arah TI **anda Tangan**	3	**PO6.2** 4. Apakah PUSTIPD mengembangkan dan memelihara kerangka kerja yang mendefinisikan pendekatan keseluruhan perusahaan terhadap risiko dan kontrol TI? 5. Apakah kerangka kerja PUSTIPD sejalan dengan kebijakan TI dan lingkungan pengendalian serta kerangka kerja risiko dan kendali perusahaan?	4. Iya pustipd mengembangkan dan memelihara kerangka kerja terhadap kontrol TI 5 Iya kerangka kerja pustipd sejalan dengan kebijakan TI dengan lingkungan pengendalian, dan kendali perusahaan
	4	**PO6.3** 6. Bagaimana PUSTIPD mengembangkan dan memelihara serangkaian kebijakan untuk mendukung strategi TI? 7. Apakah relevansi PUSTIPD dikonfirmasi dan disetujui secara teratur?	6. Dengan melakukan cross check terhadap rencana yang telah dibuat 7. Iya dikonfirmasi dan disetujui secara teratur
	3	**PO6.4** 8. Apakah PUSTIPD meluncurkan dan menegakkan kebijakan TI untuk semua staf yang relevan?	8. Iya kebijakan TI diluncurkan dan ditegakkan untuk semua staf yang relevan
	4	**PO6.5** 9. Apakah PUSTIPD mengkomunikasikan kesadaran dan pemahaman tentang tujuan dan arah bisnis dan TI kepada para pemangku kepentingan dan pengguna yang tepat di seluruh perusahaan?	9. Iya dikomunikasikan kesadaran dan pemahaman tujuan dan arah bisnis dan TI dengan cara sosialisasi, juga pengadaan pelatihan
ikripsi PO9: PO9 Menilai dan Mengelola Risiko TI angka kerja manajemen risiko dibuat dan dipelihara. angka kerja ini mendokumentasikan tingkat risiko TI umum dan disepakati, strategi mitigasi dan risiko tu. Setiap dampak potensial pada sasaran organisasi disebabkan oleh peristiwa yang tidak direncanakan ah diidentifikasi, dianalisis dan dinilai. Strategi asi risiko diadopsi untuk meminimalkan risiko ual ke tingkat yang diterima. Hasil dari penilaian dipahami oleh para pemangku kepentingan dan takan dalam istilah keuangan, untuk memungkinkan pemangku kepentingan menyelaraskan risiko dengan tingkat toleransi yang dapat diterima, dalam ungan yang kompetitif, skala ekonomis untuk staf dan	0	**PO9.1** 1. Apakah PUSTIPD menetapkan kerangka kerja manajemen risiko TI yang selaras dengan kerangka kerja manajemen risiko perusahaan?	1. Belum ada kerangka kerja manajemen risiko TI, sehingga tidak bisa dibandingkan kesesuaiannya.
	1	**PO9.2** 2. Apakah PUSTIPD menetapkan konteks dimana kerangka kerja penilaian risiko diterapkan untuk hasil yang sesuai? 3. Apakah hasil kerangka kerja penilaian risiko mencakup penentuan konteks internal dan eksternal dari setiap penilaian risiko, tujuan penilaian, dan kriteria terhadap risiko yang dievaluasi?	2. Di PUSTIPD belum ada untuk risiko, juga belum ada SDM yang fokus pada bidang tersebut. Namun terkait proses penilaian risiko yang ada pada kerangka kerja, PUSTIPD mengelompokkan untuk penanganan yang lebih terorganisir 3. Belum ada dokumentasi terhadap risiko

21



Internal Audit Department
COBIT Control Assessment Questionnaire

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
investasi sistem informasi, serta peningkatan interoperabilitas platform dan aplikasi. **Detailed Control Objectives PO3:** PO9.1 Kerangka Kerja Manajemen Risiko TI PO9.2 Pembentukan Konteks Risiko PO9.3 Identifikasi Peristiwa PO9.4 Tugas Berisiko PO9.5 Respon Risiko PO9.6 Pemeliharaan dan Pemantauan Rencana Tindakan Risiko **Tanda Tangan**	2	**PO9.3** 4. Dapatkah PUSTIPD mengidentifikasi peristiwa (ancaman realistis penting yang mengeksploitasi kerentanan signifikan yang berlaku) dengan potensi dampak negatif pada tujuan atau operasi perusahaan? 5. Apakah PUSTIPD mencatan dan memperbaiki risiko yang relevan dalam registrasi risiko?	4. Iya, pustipd dapat mengidentifikasi peristiwanya 5. Pada pustipd belum dilakukan pencatatan, namun risiko diperbaiki
	1	**PO9.4** 6. Apakah PUSTIPD menilai secara berulang kemungkinan dan dampak dari semua risiko yang diidentifikasi, dengan metode kualitatif dan kuantitatif?	6. Untuk penilaian berulang dari risiko belum dilakukan sampai saat
	1	**PO9.5** 7. Apa saja pengembangan dan pemahaman proses respon risiko, yang dirancang untuk memastikan bahwa pengendalian yang hemat biaya memitigasi risiko terhadap sebuah dasar berkelanjutan?	7. Belum ada pengembangan dan pemahaman respon risiko, namun setiap risiko dilakukan pencegahan, atau respon risiko dengan mempertimbangkan biaya penanggulangan.
	3	**PO9.6** 8. Apakah PUSTIPD memprioritaskan dan merencanakan kegiatan pengendalian di semua tingkatan untuk mengimplementasikan respon risiko? 9. Apakah PUSTIPD mendapatkan persetujuan untuk tindakan yang direkomendasikan dan penerimaan risiko residual, dan memastikan tindakannya dimiliki oleh pemilik yang terkena	8. Iya sudah diprioritaskan dan direncanakan pengendalian risiko oleh pustipd 9. Iya pustipd sudah mendapat persetujuan tindakan, serta memastikannya dimiliki oleh pemilik yang terkena risiko



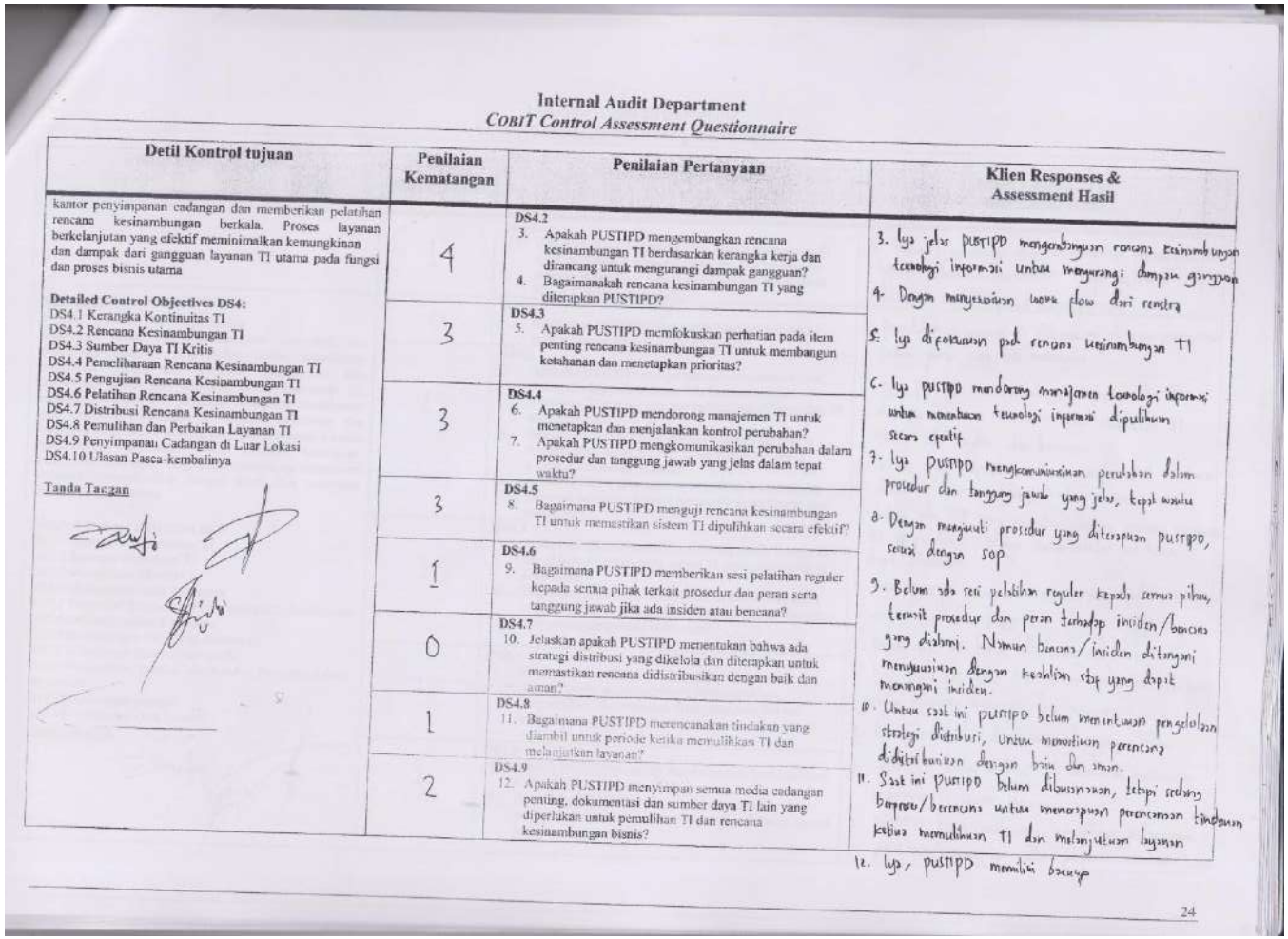
Internal Audit Department
COBIT Control Assessment Questionnaire

Control Objective: Deliver and Support

Definisi: Domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknis nya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan dan pendidikan untuk pengguna, dan pengelolaan data yang sedang berjalan. *Deliver and Support* terdapat empat *IT Process* yaitu DS2, DS4, DS5, DS11, dan DS12

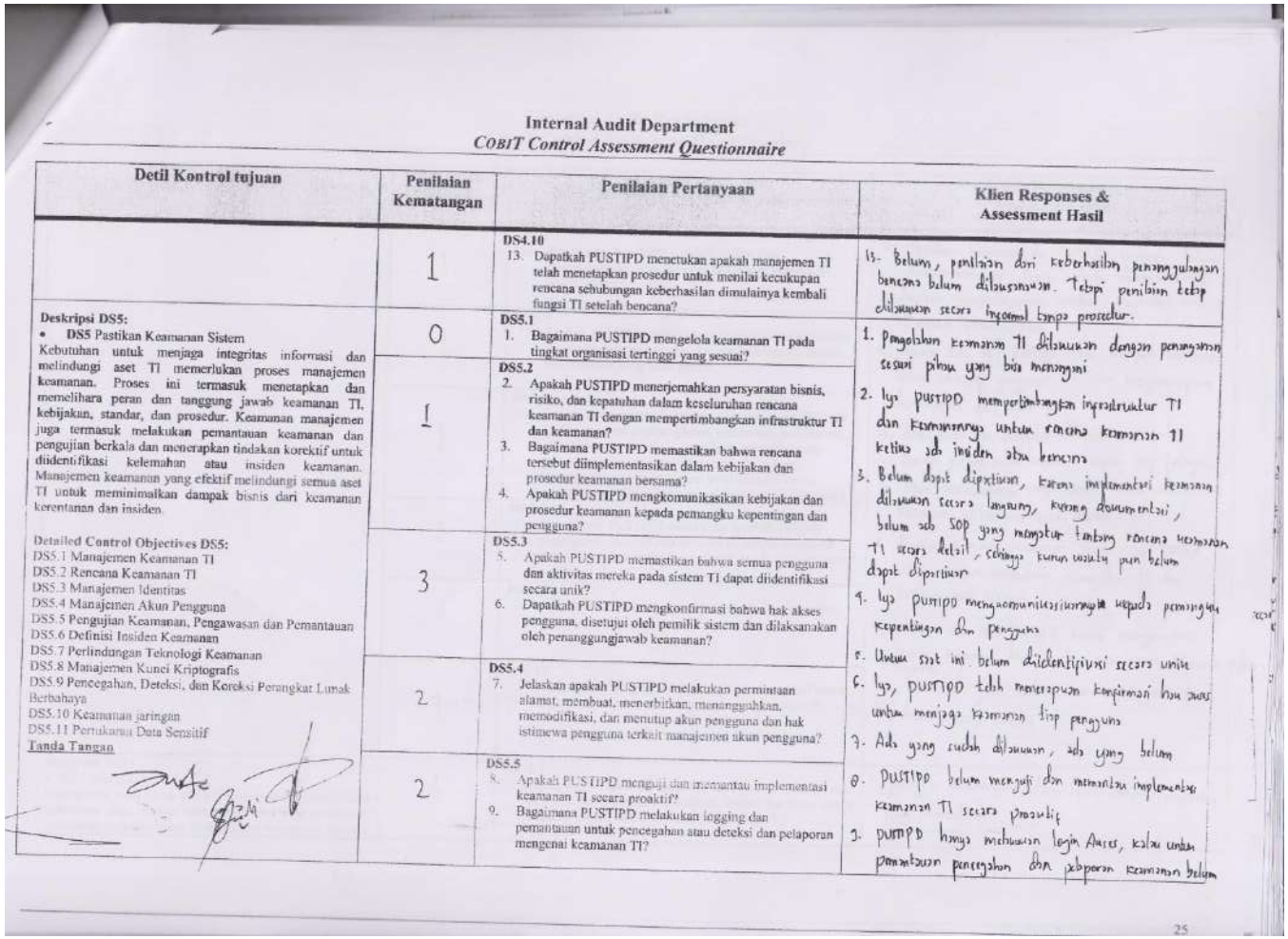
Keseluruhan Tingkat Kematangan:

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
Deskripsi DS2: • DS2 Kelola Layanan Pihak Ketiga Kebutuhan untuk memastikan bahwa layanan yang disediakan oleh pihak ketiga (pemasok, vendor, dan mitra) memenuhi persyaratan bisnis memerlukan suatu proses manajemen pihak ketiga yang efektif. Proses ini dicapai dengan mendefinisikan peran, tanggung jawab dan harapan dalam perjanjian pihak ketiga serta meninjau dan memantau perjanjian tersebut untuk efektivitas dan kepatuhan. Manajemen layanan pihak ketiga yang efektif meminimalkan risiko bisnis yang terkait dengan pemasok yang tidak berperforma baik. **Detailed Control Objectives DS2:** DS2.1 Identifikasi Semua Hubungan Pemasok DS2.2 Manajemen Hubungan Pemasok DS2.3 Manajemen Risiko Pemasok DS2.4 Pemantauan Kinerja Pemasok **Tanda Tangan**	2	**DS2.1** 1. Apakah PUSTIPD mengidentifikasi semua layanan pemasok, dan dikategorikan berdasarkan jenis, signifikansi dan kekritisan pemasok?	1. pada saat ini diidentifikasi secara umum namun belum detail pendataannya 2. iya pustipd sudah memparankan proses manajemen hubungan pemasok 3. iya kerja samanya mengatasi masalah dan memastikan kualitas, dengan ada SLA (Service Level Agreement) Seperti: ada asuransi / garansi 4. iya pada pemasok dilihat risiko yang bersiatan untuk memberikan layanan efektif dan efisien 5. Sesuai dengan kesepakatan antara kedua belah pihak 6. Dengan dilakukan evaluasi dan monitoring terhadap layanannya
	4	**DS2.2** 2. Apakah PUSTIPD memformalkan proses manajemen hubungan pemasok untuk setiap pemasok? 3. Apakah kerja sama PUSTIPD dengan pemasok mengeluarkan masalah dan memastikan kualitas hubungan berdasarkan kepercayaan dan transparansi (mis melalui SLA)?	
	4	**DS2.3** 4. Apakah PUSTIPD mengidentifikasi dan memitigasi risiko yang berkaitan dengan kemampuan pemasok untuk melanjutkan pemberian layanan efektif dan efisien? 5. Bagaimana standar kontrak bisnis pemasok pada PUSTIPD?	
	3	**DS2.4** 6. Bagaimanakah PUSTIPD menetapkan proses untuk memantau layanan pemasok?	
Deskripsi DS4: • DS4 Pastikan Layanan Berkelanjutan Kebutuhan untuk menyediakan layanan TI berkelanjutan membutuhkan pengembangan, pemeliharaan, dan pengujian rencana kontinuitas TI, memanfaatkan di luar	3	**DS4.1** 1. Apakah PUSTIPD mengembangkan kerangka kerja untuk kontinuitas TI untuk mendukung manajemen kontinuitas bisnis menggunakan proses yang konsisten? 2. Apasaja yang termasuk kedalam kerangka kerja PUSTIPD tersebut?	1. iya pustipd membangun kerangka kerjanya untuk kontinuitas TI 2. Seperti tujuannya manajemen, TI, konsep/prosedur dasar, dan pengembangan



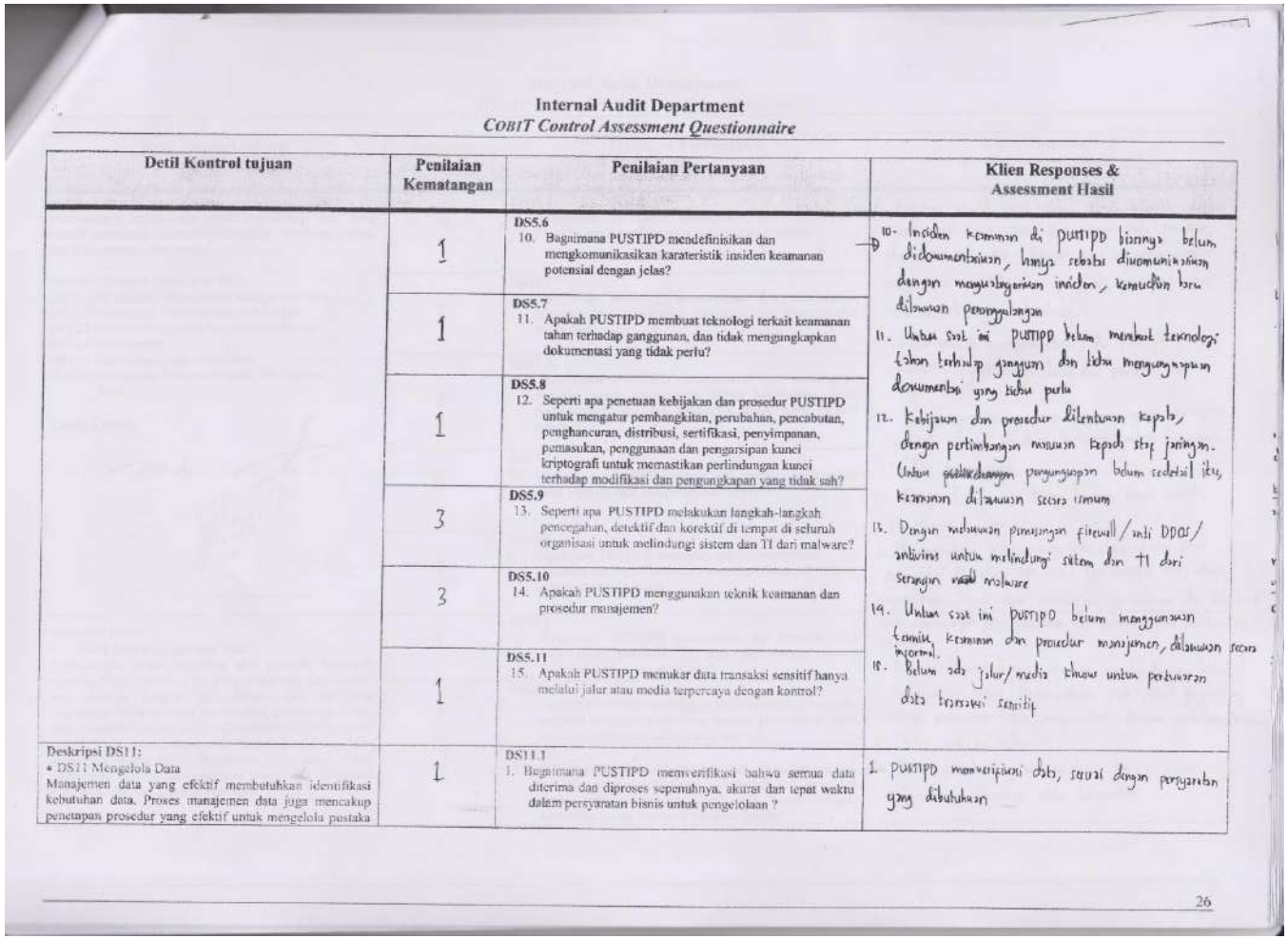
Internal Audit Department
COBIT Control Assessment Questionnaire

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
kantor penyimpanan cadangan dan memberikan pelatihan rencana kesinambungan berkala. Proses layanan berkelanjutan yang efektif meminimalkan kemungkinan dan dampak dari gangguan layanan TI utama pada fungsi dan proses bisnis utama **Detailed Control Objectives DS4:** DS4.1 Kerangka Kontinuitas TI DS4.2 Rencana Kesinambungan TI DS4.3 Sumber Daya TI Kritis DS4.4 Pemeliharaan Rencana Kesinambungan TI DS4.5 Pengujian Rencana Kesinambungan TI DS4.6 Pelatihan Rencana Kesinambungan TI DS4.7 Distribusi Rencana Kesinambungan TI DS4.8 Pemulihan dan Perbaikan Layanan TI DS4.9 Penyimpanan Cadangan di Luar Lokasi DS4.10 Ulasan Pasca-kembalinya Tanda Tangan	4	**DS4.2** 3. Apakah PUSTIPD mengembangkan rencana kesinambungan TI berdasarkan kerangka kerja dan dirancang untuk mengurangi dampak gangguan? 4. Bagaimanakah rencana kesinambungan TI yang diterapkan PUSTIPD?	3. Iya jelas PUSTIPD mengembangkan rencana kesinambungan teknologi informasi untuk mengurangi dampak gangguan 4. Dengan menyesuaikan work flow dari rencana
	3	**DS4.3** 5. Apakah PUSTIPD memfokuskan perhatian pada item penting rencana kesinambungan TI untuk membangun ketahanan dan menetapkan prioritas?	5. Iya difokuskan pada rencana kesinambungan TI
	3	**DS4.4** 6. Apakah PUSTIPD mendorong manajemen TI untuk menetapkan dan menjalankan kontrol perubahan? 7. Apakah PUSTIPD mengkomunikasikan perubahan dalam prosedur dan tanggung jawab yang jelas dalam tepat waktu?	6. Iya PUSTIPD mendorong manajemen teknologi informasi untuk menentukan teknologi informasi dipulihkan secara efektif 7. Iya PUSTIPD mengkomunikasikan perubahan dalam prosedur dan tanggung jawab yang jelas, tepat waktu
	3	**DS4.5** 8. Bagaimana PUSTIPD menguji rencana kesinambungan TI untuk memastikan sistem TI dipulihkan secara efektif?	8. Dengan mengacuti prosedur yang diterapkan pustipd, sesuai dengan sop
	1	**DS4.6** 9. Bagaimana PUSTIPD memberikan sesi pelatihan reguler kepada semua pihak terkait prosedur dan peran serta tanggung jawab jika ada insiden atau bencana?	9. Belum ada sesi pelatihan reguler kepada semua pihak, terkait prosedur dan peran terhadap insiden/bencana yang dialami. Namun bencana/insiden ditangani menyesuaikan dengan keahlian staf yang dapat menangani insiden.
	0	**DS4.7** 10. Jelaskan apakah PUSTIPD menentukan bahwa ada strategi distribusi yang dikelola dan diterapkan untuk memastikan rencana didistribusikan dengan baik dan aman?	10. Untuk saat ini pustipd belum menentukan pengelolaan strategi distribusi, untuk memastikan perencana didistribusikan dengan baik dan aman.
	1	**DS4.8** 11. Bagaimana PUSTIPD merencanakan tindakan yang diambil untuk periode ketika memulihkan TI dan melanjutkan layanan?	11. Saat ini pustipd belum dilaksanakan, tetapi sedang berproses/berencana untuk menerapkan perencanan tindakan ketika memulihkan TI dan melanjutkan layanan
	2	**DS4.9** 12. Apakah PUSTIPD menyimpan semua media cadangan penting, dokumentasi dan sumber daya TI lain yang diperlukan untuk pemulihan TI dan rencana kesinambungan bisnis?	12. Iya, pustipd memiliki backup



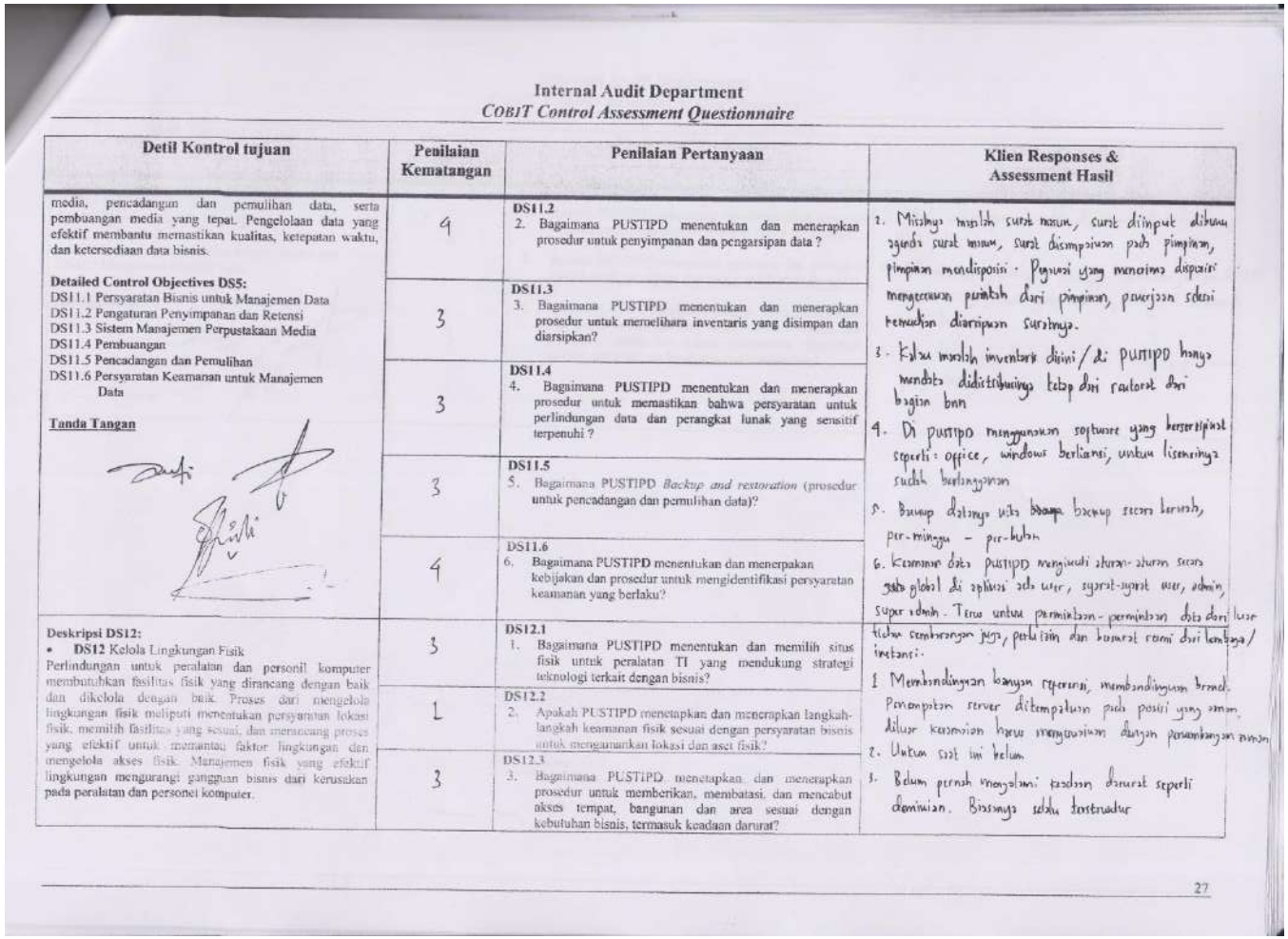
Internal Audit Department
COBIT Control Assessment Questionnaire

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
	1	**DS4.10** 13. Dapatkah PUSTIPD menetukan apakah manajemen TI telah menetapkan prosedur untuk menilai kecukupan rencana sehubungan keberhasilan dimulainya kembali fungsi TI setelah bencana?	13. Belum, penilaian dari keberhasilan penanggulangan bencana belum dilaksanakan. Tetapi penilaian tetap dilakukan secara informal tanpa prosedur.
Deskripsi DS5: • **DS5** Pastikan Keamanan Sistem Kebutuhan untuk menjaga integritas informasi dan melindungi aset TI memerlukan proses manajemen keamanan. Proses ini termasuk menetapkan dan memelihara peran dan tanggung jawab keamanan TI, kebijakan, standar, dan prosedur. Keamanan manajemen juga termasuk melakukan pemantauan keamanan dan pengujian berkala dan menerapkan tindakan korektif untuk diidentifikasi kelemahan atau insiden keamanan. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis dari kerentanan dan insiden. **Detailed Control Objectives DS5:** DS5.1 Manajemen Keamanan TI DS5.2 Rencana Keamanan TI DS5.3 Manajemen Identitas DS5.4 Manajemen Akun Pengguna DS5.5 Pengujian Keamanan, Pengawasan dan Pemantauan DS5.6 Definisi Insiden Keamanan DS5.7 Perlindungan Teknologi Keamanan DS5.8 Manajemen Kunci Kriptografis DS5.9 Pencegahan, Deteksi, dan Koreksi Perangkat Lunak Berbahaya DS5.10 Keamanan jaringan DS5.11 Pertukaran Data Sensitif Tanda Tangan	0	**DS5.1** 1. Bagaimana PUSTIPD mengelola keamanan TI pada tingkat organisasi tertinggi yang sesuai?	1. Pengelolaan keamanan TI dilakukan dengan penanganan sesuai pihak yang bisa menangani
	1	**DS5.2** 2. Apakah PUSTIPD menerjemahkan persyaratan bisnis, risiko, dan kepatuhan dalam keseluruhan rencana keamanan TI dengan mempertimbangkan infrastruktur TI dan keamanan? 3. Bagaimana PUSTIPD memastikan bahwa rencana tersebut diimplementasikan dalam kebijakan dan prosedur keamanan bersama? 4. Apakah PUSTIPD mengkomunikasikan kebijakan dan prosedur keamanan kepada pemangku kepentingan dan pengguna?	2. Iya pustipd mempertimbangkan infrastruktur TI dan kemampuannya untuk rencana keamanan TI ketika ada insiden atau bencana 3. Belum dapat dipastikan, karena implementasi keamanan dilakukan secara langsung, kurang dokumentasi, belum ada SOP yang mengatur tentang rencana keamanan TI secara detail, sehingga kurun waktu pun belum dapat dipastikan 4. Iya pustipd mengkomunikasikannya kepada pemangku kepentingan dan pengguna
	3	**DS5.3** 5. Apakah PUSTIPD memastikan bahwa semua pengguna dan aktivitas mereka pada sistem TI dapat diidentifikasi secara unik? 6. Dapatkah PUSTIPD mengkonfirmasi bahwa hak akses pengguna, disetujui oleh pemilik sistem dan dilaksanakan oleh penanggungjawab keamanan?	5. Untuk saat ini belum diidentifikasi secara unik 6. Iya, pustipd telah menerapkan konfirmasi hak akses untuk menjaga keamanan tiap pengguna
	2	**DS5.4** 7. Jelaskan apakah PUSTIPD melakukan permintaan alamat, membuat, menerbitkan, menanggahkan, memodifikasi, dan menutup akun pengguna dan hak istimewa pengguna terkait manajemen akun pengguna?	7. Ada yang sudah dilakukan, ada yang belum
	2	**DS5.5** 8. Apakah PUSTIPD menguji dan memantau implementasi keamanan TI secara proaktif? 9. Bagaimana PUSTIPD melakukan logging dan pemantauan untuk pencegahan atau deteksi dan pelaporan mengenai keamanan TI?	8. Pustipd belum menguji dan memantau implementasi keamanan TI secara proaktif 9. pustipd hanya melakukan login Access, kalau untuk pemantauan pencegahan dan pelaporan keamanan belum



Internal Audit Department
COBIT Control Assessment Questionnaire

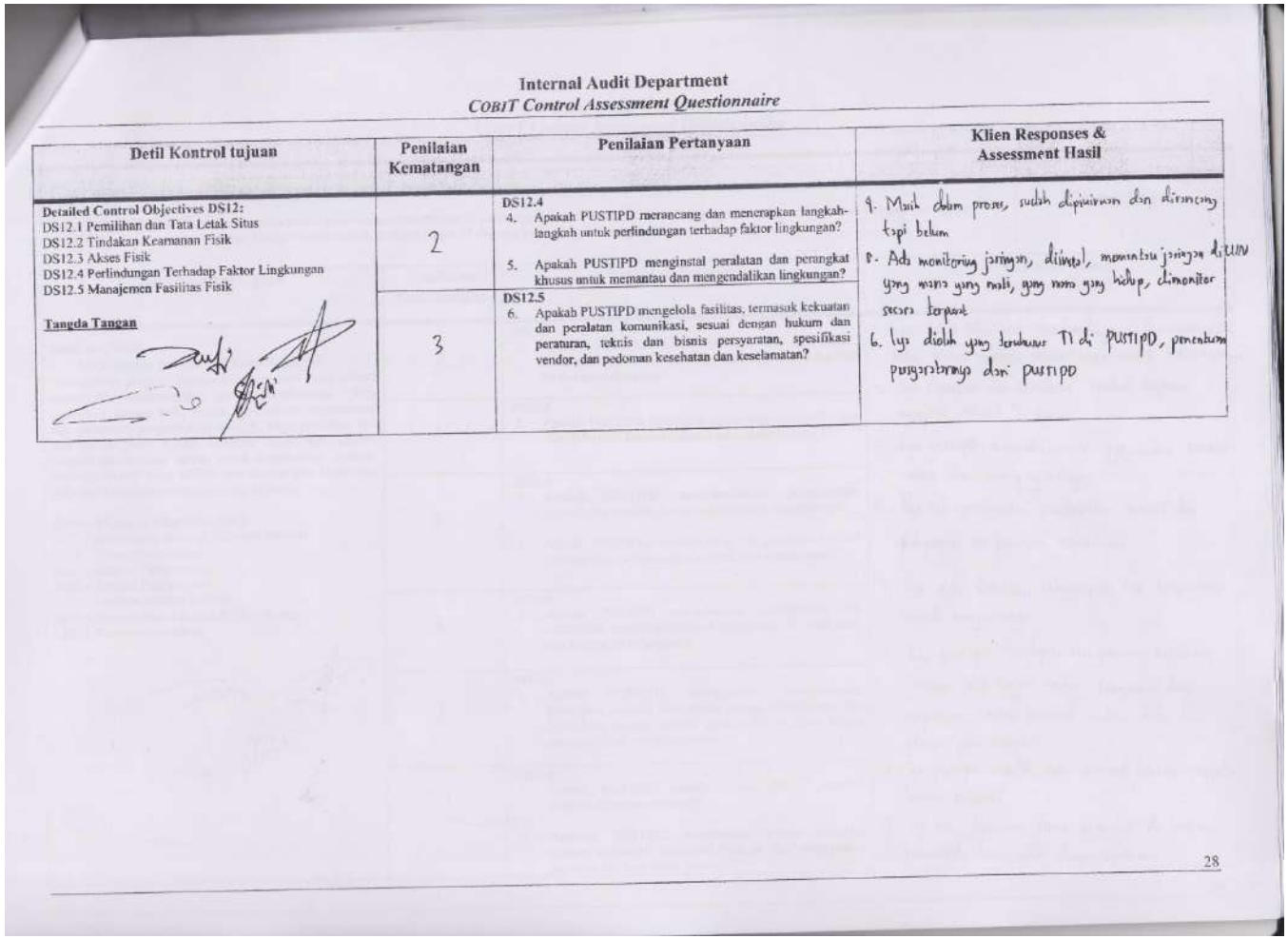
Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
	1	**DS5.6** 10. Bagaimana PUSTIPD mendefinisikan dan mengkomunikasikan karateristik insiden keamanan potensial dengan jelas?	10. Insiden keamanan di pustipd biasnya belum didokumentasikan, hanya sebatas dikomunikasikan dengan menyelenggarakan insiden, kemudian baru dilakukan penanggulangan
	1	**DS5.7** 11. Apakah PUSTIPD membuat teknologi terkait keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentasi yang tidak perlu?	11. Untuk saat ini pustipd belum membuat teknologi tahan terhadap gangguan dan tidak mengungkapkan dokumentasi yang tidak perlu
	1	**DS5.8** 12. Seperti apa penetuan kebijakan dan prosedur PUSTIPD untuk mengatur pembangkitan, perubahan, pencabutan, penghancuran, distribusi, sertifikasi, penyimpanan, pemasukan, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah?	12. Kebijakan dan prosedur ditentukan kepala, dengan pertimbangan masukan kepada staf jaringan. Untuk pengungkapan belum sedetail itu, keamanan dilakukan secara umum
	3	**DS5.9** 13. Seperti apa PUSTIPD melakukan langkah-langkah pencegahan, detektif dan korektif di tempat di seluruh organisasi untuk melindungi sistem dan TI dari malware?	13. Dengan melakukan pemasangan firewall / anti DDOS / antivirus untuk melindungi sistem dan TI dari serangan virus malware
	3	**DS5.10** 14. Apakah PUSTIPD menggunakan teknik keamanan dan prosedur manajemen?	14. Untuk saat ini pustipd belum menggunakan teknik keamanan dan prosedur manajemen, dilakukan secara informal.
	1	**DS5.11** 15. Apakah PUSTIPD menukar data transaksi sensitif hanya melalui jalur atau media tepercaya dengan kontrol?	15. Belum ada jalur/media khusus untuk pertukaran data transaksi sensitif
Deskripsi DS11: • DS11 Mengelola Data Manajemen data yang efektif membutuhkan identifikasi kebutuhan data. Proses manajemen data juga mencakup penetapan prosedur yang efektif untuk mengelola pustaka	1	**DS11.1** 1. Bagaimana PUSTIPD memverifikasi bahwa semua data diterima dan diproses sepenuhnya, akurat dan tepat waktu dalam persyaratan bisnis untuk pengelolaan ?	1. pustipd memverifikasi data, sesuai dengan persyaratan yang dibutuhkan



Internal Audit Department
COBIT Control Assessment Questionnaire

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
media, pencadangan dan pemulihan data, serta pembuangan media yang tepat. Pengelolaan data yang efektif membantu memastikan kualitas, ketepatan waktu, dan ketersediaan data bisnis. **Detailed Control Objectives DS5:** DS11.1 Persyaratan Bisnis untuk Manajemen Data DS11.2 Pengaturan Penyimpanan dan Retensi DS11.3 Sistem Manajemen Perpustakaan Media DS11.4 Pembuangan DS11.5 Pencadangan dan Pemulihan DS11.6 Persyaratan Keamanan untuk Manajemen Data **Tanda Tangan**	4	**DS11.2** 2. Bagaimana PUSTIPD menentukan dan menerapkan prosedur untuk penyimpanan dan pengarsipan data ?	2. Misalnya masuk surat masuk, surat diinput dibuat agenda surat masuk, surat disimpaikan pada pimpinan, pimpinan mendisposisi. Pegawai yang menerima disposisi mengerjakan perintah dari pimpinan, pekerjaan selesai kemudian diarsipkan suratnya.
	3	**DS11.3** 3. Bagaimana PUSTIPD menentukan dan menerapkan prosedur untuk memelihara inventaris yang disimpan dan diarsipkan?	3. Kalau masalah inventaris disini/di pustipd hanya mendata didistribusikan tetap dari rektorat dari bagian bmn
	3	**DS11.4** 4. Bagaimana PUSTIPD menentukan dan menerapkan prosedur untuk memastikan bahwa persyaratan untuk perlindungan data dan perangkat lunak yang sensitif terpenuhi ?	4. Di pustipd menggunakan software yang bersertipikat seperti: office, windows berlisensi, untuk lisensinya sudah berlangganan
	3	**DS11.5** 5. Bagaimana PUSTIPD *Backup and restoration* (prosedur untuk pencadangan dan pemulihan data)?	5. Backup datanya kita biasa backup secara berkala, per-minggu - per-bulan
	4	**DS11.6** 6. Bagaimana PUSTIPD menentukan dan menerapkan kebijakan dan prosedur untuk mengidentifikasi persyaratan keamanan yang berlaku?	6. Keamanan data pustipd mengikuti aturan-aturan secara garis global di aplikasi ada user, sysrat-sysrat user, admin, super admin. Terus untuk permintaan-permintaan data dari luar tidak sembarangan juga, perlu izin dan biasrat resmi dari lembaga/instansi.
Deskripsi DS12: • **DS12** Kelola Lingkungan Fisik Perlindungan untuk peralatan dan personil komputer membutuhkan fasilitas fisik yang dirancang dengan baik dan dikelola dengan baik. Proses dari mengelola lingkungan fisik meliputi menentukan persyaratan lokasi fisik, memilih fasilitas yang sesuai, dan merancang proses yang efektif untuk memantau faktor lingkungan dan mengelola akses fisik. Manajemen fisik yang efektif lingkungan mengurangi gangguan bisnis dari kerusakan pada peralatan dan personel komputer.	3	**DS12.1** 1. Bagaimana PUSTIPD menentukan dan memilih situs fisik untuk peralatan TI yang mendukung strategi teknologi terkait dengan bisnis?	1. Membandingkan banyak referensi, membandingkan brand. Penempatan server ditempatkan pada posisi yang aman. diluar kemungkinan harus mengasuransi dengan perusahaan asuransi
	1	**DS12.2** 2. Apakah PUSTIPD menetapkan dan menerapkan langkah-langkah keamanan fisik sesuai dengan persyaratan bisnis untuk mengamankan lokasi dan aset fisik?	2. Untuk saat ini belum
	3	**DS12.3** 3. Bagaimana PUSTIPD menetapkan dan menerapkan prosedur untuk memberikan, membatasi, dan mencabut akses tempat, bangunan dan area sesuai dengan kebutuhan bisnis, termasuk keadaan darurat?	3. Belum pernah mengalami kendala darurat seperti demikian. Biasanya sudah terstruktur

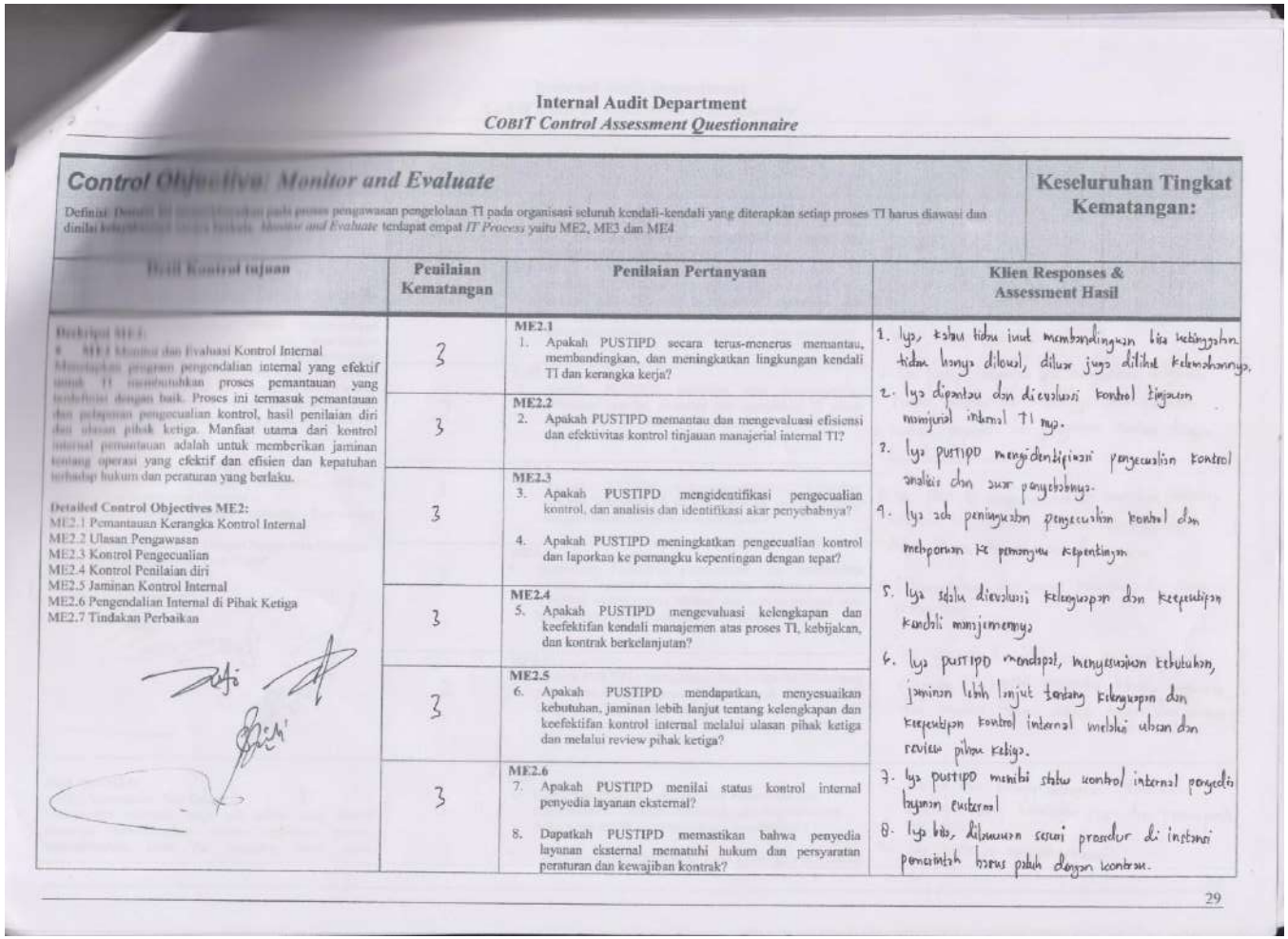
27



Internal Audit Department
COBIT Control Assessment Questionnaire

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
Detailed Control Objectives DS12: DS12.1 Pemilihan dan Tata Letak Situs DS12.2 Tindakan Keamanan Fisik DS12.3 Akses Fisik DS12.4 Perlindungan Terhadap Faktor Lingkungan DS12.5 Manajemen Fasilitas Fisik **Tanda Tangan**	2	**DS12.4** 4. Apakah PUSTIPD merancang dan menerapkan langkah-langkah untuk perlindungan terhadap faktor lingkungan? 5. Apakah PUSTIPD menginstal peralatan dan perangkat khusus untuk memantau dan mengendalikan lingkungan?	4. Masih dalam proses, sudah dipasarkan dan dirancang tapi belum 5. Ada monitoring jaringan, dikontrol, memantau jaringan dr UNY yang mana yang mati, yang mana yang hidup, dimonitor secara berjenjang
	3	**DS12.5** 6. Apakah PUSTIPD mengelola fasilitas, termasuk kekuatan dan peralatan komunikasi, sesuai dengan hukum dan peraturan, teknis dan bisnis persyaratan, spesifikasi vendor, dan pedoman kesehatan dan keselamatan?	6. Iya diolah yang berkaitan TI di PUSTIPD, pencatuan pengembangan dari PUSTIPD

28



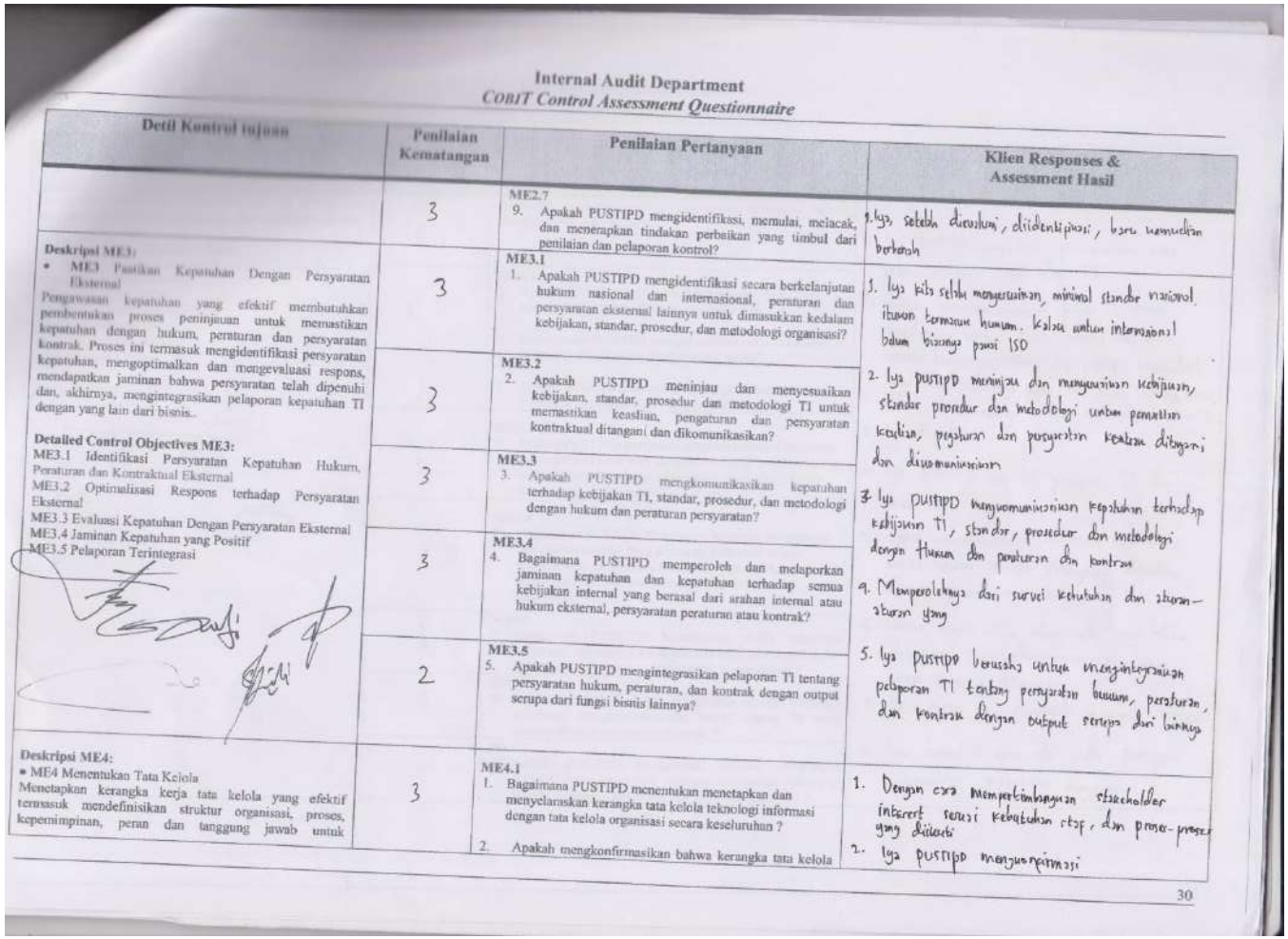
Internal Audit Department
COBIT Control Assessment Questionnaire

Control Objective: Monitor and Evaluate

Definisi: Domain ini berkaitan pada proses pengawasan pengelolaan TI pada organisasi seluruh kendali-kendali yang diterapkan setiap proses TI harus diawasi dan dinilai kebenarannya secara berkala. *Monitor and Evaluate* terdapat empat *IT Process* yaitu ME2, ME3 dan ME4

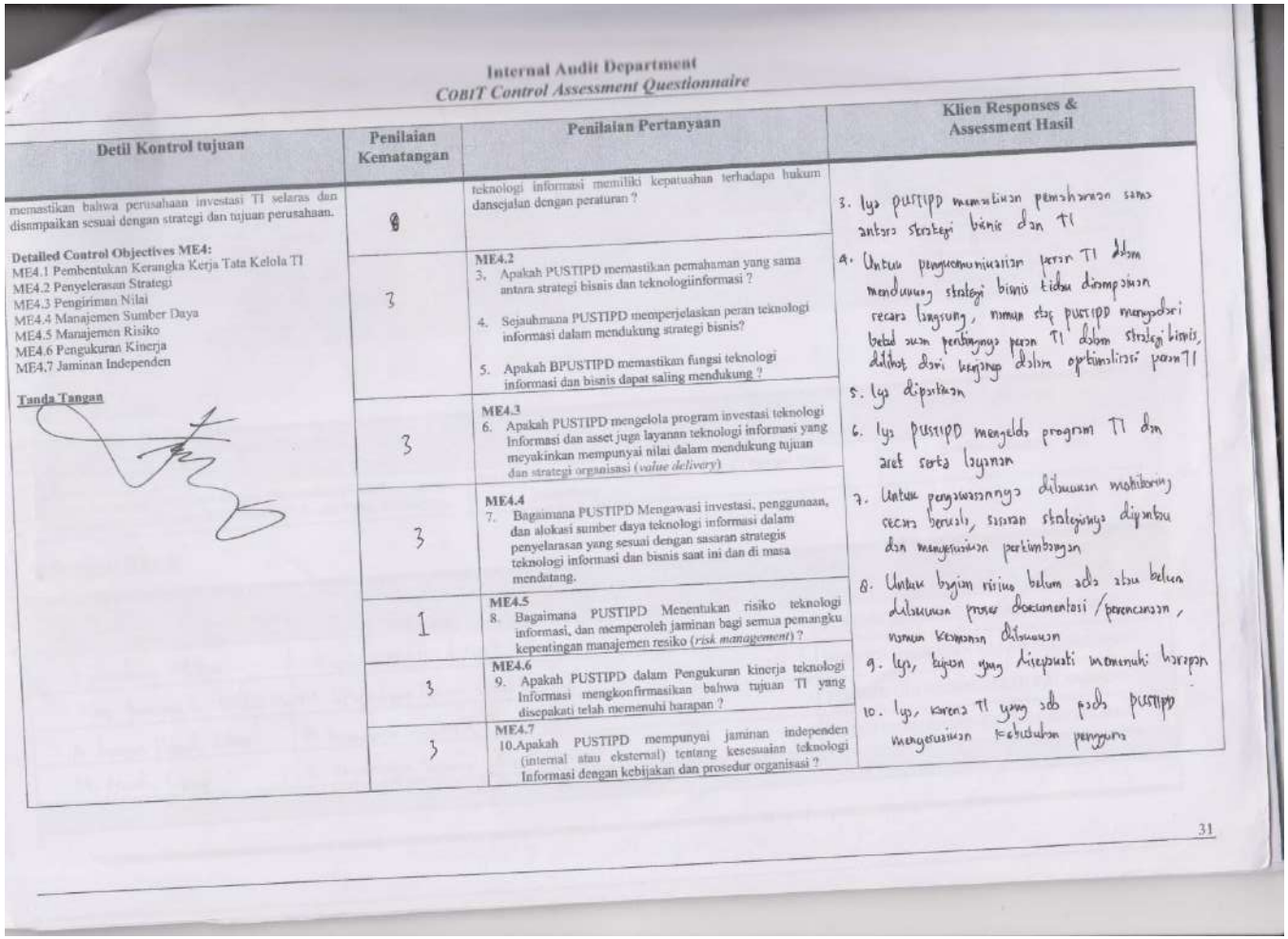
Keseluruhan Tingkat Kematangan:

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
Deskripsi ME2: ME2 Monitor dan Evaluasi Kontrol Internal Menetapkan program pengendalian internal yang efektif untuk TI membutuhkan proses pemantauan yang terdefinisi dengan baik. Proses ini termasuk pemantauan dan pelaporan pengecualian kontrol, hasil penilaian diri dan ulasan pihak ketiga. Manfaat utama dari kontrol internal pemantauan adalah untuk memberikan jaminan tentang operasi yang efektif dan efisien dan kepatuhan terhadap hukum dan peraturan yang berlaku. **Detailed Control Objectives ME2:** ME2.1 Pemantauan Kerangka Kontrol Internal ME2.2 Ulasan Pengawasan ME2.3 Kontrol Pengecualian ME2.4 Kontrol Penilaian diri ME2.5 Jaminan Kontrol Internal ME2.6 Pengendalian Internal di Pihak Ketiga ME2.7 Tindakan Perbaikan	3	**ME2.1** 1. Apakah PUSTIPD secara terus-menerus memantau, membandingkan, dan meningkatkan lingkungan kendali TI dan kerangka kerja?	1. iya, ada tidak untuk membandingkan bila ketinggalan tidak hanya dilewat, dilaur juga dilihat kelemahannya.
	3	**ME2.2** 2. Apakah PUSTIPD memantau dan mengevaluasi efisiensi dan efektivitas kontrol tinjauan manajerial internal TI?	2. iya dipantau dan dievaluasi kontrol tinjauan manjurial internal TI nya.
	3	**ME2.3** 3. Apakah PUSTIPD mengidentifikasi pengecualian kontrol, dan analisis dan identifikasi akar penyebabnya? 4. Apakah PUSTIPD meningkatkan pengecualian kontrol dan laporkan ke pemangku kepentingan dengan tepat?	3. iya PUSTIPD mengidentifikasi pengecualian kontrol analisis dan akar penyebabnya. 4. iya ada peningkatan pengecualian kontrol dan melaporkan ke pemangku kepentingan
	3	**ME2.4** 5. Apakah PUSTIPD mengevaluasi kelengkapan dan keefektifan kendali manajemen atas proses TI, kebijakan, dan kontrak berkelanjutan?	5. iya ada dievaluasi kelengkapan dan keefektifan kendali manajemennya
	3	**ME2.5** 6. Apakah PUSTIPD mendapatkan, menyesuaikan kebutuhan, jaminan lebih lanjut tentang kelengkapan dan keefektifan kontrol internal melalui ulasan pihak ketiga dan melalui review pihak ketiga?	6. iya PUSTIPD mendapat, menyesuaikan kebutuhan, jaminan lebih lanjut tentang kelengkapan dan keefektifan kontrol internal melalui ulasan dan review pihak ketiga.
	3	**ME2.6** 7. Apakah PUSTIPD menilai status kontrol internal penyedia layanan eksternal? 8. Dapatkah PUSTIPD memastikan bahwa penyedia layanan eksternal mematuhi hukum dan persyaratan peraturan dan kewajiban kontrak?	7. iya PUSTIPD menilai status control internal penyedia layanan external 8. iya bila dilakukan secara prosedur di instansi pemerintah harus patuh dengan kontrak.



Internal Audit Department
COBIT Control Assessment Questionnaire

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
	3	ME2.7 9. Apakah PUSTIPD mengidentifikasi, memulai, melacak, dan menerapkan tindakan perbaikan yang timbul dari penilaian dan pelaporan kontrol?	9. Iya, setelah diaudit, diidentifikasi, baru memperbaiki berkala
Deskripsi ME3: • **ME3** Pastikan Kepatuhan Dengan Persyaratan Eksternal Pengawasan kepatuhan yang efektif membutuhkan pembentukan proses peninjauan untuk memastikan kepatuhan dengan hukum, peraturan dan persyaratan kontrak. Proses ini termasuk mengidentifikasi persyaratan kepatuhan, mengoptimalkan dan mengevaluasi respons, mendapatkan jaminan bahwa persyaratan telah dipenuhi dan, akhirnya, mengintegrasikan pelaporan kepatuhan TI dengan yang lain dari bisnis.. **Detailed Control Objectives ME3:** ME3.1 Identifikasi Persyaratan Kepatuhan Hukum, Peraturan dan Kontraktual Eksternal ME3.2 Optimalisasi Respons terhadap Persyaratan Eksternal ME3.3 Evaluasi Kepatuhan Dengan Persyaratan Eksternal ME3.4 Jaminan Kepatuhan yang Positif ME3.5 Pelaporan Terintegrasi	3	**ME3.1** 1. Apakah PUSTIPD mengidentifikasi secara berkelanjutan hukum nasional dan internasional, peraturan dan persyaratan eksternal lainnya untuk dimasukkan kedalam kebijakan, standar, prosedur, dan metodologi organisasi?	1. Iya kita selalu menyesuaikan, minimal standar nasional ituuan termasuk hukum. Kalau untuk internasional belum bisanya pasti ISO
	3	**ME3.2** 2. Apakah PUSTIPD meninjau dan menyesuaikan kebijakan, standar, prosedur dan metodologi TI untuk memastikan keaslian, pengaturan dan persyaratan kontraktual ditangani dan dikomunikasikan?	2. Iya pustipd meninjau dan menyesuaikan kebijakan, standar prosedur dan metodologi untuk pemastian keaslian, pengaturan dan persyaratan kontrak ditangani dan dikomunikasikan
	3	**ME3.3** 3. Apakah PUSTIPD mengkomunikasikan kepatuhan terhadap kebijakan TI, standar, prosedur, dan metodologi dengan hukum dan peraturan persyaratan?	3. Iya pustipd menyosialisasikan kepatuhan terhadap kebijakan TI, standar, prosedur dan metodologi dengan Hukum dan peraturan dan kontrak
	3	**ME3.4** 4. Bagaimana PUSTIPD memperoleh dan melaporkan jaminan kepatuhan dan kepatuhan terhadap semua kebijakan internal yang berasal dari arahan internal atau hukum eksternal, persyaratan peraturan atau kontrak?	4. Memperolehnya dari survei kebutuhan dan aturan-aturan yang
	2	**ME3.5** 5. Apakah PUSTIPD mengintegrasikan pelaporan TI tentang persyaratan hukum, peraturan, dan kontrak dengan output serupa dari fungsi bisnis lainnya?	5. Iya pustipd berusaha untuk mengintegrasikan pelaporan TI tentang persyaratan hukum, peraturan, dan kontrak dengan output serupa dari lainnya
Deskripsi ME4: • ME4 Menentukan Tata Kelola Menetapkan kerangka kerja tata kelola yang efektif termasuk mendefinisikan struktur organisasi, proses, kepemimpinan, peran dan tanggung jawab untuk	3	**ME4.1** 1. Bagaimana PUSTIPD menentukan menetapkan dan menyelaraskan kerangka tata kelola teknologi informasi dengan tata kelola organisasi secara keseluruhan ? 2. Apakah mengkonfirmasikan bahwa kerangka tata kelola	1. Dengan cara mempertimbangkan stakeholder interest sesuai kebutuhan staf, dan proses-proses yang diikuti 2. Iya pustipd menyesuaikan



Internal Audit Department
COBIT Control Assessment Questionnaire

Detil Kontrol tujuan	Penilaian Kematangan	Penilaian Pertanyaan	Klien Responses & Assessment Hasil
memastikan bahwa perusahaan investasi TI selaras dan disampaikan sesuai dengan strategi dan tujuan perusahaan. **Detailed Control Objectives ME4:** ME4.1 Pembentukan Kerangka Kerja Tata Kelola TI ME4.2 Penyelerasan Strategi ME4.3 Pengiriman Nilai ME4.4 Manajemen Sumber Daya ME4.5 Manajemen Risiko ME4.6 Pengukuran Kinerja ME4.7 Jaminan Independen **Tanda Tangan**	8	teknologi informasi memiliki kepatuahan terhadapa hukum dansejalan dengan peraturan ?	3. Iya pustipd memastikan pemahaman sama antara strategi bisnis dan TI
	3	**ME4.2** 3. Apakah PUSTIPD memastikan pemahaman yang sama antara strategi bisnis dan teknologiinformasi ? 4. Sejauhmana PUSTIPD memperjelaskan peran teknologi informasi dalam mendukung strategi bisnis? 5. Apakah BPUSTIPD memastikan fungsi teknologi informasi dan bisnis dapat saling mendukung ?	4. Untuk penyampaian peran TI dlm mendukung strategi bisnis tidak disampaikan secara langsung, namun staf pustipd memberi tahu sum pentingnya peran TI dalam strategi bisnis, dilihat dari kegiatan dalam optimalisasi peran TI 5. Iya dipastikan
	3	**ME4.3** 6. Apakah PUSTIPD mengelola program investasi teknologi Informasi dan asset juga layanan teknologi informasi yang meyakinkan mempunyai nilai dalam mendukung tujuan dan strategi organisasi (*value delivery*)	6. Iya pustipd mengelola program TI dan aset serta layanan
	3	**ME4.4** 7. Bagaimana PUSTIPD Mengawasi investasi, penggunaan, dan alokasi sumber daya teknologi informasi dalam penyelarasan yang sesuai dengan sasaran strategis teknologi informasi dan bisnis saat ini dan di masa mendatang.	7. Untuk pengawasannya dilakukan monitoring secara berusl, sasaran strategisnya dipantau dan menyesuaikan perkembangan
	1	**ME4.5** 8. Bagaimana PUSTIPD Menentukan risiko teknologi informasi, dan memperoleh jaminan bagi semua pemangku kepentingan manajemen resiko (*risk management*) ?	8. Untuk bagian risiko belum ada atau belum dilakukan proses dokumentasi / perencanaan, namun kedepan dilakukan
	3	**ME4.6** 9. Apakah PUSTIPD dalam Pengukuran kinerja teknologi Informasi mengkonfirmasikan bahwa tujuan TI yang disepakati telah memenuhi harapan ?	9. Iya, tujuan yang disepakati memenuhi harapan
	3	**ME4.7** 10.Apakah PUSTIPD mempunyai jaminan independen (internal atau eksternal) tentang kesesuaian teknologi Informasi dengan kebijakan dan prosedur organisasi ?	10. Iya, karena TI yang ada pada pustipd menyesuaikan ketentuan pengguna

31

Kuesioner Management Awareness

Kuisioner I : *Management Awareness*

Kuesioner ini bertujuan untuk mendapatkan innformasi 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.

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

Untuk mempermudah responden dalam menjawab, maka kuisioner 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 kuesioner 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
Plan and Organize, mencakup proses perencanaan dan penyelarasan Teknologi Informasi (TI) dengan strategi perusahaan sehingga dapat berkontribusi dengan baik untuk organisasi?						
PO4	**Menetapkan proses TI, organisasi, dan hubungan**					
PO4.1	PUSTIPD menentukan kerangka proses TI untuk menjalankan rencana strategis TI					
PO4.2	PUSTIPD membentuk komite strategi TI di tingkat dewan direksi					

Kode	Proses	Seberapa penting tujuan tersebut bagi proses bisnis?				
		Sangat Tidak Penting	Tidak Penting	Sedikit Penting	Penting	Sangat Penting
		1	2	3	4	5

PO4.3	PUSTIPD membentuk komite pengarah TI					
PO4.4	PUSTIPD menempatkan fungsi TI didalam organisasi dalam struktur organisasi secara keseluruhan					
PO4.5	PUSTIPD membentuk struktur organisasi TI internal dan eksternal untuk memenuhi tujuan bisnis yang diharapkan dan mengubah keadaan					
PO4.6	Staff PUSTIPD memiliki tanggung jawab untuk memenuhi kebutuhan organisasi					
PO4.7	PUSTIPD memastikan bahwa organisasi memiliki tanggung jawab untuk jaminan kualitas TI					
PO4.8	PUSTIPD menetapkan peran penting untuk tanggung jawab keamanan informasi dalam mengelola risiko TI					
PO4.9	PUSTIPD melindungi data sesuai dengan tanggung jawab					
PO4.10	PUSTIPD menerapkan pengawasan TI untuk memastikan bahwa peran dan tanggung jawab itu dilakukan dengan benar					
PO4.11	PUSTIPD menerapkan pembagian peran dan tanggung jawab pada pemisahan tugas					
PO4.12	PUSTIPD mengevaluasi kebutuhan staf secara teratur atau pada saat terjadi perubahan besar pada bisnis, operasional, atau lingkungan TI					
PO4.13	PUSTIPD menentukan dan mengidentifikasi personil utama TI, dan meminimalkan ketergantungan kepada satu individu					
PO4.14	PUSTIPD memastikan bahwa para konsultan dan tenanga kontrak yang mendukung fungsi TI mengetahui dan mematuhi kebijakan organisasi					
PO4.15	PUSTIPD membangun dan memelihara koordinasi, komunikasi dan struktur penghubung yang optimal antara fungsi TI dan kepentingan lain dari fungsi TI					
PO6	**Mengkomunikasikan Tujuan dan Arah Manajemen**					
PO6.1	PUSTIPD menetukan unsur-unsur lingkungan pengendalian untuk TI yang sejalan dengan gaya operasional dan filosofi manajemen perusahaan					
PO6.2	PUSTIPD mengembangkan dan mempertahankan kerangka yang menentukan pendekatan keseluruhan perusahaan terhadap pengendalian dan risiko					
PO6.3	PUSTIPD mengembangkan dan memelihara serangkaian kebijakan untuk mendukung strategi TI					

PO6.4	PUSTIPD membangun dan menegakkan kebijakan TI untuk semua staf yang terlibat					

Kode	Proses	Seberapa penting tujuan tersebut bagi proses bisnis?				
		Sangat Tidak Penting	Tidak Penting	Sedikit Penting	Penting	Sangat Penting
		1	2	3	4	5
PO6.5	PUSTIPD mengkomunikasikan kesadaran dan pemahaman mengenai tujuan dan arah bisnis dan TI kepada *stakeholder*					
PO9	**Menilai dan Mengelola Resiko TI**					
PO9.1	PUSTIPD membangun kerangka manajemen risiko TI yang sejalan dengan kerangkan kerja manajemen risiko TI					
PO9.2	PUSTIPD Menilai secara berulang kemungkinan dan dampak dari semua risiko yang diidentifikasi, menggunakan metode kualitatif dan kuantitatif					
PO9.3	PUSTIPD mengembangkan dan mempertahankan proses respons risiko yang dirancang untuk memastikan pengendalian yang hemat biaya memitigasi risiko yang berkelanjutan					
PO9.4	PUSTIPD memprioritaskan dan merencanakan kegiatan pengendalian di semua tingkatan untuk mengimplementasikan respons risiko yang diidentifikasi					
PO9.5	PUSTIPD mengembangkan dan mengelola proses penanggulangan risiko yang dirancang untuk memastikan pengendalian biaya yang efektif untuk memitigasi eksposur risiko secara berkala					
PO9.6	PUSTIPD memprioritaskan dan merencanakan aktivitas pengendalian pada setiap tingkat untuk mengimplementasi penanggulangan risiko yang teridentifikasi					
Delivery and Support, pemenuhan layanan teknologi informasi dan keamanan sistem serta keberlanjutan dari layanan, pelatihan dan pendidikan untuk pengguna serta pemenuhan data yang berjalan?						
DS2	**Mengelola layanan pihak ketiga**					

DS2.1	PUSTIPD memelihara dokumentasi formal teknis dan hubungan organisasi yang meliputi peran dan tanggung jawab					
DS2.2	PUSTIPD menjalin hubungan dengan pelanggan dan supplier serta memastikan kualitas hubungan					
DS2.3	PUSTIPD memastikan bahwa kontrak sesuai dengan standar bisnis dan sesuai dengan persyaratan hukum					
DS2.4	PUSTIPD menetapkan proses untuk memantau penyampaian layanan untuk memastikan kebutuhan supplier terpenuhi dan terus mematuhi perjanjian					
DS4	**Memastikan kelangsungan layanan**					
DS4.1	Kerangka kerja PUSTIPD membahas struktur organisasi untuk kontuinitas TI					
DS4.2	PUSTIPD memiliki rencana kontuinitas TI yang didasarkan pemahaman risiko dan membahas persyaratan pemulihan layanan TI					

Kode	Proses	Seberapa penting tujuan tersebut bagi proses bisnis?				
		Sangat Tidak Penting	Tidak Penting	Sedikit Penting	Penting	Sangat Penting
		1	2	3	4	5
DS4.3	Fokus perhatian TI PUSTIPD dispesifikasikan sebagai yang paling kritis dalam rencana kelangsungan TI					
DS4.4	PUSTIPD mendorong manajemen TI untuk mendefinisikan dan mengeksekusi prosedur kontrol untuk memastikan perkembangan TI					
DS4.5	PUSTIPD menguji rencana kontinuitas TI secara teratur untuk memastikan sistem TI dapat pulih secara efektif					
DS4.6	PUSTIPD menyediakan semua oihak dengan sesi pelatihan reguler mengenai tata cara, peran, dan tanggung jawab terhadap insiden atau bencana					
DS4.7	PUSTIPD mendefinisikan dan mengelola strategi distribusi untuk memastikan kebenaran dan keamanannya					

DS4.8	PUSTIPD melakukan pemulihan dan penerusan layanan TI (meliputi: aktivitas situs cadangan, inisiasi proses alternatif komunikasi pelanggan, dan prosedur penerusan					
DS4.9	PUSTIPD melakukan penyimpanan *offsite* semua *backup* media kritis, dokumentasi dan sumber daya TI					
DS4.10	Manajemen TI PUSTIPD telah menetapkan prosedur untuk menilai kecukupan dari rencana dalam hal penerusan keberhasilan fungsi TI					
DS5	**Memastikan keamanan sistem**					
DS5.1	PUSTIPD mengelolah keamanan TI yang tepat sehingga manajemen keamanan TI sejalan dengan kebutuhan bisnis					
DS5.2	PUSTIPD menerjemahkan kebutuhan bisnis, risiko, dan penyesuaian kedalam rencana kemanan TI secara keseluruhan					
DS5.3	PUSTIPD memastikan semua pengguna dan aktivitas mereka pada sistem TI dapat diidentifikasi secara unik					
DS5.4	PUSTIPD mengalamatkan permintaan, pembuatan, penerbitan, penangguhan modifikasi dan penutupan akun dan hak akses pengguna terkait dengan satu set prosedur manajemen akun pengguna					
DS5.5	PUSTIPD menguji dan memantau pelaksanaan keaman TI dengan proaktif					
DS5.6	PUSTIPD mendefinisikan dan menkomunikasikan karakteristik insiden keamanan yang potensial dengan jelas					

Kode	Proses	Seberapa penting tujuan tersebut bagi proses bisnis?				
		Sangat Tidak Penting	Tidak Penting	Sedikit Penting	Penting	Sangat Penting
		1	2	3	4	5

DS5.7	PUSTIPD membuat teknologi yang berhubungan dengan keamanan yang tahan terhadap gangguan					
DS5.8	PUSTIPD menentukan bahwa ada kebijakan dan prosedur untuk mengatur pembangkitan, perubahan, pencabutan, penghancuran, distribusi,sertifikasi, penyimpanan, pemasukan, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.					
DS5.9	PUSTIPD mencegah, mendeteksi dan menkoreksi *malcious software*					
DS5.10	PUSTIPD menggunakan keamanan jaringan untuk mengotorisasi akses dan kontrol arus informasi					
DS5.11	PUSTIPD melakukan pertukaran data transaksi sensitif hanya melalui jalur dipercaya					
DS11	**Mengelolah data**					
DS11.1	PUSTIPD memverivikasi seluruh data yang dibutuhkan untuk pemrosesan diterima dan diproses secara lengkap, akurat dan berkala					
DS11.2	PUSTIPD mendefinisikan dan mengimplementasikan prosedur penyimpanan data					
DS11.3	PUSTIPD mendefinisikan dan mengimplementasikan prosedur untuk memanajemen pengumpulan media					
DS11.4	PUSTIPD mendefinisikan dan mengimplementasikan prosedur untuk menjamin kebutuhan bisnis					
DS11.5	PUSTIPD mendefinisikan dan mengimplementasikan prosedur untuk proses *backup* dan restorisasi sistem					
DS11.6	PUSTIPD mendefinisikan dan mengimplementasikan aturan dan prosedur intik kebutuhan kemananan manajemen data					
DS12	**Mengelola lingkungan fisik**					
DS12.1	PUSTIPD mendefinisikan dan memilih lokasi peralatan TI untuk mendukung strategi teknologi yang terhubung teknologi bisnis					
DS12.2	PUSTIPD mendefinisikan dan menerapkan secara tegas ukuran keamanan untuk mengamankan lokasi dan aset fisik					

DS12.3	PUSTIPD mendefinisikan dan menerapkan secara tegas prosedur untuk memberikan, membatasi, dan menarik kembali akses fisik					
Kode	Proses	Seberapa penting tujuan tersebut bagi proses bisnis?				
		Sangat Tidak Penting	Tidak Penting	Sedikit Penting	Penting	Sangat Penting
		1	2	3	4	5
DS12.4	PUSTIPD merancang dan mengimplementasian ukuran untuk potensi terhadap faktor lingkungan					
DS12.5	PUSTIPD mengelola fasilitas, meliputi peralatan sumber tenaga dan komunikasi sesuai dengan hukum dan peraturan					
Monitor and Evaluate, fokus pada masalah pengendalian yang menyeluruh, pemeriksaan internal dan eksternal serta jaminan dari independen proses pemeriksan?						
ME2	**Pengawasan dan evaluasi pengaturan internal**					
ME2.1	PUSTIPD melakukan pemantauan kerangka pengendalian internal					
ME2.2	PUSTIPD memantau dan mengevaluasi efisiensi dan efektivitas TI internal kontrol tinjauan manajerial					
ME2.3	PUSTIPD mengidentifikasi kontrol pengecualian, menganalisis dan mengidentifikasi penyebab yang mendasari *root of cause*					
ME2.4	PUSTIPD mengevaluasi kelengkapan dan efektivitas pengendalian manajemen atas proses TI, kebijakan dan kontrak melalui program penilaian diri					
ME2.5	PUSTIPD memperoleh kepastian lebih lanjut akan kelengkapan dan efektivitas pengendalian internal melalui pihak ketiga					
ME2.6	PUSTIPD menilai status kontrol internal penyedia layanan eksternal					
ME2.7	PUSTIPD mengidentifikasi, memulai, melacak dan menerapkan tindakan perbaikan yang timbul dari penilaian pengendalian					
ME3	**Penjaminan kesesuaian dengan kebutuhan eksternal**					
ME3.1	PUSTIPD mengidentifikasi eksternal persyaratan kepatuhan hukum, peraturan dan kontrak					
ME3.2	PUSTIPD meninjau dan menyesuaikan TI kebijakan, standar, prosedur dan metodelogi untuk memastikan hukum, peraturan dan kontrak					

ME3.3	PUSTIPD melakukan konfirmasi kepatuhan TI kebijakan, standar, prosedur dan metodelogi dengan persyaratan hukum dan peraturan					
ME3.4	PUSTIPD mendapatkan dan melaporakan jaminan kepatuhan dan kepatuhan terhadap semua kebijakan internal berasal dari arahan internal atau eksternal hukum					
ME3.5	PUSTIPD mengintegrasikan TI melaporkan persyaratan hukum, peraturan dan kontrak dengan output yang sama dari fungsi bisnis					
ME4	**Menyediakan *IT Governance***					
ME4.1	PUSTIPD mendefinisikan, membangun dan menyelaraskan kerangka tata kelola TI dengan tata kelola perusahaan					

Kode	Proses	Seberapa penting tujuan tersebut bagi proses bisnis?				
		Sangat Tidak Penting	Tidak Penting	Sedikit Penting	Penting	Sangat Penting
		1	2	3	4	5
ME4.2	PUSTIPD memastikan bahwa ada pemeahaman antara bisnis dan TI tentang potensi kontribusi					
ME4.3	PUSTIPD mengelola program investasi *IT-enabled* dan aset TI dan layanan untuk memastikan bahwa mereka memberikan nilai terbesar					
ME4.4	PUSTIPD mengawasi investasi, penggunaan dan alokasi sumber daya TI untuk memastikan sumber daya sejalan dengan tujuan strategis					
ME4.5	PUSTIPD memanajemen risiko tanggung jawab ke dalam organisasi, memastikan bahwa bisnis dan TI secara teratur menilai dan melaporkan berkaitan dengan risiko TI					
ME4.6	PUSTIPD mengkonfirmasi bahwa tujuan TI telah memenuhi harapan					
ME4.7	PUSTIPD memperoleh keyakinan independen tentang kesesuaian TI dengan hukum dan peraturan					

Kuesioner Maturity Level

Kuisioner 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.

Kuisioner *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 kuisioner 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 *ad-hoc* 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 distandarisasikan dan didokumentasikan
4 – Proses dikelola dan terukur	Pihak manajemen mengawasi dan mengukur kepatuhan terhadap prosedur
5 – Proses ioptimalkan	Proses yang distandarkan selalu mengalami upaya 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**
Plan and Organize, mencakup proses perencanaan dan penyelarasan Teknologi Informasi (TI) dengan strategi perusahaan sehingga dapat berkontribusi dengan baik untuk organisasi?							
PO4	**Menetapkan proses TI, organisasi, dan hubungan**						
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**
PO4.1	PUSTIPD menentukan kerangka proses TI untuk menjalankan rencana strategis TI						
PO4.2	PUSTIPD membentuk komite strategi TI di tingkat dewan direksi						
PO4.3	PUSTIPD membentuk komite pengarah TI						
PO4.4	PUSTIPD menempatkan fungsi TI didalam organisasi dalam struktur organisasi secara keseluruhan						

PO4.5	PUSTIPD membentuk struktur organisasi TI internal dan eksternal untuk memenuhi tujuan bisnis yang diharapkan dan mengubah keadaan						
PO4.6	Staff PUSTIPD memiliki tanggung jawab untuk memenuhi kebutuhan organisasi						
PO4.7	PUSTIPD memastikan bahwa organisasi memiliki tanggung jawab untuk jaminan kualitas TI						
PO4.8	PUSTIPD menetapkan peran penting untuk tanggung jawab keamanan informasi dalam mengelola risiko TI						
PO4.9	PUSTIPD melindungi data sesuai dengan tanggung jawab						
PO4.10	PUSTIPD menerapkan pengawasan TI untuk memastikan bahwa peran dan tanggung jawab itu dilakukan dengan benar						
PO4.11	PUSTIPD menerapkan pembagian peran dan tanggung jawab pada pemisahan tugas						
PO4.12	PUSTIPD mengevaluasi kebutuhan staf secara teratur atau pada saat terjadi perubahan besar pada bisnis, operasional, atau lingkungan TI						
PO4.13	PUSTIPD menentukan dan mengidentifikasi personil utama TI, dan meminimalkan ketergantungan kepada satu individu						
PO4.14	PUSTIPD memastikan bahwa para konsultan dan tenanga kontrak yang mendukung fungsi TI mengetahui dan mematuhi kebijakan organisasi						
PO4.15	PUSTIPD membangun dan memelihara koordinasi, komunikasi dan struktur penghubung yang optimal antara fungsi TI dan kepentingan lain dari fungsi TI						
PO6	**Mengkomunikasikan Tujuan dan Arah Manajemen**						
PO6.1	PUSTIPD menetukan unsur-unsur lingkungan pengendalian untuk TI yang sejalan dengan gaya operasional dan filosofi manajemen perusahaan						

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**
PO6.2	PUSTIPD mengembangkan dan mempertahankan kerangka yang menentukan pendekatan keseluruhan perusahaan terhadap pengendalian dan risiko						
PO6.3	PUSTIPD mengembangkan dan memelihara serangkaian kebijakan untuk mendukung strategi TI						
PO6.4	PUSTIPD membangun dan menegakkan kebijakan TI untuk semua staf yang terlibat						
PO6.5	PUSTIPD mengkomunikasikan kesadaran dan pemahaman mengenai tujuan dan arah bisnis dan TI kepada *stakeholder*						
PO9	**Menilai dan Mengelola Resiko TI**						
PO9.1	PUSTIPD membangun kerangka manajemen risiko TI yang sejalan dengan kerangkan kerja manajemen risiko TI						
PO9.2	PUSTIPD Menilai secara berulang kemungkinan dan dampak dari semua risiko yang diidentifikasi, menggunakan metode kualitatif dan kuantitatif						
PO9.3	PUSTIPD mengembangkan dan mempertahankan proses respons risiko yang dirancang untuk memastikan pengendalian yang hemat biaya memitigasi risiko yang berkelanjutan						
PO9.4	PUSTIPD memprioritaskan dan merencanakan kegiatan pengendalian di semua tingkatan untuk mengimplementasikan respons risiko yang diidentifikasi						
PO9.5	PUSTIPD mengembangkan dan mengelola proses penanggulangan risiko yang dirancang untuk memastikan pengendalian biaya yang efektif untuk memitigasi eksposur risiko secara berkala						

PO9.6	PUSTIPD memprioritaskan dan merencanakan aktivitas pengendalian pada setiap tingkat untuk mengimplementasi penanggulangan risiko yang teridentifikasi						
Delivery and Support, pemenuhan layanan teknologi informasi dan keamanan sistem serta keberlanjutan dari layanan, pelatihan dan pendidikan untuk pengguna serta pemenuhan data yang berjalan?							
DS2	**Mengelola layanan pihak ketiga**						
DS2.1	PUSTIPD memelihara dokumentasi formal teknis dan hubungan organisasi yang meliputi peran dan tanggung jawab						
DS2.2	PUSTIPD menjalin hubungan dengan pelanggan dan supplier serta memastikan kualitas hubungan						
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**
DS2.3	PUSTIPD memastikan bahwa kontrak sesuai dengan standar bisnis dan sesuai dengan persyaratan hukum						
DS2.4	PUSTIPD menetapkan proses untuk memantau penyampaian layanan untuk memastikan kebutuhan supplier terpenuhi dan terus mematuhi perjanjian						
DS4	**Memastikan kelangsungan layanan**						
DS4.1	kerangka kerja PUSTIPD membahas struktur organisasi untuk kontuinitas TI						
DS4.2	PUSTIPD memiliki rencana kontuinitas TI yang didasarkan pemahaman risiko dan membahas persyaratan pemulihan layanan TI						
DS4.3	Fokus perhatian TI PUSTIPD dispesifikasikan sebagai yang paling kritis dalam rencana kelangsungan TI						
DS4.4	PUSTIPD mendorong manajemen TI untuk mendefinisikan dan mengeksekusi prosedur kontrol untuk memastikan perkembangan TI						

DS4.5	PUSTIPD menguji rencana kontinuitas TI secara teratur untuk memastikan sistem TI dapat pulih secara efektif						
DS4.6	PUSTIPD menyediakan semua oihak dengan sesi pelatihan reguler mengenai tata cara, peran, dan tanggung jawab terhadap insiden atau bencana						
DS4.7	PUSTIPD mendefinisikan dan mengelola strategi distribusi untuk memastikan kebenaran dan keamanannya						
DS4.8	PUSTIPD melakukan pemulihan dan penerusan layanan TI (meliputi: aktivitas situs cadangan, inisiasi proses alternatif komunikasi pelanggan, dan prosedur penerusan						
DS4.9	PUSTIPD melakukan penyimpanan *offsite* semua *backup* media kritis, dokumentasi dan sumber daya TI						
DS4.10	Manajemen TI PUSTIPD telah menetapkan prosedur untuk menilai kecukupan dari rencana dalam hal penerusan keberhasilan fungsi TI						
DS5	**Memastikan keamanan sistem**						
DS5.1	PUSTIPD mengelolah keamanan TI yang tepat sehingga manajemen keamanan TI sejalan dengan kebutuhan bisnis						
DS5.2	PUSTIPD menerjemahkan kebutuhan bisnis, risiko, dan penyesuaian kedalam rencana kemanan TI secara keseluruhan						

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**
DS5.3	PUSTIPD memastikan semua pengguna dan aktivitas mereka pada sistem TI dapat diidentifikasi secara unik						

DS5.4	PUSTIPD mengalamatkan permintaan, pembuatan, penerbitan, penangguhan modifikasi dan penutupan akun dan hak akses pengguna terkait dengan satu set prosedur manajemen akun pengguna						
DS5.5	PUSTIPD menguji dan memantau pelaksanaan keamanan TI dengan proaktif						
DS5.6	PUSTIPD mendefinisikan dan menkomunikasikan karakteristik insiden keamanan yang potensial dengan jelas						
DS5.7	PUSTIPD membuat teknologi yang berhubungan dengan keamanan yang tahan terhadap gangguan						
DS5.8	PUSTIPD menentukan bahwa ada kebijakan dan prosedur untuk mengatur pembangkitan, perubahan, pencabutan, penghancuran, distribusi,sertifikasi, penyimpanan, pemasukan, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.						
DS5.9	PUSTIPD mencegah, mendeteksi dan menkoreksi *malcious software*						
DS5.10	PUSTIPD menggunakan keamanan jaringan untuk mengotorisasi akses dan kontrol arus informasi						
DS5.11	PUSTIPD melakukan pertukaran data transaksi sensitif hanya melalui jalur dipercaya						
DS11	**Mengelolah data**						
DS11.1	PUSTIPD memverivikasi seluruh data yang dibutuhkan untuk pemrosesan diterima dan diproses secara lengkap, akurat dan berkala						
DS11.2	PUSTIPD mendefinisikan dan mengimplementasikan prosedur penyimpanan data						
DS11.3	PUSTIPD mendefinisikan dan mengimplementasikan prosedur untuk memanajemen pengumpulan media						
DS11.4	PUSTIPD mendefinisikan dan mengimplementasikan prosedur untuk menjamin kebutuhan bisnis						
DS11.5	PUSTIPD mendefinisikan dan mengimplementasikan prosedur untuk proses *backup* dan restorisasi sistem						

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**
DS11.6	PUSTIPD mendefinisikan dan mengimplementasikan aturan dan prosedur intik kebutuhan kemananan manajemen data						
DS12	**Mengelola lingkungan fisik**						
DS12.1	PUSTIPD mendefinisikan dan memilih lokasi peralatan TI untuk mendukung strategi teknologi yang terhubung teknologi bisnis						
DS12.2	PUSTIPD mendefinisikan dan menerapkan secara tegas ukuran keamanan untuk mengamankan lokasi dan aset fisik						
DS12.3	PUSTIPD mendefinisikan dan menerapkan secara tegas prosedur untuk memberikan, membatasi, dan menarik kembali akses fisik						
DS12.4	PUSTIPD merancang dan mengimplementasian ukuran untuk potensi terhadap faktor lingkungan						
DS12.5	PUSTIPD mengelola fasilitas, meliputi peralatan sumber tenaga dan komunikasi sesuai dengan hukum dan peraturan						
Monitor and Evaluate, fokus pada masalah pengendalian yang menyeluruh, pemeriksaan internal dan eksternal serta jaminan dari independen proses pemeriksan?							
ME2	**Pengawasan dan evaluasi pengaturan internal**						
ME2.1	PUSTIPD melakukan pemantauan kerangka pengendalian internal						
ME2.2	PUSTIPD memantau dan mengevaluasi efisiensi dan efektivitas TI internal kontrol tinjauan manajerial						

ME2.3	PUSTIPD mengidentifikasi kontrol pengecualian, menganalisis dan mengidentifikasi penyebab yang mendasari *root of cause*						
ME2.4	PUSTIPD mengevaluasi kelengkapan dan efektivitas pengendalian manajemen atas proses TI, kebijakan dan kontrak melalui program penilaian diri						
ME2.5	PUSTIPD memperoleh kepastian lebih lanjut akan kelengkapan dan efektivitas pengendalian internal melalui pihak ketiga						
ME2.6	PUSTIPD menilai status kontrol internal penyedia layanan eksternal						
ME2.7	PUSTIPD mengidentifikasi, memulai, melacak dan menerapkan tindakan perbaikan yang timbul dari penilaian pengendalian						
ME3	**Penjaminan kesesuaian dengan kebutuhan eksternal**						
ME3.1	PUSTIPD mengidentifikasi eksternal persyaratan kepatuhan hukum, peraturan dan kontrak						
ME3.2	PUSTIPD meninjau dan menyesuaikan TI kebijakan, standar, prosedur dan metodelogi untuk memastikan hukum, peraturan dan kontrak						
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**
ME3.3	PUSTIPD melakukan konfirmasi kepatuhan TI kebijakan, standar, prosedur dan metodelogi dengan persyaratan hukum dan peraturan						
ME3.4	PUSTIPD mendapatkan dan melaporakan jaminan kepatuhan dan kepatuhan terhadap semua kebijakan internal berasal dari arahan internal atau eksternal hukum						
ME3.5	PUSTIPD mengintegrasikan TI melaporkan persyaratan hukum, peraturan dan kontrak dengan output yang sama dari fungsi bisnis						
ME4	**Menyediakan *IT Governance***						

ME4.1	PUSTIPD mendefinisikan, membangun dan menyelaraskan kerangka tata kelola TI dengan tata kelola perusahaan						
ME4.2	PUSTIPD memastikan bahwa ada pemeahaman antara bisnis dan TI tentang potensi kontribusi						
ME4.3	PUSTIPD mengelola program investasi *IT-enabled* dan aset TI dan layanan untuk memastikan bahwa mereka memberikan nilai terbesar						
ME4.4	PUSTIPD mengawasi investasi, penggunaan dan alokasi sumber daya TI untuk memastikan sumber daya sejalan dengan tujuan strategis						
ME4.5	PUSTIPD memanajemen risiko tanggung jawab ke dalam organisasi, memastikan bahwa bisnis dan TI secara teratur menilai dan melaporkan berkaitan dengan risiko TI						
ME4.6	PUSTIPD mengkonfirmasi bahwa tujuan TI telah memenuhi harapan						
ME4.7	PUSTIPD memperoleh keyakinan independen tentang kesesuaian TI dengan hukum dan peraturan						

Rekapitulasi Jawaban Audit

Rekaitulasi Jawaban Responden PO4

Responden	Jumlah Pernyataan															Total
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1	3	4	3	2	3	3	4	4	3	3	4	4	3	4	3	50

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

Indeks =$\frac{50}{15\ x\ 1}$

Indeks =$\frac{50}{15}$ = 3,5

Maka hasil perhitungan maturity level nilai dari subdomain *Define the IT Processses, Organization and Relationships* yaitu 3,33

Rekaitulasi Jawaban Responden PO6

Responden	Jumlah Pernyataan					Total
	1	2	3	4	5	
1	4	3	4	3	4	18

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

Indeks =$\frac{18}{5\ x\ 1}$

Indeks =$\frac{18}{5}$ = 3,6

Maka hasil perhitungan maturity level nilai dari subdomain *Communicate Management Aims and Direction* yaitu 3,6.

Rekaitulasi Jawaban Responden PO9

Responden	Jumlah Pernyataan						Total
	1	2	3	4	5	6	
1	0	1	2	1	1	3	8

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

Indeks =$\frac{8}{6\ x\ 1}$

Indeks =$\frac{8}{6}$ = 1,33

Maka hasil perhitungan maturity level nilai dari subdomain *Assess and Manage IT Risk* yaitu 1,33.

Rekaitulasi Jawaban Responden DS2

Responden	Jumlah Pernyataan				Total
	1	2	3	4	
1	2	4	4	3	13

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

Indeks =$\frac{13}{4\ x\ 1}$

Indeks =$\frac{13}{4}$ = 3,25

Maka hasil perhitungan maturity level nilai dari subdomain *Manage Third-party Services* yaitu 3,25.

Rekaitulasi Jawaban Responden DS4

Responden	Jumlah Pernyataan										Total
	1	2	3	4	5	6	7	8	9	10	
1	3	4	3	3	3	1	0	1	2	1	21

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

Indeks =$\frac{21}{10\ x\ 1}$

Indeks =$\frac{21}{10}$ = 2,1

Maka hasil perhitungan maturity level nilai dari subdomain *Ensure Continuous Service* yaitu 2,1.

Rekaitulasi Jawaban Responden DS5

Responden	Jumlah Pernyataan											Total
	1	2	3	4	5	6	7	8	9	10	11	
1	0	1	3	2	2	1	1	1	3	3	1	18

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

Indeks =$\frac{18}{11\ x\ 1}$

Indeks =$\frac{18}{11}$ = 1,64

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

Rekaitulasi Jawaban Responden DS11

Responden	Jumlah Pernyataan						Total
	1	2	3	4	5	6	
1	1	4	3	3	3	4	18

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

Indeks =$\frac{18}{6\ x\ 1}$

Indeks =$\frac{18}{6}$ = 3

Maka hasil perhitungan maturity level nilai dari subdomain *Manage Data* yaitu 3.

Rekaitulasi Jawaban Responden DS12

Responden	Jumlah Pernyataan					Total
	1	2	3	4	5	
1	3	1	3	2	3	12

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

Indeks = $\frac{12}{5\ x\ 1}$

Indeks = $\frac{12}{5}$ = 2,4

Maka hasil perhitungan maturity level nilai dari subdomain *Manage the Physical Environment* yaitu 2,4.

Rekaitulasi Jawaban Responden ME2

Responden	Jumlah Pernyataan							Total
	1	2	3	4	5	6	7	
1	3	3	3	3	3	3	3	21

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

Indeks = $\frac{21}{7\ x\ 1}$

Indeks = $\frac{21}{7}$ = 3

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

Rekaitulasi Jawaban Responden ME3

Responden	Jumlah Pernyataan					Total
	1	2	3	4	5	
1	3	3	3	3	2	14

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

Indeks =$\frac{14}{5\ x\ 1}$

Indeks =$\frac{14}{5}$ = 2,8

Maka hasil perhitungan maturity level nilai dari subdomain *Ensure Compliance With External Requirements* yaitu 2,8.

Rekaitulasi Jawaban Responden ME4

Responden	Jumlah Pernyataan							Total
	1	2	3	4	5	6	7	
1	3	3	3	3	1	3	3	19

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

Indeks =$\frac{19}{7\ x\ 1}$

Indeks =$\frac{19}{7}$ = 2,71

Maka hasil perhitungan maturity level nilai dari subdomain *Provide IT Governance* yaitu 2,71.

Hasil Analisis SWOT

Kondisi Internal PUSTIPD (*Strenght or Weakness*)
***Strenght* (Kekuatan)**
- PUSTIPD memiliki sistem berkualitas yang digunakan sebagai alat bantu pendukung pengambilan keputusan - PUSTIPD mengutamakan kualitas SDM - PUSTIPD memiliki struktur organisasi yang memperhatikan spesialisasi, koordinasi, mekanisme pengambilan keputusan - Fasilitas fisik TI sudah lengkap (seperti: Server, subsistem penyimpanan, perangkat jaringan (switch, router, dan kabel fisik), peralatan khusus seperti jaringan firewall. - PUSTIPD selalu melakukan update aplikasi sesuai kebutuhan dari keluhan-keluhan user - Teknologi PUSTIPD sudah lengkap - Sistem dibangun oleh developer internal
***Weakness* (Kekurangan)**
- Koordinasi masih konvensional - Sistem belum terhubung secara keseluruhan - PUSTIPD belum memiliki proses *planning, organizing, actuating,* dan *controlling* yang baik - Belum melakukan riset sejak tahun 2010, pengembangan sistem dilakukan namun tidak tentu jangka waktunya, bisa 1x setahun. - Kurangnya dokumentasi pada pengolaan risiko - Belum ada blueprint database, jaringan dll. Sehingga pada saat pengembangan sistem kedepan harus melakukan perombakan ulang - Jumlah alat terbatas dibanding dengan perguruan tinggi lain di Palembang - Data server mash central, tidak ada backup
Kondisi Eksternal PUSTIPD *(Opportunities or Thread)*
***Opportunities* (Peluang)**
- Regulasi pemerintah, menjadi inovasi teknologi - Adopsi teknologi informasi baru, meningkatkan kualitas produk - Permintaan/kebijakan fakultas, sebagai acuan pengembangan sistem
***Thread* (Ancaman)**
- Serangan Hacker - Adopsi teknologi membutuhkan banyak anggaran

Detail Control Objective Fokus Area Utama Manajemen Risiko

Plan and Organize		
PO4	**Menetapkan Proses TI, Organisasi, dan Hubungan**	
PO4.1	Kerangka Proses TI	Menentukan kerangka proses TI untuk menjalankan rencana strategis TI. Kerangka ini harus meliputi struktur proses TI, kepemilikan, pengukuran kinerja, perbaikan, kepatuhan, target kualitas, dan rencana untuk menncapainya.
PO4.2	Komite Strategi TI	Membentuk komite strategi TI di tingkat dewan direksi. Komite ini harus memastikan bahwa tata kelola TI berjalan dengan baik, memberikan saran tentang arah strategi, dan mengkaji investasi besar atas nama direksi.
PO4.3	Komite Pengarah TI	Membentuk komite pengarah TI yang terdiri dari eksekutif, manajemenn bisnis dan TI untuk: - Menentukan prioritas investasi TI yang sejalan dengan strategi bisnis dan prioritas perusahaan. - Melacak status proyek dan menyelesaikan masalah yang berhubungan dengan sumber daya. - Memantau tingkat layanan dan meningkatkan kualitas layanan.
PO4.4	Penempatan Fungsi TI di dalam Organisasi	Menempatkan fungsi TI didalam struktur organisasi secara keselluruhan dengan menggunakan model bisnis yang mengutamakan pentingnya TI dalam perusahaan, khususnya untuk strategi bisnis dan tingkat ketergantungan operasional pada TI.
PO4.7	Tanggung Jawab untuk Penjaminan Kualitas TI	Menetapkan tanggung jawab untuk kinerja fungsi QA dan menyediakan kelompok QA yang sesuai dengan sistem, kontrol, dan keahlian komunikasi.
PO4.8	Tanggung Jawab untuk Risko, Keamanan, dan Kepatuhan	Menanamkan kepemilikan dan tanggung jawab terhadap risiko-risiko yang berhubungan dengan TI didalam bisnis. Menentukan dan menetapkan peran penting untuk mengelola risiko-risiko yang berhubungan dengan TI, termasuk tanggung jawab khusus untuk keamanan informasi, keamanan fisik, dan kepatuhan.
PO4.9	Kepemilikan Sistem dan Data	Menyediakan prosedur dan perangkan didalam bisnis untuk membantu memenuhi tanggung jawabnya terhadap kepemilikan data dan sistem informasi. Pemilik harus membuat keputusan tentang mengklarifikasikan sistem dan informasi dan melindunginya sesuai dengan klarifikasi tersebut.
PO4.10	Pengawasan	Menerapkan praktik-praktik pengawasan yang ketat didalam fungsi TI untuk memastikan bahwa peran dan tanggung jawab dilaksanakan dengan benar, untuk menilai apakah semua personil memiliki kewenangan dan sumber daya yang cukup untuk melaksanakan peran dan tanggung jawab mereka, dan untuk meninjau kinerja mereka.
PO4.12	Staf TI	Mengevaluasi kebutuhan staf secara teratur atau pada saat terjadi perubahan besar pada bisnis, operasional, atau lingkungan TI, untuk memastikan bahwa fungsi TI memiliki sumber daya yang cukup untuk mendukung tujuan bisnis.
PO4.13	Personil Utama TI	Menentukan dan mengidentifikasi personil utama TI, dan meminimalkan ketergantungan kepada

		satu individu yang melakukan pekerjaan yang sangat penting.
PO4.14	Kontrak Prosedur dan Kebijakan Staf	Memastikan bahwa para konsultan dan tenanga kontrak yang mendukung fungsi TI mengetahui dan mematuhi kebijakan organisasi untuk perlindungan aset informasi organissi sehingga mereka memenuhi persyaratakn yang disepakati kontrak.
PO4.15	Hubungan	Membangun dan mempertahankan struktur koordinasi, komunikasi, dan struktur perhubungan diantara fungsi dan berbagai kepentingan lain didalam dan diluar fungsi TI, seperti dewan, eksekutif, unit bisnis, pengguna individu, pemasok, petugas keamanan, manajer risiko, kelompok kepatuhan perusahaan, agen *outsourcing* dan manajemen luar kantor.
PO6	**Mengkomunikasikan Tujuan dan Arah Manajemen**	
PO6.2	Kerangka Pengendalian dan Risiko TI Perusahaan	Mengembangkan dan mempertahankan kerangka yang menentukan pendekatan keseluruhan perusahaan terhadap pengendalian dan risiko TI dan yang sejalan dengan kebijakan TI dan lingkungan pengendalian dan risko perusahaan dan kerangka pengendalian.
PO6.3	Mengelola Kebijakan TI	Mengembangkan dna memelihara serangkaian kebijakan untuk mendukung strategi TI. Kebijakan ini harus mencakup tujuan kebijakan, peran, dan tanggung jawab, proses pengecualian, pendekatan kepatuhan, referensi dengan prosedur, standar dan pedoman.
PO6.4	Meluncurkan Kebijakan, Standar, dan Prosedur	Membangun dan menegakkan kebijakan TI untuk semua staf yang terlibat, sehingga mereka semua menjadi satu bagian dengan operasi perusahaan.
PO6.5	Mengkomunikasikan Tujuan dan Arah TI	Mengkomunikasikan kesadaran dan pemahaman mengenai tujuan dan arah bisnis dan TI kepada para *stakeholder* yang sesuai dan pengguna di seluruh perusahaan.
PO9	**Menilai dan Mengelola Risiko TI**	
PO9.1	Kerangka Kerja Manajemen Risiko TI	Menetapkan kerangka kerja manajemen risiko TI yang selaras dengan kerangka kerja manajemen risiko organisasi (perusahaan).
PO9.2	Pembentukan Konteks Risiko	Tetapkan konteks dimana kerangka kerja penilaian risiko diterapkan untuk memastikan hasil yang sesuai. Ini harus mencakup menentukan konteks internal dan eksternal dari setiap penilaian risiko, tujuan penilaian, dan kriteria terhadap risiko yang mana dievaluasi.
PO9.3	Identifikasi Peristiwa	Identifikasi peristiwa (ancaman realistis penting yang mengeksploitasi kerentanan signifikan yang berlaku) dengan potensi dampak negatif pada tujuan atau operasi perusahaan, termasuk bisnis, peraturan, hukum, teknologi, mitra dagang, sumber daya manusia dan aspek operasional. Tentukan dampak dan pertahankan informasi ini. Catat dan pertahankan risiko yang relevan dalam risiko registrasi.
PO9.4	Penilaian Risiko	Menilai secara berulang kemungkinan dan dampak dari semua risiko yang diidentifikasi, menggunakan metode kualitatif dan kuantitatif. Itu kemungkinan dan dampak yang terkait dengan risiko inheren dan residual harus ditentukan secara individual, berdasarkan kategori dan portofolio dasar.

PO9.5	Respon Risiko	Kembangkan dan pertahankan proses respons risiko yang dirancang untuk memastikan bahwa pengendalian yang hemat biaya memitigasi risiko terhadap a dasar berkelanjutan. Proses respons risiko harus mengidentifikasi strategi risiko seperti penghindaran, pengurangan, pembagian atau penerimaan; menentukan tanggung jawab terkait; dan mempertimbangkan tingkat toleransi risiko.
PO9.6	Pemeliharaan dan Pemantauan Rencana Tindakan Risiko	Prioritaskan dan rencanakan kegiatan pengendalian di semua tingkatan untuk mengimplementasikan respons risiko yang diidentifikasi perlu, termasuk identifikasi biaya, manfaat dan tanggung jawab untuk pelaksanaan. Dapatkan persetujuan untuk tindakan yang direkomendasikan dan penerimaan risiko residual, dan memastikan bahwa tindakan yang dilakukan dimiliki oleh pemilik proses yang terkena dampak. Pantau pelaksanaan rencana, dan laporkan penyimpangan ke manajemen senior.

Deliver and Support		
DS2	**Mengelola layanan pihak ketiga**	
DS2.1	Mengidentifikasi hubungan semua pemasok	Memelihara dokumentasi formal teknis dan hubungan organisasi yang meliputi peran dan tanggung jawab, tujuan, penyampaian, yang diharapkan, dan mandat dari wakil-wakil pemasok.
DS2.2	Manajemen hubungan pemasok	Pemilik hubungan harus menjalin hubungan pada isu pelanggan dan supplier serta memastikan kualitas hubungan berdasarkan kepercayaan dan transparansi.
DS2.3	Manajemen risiko pemasok	Salah satu yang harus dilakukan adalah memastikan bahwa kontrak sesuai dengan standar bisnis yang universal dan sesuai dengan persyaratan hukum dan peraturan.
DS2.4	Pemantauan risiko pemasok	Menetapkan proses untuk memantau penyampaian layanan untuk memastikan bahwa kebutuhan bisni supplier saat ini terpenuhi dan terus mematuhi perjanjian kontrak dan SLA, dan kinerja yang kompetitif dengan suplier alternatif dan kondisi pasar.
DS4	**Memastikan Kelangsungan Layanan**	
DS4.1	Kerangka Kerja Kontunitas TI	Kerangka kerja ini harus membahas struktur organisasi untuk manajemen kontinuitas, yang meliputi peran, tugas dan tanggung jawab penyedia layanan internal dan eksternal, manajemen mereka dan pelanggan mereka, dan proses perencanaan yang menciptakan aturan dan struktur untuk dokumen, pengujian dan melaksanakan pemulihan bencana TI dan rencana kontingensi.
DS4.2	Rencana Kontinuitas TI	Rencana harus didasarkan pada pemahaman risiko potensi dampak bisnis dan membahas persyaratan untuk ketahanan, pengolahan alternatif dan kemampuan pemulihan dari semua layanan TI kritis.
DS4.3	Sumber Daya TI Kritis	Fokuskan perhatian pada bagian TI yang dispesifikasikan sebagai yang paling kritis dalam

		rencana kelangsungan TI untuk membangun ketahanan dan menetapkan prioritas dalam situasi pemulihan.
DS4.4	Pemeliharaan Rencana Kontinuitas TI	Mendorong manajemen TI untuk mendefinisikan dan mengeksekusi prosedur kontrol perubahan untuk memastikan bahwa rencana kontinuitas TI terus berkembang dan mencerminkan kebutuhan bisnis yang sebenarnya secara terus-menerus.
DS4.5	Pengujian Rencana Kontinuitas TI	Menguji rencana kontinuitas TI secara teratur untuk memastikan bahwa sistem TI dapat pulih secara efektif, menangani kekurangan dan menjaga rencana tetap relevan.
DS4.6	Pelatihan Rencana Kontinuitas TI	Menyediakan semua pihak terkait dengan sesi pelatihan reguler mengenai tata cara serta peran dan tanggung jawab mereka jika terjadi insiden atau bencana.
DS4.7	Distribusi Rencana Kontinuitas TI	Tentukan bahwa adanya pendefinisian dan pengelolaan strategi distribusi untuk memastikan bahwa rencana didistribusikan dengan benar dan aman serta tersedia bagi pihak berwenang yang berkepentingan, kapan dan dimana diperlukan.
DS4.8	Pemulihan dan Penerusan Layanan TI	Hal ini termasuk aktivasi dari situs cadangan, intisiasi proses alternatif, komunikasi pelanggan dan *stakeholder,* dan prosedur penerusan.
DS4.10	Paska-Penerusan Ulasan	Tentukan apakah manajemen TI telah menetapkan prosedur untuk menilai kecukupan dari rencana dalam hal penerusan keberhasilan fungsi TI setelah bencana, dan memperbarui rencana yang sesuai.
DS5	**Memastikan keamanan sistem**	
DS5.1	Manajemen Keamanan TI	Kelola keamanan TI pada tingkat organisasi tertinggi yang sesuai, sehingga pengelolaan tindakan keamanan sejalan dengan persyaratan bisnis.
DS5.2	Rencana Keamanan TI	Menerjemahkan persyaratan bisnis, risiko, dan kepatuhan ke dalam keseluruhan rencana keamanan TI, dengan mempertimbangkan infrastruktur TI dan budaya keamanan. Pastikan bahwa rencana tersebut diimplementasikan dalam kebijakan dan prosedur keamanan bersama dengan yang sesuai investasi dalam layanan, personel, perangkat lunak, dan perangkat keras. Mengkomunikasikan kebijakan dan prosedur keamanan kepada para pemangku kepentingan dan pengguna.
DS5.3	Manajemen Identitas	Pastikan bahwa semua pengguna (internal, eksternal dan sementara) dan aktivitas mereka pada sistem TI (aplikasi bisnis, lingkungan TI, operasi sistem, pengembangan dan pemeliharaan) dapat diidentifikasi secara unik. Aktifkan identitas pengguna melalui mekanisme otentikasi. Konfirmasikan bahwa hak akses pengguna ke sistem dan data sejalan dengan kebutuhan bisnis yang ditentukan dan didokumentasikan serta pekerjaan itu persyaratan terlampir pada identitas pengguna. Pastikan bahwa hak akses pengguna diminta oleh manajemen pengguna, disetujui oleh sistem pemilik dan dilaksanakan oleh orang yang bertanggung jawab keamanan. Pertahankan identitas pengguna dan hak akses dalam repositori pusat. Menyebarkan langkah-langkah teknis dan prosedural yang hemat biaya, dan menjaga mereka

		tetap terkini untuk membangun identifikasi pengguna, mengimplementasikan otentikasi dan menegakkan hak akses.
DS5.4	Manajemen Akun Pengguna	Alamat yang meminta, membuat, menerbitkan, menangguhkan, memodifikasi, dan menutup akun pengguna dan hak istimewa pengguna terkait dengan serangkaian prosedur manajemen akun pengguna. Sertakan prosedur persetujuan yang menjabarkan data atau pemilik sistem yang memberikan akses hak istimewa. Prosedur ini harus berlaku untuk semua pengguna, termasuk administrator (pengguna istimewa) dan pengguna internal dan eksternal, untuk kasus normal dan darurat. Hak dan kewajiban relatif terhadap akses ke sistem dan informasi perusahaan seharusnya diatur secara kontrak untuk semua jenis pengguna. Lakukan tinjauan manajemen secara teratur terhadap semua akun dan hak istimewa terkait.
DS5.5	Pengujian Keamanan, Pengawasan dan Pemantauan	Menguji dan memantau implementasi keamanan TI secara proaktif. Keamanan TI harus diakreditasi ulang secara tepat waktu untuk memastikan bahwa garis dasar keamanan informasi perusahaan yang disetujui dipertahankan. Fungsi logging dan pemantauan akan memungkinkan awal pencegahan dan / atau deteksi dan pelaporan tepat waktu berikutnya dari kegiatan tidak biasa dan / atau abnormal yang mungkin perlu ditangani.
DS5.6	Definisi Insiden Keamanan	Mendefinisikan dan mengkomunikasikan karakteristik insiden keamanan potensial dengan jelas sehingga dapat diklasifikasikan dengan benar dan ditangani oleh insiden dan proses manajemen masalah.
DS5.8	Manajemen Kunci Kriptografis	Menentukan bahwa ada kebijakan dan prosedur untuk mengatur pembangkitan, perubahan, pencabutan, penghancuran, distribusi, sertifikasi, penyimpanan, pemasukan, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.
DS5.9	Pencegahan, Deteksi, dan Koreksi Perangkat Lunak Berbahaya	Letakkan langkah-langkah pencegahan, detektif dan korektif di tempat (terutama patch keamanan terbaru dan kontrol virus) di seluruh organisasi untuk melindungi sistem dan teknologi informasi dari malware (mis., virus, worm, spyware, spam).
DS5.11	Pertukaran Data Sensitif	Tukar data transaksi sensitif hanya melalui jalur atau media tepercaya dengan kontrol untuk memberikan keaslian konten, bukti pengajuan, bukti penerimaan dan penolakan asal.
DS11	**Mengelola Data**	
DS11.1	Persyaratan Bisnis untuk Manajemen Data	Verifikasi bahwa semua data yang diharapkan untuk diproses diterima dan diproses sepenuhnya, akurat, dan tepat waktu, serta semua output dikirimkan sesuai dengan persyaratan bisnis. Mendukung restart dan kebutuhan pemrosesan ulang.
DS11.3	Sistem Manajemen Perpustakaan Media	Tetapkan dan terapkan prosedur untuk mempertahankan inventaris media yang disimpan dan diarsipkan untuk memastikan kegunaan dan integritasnya.
DS11.4	Pembuangan	Tetapkan dan terapkan prosedur untuk memastikan bahwa persyaratan bisnis untuk perlindungan data sensitif dan perangkat lunak

		dipenuhi saat data dan perangkat keras dibuang atau ditransfer.
DS11.6	Persyaratan Keamanan untuk Manajemen Data	Tetapkan dan terapkan kebijakan dan prosedur untuk mengidentifikasi dan menerapkan persyaratan keamanan yang berlaku untuk penerimaan, pemrosesan, penyimpanan dan output data untuk memenuhi tujuan bisnis, kebijakan keamanan organisasi dan persyaratan peraturan.
DS12	**Mengelola Lingkungan Fisik**	
DS12.1	Pemilihan Lokasi dan Tata Letak	Mendefinisikan dan memilih lokasi peralatan TI untuk mendukung strategi teknologi yang terhubung pada strategi bisnis. Pemilihan dan perancangan dari tata letak harus mempertimbangkan risiko yang berhubungan dengan bencana alam dan akibat kelalaian manusia, serta peraturan dan hukum relevan seperti *occupational healt* dan *safety regulation.*
DS12.2	Pengukuran Keamanan Fisik	Mendefinisikan dan menerapkan secara tegas ukuran keamanan fisik yang sejalan dengan kebutuhan bisnis untuk mengamankan lokasi dan aset fisik. Ukuran keamanan fisik harus dapat secara efektif mencegah, mendeteksi dan memitigasi risiko terkait pencurian, temperatur, kebakaran, asap, api, getaran, terror, pengrusakan, pemadaman listrik, kimia ataupun bahan peledak.
DS12.3	Akses Fisik	Mendefinisikan dan menerapkan secara tegas prosedur untuk memberikan, membatasi, dan menarik kembali akses untuk tempat, bangunan dan area, sesuai dengna kebutuhan bisnis, meliputi emergencies. Akses ke tempat, bangunan dan area harus dijustifikasi, diotorisasi, dicatat dan dipantau. Hal ini harus diaplikasikam ke setiap orang yang memasuki tempat, termasuk staf, staf sementara, klien pemasok, tamu ataupun pihak ketiga lain.
DS12.4	Perlindungan Terhadap Faktor Lingkungan	Merancangn dan mengimplementasikan ukuran untuk proteksi terhadap faktor lingkungan. Menginstall peralatan dan mesin khusus untuk pemantauan.
DS12.5	Manajemen Fasilitas Fisik	Mengolah fasilitas, meliputi peralatan sumber tenaga dan komunikasi, yang sesuai dengan hukum dan peraturan, aspek teknis dan bisnis.

Monitor and evaluate		
ME2	**Pengawasan dan Evaluasi Pengaturan Internal**	
ME2.1	Pemantauan Kerangka Pengendalian Internal	Terus *monitor, benchmark* dan meningkatkan TI mengendalikan lingkungan dan kerangka kontrol untuk memenuhi tujuan organisasi.
ME2.2	Pengawas Tinjauan	Memantau dan mengevaluasi efisiensi dan efektivitas TI internal kontrol tinjauan material.
ME2.3	Kontrol Pengecualian	Mengidentifikasi kontrol pengecualian, menganalisis dan mengidentifikasi penyebab yang mendasarinya *roof of cause.* Meningkatkan kontrol pengecualian dan melaporkan tepat kepada *stakeholder.* Tindakan korektif yang diperlukan.
ME2.4	Kontrol *self-assessment*	Mengevaluasi kelengkapan dan efektivitas pengendalian manajemen dan proses TI, kebijakan dan kontrak melalui terus

ME2.5	Jaminan Pengendalian Internal	Memperoleh, sesuai kebutuhan, kepastian lebih lanjut akan kelengkapan dan efektivitas pengendalian internal melalui pihak ketiga tinjauan.
ME2.6	Pengendalian Internal Pada Pihak Ketiga	Menilai status kontrol internal penyedia layanan eksternal mematuhi hukum dan peraturan persyaratan dan kewajiban kontrak.
ME2.7	*Remedial* Aksi	Mengidentifikasi, memulai, melacak dan menerapkan tindakan perbaikan yang timbul dari penilaian pengendalian dan pelaporan.
ME3	**Penjamin Kesesuaian dengan Kebutuhan Eksternal**	
ME3.1	Identifikaai Eksternal Persyaratan Kepatuhan Hukum, Peraturan dan Kontrak	Mengidentifikasi, secara terus menerus, hukum lokal dan internasional, peraturan dan persyaratan eksternal lainnya yang harus dipatuhi untuk dimasukkan ke TI organisasi kebijakan, standar, prosedur dan metodelogi.
ME3.2	Optimalisasi Respon Untuk Kebutuhan Eksternal	Meninjau dan menyesuaikan TI kebijakan, standar, prosedur dan metodologi untuk memastikan bahwa hukum, peraturan dan kontrak persyaratan dibahas dan dikomunikasikan.
ME3.3	Evaluasi Kepatuhan dengan Persyaratan Eksternal	Konfirmasi kepatuhan TI kebijakan, standar, prosedur dan metodologi dengan persyaratan hukum dan peraturan.
ME3.4	Positif Jaminan Kepatuhan	Mendapatkan dan melaporkan jaminan kepatuhan dan kepatuhan terhadap semua kebijakan internal berasal dari arahan internal atau eksternal hukum, peraturan atau persyaratan kontrak, yang menyatakan bahwa tindakan korektif untuk mengatasi kesenjangan kepatuhan telah dilakukan oleh pemilik bertanggung jawab proses pada waktu yang tepat.
ME3.5	Terpadu Pelaporan	Mengintegrasikan TI melaporkan persyaratan hukum, peraturan dan kontrak dengan output yang sama dari fungsi bisnis lainnya.
ME4	**Menyediakan *IT Governance***	
ME4.1	Pembentukan Kerangka *IT Governance*	Mendifiniksikan, membangun dan menyelaraskan kerangka kerja tata kelola TI dengan tata kelola perusahaan secara keseluruhan dan lingkungan pengendalian. Mendasarkan kerangka kerja pada proses TI yang cocok dan model kontrol dan memberikan pertanggungjawaban jelas dan praktek untuk menghindari gangguan dalam pengendalian internal dan pengawasan. Konfirmasikan bahwa kerangka tata kelola TI memastikan kepatuhan terhadap hukum dan peraturan dan sejajar, dan menegaskan pengiriman, strategi perusahaan dan tujuan, laporakan status TI dan masalah.
ME4.2	Strategis Keselarasan	Aktifkan papan dan pemahaman eksekutif strategis masalah TI, seperti peran TI, teknologi dan kemampuan. Memastikan bahwa ada pemahaman bersama antara bisnis dan TI tentang potensi kontribusi TI dengan strategi bisnis. Bekerja dengan papan dan badan pemerintahan., seperti komite strategi TI, untuk memberikan arah strategis relatif terhadap manajemen TI, memastikan bahwa strategi dan tujuan yang mengalir ke unit bisnis dan fungsi TI, dan bahwa keyakinan dan kepercayaan yang dikembangkan antara bisnis dan TI. Aktifkan penyelarasan TI dengan bisnis dalam strategi dan operasi,

		mendorong tanggung jawab bersama antara bisnis dan TI untuk membuat keputusan strategis dan memperoleh manfaat dari *IT-enabled* investasi.
ME4.3	Nilai Pengiriman	Mengolah *protgram* investasi *IT-enabled* dan aset TI dan layanan untuk memastikan bahwa mereka memberikan nilai terbesar yang mungkin dalam mendukung strategi perusahaan dan tujuan. Pastikan bahwa hasil bisnis yang diharapkan dari investasi *IT-enabled* dan lingkup penuh upaya yang diperlukan untuk mencapai hasil dipahami, bahwa kasus bisnis yang komprehensif dan konsisten diciptakan dan disetujui *stakeholder;* bahwa aset dan investasi yang dikelola sepanjang siklus kehidupan ekonomi mereka, dan bahwa tidak aktif pengelolaan realisasi manfaat, seperti kontribusi terhadapa layanan baru, peningkatan efisiensi dan peningkatan responsitivitas untuk pelanggan tuntutan. Menegakkan pendekatan disiplin untuk portofolio, program dan manajemen proyek, bersikeras bahwa bisnis mengambil kepemilikan semua *IT-enabled* investasi TI dan memastikan optimalisasi biaya memberikan kemampuan TI dan jasa.
ME4.4	Manajemen Sumber Daya	Mengawasi investasi, penggunaan dan alokasi sumber daya TI melalui penilaian reguler inisiatif TI dan operasi untuk memastikan sesuai sumber daya dan sejalan dengan tujuan strategis saat ini dan masa depan dan imperatif bisnis.
ME4.5	Manajemen Risiko	Bekerja dengan dewan untuk mendefinisikan selera perusahaan untuk risiko TI, dan memperoleh keyakinan memadai bahwa manajemen risiko TI praktek yang tepat untuk menjamin bahwa risiko TI yang sebenarnya tidak melebihi risiko keinginan dewan. Manajemen risiko bertanggung jawab ke dalam organisasi, memastikan bahwa bisnis dari TI secara teratur menilai dan melaporkan berkaitan dengan TI risiko dan dampaknya dan bahwa TI posisi risiko perusahaan itu transparan bagi semua *stakeholder.*
ME4.6	Pengukuran Kinerja	Konfirmasikan bahwa sasaran TI yang disepakati telah dipenuhi atau dilampaui, atau bahwa kemajuan menuju sasaran TI memenuhi harapan. Dimana tujuan yang disepakati telah terlewatkan atau kemajuan tidak seperti yang diharapkan, tinjau tindakan perbaikan manajemen. Laporkan ke dewan portofolio yang relevan, kinerja program dan TI, didukung oleh laporan untuk memungkinkan manajemen senior untuk meninjau perusahaan kemajuan menuju tujuan yang diidentifikasi
ME4.7	Independen Jaminan	Memperoleh jaminan independen (internal atau eksternal) tentang kesesuaian TI dengan undang-undang dan peraturan yang relevan; kebijakan, standar, dan prosedur organisasi; praktik yang diterima secara umum; dan kinerja TI yang efektif dan efisien.

RIWAYAT HIDUP

Bahwa yang bertanda tangan dibawah ini :

Nama	:	Syafira Rohadatul ‘Aisy
Tempat / Tanggal Lahir	:	Tanjung Batu, 03 Agustus 1997
Jenis Kelamin	:	Perempuan
Agama	:	Islam
Alamat	:	Jln. Letnan Yasin No.781, RT 014, RW 005 20 Ilir D III Ilir Timur I Palembang
No. Telp / HP	:	081361163821

PENDIDIKAN FORMAL

Tahun 2004-2009	:	SD Negeri 3 Tanjung Batu
Tahun 2009-2012	:	SMP Negeri 1 Tanjung Batu
Tahun 2012-2015	:	SMA Negeri 1 Tanjung Batu

Demikianlah daftar riwayat hidup ini saya buat dengan sebenarnya.

Palembang, Februari 2020

Syafira Rohadatul ‘Aisy

Laporan Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UIN Raden Fatah Palembang

Laporan Audit Teknologi Informasi

Syafira Rohadatul 'Aisy (1535400175)

Report : Februari 2020

Laporan Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UIN Raden Fatah Palembang

Report

Februari 2020

Penanggung Jawab Audit I	Penanggung Jawab Audit II
Rusmala Santi, M.Kom	Irfan Dwi Jaya, M.Kom

Mengetahui

Fahruddin, M. Kom

LAPORAN AUDIT TEKNOLOGI INFORMASI

Laporan audit teknologi informasi ini dipersiapkan untuk ditujukan pada organisasi PUSTIPD UIN Raden Fatah yang berisikan temuan audit, rekomendasi dan langkah yang harus diambil untuk tidakan kedepannya.

Laporan ini berfokus pada teknologi informasi untuk manajemen risiko dengan mengggunkan framework COBIT 4.1. Audit teknologi informasi dilakukan di PUSTIPD UIN Raden Fatah Palembang.

Syafira Rohadatul ‘Aisy

AUDITOR

Februari 2020

Kesimpulan Audit

5. Pada PUSTIPD dalam mengolah strategi dan taktik teknologi informasi yaitu pada domain *plan and organize* dengan *control objective* PO4, PO6 dan PO9 hasil audit dan responden berada pada tingkat 3 (*defined*). Pada level 3 proses sebagaian besar sudah dijalankan dan mencapai tujuan, namun pada kenyataanya untuk penilaian dan pengelolaan risiko masih terdapat proses yang belum terpenuhi. Rekomendasi yang diberikan mengusulkan langkah yang perlu dilakukan untuk mencapai tingkat *maturity level* 3 sesuai yang diharapkan responden.
6. PUSTIPD dalam melakukan pengiriman dari layanan yang dibutuhkan yaitu pada domain *deliver and support* dengan *control objective* DS2, DS4, DS5, DS11 dan DS12 hasil audit berada pada tingkat 2 (*repeatable but intuitive)* sedangkan untuk penilaian responden berada pada tingkat 3. Dari temuan audit untuk pemastian layanan berkelanjutan dan sistem keamanan penugasannya pada koordinator keamanan TI meskipun otoritasnya terbatas. Rekomendasi yang diberikan mengusulkan tindakan yang perlu dilakukan untuk mencapai tingkat 3 sesuai dengan harapan dari penilaian responden.
7. Pada PUSTIPD dalam manajemen kinerja, pemantauan pengendalian, kepatuhan peraturan dan tata kelola pada domain *monitor and evaluate* dengan *control objective* ME2, ME3, dan ME4 hasil audit dan penilaian responden berada pada tingkat 3 (*defined*). Namun untuk manajemen risiko belum terdapat penentuan manajemen risiko serta penjamin praktiknya telah sesuai. Rekomendasi diberikan untuk mengusulkan tindakan yang harus dilakukan organisasi dalam mencapai tingkat yang sesuai dengan harapan dari penilaian responden.

Daftar Isi

BAB I

Tahapan Audit Teknologi Informasi

5. Tahapan Perencanaan

   Sebagai suatu pendahuluan mutlak yang dilakukan auditor, untuk mengenal objek yang akan diperiksa sehingga menghasilkan suatu program audit yang didesain sedemikian rupa agar pelaksanaanya akan berjalan efektif dan efisien.

6. Mengidentifikasikan Risiko dan Kendali

   Untuk memastikan bahwa *qualified resource* sudah dimiliki, dalam hal ini aspek SDM yang berpengalaman dan juga referensi praktik-praktik terbaik.

7. Mengevaluasi Kendali dan Mengumpulkan Bukti-bukti

   Melalui berbagai teknik pengumpulan data, seperti penyebaran kuesioner, observasi dan melakukan wawancara untuk pengumpulan bukti.

8. Mendukomentasikan

   Mengumpulkan temuan-temuan dan mengidentifikasikan dengan audit.

9. Menyusun Laporan

   Mencakup tujuan pemeriksaan, sifat, dan kedalaman pemeriksaan yang dilakukan

Alat dan Bahan Audit

Peneliti menggunakan alat-alat yang mendukung penelitian, yaitu: *microsoft word* untuk pembuatan dokumen skripsi, *handphone* sebagai alat bantu rekam suara, foto, dan video, SPSS *versi* 23 untuk menguji validitas dan realibilitas kuisioner dan *microsoft excel* 2013 untuk pengolahan data dalam menghitung penentuan *maturity level*, dan selanjutnya digambarkan dalam bentuk *spider chart* (grafik radar).

Bahan pada penelitian terbagi atas beberapa bagian yaitu bukti langsung/tidak langsung, bukti utama (primer/sekunder), dan *record/ testimonial evidence*. Berikut bahan penelitian melakukan audit yang diperlukan didalam penelitian ini yaitu sebagai berikut :

4. Bukti langsung/ tidak langsung. Bahan bukti yaitu surat balasan tentang pelaksanaan audit pada PUSTIPD UIN Raden Fatah Palembang,

   hasil wawancara dan analisis swot berupa gambaran awal yang diperlukan sebagai informasi dasar mengenai TI yang ada pada PUSTIPD, data/informasi mengenai TI yang akan di audit.

5. Bukti utama primer/sekunder. Bahan bukti yaitu tampilan/data tentang TI pada PUSTIPD UIN Raden Fatah sebagai bukti utama untuk melakukan audit didalam penelitian ini. Serta bukti bahwa telah melakukan penyebaran kuisioner berupa berita acara terhadap pihak terkait sebagai pokok yang menjadi inti utama dalam melakukan audit.
6. *Record/ Testimonial Evidence*, yaitu hasil wawancara dengan pihak terkait pada penelitian.

Dalam penelitian ini yang akan dilakukan audit yaitu, teknologi informasi menggunakan framework COBIT 4.1 untuk manajemen risiko pada PUSTIPD. Penelitian ini terdapat tiga komponen tata kelola TI yang akan dilakukan audit, tiga komponen tersebut berdasarkan Cobit 4.1 adalah sebagai berikut :

4. Kebijakan PUSTIPD UIN Raden Fatah Palembang
5. Standar PUSTIPD UIN Raden Fatah Palembang

Prosedur PUSTIPD UIN Raden Fatah Palembang

Responden Audit

RACI Roles	***Organisation Roles***
CEO (*Chief executive officer)*	Rektor (PROF. DRS.H.M. SIROZI. M A . PH.D)
CFO (*Chief finance officer)*	Kepala Bagian Perencanaan dan Keuangan (MUSLI DAROSAN. S.AG.M.SI)
CIO (*Chief Information officer)*	Kepala PUSTIPD (FAHRUDDIN. M.KOM)
Head Operation	Difisi Pengembangan Software (KMS.Jumansyah.HM. S.SI.ITIL.MTA A.Arroyan Rasyid. S.Kom M. Aswadi, S.Kom)
Chief architect	
Head development	
Head IT Administrasi	Awang Sugiarto, S.Kom.,IT-IL.MTA
CAS (Compliance, audit, rist & security)	Dr. Fajri Ismail,

Survey dilakukan dengan menyebar 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.

BAB II

Audit Teknologi Informasi dengan Framework COBIT 4.1 untuk Manajemen Risiko pada PUSTIPD UIN Raden Fatah Palembang

Latar Belakang

Pusat teknologi informasi dan pangkalan data (PUSTIPD) UIN Raden Fatah Palembang sebagai lembaga pusat teknologi informasi yang memiliki tanggung jawab *service* sekaligus pengembang beberapa sistem, yaitu: SIMAK UIN Raden Fatah, E-lkp, E-jurnal, Slims, E-repository, dan Lpse UIN Raden Fatah. PUSTIPD dalam menjalankan kegiatannya, menggunakan teknologi informasi sebagai basis dalam menciptakan layanan yang berkualitas ataupun dalam optimalisasi proses bisnisnya. Penggunaan teknologi informasi kadang tidak sesuai dengan harapan, proses dokumentasi pada PUSTIPD belum tersusun dengan rapi, mulai dari proses *planning, organizing, actuating* dan *controlling* yang dilakukan. Server data PUSTIPD masih sentral sehingga kemungkinan kehilangan data cukup besar, sistem yang berjalan belum mendukung sebagai alat bantu koordinasi yang diharapkan. Mengingat sistem berbasis teknologi informasi akan mempunyai potensi adanya risiko pada tingkat organisasi yang makin besar. Risiko yang makin besar mendorong perlunya kontrol yang makin memadai. Hal tersebut yang mendasari perlunya audit terhadap teknologi informasi.

Kesimpulan

Untuk mengetahui apakah teknologi informasi dalam mengolah risiko sudah dilengkapi kontrol yang memadai dan apakah kontrol tersebut sudah benar-benar dijalankan, maka perlu dilakukan audit TI untuk manajemen risiko, dengan menanamkan kesadaran risiko (*risk awareeness*) pada perusahaan, memberikan pengertian yang jelas dari pandangan perusahaan terhadap risiko, memberikan pengertian kebutuhan kesesuaian, transparansi tentang risiko signifikan, dan menanamkan tanggungjawab risiko dalam perusahaan.

Temuan Audit

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.

1. ***Plan and Organize* (PO)**

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

Tabel 1 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, namum pencapaian kerangka kerja teknologi informasi tidak seluruhnya telah dilakukan.	3	3	Sesuai
PO4.2	Terdapat strategi teknologi informasi, komite strategi teknologi informasi terlah 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 *job desk*	4	3	Sesuai
PO4.7	Terdapat tanggung jawab untuk jaminan kualitas teknologi informasi	3	3	Sesuai
PO4.8	Terdapat tanggung jawab untuk keamanan dilakukan *monitoring* secara berkala dan *maintenance* 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 penetuan dan identifikasi staf teknologi informasi secara umum	3	3	Sesuai
PO4.14	Terdapat kebijakan dan prosedur staf yang terkontrak	4	3	Sesuai
PO4.15	Terdapat hubungan teknologi informasi dengan bisinis teknologi informasi.	4	3	Sesuai

Rata-rata	3,33	2,98	Sesuai

1.2 PO6 *Communicate Management Aims and Direction*

Tabel 2 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

1.3 PO9 *Assess and Manage IT Risk*

Tabel 3 Keadaan TI 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, namum 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

2. *Deliver and Support* (DS)

2.1 DS2 *Manage Third-party Services*

Tabel 4 Keadaan TI 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

Control Objective	Keadaan TI saat ini	*Maturity Level* Audit	*Maturity Level* Responden	Keterangan
DS2.2	Terdapat formalitas proses manajemen hubungan pemasok, penyelesaian masalah dan pemastian kualitas berdasrakan SLA	4	3	Sesuai
DS2.3	Terdapat identifikasi dan mitigasi risiko pemasok	4	3	Sesuai
DS2.4	Terdapat pengawasan kinerja pemasok dengan evaluasi dan *monitoring*	3	3	Sesuai
Rata-rata		3,25	3,18	Sesuai

2.2 DS4 *Ensure Continuous Service*

Tabel 5 Keadaan TI DS4 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
DS5.9	Terdapat pengcegahan, 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

2.3 DS5 *Ensure Systems Security*

Tabel 6 Keadaan TI 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
DS5.9	Terdapat pengcegahan, 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

2.4 DS11 *Manage Data*

Tabel 7 Keadaan TI 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 memelihaea 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	Terdapar persyaratan keamanan untuk manajemen data	4	3	Sesuai

Rata-rata	3	3,26	Sesuai

2.5 DS12 *Manage the Physical Environment*

Tabel 8 Keadaan TI 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

3. *Monitor and Evaluate* (ME)

3.1 ME2 *Monitor and Evaluate Internal Control*

Tabel 9 Keadaan TI 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
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

3.2 ME3 *Ensure Compliance With External Requirements*

Tabel 10 Keadaan TI ME3 Saat Ini

Control Objective	Keadaan TI saat ini	*Maturity Level* Audit	*Maturity Level* Responden	Keterangan
ME3.1	Terdapat identifikasi persyaratan hukumm, peraturan dan kontrak eksternal dengnan penyesuaian	3	3	Sesuai

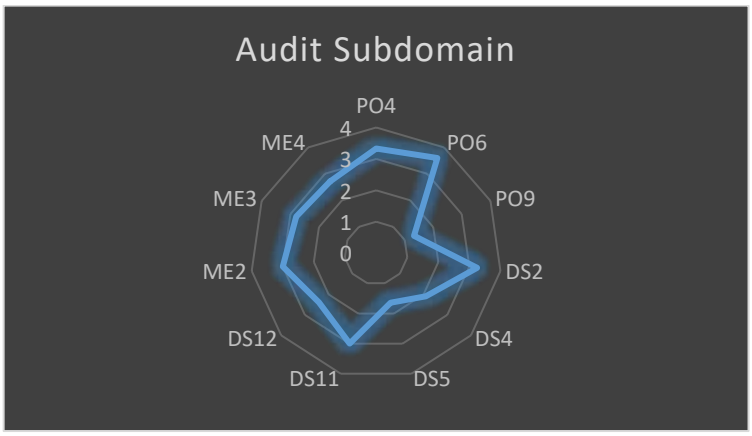
Control Objective	Keadaan TI saat ini	*Maturity Level* Audit	*Maturity Level* Responden	Keterangan
ME3.2	Terdapat peninjauan dan penyesuaian kebijakan, standar, prosedur dan metodologi TI	3	3	Sesuai
ME3.3	Terdapat evaluasi kepatuhan	3	3	Sesuai
ME3.4	Terdapat jaminan kepatuhan yang diperoleh dari survei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

3.3 ME4 *Provide IT Governance*

Tabel 11 Keadaan TI ME4 Saat Ini

Control Objective	Keadaan TI saat ini	*Maturity Level* Audit	*Maturity Level* Responden	Keterangan
ME4.1	Terdapat penetapan dan penyelarasan tata kelola TI dengan mempertimbangkan kebutuhan	3	4	Tidak sesuai
ME4.2	Terdapat proses penyelarasan 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 *monitoring*	3	3	Sesuai
ME4.5	Belum ada penentuan manajemen risiko namun kemanan 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

Berikut ini grafik radar sebagai gambaran rata-rata *maturity level* subdomain:



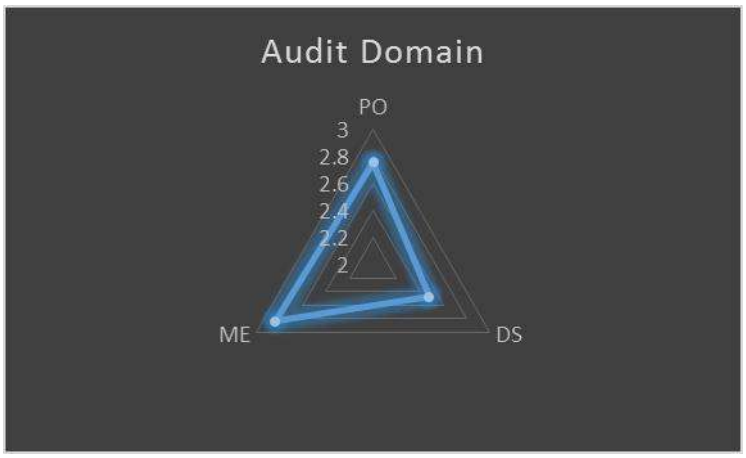
Gambar 1 Grafik Radar Audit Subdomain

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 12 sebagai berikut:

Tabel 12 Hasil Pengujian Audit Domain

No	Domain	*Indeks Maturity*	*Maturity Level*	Keterangan
1.	*Plan and Organize*	2,75	3	*Defined*
2.	*Delivery and Support*	2,48	2	*Reapetable*
3.	*Monitor and Evaluate*	2,84	3	*Defined*
Tingkat kematangan keseluruhan		2,69	3	*Defined*

Berikut adalah gambaran grafik radar *maturity level* domain:



Gambar 2 Grafik Radar Audit Domain

BAB II
Rekomendasi

Dalam proses melakukan audit, hasil audit menunjukkan terdapat beberapa kontrol yang belum tepat, sehingga tujuan belum dapat dicapai. Untuk itu diberikan rekomendasi yang mengacu pada COBIT untuk proses TI yang lebih baik :

1. *Plan and Organize* (PO)

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

Tabel 13 Rekomendasi PO4

Control Objective	Rekomendasi
PO4.1	Melakukan pengukuran kerangka kerja teknologi informasi secara keseluruhan, mulai dari struktur proses dan hubungan TI, kepemilikan, kedewasaam, pengukuran kinerja, piningkatan, 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
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,

1.2 PO6 *Communicate Management Aims and Direction*

Tabel 14 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 peluncurkan 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.

1.3 PO9 *Assess and Manage IT Risk*

Tabel 15 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

2 *Deliver and Support* (DS)

2.1 DS2 *Manage Third-party Services*

Tabel 16 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.

2.2 DS4 *Ensure Continuous Service*

Tabel 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 kembalnyai fungsi TI setelah bencana, dan perbarui rencana yang sesuai.

2.3 DS5 *Ensure Systems Security*

Tabel 18 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, menangguhkan, 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 direakreditasi secara tepat waktu untuk memastikan bahwa *baseline* 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.

2.4 DS11 *Manage Data*

Tabel 19 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

2.5 DS12 *Manage the Physical Environment*

Tabel 20 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.
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

Control Objective	Rekomendasi
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.

3 *Monitor and Evaluate* (ME)

3.1 ME2 *Monitor and Evaluate Internal Control*

Tabel 21 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.

3.2 ME3 *Ensure Compliance With External Requirements*

Tabel 22 Rekomendasi ME3

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

3.3 ME4 *Provide IT Governance*

Tabel 23 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 yang diperlukan.
ME4.4	Lakukan pengawasan melalui penilaian rutin atas inisiatif dan operasi TI untuk memastikan sumber daya dan penyelarasan 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