

**TESIS**

**MODEL PENGELOLAAN RISIKO TI BERBASIS COBIT  
UNTUK MENINGKATKAN LAYANAN AKADEMIK  
DI POLITEKNIK NEGERI SRIWIJAYA**



Disusun oleh:

**Nama : Nurul Ilma Hasana Kurno**  
**NIM : 20.51.1327**  
**Konsentrasi : Digital Transformation Intelligence**

**PROGRAM STUDI S2 TEKNIK INFORMATIKA  
PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2022**

**TESIS**

**MODEL PENGELOLAAN RISIKO TI BERBASIS COBIT  
UNTUK MENINGKATKAN LAYANAN AKADEMIK  
DI POLITEKNIK NEGERI SRIWIJAYA**

**IT RISK MANAGEMENT MODEL BASED ON COBIT  
TO IMPROVE ACADEMIC SERVICES  
IN STATE POLYTECHNIC OF SRIWIJAYA**

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Magister



Disusun oleh:

**Nama : Nurul Ilma Hasana Kuntio**  
**NIM : 20.51.1327**  
**Konsentrasi : Digital Transformation Intelligence**

**PROGRAM STUDI S2 TEKNIK INFORMATIKA  
PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2022**

## HALAMAN PENGESAHAN

**MODEL PENGELOLAAN RISIKO TI BERBASIS COBIT  
UNTUK MENINGKATKAN LAYANAN AKADEMIK  
DI POLITEKNIK NEGERI SRIWIJAYA**

**IT RISK MANAGEMENT MODEL BASED ON COBIT  
TO IMPROVE ACADEMIC SERVICES  
IN STATE POLYTECHNIC OF SRIWIJAYA**

Dipersiapkan dan Disusun oleh

**Nurul Ilma Hasana Kunto**

**20.51.1327**

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis  
Program Studi S2 Teknik Informatika  
Program Pascasarjana Universitas AMIKOM Yogyakarta  
pada hari Selasa, 5 Juli 2022

Tesis ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Magister Komputer.

Yogyakarta, 5 Juli 2022

**Rektor**

**Prof. Dr. M. Suyanto, M.M.**  
**NIK. 190302001**

## HALAMAN PERSETUJUAN

### MODEL PENGELOLAAN RISIKO TI BERBASIS COBIT UNTUK MENINGKATKAN LAYANAN AKADEMIK DI POLITEKNIK NEGERI SRIWIJAYA

### IT RISK MANAGEMENT MODEL BASED ON COBIT TO IMPROVE ACADEMIC SERVICES IN STATE POLYTECHNIC OF SRIWIJAYA

Dipersiapkan dan Disusun oleh

**Nurul Ilma Hasana Kunio**

20.51.1327

Telah Ditujikan dan Dipertahankan dalam Sidang Ujian Tesis  
Program Studi S2 Teknik Informatika  
Program Pascasarjana Universitas AMIKOM Yogyakarta  
pada hari Selasa, 5 Juli 2022

**Pembimbing Utama**

Prof.Dr.Ema Utami,S.Si,M.Kom  
NIK. 190302037

**Anggota Tim Penguji**

Dr. Andi Sunyoto,M.Kom  
NIK. 190302052

**Pembimbing Pendamping**

Alva Hendi Muhammad,S.T,M.Eng,Ph.D  
NIK. 190302493

Dhani Ariatmanto,M.Kom,Ph.D  
NIK. 190302197

Prof.Dr.Ema Utami,S.Si,M.Kom  
NIK. 190302037

Tesis ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Magister Komputer

Yogyakarta, 5 Juli 2022

**Direktur Program Pascasarjana**

Prof. Dr. Kusrini, M.Kom.  
NIK. 190302106



## PALAMAN PERNYATAAN KEASLIAN TESIS

Yang beresidatangi di bawah ini,

Nama mahasiswa : Nurul Hana Husana Kurnia  
NIM : 20.51.1337  
Konsentrasi : Digital Transformation Intelligence

Menyatakan bahwa Tesis dengan judul berikut  
Model Pengalasan Risiko TI Berbasis COBIT untuk Meningkatkan  
Layanan Akademik di Politeknik Negeri Surabaya

Dosen Pembimbing Utama : Prof. Dr. Ema Utami, S.Si, M.Eng., Ph.D.  
Dosen Pembimbing Pendamping : Alfa Hendi Muhammad, S.T.M, Eng., Ph.D.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH digunakan untuk mendapatkan gelar akademik, baik di Universitas ANIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, pemikiran dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai kutipan dalam tubuh dengan disertai nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, tidak menanggung jawab Universitas ANIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat pelanggaran dan ketidakjujuran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan penulisan ulang yang sudah diperbaiki, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 7 Juli 2022  
Yang Menyatakan



Nurul Hana Husana Kurnia

## HALAMAN MOTTO

Always remember that there is someone out there working harder than you, so you must work your hardest to be the best. – Slam Dunk

Once you have made up your mind, stick to it; there no longer any if or but. – Napoleon Bonaparte

Until you spread your wings, you'll have no idea how far you can fly. – Napoleon Bonaparte



## KATA PENGANTAR

Puji syukur kehadiran Allah SWT sehingga atas limpahan rahmat dan karunia-Nya penulis dapat menyelesaikan tesis dengan judul “Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya”. Tesis ini disusun untuk memenuhi salah satu persyaratan dalam memperoleh gelar Magister Teknik Informatika Universitas AMIKOM Yogyakarta.

Penulis menyadari bahwa penyusunan tesis ini tidak terlepas dari bantuan, bimbingan, serta dorongan dari berbagai pihak. Oleh karena itu penulis ingin menyampaikan terimakasih kepada pihak-pihak yang telah membantu dalam penyelesaian tesis ini.

1. Ibu Prof. Dr. Kusrini, M.Kom selaku Direktur Program Pascasarjana Universitas AMIKOM Yogyakarta.
2. Ibu Prof. Dr. Ema Utami, S.Si, M.Kom selaku dosen pembimbing 1 yang telah membimbing, mengarahkan, dan meluangkan waktunya selama penyelesaian tesis ini.
3. Bapak Alva Hendi Muhammad, S.T., M.Eng, Ph.D selaku dosen pembimbing 2 yang telah membimbing dan selalu memberikan masukan, arahan, serta pencerahan.
4. Bapak Dr. Andi Sunyoto, M.Kom dan Bapak Dhani Ariatmanto, M.Kom, Ph.D selaku dosen penguji yang telah memberikan masukan dan saran untuk penyempurnaan tesis ini.

5. Bapak Dr. Ing. Ahmad Taqwa, M.T. selaku Direktur Politeknik Negeri Sriwijaya.
6. Bapak Carlos RS, S.T., M.T. selaku Pembantu Direktur I Politeknik Negeri Sriwijaya.
7. Bapak Ir. Zulkarnaini, M.T. selaku Kepala UPT Teknologi Informasi dan Komunikasi (TIK) Politeknik Negeri Sriwijaya serta seluruh Staff, Dosen, dan Tenaga Kependidikan di lingkungan Politeknik Negeri Sriwijaya.
8. Dr. Dra. Hj. Mikhriani, M.M selaku Lead Auditor AMI UIN Sunan Kalijaga yang telah membantu memberi masukan dan arahan.
9. Keluarga yang selalu memberikan dukungan, semangat, serta bantuan sehingga penulis dapat menyelesaikan tesis ini.
10. Semua pihak yang telah membantu dan tidak dapat penulis sebutkan satu persatu disini.

Penulis menyadari bahwa tesis ini masih jauh dari sempurna. Oleh karena itu penulis mengharapkan saran dan kritik sebagai masukan untuk pengembangan penelitian selanjutnya. Penulis berharap semoga tesis ini dapat bermanfaat dan menambah wawasan khususnya bagi penulis sendiri.

Yogyakarta, 29 Juni 2022

Penulis

## DAFTAR ISI

HALAMAN JUDUL.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERSETUJUAN.....	iv
HALAMAN MOTTO.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xiv
INTISARI.....	xv
<i>ABSTRACT</i> .....	xvi
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah.....	7
1.3. Batasan Masalah.....	8
1.4. Tujuan Penelitian.....	8
1.5. Manfaat Penelitian.....	9
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>10</b>
2.1. Tinjauan Pustaka.....	10
2.2. Keaslian Penelitian.....	14
2.3. Landasan Teori.....	20
<b>BAB III METODE PENELITIAN.....</b>	<b>61</b>

3.1. Jenis, Sifat, dan Pendekatan Penelitian.....	61
3.2. Metode Pengumpulan Data.....	61
3.3. Metode Analisis Data.....	62
3.4. Alur Penelitian.....	67
<b>BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....</b>	<b>69</b>
4.1. Tahap Identifikasi Masalah dan Literatur Review.....	69
4.2. Tahap Pengumpulan Data.....	69
4.3. Tahap Analisis.....	85
4.3.1. Hasil Audit BAI06 Managed IT Changes.....	87
4.3.2. Hasil Audit BAI10 Managed Configuration.....	96
4.3.3. Hasil Audit DSS01 Managed Operations.....	105
4.3.4. Hasil Audit DSS02 Managed Service Requests and Incident.....	117
4.4. Tahap Rekomendasi.....	130
<b>BAB V PENUTUP.....</b>	<b>142</b>
5.1. Kesimpulan.....	142
5.2. Saran.....	143
<b>DAFTAR PUSTAKA.....</b>	<b>145</b>
<b>LAMPIRAN.....</b>	<b>148</b>



## DAFTAR TABEL

Tabel 2.1. Matriks literatur review dan posisi penelitian Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya.....	14
Tabel 2.2. COBIT Stakeholder.....	30
Tabel 2.3. Enterprise Strategy Design Factor.....	36
Tabel 2.4. Enterprise Goals Design Factor.....	36
Tabel 2.5. Risk Profile Design Factor.....	37
Tabel 2.6. I&T Related Issues Design Factor.....	43
Tabel 2.7. Threat Landscape Design Factor.....	44
Tabel 2.8. Compliance Requirement Design Factor.....	44
Tabel 2.9. Role of IT Design Factor.....	45
Tabel 2.10. Sourcing Model for IT Design Factor.....	45
Tabel 2.11. IT Implementation Method.....	45
Tabel 2.12. Technology Adoption Strategy Design Factor.....	46
Tabel 2.13. Enterprise Size Design Factor.....	46
Tabel 2.14. Goals Cascade: Enterprise Goals and Metrics.....	47
Tabel 2.15. Goals Cascade: Alignment Goals and Metrics.....	50
Tabel 2.16. Governance and Management Objective and Purpose.....	52
Tabel 3.1. Deskripsi role menurut COBIT 2019.....	63
Tabel 4.1. Design factor 1 enterprise strategy.....	73
Tabel 4.2. Penyelarasan dengan design factor 2 stakeholder needs.....	73



Tabel 4.3. Design factor 2 enterprise goals.....	74
Tabel 4.4. Alignment goals .....	75
Tabel 4.5. Design factor 3 risk profile .....	75
Tabel 4.6. Design factor 4 IT related issues .....	77
Tabel 4.7. Hasil pemetaan RACI Chart COBIT 2019 .....	82
Tabel 4.8. Pemetaan role domain BAI06 .....	83
Tabel 4.9. Pemetaan role domain BAI10 .....	83
Tabel 4.10. Pemetaan role domain DSS01 .....	84
Tabel 4.11. Pemetaan role domain DSS02 .....	84
Tabel 4.12. Jadwal kegiatan.....	85
Tabel 4.13. Dokumen pendukung penelitian .....	86
Tabel 4.14. Hasil kuisisioner domain BAI06.01 .....	88
Tabel 4.15. Hasil kuisisioner domain BAI06.02 .....	90
Tabel 4.16. Hasil kuisisioner domain BAI06.03 .....	92
Tabel 4.17. Hasil kuisisioner domain BAI06.04 .....	93
Tabel 4.18. Hasil keseluruhan proses domain BAI06.....	95
Tabel 4.19. Hasil kuisisioner domain BAI10.01 .....	97
Tabel 4.20. Hasil kuisisioner domain BAI10.02 .....	98
Tabel 4.21. Hasil kuisisioner domain BAI10.03 .....	99
Tabel 4.22. Hasil kuisisioner domain BAI10.04 .....	100
Tabel 4.23. Hasil kuisisioner domain BAI10.05 .....	102
Tabel 4.24. Hasil keseluruhan proses domain BAI10.....	103
Tabel 4.25. Hasil kuisisioner domain DSS01.01 .....	106

Tabel 4.26. Hasil kuisisioner domain DSS01.02 .....	107
Tabel 4.27. Hasil kuisisioner domain DSS01.03 .....	109
Tabel 4.28. Hasil kuisisioner domain DSS01.04 .....	110
Tabel 4.29. Hasil kuisisioner domain DSS01.05 .....	112
Tabel 4.30. Hasil keseluruhan proses domain DSS01 .....	115
Tabel 4.31. Hasil kuisisioner domain DSS02.01 .....	117
Tabel 4.32. Hasil kuisisioner domain DSS02.02 .....	119
Tabel 4.33. Hasil kuisisioner domain DSS02.03 .....	120
Tabel 4.34. Hasil kuisisioner domain DSS02.04 .....	121
Tabel 4.35. Hasil kuisisioner domain DSS02.05 .....	123
Tabel 4.36. Hasil kuisisioner domain DSS02.06 .....	124
Tabel 4.37. Hasil kuisisioner domain DSS02.07 .....	125
Tabel 4.38. Hasil keseluruhan proses domain DSS02 .....	126
Tabel 4.39. Rekapitulasi hasil audit keseluruhan .....	130
Tabel 4.40. Rekomendasi hasil audit .....	131
Tabel 4.41. Perbandingan hasil audit iso 9001 dengan COBIT 2019 .....	135
Tabel 4.42. Justifikasi dari rekomendasi yang diusulkan .....	135
Tabel 4.43. Form daftar temuan audit berdasar kaidah PLOR .....	137
Tabel 4.44 Rencana tindakan koreksi .....	138

## DAFTAR GAMBAR

Gambar 2.1. Context Enterprise Governance of I&T .....	22
Gambar 2.2. Governance System Principles .....	23
Gambar 2.3. ITIL Service Lifecycle .....	25
Gambar 2.4. Struktur Dokumen TOGAF .....	27
Gambar 2.5. COBIT Core Model .....	32
Gambar 2.6. Governance System Design Workflow .....	34
Gambar 2.7. COBIT Design Factor .....	35
Gambar 2.8. Goal Cascade .....	46
Gambar 2.9. Capability Level Proses .....	57
Gambar 3.1. Alur Penelitian .....	67
Gambar 4.1. Dokumentasi wawancara .....	70
Gambar 4.2. Dokumentasi pengisian kuisioner .....	70
Gambar 4.3. COBIT Design Factor 1-4 .....	71
Gambar 4.4. Kustomisasi COBIT 2019 di Dunia Pendidikan .....	71
Gambar 4.5. Grafik identifikasi design factor .....	79
Gambar 4.6. Nilai capability level per aktivitas proses BAI06.01 .....	89
Gambar 4.7. Hasil audit BAI06 .....	95
Gambar 4.8. Hasil audit BAI10 .....	103
Gambar 4.9. Hasil audit DSS01 .....	115
Gambar 4.10. Hasil audit DSS02 .....	127
Gambar 4.11. Tingkat kapabilitas Politeknik Negeri Sriwijaya .....	130

## INTISARI

Penggunaan COBIT sebagai framework IT Governance kebanyakan berfokus pada sektor finansial dan akuntansi. Sehingga diperlukan eksplorasi COBIT dalam sektor pendidikan yang dilakukan dengan mengkustomisasi COBIT. Penelitian yang berjudul Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya bertujuan untuk mengetahui tingkat *capability level* Polsri saat ini bila diukur menggunakan COBIT 2019, serta mengetahui langkah analisis pengelolaan risiko dengan menggunakan COBIT 2019 di Polsri. Penelitian ini dibatasi hanya pada kegiatan layanan akademik dengan menggunakan *Design Factor* (DF) 1 sampai DF4 pada COBIT 2019.

Penelitian ini dilakukan dengan melakukan eksplorasi COBIT 2019 pada sektor pendidikan. Eksplorasi dilakukan dengan melakukan kustomisasi COBIT pada DF1 sampai DF4. Pada DF1 terjadi penyesuaian sasaran strategis perguruan tinggi, kemudian pada DF2 terjadi penyesuaian pada tujuan perguruan tinggi, pada DF3 dilakukan pengamatan terhadap profil risiko perguruan tinggi, dan pada DF4 dilakukan pengamatan terhadap isu terkait IT di perguruan tinggi.

Berdasar hasil penelitian dapat disimpulkan bahwa pengukuran risiko Polsri berada pada *capability level* 3 untuk proses BAI10 dan DSS01; serta level 2 pada proses BAI06 dan DSS02. Setiap fakta temuan dari setiap proses yang diukur kemudian dipergunakan untuk pembuatan rekomendasi.

Kata kunci: cobit, kustomisasi, design factor, risiko.

## **ABSTRACT**

*The use of COBIT as an IT Governance framework mostly focuses on the financial and accounting sectors. So it is necessary to explore COBIT in the education sector by customizing COBIT. The research, entitled COBIT-Based IT Risk Management Model to improve Academic Services at the Politeknik Negeri Sriwijaya, aims to determine the current level of capability of Polsri measured using COBIT 2019, and to find out the analytical steps in utilizing COBIT 2019 at the Polsri. This research is limited to academic service activities using Design Factors (DF) 1 to DF4 in COBIT 2019.*

*This research was conducted by exploring COBIT 2019 in the education sector. Exploration is carried out by customizing COBIT on DF1 to 4. In DF1 there is an alignment of the university's strategic goals, then in DF2 there is an alignment with the goals of the university, in DF3 observing the risk profile of universities, and DF4 is an observation of issues related to IT in universities.*

*Based on the results of the research, it can be ensured that the Polsri risk measurement is at capability level 3 for the BAI10 and DSS01 processes; and level 2 on BAI06 and DSS02 processes. Each fact from each measured process is then used for making recommendations.*

*Keyword: cobit, customization, design factor, risk*



# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang Masalah

Pendidikan merupakan pondasi kemajuan bangsa. Salah satu hal yang dapat dilakukan untuk meningkatkan kinerja sektor pendidikan, utamanya di perguruan tinggi adalah dengan melakukan pengawasan mutu perguruan tinggi. Di Indonesia, pengawasan terhadap mutu perguruan tinggi diawasi oleh BAN-PT (Badan Akreditasi Nasional Perguruan Tinggi), baik itu bagi Perguruan Tinggi Negeri maupun Perguruan Tinggi Swasta. Salah satu bentuk kriteria penilaian yang dipergunakan sebagai akreditasi adalah dari kinerja perguruan tinggi. Kinerja perguruan tinggi dapat ditingkatkan dengan memperhatikan sisi layanan akademik, salah satunya adalah dengan memperhatikan proses tata kelola IT (*IT Governance*) utamanya dalam pengelolaan (manajemen) risiko.

Terdapat beberapa penelitian yang mengangkat tema IT Governance, diantaranya penelitian yang dilakukan Afifah Dewi (2020) berjudul "*Activity and Risk Identification in Audit Process on Integrated Management System to Increase Performance Efficiency of Construction Services Organization in Indonesia*". Dari penelitian tersebut diketahui bahwa perlu adanya proses identifikasi kegiatan, penentuan tujuan kegiatan, dan identifikasi risiko di dalam audit, untuk memahami bagaimana mengelola risiko dengan studi kasus penelitian tersebut di Organisasi Jasa Konstruksi Indonesia[1]. Pada penelitian lain oleh

Xiong Wang (2021) berjudul "*An Integrated FAHP-MCGP Approach to Project Selection and Resource Allocation in Risk-based Internal A*

*udit Planning: A Case Study*" mengusulkan pendekatan baru dengan menggabungkan *Fuzzy Analytic Hierarchy Process (FAHP)* dan *Multi-Choice Goal Programming (MCGP)* untuk melakukan optimalisasi proyek audit dan alokasi waktu audit internal[2]. Sedangkan Jana van Wyk (2019) dalam penelitiannya "*COBIT 5 Compliance: Best Practices Cognitive Computing Risk Assessment and Control Checklist*" melakukan penelitian menggunakan COBIT 5 dengan mengembangkan daftar checklist yang komprehensif untuk mengidentifikasi dan mengevaluasi risiko dalam *Cognitive Systems (CSs)*, serta membantu merumuskan mitigasi risiko dalam pengendalian internal[3]. Penelitian lain yang dibuat Sonia Gantman (2016) berjudul "*Communication and Control in Outsourced IS (Information System) Development Projects: Mapping to COBIT Domains*", mengusulkan pengujian mekanisme kontrol informasi sesuai dengan framework COBIT pada alat komunikasi berbasis web pada client-vendor yang digunakan dalam proyek ISD (*Information System Development*)[4]. Sedangkan penelitian yang dibuat Farida Veerankutty (2018) berjudul "*Information Technology Governance on Audit Technology Performance among Malaysian Public Sector Auditors*" menyelidiki tentang dampak IT *Governance* pada audit performa teknologi[5]. Penelitian ini memiliki sampel yang terbatas hanya pada Departemen Audit Nasional Malaysia, sehingga diperlukan penelitian lain dengan domain yang berbeda. Pavankumar (2019) membuat penelitian mengenai "*Strengthening IT Governance and Controls Using COBIT A Systematic*



*Literature Review*” yang melakukan eksplorasi framework COBIT sejak awal hingga saat ini dengan sistematik literatur review[6]. Penelitian ini mengungkapkan *overview* tentang COBIT, kekuatan dan kelemahan dari setiap framework, serta bagaimana setiap versi mengatasi kekurangan dari versi sebelumnya. Selain itu, terdapat juga analisis terperinci mengenai bagaimana framework COBIT dimanfaatkan oleh organisasi untuk mengidentifikasi dan mengurangi risiko TI. Dari penelitian di atas diketahui bahwa IT *Governance* memiliki peranan penting bagi perusahaan.

Pemilihan COBIT 2019 sebagai framework yang dipergunakan untuk penelitian, berangkat dari perbandingan antara framework COBIT dengan berbagai framework lain. Berikut beberapa perbandingan dari framework tersebut: ITIL utamanya lebih dikenal untuk penggunaan dalam IT *Service Management* (Great Britain, 2007); sedangkan ISO 9001 berisi tentang Sistem Manajemen Mutu (Kymal, 2016); ISO 27001 berisi tentang Sistem Manajemen Keamanan Informasi; COSO dipergunakan dalam sistem pengendalian internal (Moeller, 2014); TOGAF dipergunakan dalam pengembangan arsitektur perusahaan (The Open Group, 2010); CMMI-DEV digunakan untuk proses pengembangan produk dan jasa; CMMI-ACQ digunakan untuk manajemen *supplychain*, akuisisi, serta mengontrol proses *outsourcing* (Burwick, 2007). Sedangkan COBIT sebagai framework memiliki peranan penting melalui *enabler*-nya yang memberikan dua perspektif yaitu sebagai *risk function perspective* dan *risk management perspective* (ISACA, 2020). *Risk management perspective* dalam hal ini dapat

digunakan untuk mengurangi kerentanan pada keamanan sistem, mengurangi risiko kemungkinan kehilangan data, serta melakukan penilaian risiko.

Selain itu dalam penelitian Pavankumar (2019) disebutkan bahwa penggunaan COBIT sebagai framework IT *Governance* saat ini lebih berfokus pada ruang lingkup finansial dan akuntansi saja, sehingga diperlukan eksplorasi dalam berbagai industri lainnya termasuk dalam sektor pendidikan. Eksplorasi yang dilakukan dalam penelitian ini yaitu bagaimana melakukan kustomisasi COBIT di dalam sektor pendidikan dengan studi kasus di Politeknik Negeri Sriwijaya. Pemilihan COBIT 2019 bila dibandingkan dengan versi sebelumnya karena COBIT 2019 sudah mencakup dan menyempurnakan komponen pada versi sebelumnya. Selain itu rekomendasi yang dihasilkan dengan menggunakan COBIT 2019 bisa membantu dalam meminimalkan risiko pada bidang pengelolaan IT. COBIT 2019 yang dikembangkan oleh ISACA melakukan evolusi secara konstan dan berkelanjutan sehingga mampu menjaga tata kelola TI dan operasi manajemen (ISACA, 2020).

Tujuan tata kelola dan manajemen dalam COBIT dikelompokkan kedalam lima domain yang mengungkapkan tujuan utama dan bidang kegiatan tujuan yang dikandung didalamnya[7]:

1. Tujuan tata kelola (*governance objective*) yang dikelompokkan dalam domain *Evaluate, Direct, Monitor* (EDM). Dalam domain ini, *governance* melakukan evaluasi opsi strategis, mengarahkan manajemen senior pada opsi strategis yang dipilih, dan memantau pencapaian strategi.

2. Tujuan pengelolaan (*management objective*) yang dikelompokkan dalam empat domain, yaitu:

- a. *Align, Plan, Organize* (APO) membahas keseluruhan organisasi, strategi, dan kegiatan pendukung untuk I&T;
- b. *Build, Acquire, Implement* (BAI) membahas definisi, akuisisi, dan implementasi solusi I&T, serta integrasi dalam proses bisnis;
- c. *Deliver, Service, Support* (DSS) membahas *operational delivery* dan dukungan layanan I&T, termasuk keamanan;
- d. *Monitor, Evaluate, Assess* (MEA) membahas pemantauan kinerja dan kesesuaian I&T dengan target performa internal, *internal control objectives*, dan *external requirement*.

Pada penelitian ini studi kasus yang digunakan yaitu pada Politeknik Negeri Sriwijaya. Politeknik Negeri Sriwijaya sebagai salah satu lembaga pendidikan yang berada di kota Palembang sudah menggunakan layanan Sistem Informasi Manajemen terintegrasi. Sistem ini bertujuan untuk menunjang dalam pengambilan keputusan dari proses kegiatan akademik. Sistem informasi yang ada di Politeknik Negeri Sriwijaya meliputi Sistem Informasi Akademik, Sistem Informasi Mahasiswa, Sistem Informasi SDM, Sistem Informasi Keuangan, Sistem Informasi Perpustakaan, Sistem Informasi Aset dan Fasilitas, Sistem Informasi Penelitian, Sistem Informasi Pelaporan, Sistem Informasi *E-learning*, Sisrem Informasi P2M (Penjamin Mutu), Sistem Informasi Beasiswa, Sistem Informasi SISAK, dan Sistem Informasi *Business Intelligent*.

Politeknik Negeri Sriwijaya menyadari pentingnya penggunaan IT dalam mengelola segala aktivitas, namun terkadang terjadi beberapa risiko dalam pelaksanaan aktivitas bisnisnya. Penggunaan audit sudah mulai dipergunakan oleh Polsri diantaranya dengan menggunakan Standar Manajemen Mutu ISO 9001:2015 di bulan November 2019 tersebut menemukan bahwa belum ada kesalahan mayor dan minor yang terdeteksi.

Dari beberapa layanan Sistem Informasi Manajemen di Politeknik Negeri Sriwijaya yang disebutkan sebelumnya, masih ada yang belum terintegrasi dengan optimal. Beberapa sistem informasi masih bersifat *offline* diantaranya yaitu Sistem Informasi Mahasiswa, SIM Keuangan, dan SIM Penelitian. Beberapa kendala lain yang terjadi diantaranya belum adanya *Standard Operational Procedure (SOP)* yang terkait dengan pengelolaan resiko IT. SOP yang ada saat ini di Polsri meliputi SOP Usulan Sertifikasi Dosen, SOP Penyusunan RAP DIPA PNBP UNS, SOP Pengadaan Barang/Jasa, SOP Penghapusan Barang Milik Negara, SOP Pemberian Beasiswa, SOP Pemberian Keringanan SPP, SOP Penerimaan CPNS, dan SOP Perencanaan Program dan Penganggaran Tahunan.

Permasalahan utama dalam penelitian ini adalah masih sedikitnya penelitian dengan menggunakan framework COBIT 2019 di sektor pendidikan, sehingga perlu kustomisasi dalam penggunaannya. Untuk menutup kekosongan pengetahuan mengenai penggunaan COBIT 2019 dalam instansi pendidikan maka dibuatlah penelitian ini. Selain itu masalah ketiadaan SOP untuk pengelolaan risiko IT contohnya pada studi kasus yang dilakukan yaitu di Polsri tentunya dapat mengganggu serta menghambat pelaksanaan aktivitas bisnis di Polsri. Solusi dari



permasalahan tersebut adalah dengan melakukan pengukuran risiko terhadap penerapan teknologi informasi. Pengukuran risiko dilakukan dengan terlebih dahulu mengetahui profil risiko dari Polsri, kemudian melakukan analisis terhadap risiko yang ditemukan, dan merespon pengelolaan risiko (manajemen risiko). Hasil output yang diharapkan dari penelitian ini adalah mengenai pengukuran tingkat kapabilitas pada Polsri dan rekomendasi untuk melakukan pengelolaan risiko (manajemen risiko). Pengujian penelitian dilakukan dengan melakukan validasi data hasil audit dengan kenyataan di lapangan.

Dari latar belakang yang disebutkan diatas, peneliti mengambil judul “Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya”.

## **1.2. Rumusan Masalah**

Berdasarkan latar belakang masalah diatas, peneliti merumuskan beberapa masalah diantaranya sebagai berikut:

1. Berapa tingkat *capability* level Politeknik Negeri Sriwijaya saat ini bila diukur menggunakan COBIT 2019?
2. Bagaimana cara melakukan eksplorasi dan kustomisasi COBIT 2019 di sektor pendidikan?
3. Bagaimana langkah melakukan analisis pengelolaan risiko dengan menggunakan COBIT 2019 di Politeknik Negeri Sriwijaya?

### 1.3. Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut:

1. Penelitian mengenai pengelolaan risiko ini dibatasi pada kegiatan layanan akademik dengan studi kasus di Politeknik Negeri Sriwijaya, dan tidak membahas kegiatan layanan lain yang berada di Politeknik Negeri Sriwijaya.
2. Hasil temuan dan solusi yang ada merupakan hasil dari penelitian mengenai pengelolaan risiko pada layanan akademik di Politeknik Negeri Sriwijaya.
3. Framework penelitian hanya menggunakan COBIT 2019 sebagai standar audit dengan menggunakan cobit DFI sampai DF4.
4. Responden penelitian ini adalah pegawai tetap Politeknik Negeri Sriwijaya dengan kriteria responden berdasar panduan yang ada di COBIT 2019.
5. Perhitungan kuisioner yang dilakukan pada penelitian ini menggunakan Skala Guttman dengan menggolongkan jawaban dari responden menjadi dua bagian yaitu Ya atau Tidak.
6. Penelitian yang dilakukan hanya terbatas pada audit sistem layanan akademik dan pemberian rekomendasi.

### 1.4. Tujuan Penelitian

Berdasarkan uraian penelitian di atas, penelitian ini memiliki tujuan sebagai berikut:

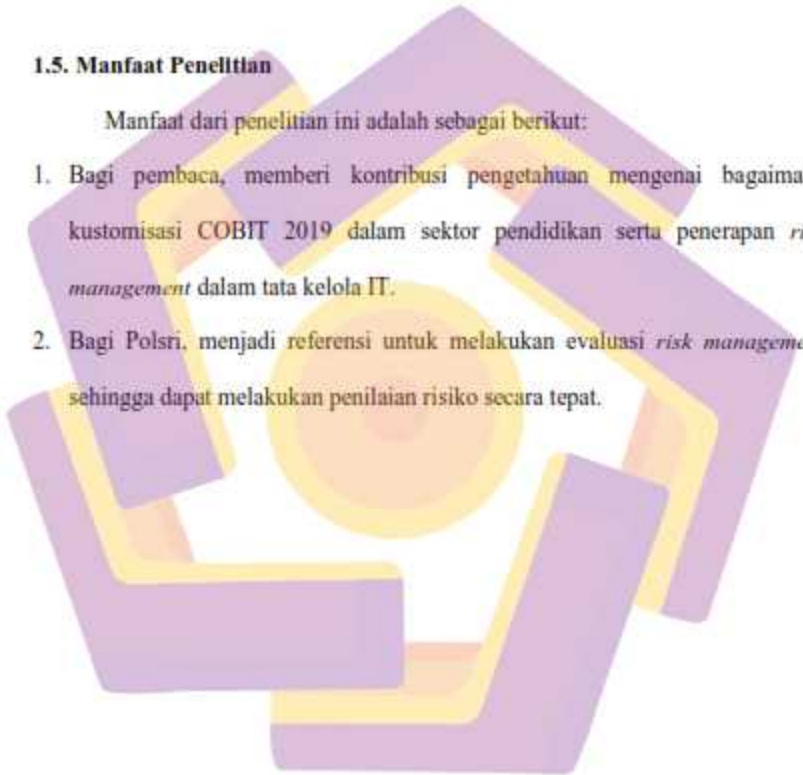
1. Mengetahui tingkat *capability* level Politeknik Negeri Sriwijaya saat ini bila diukur menggunakan COBIT 2019.

2. Mengetahui cara melakukan eksplorasi dan kustomisasi COBIT 2019 di sektor pendidikan.
3. Mengetahui langkah analisis pengelolaan risiko dengan menggunakan COBIT 2019 di Politeknik Negeri Sriwijaya.

### **1.5. Manfaat Penelitian**

Manfaat dari penelitian ini adalah sebagai berikut:

1. Bagi pembaca, memberi kontribusi pengetahuan mengenai bagaimana kustomisasi COBIT 2019 dalam sektor pendidikan serta penerapan *risk management* dalam tata kelola IT.
2. Bagi Polsri, menjadi referensi untuk melakukan evaluasi *risk management* sehingga dapat melakukan penilaian risiko secara tepat.





## BAB II

### TINJAUAN PUSTAKA

#### 2.1. Tinjauan Pustaka

Penelitian ini membahas mengenai model pengelolaan risiko teknologi informasi berbasis COBIT untuk meningkatkan layanan akademik di Politeknik Negeri Sriwijaya. Penelitian ini akan melakukan pengukuran risiko terhadap penerapan teknologi informasi di Polsri. Pengukuran risiko dilakukan dengan terlebih dahulu mengetahui profil risiko, kemudian melakukan analisis terhadap risiko yang ditemukan, dan merespon pengelolaan risiko (manajemen risiko).

Penelitian pertama dilakukan oleh Afifah Dewi (2020) bertujuan untuk mengidentifikasi kegiatan yang dilakukan dalam proses audit yang mempengaruhi efisiensi kinerja organisasi jasa konstruksi di Indonesia, menentukan tujuan kegiatan audit, mengidentifikasi risiko dari aktivitas, serta memahami bagaimana melakukan pengelolaan risiko. Hasil dari penelitian ini berupa *form* berisi kegiatan, tujuan, dan risiko yang diintegrasikan dalam proses audit manajemen. Dari hasil penelitian tersebut dapat dilihat apakah kegiatan, tujuan, dan risiko tersebut berpengaruh terhadap peningkatan efisiensi kinerja organisasi jasa konstruksi di Indonesia, serta mengetahui cara pengelolaan risiko. Audit yang dilakukan dalam penelitian ini menggunakan framework ISO dengan metode analisa *survey* menggunakan model Delphi.

Penelitian yang dibuat oleh Xiong Wang (2021) mengusulkan pendekatan baru dengan menggabungkan *Fuzzy Analytic Hierarchy Process (FAHP)* dan

*Multi-Choice Goal Programming* (MCGP) yang digunakan untuk optimalisasi proyek audit dan perhitungan alokasi waktu audit internal. Dari penelitian tersebut diketahui bahwa pendekatan FAHP-MCGP dapat dimanfaatkan dalam mengoptimalkan masalah perencanaan suatu proyek audit, penugasan, pengambilan keputusan dalam pemilihan proyek dan alokasi sumber daya. Penelitian ini menggunakan *Risk-based internal auditing* dengan menggunakan standar *International Standards for The Professional Practice of Internal Auditing* dan pendekatan baru dengan menggabungkan *Fuzzy Analytic Hierarchy Process* (FAHP) dan *Multi-Choice Goal Programming* (MCGP).

Penelitian lainnya dibuat oleh Jana van Wyk (2019) bertujuan untuk mengembangkan daftar *checklist* yang komprehensif untuk digunakan dalam mengidentifikasi dan mengevaluasi risiko dalam *Cognitive Systems* (CSs) yang membantu dalam merumuskan mitigasi pengendalian internal untuk mengatasi risiko. Menurut penelitian ini pada tingkat strategis, perusahaan harus mengembangkan tata kelola CC (*Cognitive Computing*) yang disertai dengan daftar kebijakan komprehensif untuk memberikan pedoman praktis dalam implementasi dan perancangan strategi sumber daya manusia. Sementara pada tingkat operasional atau teknologi, perusahaan harus menerapkan teknik untuk mendeteksi dan mengurangi risiko (termasuk di dalamnya *data control*, *infrastructure control*, *supplier control*, dan *lifecycle control*). Dari penelitian ini diketahui bahwa implementasi COBIT dapat memberikan pengendalian internal dan mengatasi risiko dengan melakukan kontrol di tingkat strategis maupun

operasional atau teknologi. Hasil dari penelitian ini berupa daftar *checklist* yang menyoroti *risk exposure* yang perlu ditangani.

Penelitian yang dilakukan oleh Sonia Gantman (2016) mengusulkan pengujian mekanisme kontrol informasi sesuai dengan framework COBIT pada alat komunikasi *client-vendor* yang digunakan dalam proyek ISD (*Information System Development*). Dari penelitian ini dapat disimpulkan bahwa alat komunikasi berbasis web (seperti *shared online document*, wiki, dan forum diskusi) yang fleksibel dapat membantu dalam melakukan aktivitas pengendalian (*control purpose*) bila disusun sesuai panduan dalam framework COBIT, terutama dalam manajemen risiko dan penilaian kinerja. Pada penelitian ini menggunakan COBIT 5 dengan domain APO06, BAI02, BAI06, DSS03, dan MEA01. Penelitian ini memberi landasan untuk penelitian selanjutnya tentang peran *control internal* dalam *communication practices* dengan vendor eksternal. Dengan melakukan analisis terhadap *type tools*, *control objective* dan *project*. Selain itu diperlukan audit dalam kontrol formal dan informal dalam pengendalian.

Sedangkan Farida Veerankutty (2018) menyelidiki dampak IT *Governance* pada audit *technology performance*. Sampel *survey* yang dilakukan pada penelitian ini terbatas pada *National Audit Department of Malaysia*. Dari penelitian yang dilakukan didapat bahwa IT *Governance* memiliki peran penting dalam memastikan keberhasilan pemanfaatan audit teknologi. Mekanisme IT *Governance* seperti IT strategi dan manajemen *support* memiliki pengaruh signifikan terhadap audit *technology performance*. Pengujian hipotesis dalam IT *Governance* dilakukan dengan menggunakan teknik *Partial Least Square (PLS)*.

Pavankumar (2019) melakukan eksplorasi framework COBIT sejak awal hingga saat ini dengan menggunakan metode sistematik literatur review, memberikan overview tentang *the need of COBIT*, kekuatan dan kelemahan setiap framework, dan bagaimana setiap versi mengatasi kekurangan dari versi sebelumnya. Selain itu penelitian ini juga membahas *state of art* dari framework COBIT 5 serta menyajikan analisis terperinci mengenai bagaimana COBIT dimanfaatkan oleh organisasi untuk mengidentifikasi dan mengurangi risiko TI. Di dalam penelitian ini diketahui bahwa COBIT sudah dipergunakan sejak tahun 1996 dan menjadi salah satu standar yang sudah *acceptable* sebagai panduan dalam kontrol IT. COBIT diklasifikasikan ke dalam empat major domain yaitu *planning and organization, acquisition and implementation, delivery and support, dan monitoring*. Dari hasil sistematik literatur review terhadap sebagian besar makalah penelitian, lebih dari 50 penelitian diterbitkan setelah pengenalan COBIT 4.1. Dapat dikatakan bahwa setiap kemunculan versi baru dari COBIT semakin banyak juga perhatian baik dari pihak industri maupun dari para peneliti. Selain itu diketahui juga bahwa penggunaan framework COBIT memiliki peranan penting melalui *enabler*-nya yang memberikan dua perspektif yaitu sebagai *risk function perspective* dan *risk management perspective*.



## 2.2. Keaslian Penelitian

Tabel 2.1. Matriks literatur review dan posisi penelitian Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	<i>Activity and Risk Identification in Audit Process on Integrated Management System to Increase Performance Efficiency of Construction Services Organization In Indonesia</i>	Afifah Dewi, IOP Conference Series: Earth and Environmental Science, 2020	<ul style="list-style-type: none"> <li>a. Mengidentifikasi kegiatan yang dilakukan dalam proses audit</li> <li>b. Menentukan tujuan kegiatan dalam proses audit</li> <li>c. Mengidentifikasi risiko dari aktivitas di dalam domain</li> <li>d. Memahami bagaimana cara pengelolaan risiko</li> </ul>	Kegiatan identifikasi didalam proses audit digunakan untuk mengetahui risiko mana yang paling dominan dalam suatu perusahaan serta menemukan strategi manajemen risiko yang tepat.	Pada penelitian ini aktivitas yang mengarah pada risiko dominan adalah aktivitas yang berkaitan dengan manajemen organisasi, komunikasi dalam organisasi, tanggung jawab setiap individu dalam organisasi, pemahaman tentang sistem manajemen terintegrasi dan cara menerapkannya.	Penelitian ini menggunakan framework ISO dengan metode analisa <i>survey</i> model Delphi untuk mengetahui risiko dominan dan strategi manajemen risiko yang tepat di organisasi jasa konstruksi di Indonesia. Penelitian yang diusulkan menggunakan framework COBIT 2019 dengan perhitungan menggunakan skala guttman. Domain yang dipergunakan yaitu domain BAI06, BAI10, DSS01, DSS02. Selain untuk mengetahui tingkat <i>capability</i> level pada Polstri, penelitian bertujuan untuk mengetahui bagaimana kustomisasi COBIT di dunia pendidikan dalam hal ini di Polstri.

Tabel 2.1. Matriks literatur review dan posisi penelitian (lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
2	<i>An Integrated FAHP-MCGP Approach to Project Selection and Resource Allocation in Risk-Based Internal Audit Planning</i>	Xiong Wang, Jurnal <i>Computers &amp; Industrial Engineering</i> , 2021	Mengusulkan pendekatan baru dengan menggabungkan <i>Fuzzy Analytic Hierarchy Process (FAHP)</i> dan <i>Multi-Choice Goal Programming (MCGP)</i> untuk mengisi gap antara teknik prioritas dan alokasi (untuk optimalisasi proyek audit dan alokasi waktu audit internal)	Pendekatan FAHP-MCGP berguna untuk memilih proyek potensial dan mengalokasikan waktu staf selama audit internal berbasis risiko	Pendekatan FAHP-MCGP dapat dimanfaatkan dalam mengoptimalkan masalah perencanaan suatu proyek audit, penugasan, pengambilan keputusan, termasuk pemilihan proyek dan alokasi sumber daya perusahaan.	Penelitian ini menggunakan <i>Risk-based internal auditing</i> dengan menggunakan standar <i>International Standards for The Professional Practice of Internal Auditing</i> dan pendekatan baru dengan menggabungkan <i>Fuzzy Analytic Hierarchy Process (FAHP)</i> dan <i>Multi-Choice Goal Programming (MCGP)</i> . Penelitian yang diusulkan menggunakan framework COBIT 2019 akan melakukan eksplorasi cobit di sektor pendidikan. Eksplorasi ini dilakukan dengan melakukan kustomisasi DF1 sampai DF4 sehingga selaras dengan tata kelola yang berjalan di Polstri.

Tabel 2.1. Matriks literatur review dan posisi penelitian (lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
3	<i>COBIT 5 Compliance: --Best Practices Cognitive Computing Risk Assessment and Control Checklist</i>	Jana van Wyk, Jurnal Meditari Accountancy Research, 2019	Mengembangkan daftar <i>checklist</i> yang komprehensif untuk digunakan dalam mengidentifikasi dan mengevaluasi risiko dalam <i>Cognitive Systems (CSs)</i> dan membantu dalam merumuskan mitigasi pengendalian internal yang dapat mengatasi risiko	<p>a. Pada tingkat strategis, perusahaan harus mengembangkan tata kelola CC (<i>Cognitive Computing</i>) yang disertai dengan daftar kebijakan komprehensif untuk memberikan pedoman praktis dalam implementasi dan perancangan strategi SDM</p> <p>b. Pada tingkat operasional atau teknologi, perusahaan harus menerapkan teknik untuk mendeteksi dan mengurangi risiko (termasuk data <i>control, infrastructure control, supplier control, dan lifecycle control</i>)</p>	Implementasi COBIT dapat memberikan pengendalian internal dan mengatasi risiko baik dalam kontrol tingkat strategis maupun tingkat operasional atau teknologi	Penelitian ini menggunakan framework COBIT 5 dan menghasilkan daftar <i>checklist</i> yang menyoroti <i>risk exposure</i> yang perlu ditangani. Penelitian yang diusulkan menggunakan COBIT 2019 akan menghasilkan daftar usulan atau rekomendasi dokumen yang perlu dibuat oleh Polsri untuk menangani dan memonitor pengelolaan risiko di Polsri. Selain itu terdapat juga justifikasi berdasar kebutuhan Polsri terhadap rekomendasi yang diusulkan.



Tabel 2.1. Matriks literatur review dan posisi penelitian (lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
4	<i>Communication and Control in Outsourced IS (Information System) Development Projects: Mapping to COBIT Domains</i>	Sonia Gantman, <i>International Journal of Accounting Information System</i> , 2016	Mengusulkan pengujian mekanisme kontrol informasi sesuai framework COBIT pada alat komunikasi <i>client-vendor</i> yang digunakan dalam proyek ISD ( <i>Information System Development</i> )	Alat komunikasi berbasis web (seperti <i>shared online document</i> , wiki, dan forum diskusi) yang fleksibel dapat membantu dalam melakukan aktivitas pengendalian bila digunakan sesuai panduan dalam framework COBIT, terutama dalam manajemen risiko dan penilaian kinerja.	Penelitian ini memberi landasan untuk penelitian lanjutan tentang peran kontrol internal dalam <i>communication practices</i> dengan vendor eksternal. Dengan melakukan analisis terhadap tipe <i>tools</i> , <i>control objective</i> , dan <i>project</i> . Selain itu diperlukan audit dalam kontrol formal dan informal dalam pengendalian	Penelitian ini memberikan pengetahuan bahwa diperlukan audit dalam kontrol formal dan informal untuk pengendalian. Penelitian yang diusulkan akan memberikan pengetahuan mengenai kustomisasi COBIT di dunia pendidikan untuk meningkatkan layanan akademik.
5	<i>Information Technology Governance on Audit Technology Performance among Malaysian Public Sector Auditors</i>	Farida Veerankutty, <i>Social Sciences</i> , 2018	Menyelidiki dampak IT Governance pada audit <i>technology performance</i>	IT Governance memiliki peran penting dalam memastikan keberhasilan pemanfaatan audit teknologi.	Sampel <i>survey</i> terbatas pada <i>National Audit Department of Malaysia</i> , penelitian lain yang dilakukan harus lebih teliti bila dilakukan di domain berbeda. Hasil data dengan ukuran efek kecil disebabkan tidak ada variabel lain yang relevan dalam penelitian.	Penelitian ini menggunakan model IT Governance dengan teknik <i>Partial Least Square (PLS)</i> dalam pengujian hipotesis. Justifikasi hasil rekomendasi pada penelitian diusulkan menggunakan metode diskusi untuk mengetahui apakah rekomendasi sudah sesuai dengan kebutuhan Polstri.

Tabel 2.1. Matriks literatur review dan posisi penelitian (lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
6	<i>Strengthening IT Governance and Controls Using COBIT A Systematic Literatur Review</i>	Pavankumar Mulgund, <i>International Journal of Risk and Contingency Management</i> , 2019	<p>a. Melakukan eksplorasi framework COBIT sejak awal hingga saat ini dengan metode SLR.</p> <p>b. Memberi overview COBIT kekuatan dan kelemahan, serta bagaimana setiap versi mengatasi kekurangan versi sebelumnya.</p> <p>c. Membahas <i>state of art</i> COBIT 5.</p> <p>d. Menyajikan analisis terperinci bagaimana COBIT dimanfaatkan organisasi</p>	<p>Penggunaan COBIT sebagai framework memiliki peranan penting melalui enablnernya yang memberikan perspektif:</p> <p>a. <i>Risk function perspective</i></p> <p>b. <i>Risk management perspective</i></p>	<p>Untuk penelitian lebih lanjut dapat meneliti mengenai:</p> <p>a. Bagaimana transisi organisasi dari versi COBIT sebelumnya ke saat ini</p> <p>b. Bagaimana menerapkan COBIT ketika sudah ada framework lain</p> <p>c. Bagaimana eksplorasi penggunaan COBIT dalam berbagai industri lain (saat ini lebih berfokus pada bidang keuangan dan akuntansi)</p>	<p>Penelitian ini menggunakan model sistematis literatur review dengan melihat berbagai macam paper yang mengulas tentang penggunaan COBIT dari versi awal hingga saat ini.</p> <p>Penelitian diusulkan membahas penerapan COBIT ketika sudah ada framework lain dipergunakan di Polsri (Standar Manajemen Mutu ISO 9001:2015) meski berada pada ruang lingkup berbeda.</p> <p>Penelitian yang diusulkan akan membantu menjawab saran dari penelitian Pavankumar mengenai bagaimana eksplorasi penggunaan COBIT dalam sektor lain (dalam hal ini sektor pendidikan) serta bagaimana COBIT digunakan untuk mengelola risiko dalam layanan akademik.</p>

Berdasar Tabel 2.1 diketahui bahwa kegiatan identifikasi (audit) diperlukan untuk mengetahui risiko mana yang paling dominan dalam suatu perusahaan serta untuk menemukan strategi manajemen risiko yang tepat. Selain itu implementasi COBIT dapat membantu dalam memberikan pengendalian internal dan mengatasi risiko baik dalam kontrol tingkat strategis maupun kontrol dalam tingkat operasional maupun teknologi. Eksplorasi penggunaan COBIT dapat pula dipergunakan pada sektor selain keuangan dan akuntansi, contohnya yaitu pada sektor pendidikan.

Untuk sukses melakukan kustomisasi COBIT, peneliti perlu mengetahui dan memahami terlebih dahulu kebutuhan organisasi atau dalam hal ini kebutuhan pihak perguruan tinggi. Langkah yang dilakukan adalah dengan memahami tata kelola IT yang sedang berjalan di dalamnya. Rafeq (2021) menyebutkan terdapat 7 langkah yang harus digunakan saat memilih dan melakukan kustomisasi COBIT.

Langkah 1 : Mengidentifikasi kebutuhan pemangku kepentingan

Langkah 2 : Mengidentifikasi sasaran perusahaan dan sasaran penyesuaian

Langkah 3 : Mengidentifikasi tujuan tata kelola dan manajemen

Langkah 4 : Memilih dan menyesuaikan sasaran dan metrik untuk sasaran perusahaan dan penyesuaian

Langkah 5 : Memilih dan menyesuaikan komponen tata kelola dan manajemen

Langkah 6 : Menyiapkan konten COBIT yang disesuaikan dan mengintegrasikan ke dalam praktik perusahaan

Langkah 7 : Mengimplementasikan performa dan memonitor untuk mengkonfirmasi hasil dan rekomendasi perbaikan

Ketujuh langkah yang disebutkan diatas selanjutnya akan dijelaskan di dalam COBIT Design Factor (DF) pada penelitian ini.

### **2.3. Landasan Teori**

#### **2.3.1. Konsep Dasar Audit Sistem Informasi**

Informasi merupakan salah satu sumber daya strategis suatu organisasi. Oleh karena itu, untuk mendukung tercapainya visi dan misi suatu organisasi, pengelolaan informasi menjadi salah satu kunci sukses[8]. Audit sistem informasi perlu dilakukan mengingat besarnya risiko berkaitan dengan penggunaan teknologi informasi yang dihadapi oleh organisasi, yang meliputi (Swastika, 2016):

1. Kehilangan data,
2. Kesalahan dalam pengambilan keputusan,
3. Risiko kemungkinan penyalahgunaan komputer,
4. Nilai investasi dalam teknologi informasi yang tidak sedikit dan cenderung sulit dikendalikan,
5. Aspek privasi yang tersimpan dalam sistem komputer, dan
6. Kesalahan dalam pengoperasian komputer.

Tujuan dari audit sistem informasi adalah menilai apakah pengendalian sistem informasi dapat memberikan (Swastika, 2016):



1. Pengamanan aset. Yang mencakup perangkat keras, perangkat lunak, fasilitas teknologi informasi, personil, file data, dokumentasi sistem, dan perangkat lain.
2. Integritas data. Merupakan konsep dasar audit sistem yang meliputi atribut kelengkapan, baik dan dipercaya, kemurnian, dan ketelitian.
3. Efektivitas. Sistem informasi bisa dikatakan efektif jika sistem dapat mencapai tujuannya. Untuk melakukan penilaian efektivitas dari suatu sistem perlu diketahui kebutuhan pengguna sistem, dan melakukan penilaian apakah sistem menghasilkan laporan atau informasi bermanfaat bagi *user*.
4. Efisiensi. Mencakup penggunaan sumber daya seminimal mungkin untuk menghasilkan *output* yang dibutuhkan.

### **2.3.2. Manajemen Risiko**

Manajemen risiko didorong oleh kebutuhan perusahaan untuk menunjukkan tata kelola perusahaan yang baik. Perusahaan harus mengelola risiko dengan memastikan adanya transparansi tentang risiko signifikan bagi perusahaan dan mengklarifikasi pengambilan risiko atau kebijakan penghindaran risiko. Tata kelola perusahaan yang efektif untuk pengeluaran TI dapat menghasilkan penghematan biaya yang signifikan dan menempatkan perusahaan dalam posisi kuat untuk mengambil inisiatif baru yang bermanfaat[9].

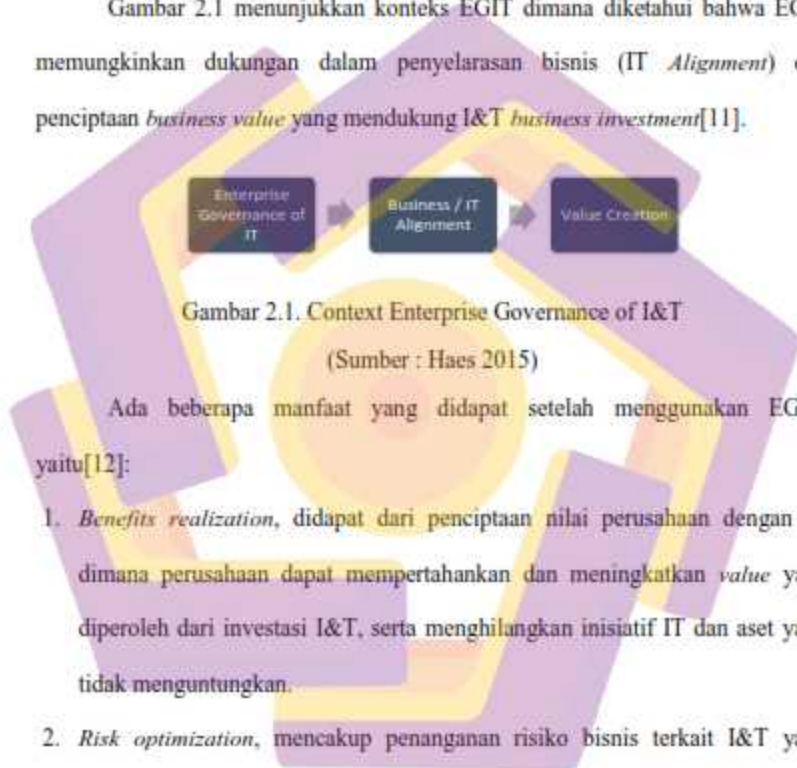
### **2.3.3. Tata Kelola TI (IT Governance)**

Tata kelola TI (*IT Governance*) berupaya menyelaraskan tujuan bisnis dengan strategi TI untuk memberikan nilai bisnis[10]. I&T dinilai penting bagi



manajemen risiko perusahaan dan *value generation*. Fokus khusus terhadap *Enterprise Governance of Information and Technology* (EGIT) sudah muncul sejak tiga dekade terakhir. EGIT merupakan suatu tata kelola informasi dan teknologi pada perusahaan yang menjadi bagian penting bagi perusahaan.

Gambar 2.1 menunjukkan konteks EGIT dimana diketahui bahwa EGIT memungkinkan dukungan dalam penyelarasan bisnis (*IT Alignment*) dan penciptaan *business value* yang mendukung I&T *business investment*[11].



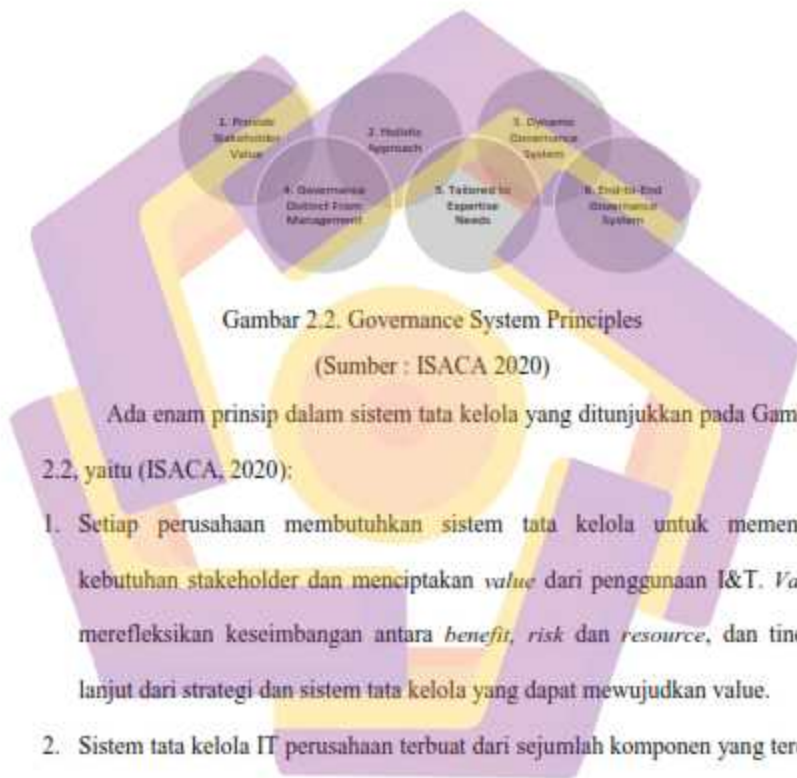
Gambar 2.1. Context Enterprise Governance of I&T

(Sumber : Haes 2015)

Ada beberapa manfaat yang didapat setelah menggunakan EGIT, yaitu[12]:

1. *Benefits realization*, didapat dari penciptaan nilai perusahaan dengan IT dimana perusahaan dapat mempertahankan dan meningkatkan *value* yang diperoleh dari investasi I&T, serta menghilangkan inisiatif IT dan aset yang tidak menguntungkan.
2. *Risk optimization*, mencakup penanganan risiko bisnis terkait I&T yang berdampak pada bisnis. Manajemen risiko terkait I&T harus dapat diintegrasikan dan diukur dengan melihat dampak dan kontribusi dari optimisasi risiko bisnis terkait I&T.

3. *Resource optimization*, mencakup pengetahuan mengenai kemampuan perusahaan dalam melaksanakan *strategic plan* dengan penyediaan sumber daya yang memadai, tepat dan efektif.



Gambar 2.2. Governance System Principles

(Sumber : ISACA 2020)

Ada enam prinsip dalam sistem tata kelola yang ditunjukkan pada Gambar 2.2, yaitu (ISACA, 2020):

1. Setiap perusahaan membutuhkan sistem tata kelola untuk memenuhi kebutuhan stakeholder dan menciptakan *value* dari penggunaan I&T. *Value* merefleksikan keseimbangan antara *benefit*, *risk* dan *resource*, dan tindak lanjut dari strategi dan sistem tata kelola yang dapat mewujudkan *value*.
2. Sistem tata kelola IT perusahaan terbuat dari sejumlah komponen yang terdiri dari tipe yang berbeda dan bekerja sama dengan *holistic*.
3. Sistem perusahaan harus dinamis dalam menerima perubahan. Karena setiap ada perubahan (misal perubahan strategi atau teknologi), dampak yang berpengaruh pada sistem EGIT harus bisa dipertimbangkan, sehingga sistem EGIT layak dan bertahan.

4. Sistem tata kelola harus dapat membedakan antara kegiatan dan aktivitas perusahaan serta manajemen.
5. Sistem tata kelola harus disesuaikan dengan kebutuhan perusahaan dengan DF sesuai parameter untuk kustomisasi dan memprioritaskan komponen sistem tata kelola.
6. Sistem tata kelola harus mencakup keseluruhan perusahaan, dengan fokus tidak hanya pada fungsi IT tetapi pada semua proses IT di perusahaan untuk mencapai tujuan.

#### 2.3.4. Framework IT Governance

Terdapat beberapa framework yang dipergunakan dalam melakukan audit IT Governance diantaranya adalah ITIL, ISO 9001:2015, COSO, TOGAF, CMMI, dan COBIT.

##### 2.3.4.1. ITIL

ITIL (*Information Technology Infrastructure Library*) memberi penjelasan rinci mengenai beberapa IT *practices* yang penting dengan menggunakan *checklist*, *task*, prosedur, dan *responsibility* yang dapat disesuaikan dengan organisasi IT apa saja. Sejauh ini ITIL lebih dikenal dalam IT *Service Management*[13].



Gambar 2.3. ITIL Service Lifecycle  
(Sumber : Great Britain 2007)

ITIL *Service Management* seperti yang terlihat pada Gambar 2.3 berfokus pada *business value* sebagai tujuan utamanya. Setiap *practice* yang ada digunakan untuk memastikan bahwa segala yang dilakukan oleh *service provider* untuk manage IT *service* bagi pelanggan bisnis dapat diukur dan dikuantifikasi sesuai dengan aturan dalam *business value*[14].

#### 2.3.4.2. ISO 9001:2015

ISO (*International Organization for Standardization*) merupakan organisasi keanggotaan non pemerintah yang membuat standar internasional di dunia. ISO secara resmi mulai beroperasi sejak 1947 dan menerbitkan standar internasional di hampir semua bidang baik teknologi maupun manufaktur. Produk ISO memiliki dua standar yaitu yang terkait dengan sistem manajemen dan non manajemen (standar teknis). Contoh produk ISO sistem manajemen yaitu ISO 9001 tentang Sistem Manajemen Mutu, ISO 14001 tentang Sistem Manajemen

Lingkungan, ISO 27001 tentang Sistem Manajemen Keamanan Informasi, dan lain-lain. Sedangkan contoh produk ISO non manajemen yaitu ISO 7810 tentang Standar Ukuran Kartu dan lain-lain.

ISO 9001 mulai digunakan sejak tahun 1987 dan pada awalnya berfokus pada bidang manufaktur. ISO 9001 membahas mengenai bagaimana suatu organisasi menerapkan praktek sistem manajemen mutu secara konsisten dalam memenuhi kebutuhan pelanggan serta pasar.

ISO 9001:2015 merupakan versi terbaru dari ISO 9001 yang memiliki beberapa perubahan dari versi sebelumnya (ISO 9001:2008), diantaranya yaitu perubahan struktur, perubahan terminologi atau istilah, konteks organisasi, pihak yang berkepentingan, *risk based thinking*, *exclusions*, *documented information*, *knowledge management*, serta kontrol proses, produk dan servis dari *provider external*[15].

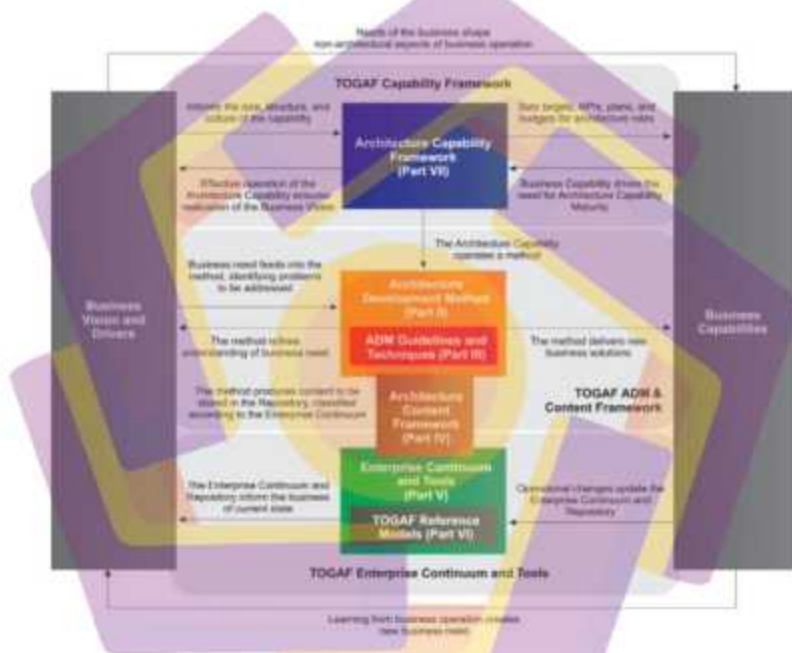
#### 2.3.4.3. COSO

COSO (*Committee of Sponsoring Organizations*) internal kontrol framework dirilis tahun 1992. COSO bukan standar formal atau standar regulasi dari pemerintah tetapi sebuah framework yang menguraikan karakteristik dan konsep sistem pengendalian internal yang efektif untuk perusahaan dari semua jenis dan ukuran[16]. Framework ini tidak mengalami perubahan sejak dirilis tahun 1992 sehingga tidak lagi mencerminkan perubahan besar dalam IT dan sistem bisnis yang ada saat ini. Namun terdapat revisi internal *control framework* COSO pada Mei 2013.



#### 2.3.4.4. TOGAF

TOGAF (*The Open Group Architecture Framework*) merupakan sebuah framework yang memiliki metode terperinci dan alat pendukung untuk mengembangkan arsitektur perusahaan[17]. TOGAF dikembangkan dan dipelihara oleh anggota The Open Group. TOGAF versi 1 dirilis tahun 1995.



Gambar 2.4. Struktur Dokumen TOGAF

(Sumber : The Open Group 2020)

Struktur dokumen TOGAF dalam Gambar 2.4 terdiri atas tujuh part utama yaitu *Introduction*, *Architecture Development Method*, *ADM Guidelines and Techniques*, *Architecture Content Framework*, *Enterprise Continuum and Tools*, *TOGAF Reference Models*, dan *Architecture Capability Framework*.

#### 2.3.4.5. CMMI

Tahun 1986 *Software Engineering Institute of Carnegie Mellon University* mulai mengembangkan framework untuk membantu organisasi dalam meningkatkan software *process*. Pengembangan framework dimulai dengan munculnya CMM (*Capability Maturity Model*) versi 1. CMM kemudian berkembang menjadi SE-CMM (*Systems Engineering Capability Maturity Model*) versi 1.1 di tahun 1995. SE-CMM kemudian diganti oleh CMMI. Tujuan dari penggunaan CMMI (*Capability Maturity Model Integration*) adalah untuk memberikan organisasi panduan mengenai bagaimana mengontrol proses dengan berfokus pada serangkaian kegiatan perbaikan yang terbatas dan bekerja secara agresif untuk mencapainya[18]. Dengan melakukan hal tersebut, organisasi dapat terus meningkatkan prosesnya dan memiliki kemampuan untuk bertahan. CMMI versi 1.2 memiliki dua buah model yaitu CMMI-DEV (*CMMI for Development*) yang dipergunakan untuk mengontrol proses pengembangan produk dan jasa, serta CMMI-ACQ (*CMMI for Acquisition*) yang dipergunakan untuk melakukan manajemen *supplychain*, akuisisi, serta mengontrol proses *outsourcing government* dan industri.

#### 2.3.4.6. COBIT

COBIT (*Control Objectives for Information and [related] Technology*) merupakan kerangka kerja tata kelola TI berbasis proses yang mewakili konsensus para ahli di seluruh dunia. COBIT dikembangkan oleh IT *Governance Institute* dan ISACA—dan pertama kali dirilis pada tahun 1996 sebagai perangkat *control*

*objective* untuk membantu auditor. COBIT 5 dirilis tahun 2012 sedangkan versi terbaru yang ada saat ini adalah COBIT 2019.

COBIT telah diselaraskan dengan standar framework lainnya seperti ITIL (*IT Infrastructure Library*), COSO (*Committee of Sponsoring Organizations of the Treadway Commission*), ISO 27001/2, PMBOK (*Project Management Book of Knowledge*), dan framework lainnya dalam pengembangan dan pengoperasian teknologi informasi. COBIT membahas tentang *business risk* (risiko bisnis), *control requirements* (persyaratan control), *compliance* (kepatuhan), dan *technical issues* (masalah teknis).

Di dalam COBIT 2019 terdapat beberapa perubahan dan update diantaranya sebagai berikut (ISACA, 2020):

1. COBIT 2019 memperkenalkan konsep baru dan penjelasan terminologi. Pada COBIT *Core Model* terdapat 40 *governance* dan *management objective* yang tergabung di dalam platform untuk memandu pengelolaan tata kelola IT.
2. Performa *management system* sudah diperbarui dan memungkinkan fleksibilitas dalam melakukan *maturity measurements* (pengukuran tingkat kematangan) serta *capability measurement* (pengukuran tingkat kemampuan).
3. Pada bagian *introduction design factor* dan fokus area terdapat panduan tambahan sehingga lebih memudahkan dalam mengadopsi COBIT 2019, baik untuk proyek tertentu maupun untuk implementasi penuh.

COBIT menawarkan berbagai macam kontrol seperti (ISACA, 2020):

1. Memotong risiko sambil mendapatkan *business value* dengan berpayung pada framework yang diterima secara global;
2. Membantu dalam memenuhi *compliance requirement*;
3. Memanfaatkan pendekatan terstruktur untuk pelaporan dan pengambilan keputusan manajemen yang lebih baik;
4. Serta memberikan solusi untuk mengontrol penilaian dan implementasi proyek untuk meningkatkan teknologi informasi dan pengendalian aset informasi.

Dalam COBIT framework terdapat empat domain IT yang berisi 40 *governance* dan *management objective IT processes* dan juga *control objective* yang dipetakan kedalam empat spesifik IT *processes*, yaitu *plan and organize*, *acquire and implement*, *deliver and support*, serta *monitor and evaluate*.

#### 2.3.4.6.1. Pemangku Kepentingan dalam Tata Kelola

Target *audience* COBIT merupakan para pemangku kepentingan EGIT yang digunakan untuk tata kelola perusahaan.

Tabel 2.2. COBIT Stakeholder

<i>Stakeholder</i>	<i>Benefit of COBIT</i>
<i>Internal Stakeholder</i>	
<i>Boards</i>	Memberi wawasan bagaimana mendapat <i>value</i> dari penggunaan I&T dan menjelaskan tanggung jawab yang terkait.
<i>Executive Management</i>	Memberi panduan bagaimana cara mengorganisasi dan memonitor performa IT di seluruh perusahaan.
<i>Business Managers</i>	Membantu memahami bagaimana mendapatkan solusi I&T yang dibutuhkan oleh perusahaan dan bagaimana cara terbaik dalam memanfaatkan teknologi baru untuk peluang strategis baru.

Tabel 2.2. COBIT Stakeholder (lanjutan)

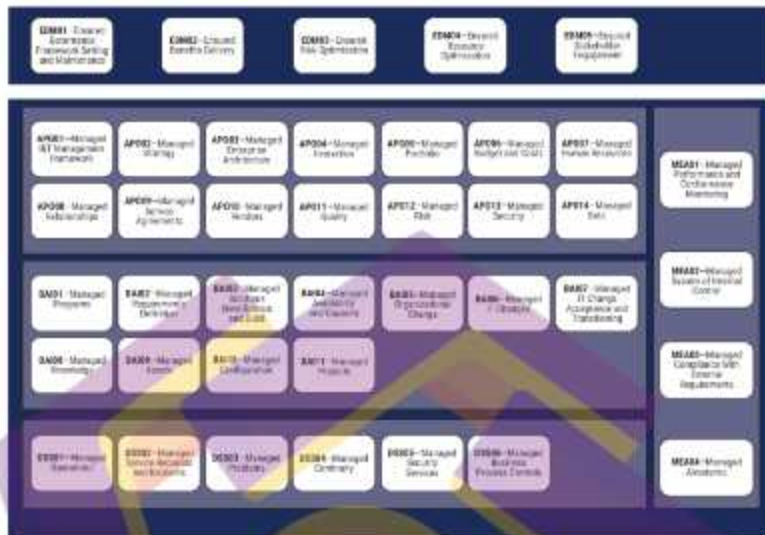
<i>Stakeholder</i>	<i>Benefit of COBIT</i>
<i>IT Managers</i>	Memberi panduan bagaimana cara terbaik membangun dan menyusun struktur dari departemen IT, manage performa IT, mengoperasikan IT yang efisien dan efektif, mengontrol biaya IT, menyelaraskan IT strategi ke prioritas bisnis, dan lain-lain.
<i>Assurance Providers</i>	Membantu manage ketergantungan pada eksternal servis provider, mendapatkan jaminan keamanan dalam IT, dan memastikan sistem kontrol internal yang efektif dan efisien.
<i>Risk Management</i>	Membantu dalam mengidentifikasi dan mengelola semua risiko terkait IT.
<i>External Stakeholders</i>	
<i>Regulators</i>	Membantu memastikan perusahaan mematuhi peraturan dan regulasi yang berlaku, serta memastikan perusahaan memiliki sistem tata kelola yang tepat dalam manage dan mempertahankan kepatuhan.
<i>Business Partners</i>	Membantu memastikan bahwa operasi bisnis partner aman, handal, dan sesuai dengan peraturan dan regulasi yang berlaku.
<i>IT Vendors</i>	Membantu memastikan bahwa operasi IT vendor aman, handal, dan sesuai dengan peraturan dan regulasi yang berlaku.

Target audiens ini mencakup semua yang bertanggungjawab dalam siklus hidup solusi tata kelola, yang dimulai dari proses desain, eksekusi, dan *assurance*.

#### 2.3.4.6.2. COBIT Core Model

COBIT *Core Model* yang memuat tujuan tata kelola dan manajemen dalam COBIT ditunjukkan pada Gambar 2.5.





Gambar 2.5. COBIT Core Model

(Sumber : ISACA 2020)

Tujuan tata kelola dan manajemen dalam COBIT dikelompokkan kedalam lima domain yang mengungkapkan tujuan utama dan bidang kegiatan tujuan yang dikandung di dalamnya (ISACA, 2020):

1. Tujuan tata kelola (*governance objective*) yang dikelompokkan dalam domain *Evaluate, Direct, Monitor* (EDM). Dalam domain ini, *governance* melakukan evaluasi opsi strategis, mengarahkan manajemen senior pada opsi strategis yang dipilih, dan memantau pencapaian strategi.
2. Tujuan pengelolaan (*management objective*) yang dikelompokkan dalam empat domain berikut:
  - a. *Align, Plan, Organize* (APO) membahas keseluruhan organisasi, strategi, dan kegiatan pendukung untuk I&T;

- b. *Build, Acquire, Implement* (BAI) membahas definisi, akuisisi, dan implementasi solusi I&T, serta integrasi dalam proses bisnis;
- c. *Deliver, Service, Support* (DSS) membahas *operational delivery* dan dukungan layanan I&T, termasuk keamanan;
- d. *Monitor, Evaluate, Assess* (MEA) membahas pemantauan kinerja dan kesesuaian I&T dengan target performa internal, *internal control objectives*, dan *external requirement*.

Untuk memenuhi tujuan tata kelola dan manajemen, setiap perusahaan perlu menetapkan, menyesuaikan, dan mempertahankan sistem tata kelola yang sudah dibangun. Komponen ini merupakan suatu faktor yang memberikan kontribusi baik pada sistem tata kelola IT di perusahaan. Komponen sistem tata kelola ini mencakup struktur organisasi, kebijakan dan prosedur, informasi, budaya dan kebiasaan, keterampilan dan kompetensi, serta servis, infrastruktur, dan aplikasi.

#### **2.3.4.6.3. Perancangan Sistem Tata Kelola**

Perancangan sistem tata kelola berdasarkan COBIT 2019 digambarkan dalam bentuk COBIT *Design Guide* yang ditunjukkan pada Gambar 2.6.



Gambar 2.6: Governance System Design Workflow

(Sumber : ISACA 2020)

Perancangan sistem tata kelola memiliki empat langkah sebagai berikut (ISACA, 2020):

1. Langkah 1 : *Understand the Enterprise Context and Strategy*

Pada langkah ini perusahaan harus memahami bagaimana konteks, strategi, dan lingkungan bisnisnya. Beberapa hal yang perlu diperhatikan yaitu *enterprise strategy*, *enterprise goals*, *I&T risk profile*, dan mengetahui *current IT related issues*. Info yang didapat kemudian diterjemahkan dalam tujuan tata kelola dan manajemen untuk membuat *initial scope* dari sistem tata kelola perusahaan.

2. Langkah 2 : *Determine the Initial Scope of the Governance System*

Pada langkah ini terdapat dua pendekatan yaitu pendekatan kualitatif dan kuantitatif. Pendekatan kualitatif lebih mempertimbangkan tujuan tata kelola dan manajemen yang paling relevan dalam menilai DF. Pendekatan kuantitatif melibatkan *mapping table* untuk setiap DF. Mapping table di COBIT 2019

biasanya berisi nilai antara 0 sampai 4. Angka 4 menunjukkan relevansi maksimal antara tujuan tata kelola atau manajemen dengan nilai DF tertentu, sedangkan angka 0 menunjukkan tidak ada relevansi.

### 3. Langkah 3 : *Refine the Scope of the Governance System*

Pada langkah ini melihat pertimbangan terhadap *landscape* ancaman, pertimbangan persyaratan kepatuhan, *role of IT*, *sourcing* model, metode implementasi IT, pertimbangan adopsi IT *strategy*, dan ukuran dari perusahaan.

### 4. Langkah 4 : *Conclude the Governance System Design*

Pada langkah ini terjadi penyelesaian permasalahan bawaan, penyimpulan desain sistem tata kelola perusahaan.

#### 2.3.4.6.4. COBIT Design Factor

*Design factor* (DF) merupakan sebuah faktor yang mempengaruhi desain dan posisi dari sistem tata kelola perusahaan sehingga bisa mendorong kesuksesan dalam penggunaan I&T (ISACA, 2020). DF dapat dibuat sesuai kebutuhan perusahaan dengan menggunakan *toolkit* bawaan COBIT 2019. Gambar 2.7 menunjukkan COBIT *design factor* dalam COBIT 2019.



Gambar 2.7. COBIT Design Factor

(Sumber : ISACA 2020)



1. *Enterprise Strategy*. Suatu perusahaan bisa memiliki strategi yang berbeda-beda, yang ditunjukkan dalam satu atau lebih tipe dalam *Enterprise Strategy Design Factor*. Suatu organisasi biasanya memiliki satu strategi utama dan paling tidak ada satu buah strategi cadangan.

Tabel 2.3. Enterprise Strategy Design Factor

Strategy Archetype	Explanation
<i>Growth/Acquisition</i>	Perusahaan berfokus pada pertumbuhan (pendapatan).
<i>Innovation/Differentiation</i>	Perusahaan berfokus menawarkan produk dan layanan yang berbeda dan inovatif ke client.
<i>Cost Leadership</i>	Perusahaan berfokus meminimalisasi biaya jangka pendek.
<i>Client Service/Stability</i>	Perusahaan berfokus pada penyediaan layanan yang stabil dan berorientasi pada klien.

2. *Enterprise Goals* yang mendukung *enterprise strategy*. *Enterprise strategy* diwujudkan dengan pencapaian dalam *enterprise goals*. Sasaran tersebut didefinisikan dalam framework COBIT yang tersusun dalam Dimensi *Balanced Scorecard* (BSC), dan mencakup hal di dalam Tabel 2.4.

Tabel 2.4. Enterprise Goals Design Factor

Reference	Dimensi Balance Scorecard (BSC)	Enterprise Goals
EG01	<i>Financial</i>	Portofolio produk dan layanan yang kompetitif.
EG02	<i>Financial</i>	Pengelolaan risiko bisnis.
EG03	<i>Financial</i>	Kepatuhan pada hukum dan peraturan eksternal.
EG04	<i>Financial</i>	Kualitas informasi keuangan.
EG05	<i>Customer</i>	Budaya layanan berorientasi pelanggan.
EG06	<i>Customer</i>	Kontinuitas dan ketersediaan layanan bisnis.
EG07	<i>Customer</i>	Kualitas dalam informasi manajemen.
EG08	<i>Internal</i>	Optimalisasi fungsionalitas proses bisnis internal.
EG09	<i>Internal</i>	Optimalisasi biaya dalam proses bisnis.
EG10	<i>Internal</i>	Keterampilan, motivasi, dan produktivitas staf.
EG11	<i>Internal</i>	Kepatuhan terhadap kebijakan internal.
EG12	<i>Growth</i>	Me-managed program transformasi digital.
EG13	<i>Growth</i>	Inovasi dalam produk dan bisnis.

3. *Risk Profile* dan *current issues* yang terkait dengan IT. *Risk profile* mengidentifikasi jenis risiko IT yang saat ini dihadapi oleh perusahaan dan menunjukkan area mana yang melebihi *risk appetite*.



Tabel 2.5. Risk Profile Design Factor

<i>Reference</i>	<i>Risk Category</i>	<i>Example Risk Scenarios</i>
1	Pengambilan keputusan dalam <i>IT-investment</i> , definisi, dan pemeliharaan portofolio	<ul style="list-style-type: none"> <li>a. Program yang dipilih untuk diimplementasi tidak selaras dengan strategi dan prioritas perusahaan.</li> <li>b. Kegagalan terkait <i>IT-investment</i> dalam mendukung strategi digital perusahaan.</li> <li>c. Pemilihan perangkat lunak yang salah untuk akusisi dan implementasi (baik dalam hal biaya, performa, fitur, kompatibilitas, redundansi, dan lainnya).</li> <li>d. Pemilihan infrastruktur yang salah untuk implementasi (dalam hal biaya, performa, fitur, kompatibilitas, dan lainnya).</li> <li>e. Duplikasi atau <i>important overlaps</i> antara inisiatif investasi yang berbeda.</li> <li>f. Ketidakcocokan jangka panjang antara <i>investment program</i> baru dan arsitektur perusahaan.</li> <li>g. <i>Misallocation</i>, manajemen yang tidak efektif, dan atau persuingan sumber daya yang tidak selaras dengan prioritas bisnis.</li> </ul>
2	Manajemen siklus hidup program dan proyek	<ul style="list-style-type: none"> <li>a. Kegagalan senior manajemen dalam menghentikan proyek yang gagal (baik karena biaya berlebihan, penundaan terlalu lama, ruang lingkup terlalu besar, maupun prioritas bisnis yang berubah).</li> <li>b. Pembengkakan anggaran proyek I&amp;T.</li> <li>c. Kualitas proyek I&amp;T yang kurang.</li> <li>d. Keterlambatan pengiriman proyek I&amp;T.</li> <li>e. Kegagalan pihak ketiga (<i>outsourcing</i>) dalam mengirimkan proyek sesuai perjanjian kontrak (bisa karena kombinasi masalah antara anggaran yang terlalu besar, masalah kualitas, <i>missing functionality</i>, maupun <i>late delivery</i>).</li> </ul>
3	IT cost dan <i>oversight</i>	<ul style="list-style-type: none"> <li>a. Ketergantungan yang terlalu besar serta penggunaan <i>user-created</i>, <i>user-defined</i>, <i>user-maintained</i> dan solusi ad hoc.</li> <li>b. Biaya yang berlebihan dan atau ketidakefektifan dalam pembelian terkait I&amp;T di luar proses pengadaan I&amp;T.</li> <li>c. Persyaratan yang tidak terpenuhi mengakibatkan tidak efektifnya <i>Service Level Agreement (SLA)</i>.</li> <li>d. Kurangnya dana untuk investasi I&amp;T.</li> </ul>

Tabel 2.5. Risk Profile Design Factor (lanjutan)

<i>Reference</i>	<i>Risk Category</i>	<i>Example Risk Scenarios</i>
4	IT expertise, skill dan behavior	<ul style="list-style-type: none"> <li>a. Kurang terampil dalam penggunaan IT (misal karena teknologi terbaru dan metode kerja).</li> <li>b. Staf IT kurang memahami bisnis sehingga mempengaruhi dalam <i>service delivery</i> ataupun kualitas proyek.</li> <li>c. Tidak mampu merekrut dan mempertahankan staf IT.</li> <li>d. Profil rekrutmen tidak sesuai dengan kebutuhan karena kurang teliti dalam proses rekrutmen.</li> <li>e. Kurangnya pelatihan dalam bidang I&amp;T.</li> <li>f. Ketergantungan terhadap IT servis dari staf tertentu.</li> </ul>
5	Enterprise Architecture	IT <ul style="list-style-type: none"> <li>a. <i>Enterprise Architecture</i> yang kompleks dan kurang fleksibel sehingga menghalangi evolusi dan ekspansi yang menyebabkan hilangnya <i>business opportunities</i>.</li> <li>b. Kegagalan dalam mengadopsi dan memanfaatkan infrastruktur baru dalam waktu yang tepat, atau adanya sikap mengabaikan infrastruktur sebelumnya.</li> <li>c. Kegagalan dalam mengadopsi dan memanfaatkan software baru (baik dari sisi fungsionalitas, optimasi, dan lain-lain) secara tepat waktu, atau kesulitan dalam meninggalkan aplikasi sebelumnya.</li> <li>d. <i>Enterprise architecture</i> tidak terdokumentasi sehingga menyebabkan inefisiensi dan duplikasi.</li> <li>e. Jumlah pengecualian dalam standar <i>enterprise architecture</i> terlalu banyak.</li> </ul>

Tabel 2.5. Risk Profile Design Factor (lanjutan)

<i>Reference</i>	<i>Risk Category</i>	<i>Example Risk Scenarios</i>
6	IT <i>operational infrastructure incidents</i>	<ul style="list-style-type: none"> <li>a. Rusaknya alat IT secara tidak sengaja.</li> <li>b. Kesalahan staf IT selama <i>backup</i>, <i>upgrade</i> sistem, serta <i>maintenance</i>.</li> <li>c. Kesalahan input informasi oleh staf IT ataupun user sistem.</li> <li>d. Rusaknya data <i>center</i> (adanya sabotase dan lain-lain) oleh staf.</li> <li>e. Pencurian perangkat yang berisi data sensitif.</li> <li>f. Pencurian komponen infrastruktur utama.</li> <li>g. <i>Error</i> dalam konfigurasi <i>hardware</i>.</li> <li>h. Pengrusakan <i>hardware</i> secara sengaja (<i>security device</i> dan lain-lain).</li> <li>i. Penyalahgunaan hak akses untuk mengakses IT <i>infrastructure</i>.</li> <li>j. Hilangnya file <i>backup</i> atau tidak efektifnya file <i>backup</i> yang ada.</li> <li>k. Hilangnya data disebabkan <i>cloud provider</i>.</li> <li>l. Gangguan layanan operasional oleh <i>cloud provider</i>.</li> </ul>
7	<i>Unauthorized actions</i>	<ul style="list-style-type: none"> <li>a. Adanya gangguan pada <i>software</i>.</li> <li>b. Modifikasi atau manipulasi <i>software</i> dengan sengaja sehingga menyebabkan data <i>incorrect</i>.</li> <li>c. Modifikasi atau manipulasi <i>software</i> dengan sengaja yang mengarah ke penipuan.</li> <li>d. Modifikasi <i>software</i> secara tidak sengaja sehingga menyebabkan <i>inaccurate result</i>.</li> <li>e. Konfigurasi yang tidak disengaja dan <i>error</i> dalam <i>change-management</i>.</li> </ul>
8	<i>Software adoption/usage problems</i>	<ul style="list-style-type: none"> <li>a. Tidak diadopsinya aplikasi <i>software</i> terbaru oleh pengguna.</li> <li>b. Penggunaan <i>software</i> baru oleh user tidak efisien.</li> </ul>

Tabel 2.5. Risk Profile Design Factor (lanjutan)

<i>Reference</i>	<i>Risk Category</i>	<i>Example Risk Scenarios</i>
9	<i>Hardware incidents</i>	<ul style="list-style-type: none"> <li>a. Sistem tidak stabil setelah instal infrastruktur baru yang menyebabkan <i>operational incident</i>.</li> <li>b. Tidak mampunya sistem dalam melakukan penanganan volume transaksi saat volume pengguna meningkat.</li> <li>c. Ketidakmampuan sistem dalam menangani beban saat ada aplikasi atau inisiatif baru diterapkan.</li> <li>d. <i>Utilities failure</i> (telekomunikasi, listrik).</li> <li>e. Kegagalan <i>hardware</i> karena <i>overheat</i> dan atau kondisi lingkungan lainnya.</li> <li>f. Rusaknya <i>hardware</i> yang menyebabkan destruksi data oleh <i>staf internal</i>.</li> <li>g. Hilangnya atau <i>disclosure media portable</i> yang berisi data sensitif (CD, <i>drive USB</i>, <i>disk portable</i>, dan lain-lain).</li> <li>h. Resolusi <i>time</i> diperpanjang atau <i>support delay</i> saat terjadi <i>hardware insiden</i>.</li> </ul>
10	<i>Software failure</i>	<ul style="list-style-type: none"> <li>a. Ketidakmampuan dalam menggunakan <i>software</i> sesuai keinginan (misal kegagalan dalam membuat <i>business model</i> atau perubahan organisasi).</li> <li>b. Implementasi <i>software</i> tidak menyeluruh (<i>early adopters</i>, adanya <i>bug</i>, dan lain-lain).</li> <li>c. Gangguan operasional saat mengoperasikan <i>software</i> baru.</li> <li>d. Kerusakan <i>regular software</i> di <i>software aplikasi</i> yang penting.</li> <li>e. <i>Software aplikasi</i> sudah usang (<i>outdate</i>, pendokumentasian buruk, biaya <i>maintenance</i> mahal, susah untuk <i>diextend</i>, tidak terintegrasi dalam arsitektur yang ada saat ini).</li> <li>f. Ketidakmampuan untuk kembali ke versi sebelumnya bila terjadi masalah operasional dengan versi baru.</li> <li>g. Kerusakan <i>software</i> karena rusaknya <i>database</i> sehingga data tidak bisa diakses.</li> </ul>

Tabel 2.5. Risk Profile Design Factor (lanjutan)

Reference	Risk Category	Example Risk Scenarios
11	<i>Logical attacks (hacking, malware, dan lain-lain)</i>	<ul style="list-style-type: none"> <li>a. <i>Unauthorized user</i> mencoba membobol sistem.</li> <li>b. <i>Service interrupt</i> karena <i>denial-of-service (DoS) attack</i>.</li> <li>c. Pengrusakan website.</li> <li>d. Serangan malware.</li> <li>e. <i>Spionase industry</i>.</li> <li>f. <i>Hactivism</i>.</li> <li>g. Pegawai yang tidak merasa puas sehingga dapat menyebabkan hilangnya data.</li> <li>h. Data perusahaan dicuri melalui <i>unauthorized access</i> dari <i>phising</i>.</li> <li>i. <i>Foreign government attacks</i> ke dalam kritikal sistem.</li> </ul>
12	<i>Third-party/supplier incidents</i>	<ul style="list-style-type: none"> <li>a. Performa <i>outsourse</i> tidak memadai dalam pengaturan <i>outsourse</i> jangka panjang (misal kurangnya pengujian <i>supplier</i> dalam kelayakan finansial, kemampuan pengiriman, dan <i>sustainability supplier service</i>).</li> <li>b. Menerima persyaratan bisnis yang tidak masuk akal dari IT <i>supplier</i>.</li> <li>c. Tidak memadainya <i>support</i> dan <i>service</i> yang diberi vendor, tidak sesuai dengan <i>Service Level Agreement (SLA)</i>.</li> <li>d. Ketidapatuhan terhadap <i>software license agreement</i> (baik dalam penggunaan atau distribusi <i>software</i> tidak berlisensi).</li> <li>e. Ketidakmampuan transfer ke alternatif <i>supplier</i> karena ketergantungan berlebih terhadap <i>supplier</i> saat ini.</li> <li>f. Pembelian IT servis (khususnya <i>cloud services</i>) tanpa melakukan konsultasi atau keterlibatan pihak IT, sehingga menyebabkan ketidakmampuan dalam mengintegrasikan servis dengan <i>in-house service</i>.</li> <li>g. SLA tidak dapat diterapkan untuk mendapatkan servis ataupun pinalti bila terdapat ketidapatuhan.</li> </ul>



Tabel 2.5. Risk Profile Design Factor (lanjutan)

<i>Reference</i>	<i>Risk Category</i>	<i>Example Risk Scenarios</i>
13	<i>Noncompliance</i>	<ul style="list-style-type: none"> <li>a. Ketidakpatuhan terhadap regulasi nasional ataupun internasional (misal <i>privacy</i>, <i>accounting</i>, manufaktur, <i>environmental</i>, dan lain-lain).</li> <li>b. Kurang sadar akan potensi perubahan peraturan yang mungkin berdampak pada bisnis.</li> <li>c. Hambatan operasional karena regulasi.</li> <li>d. Kegagalan dalam mematuhi prosedur internal.</li> </ul>
14	<i>Geopolitical issues</i>	<ul style="list-style-type: none"> <li>a. Akses yang kurang karena gangguan insiden di tempat lain.</li> <li>b. Campur tangan pemerintah dan kebijakan nasional yang mempengaruhi bisnis.</li> <li>c. <i>Targeted action</i> dari grup atau agensi yang disponsori pemerintah.</li> </ul>
15	<i>Industrial action</i>	<ul style="list-style-type: none"> <li>a. Fasilitas dan bangunan tidak bisa dipergunakan karena mogok kerja.</li> <li>b. <i>Third-party provider</i> tidak memberi layanan karena mogok.</li> <li>c. Tidak adanya staf kunci karena aksi industri (misal adanya mogok transportasi atau utilitas).</li> </ul>
16	<i>Acts of nature</i>	<ul style="list-style-type: none"> <li>a. Gempa bumi yang menyebabkan rusaknya infrastruktur IT yang penting.</li> <li>b. Tsunami yang menghancurkan tempat penting.</li> <li>c. Badai besar dan siklon tropis atau tornado yang merusak infrastruktur penting.</li> <li>d. Kebakaran besar.</li> <li>e. Banjir.</li> <li>f. Naiknya permukaan air sehingga tidak ada akses ke tempat penting.</li> <li>g. Naiknya suhu sehingga menyebabkan <i>uneconomical location</i> tidak dapat beroperasi.</li> </ul>

Tabel 2.5. Risk Profile Design Factor (lanjutan)

<i>Reference</i>	<i>Risk Category</i>	<i>Example Risk Scenarios</i>
17	<i>Technology-based innovation</i>	<ul style="list-style-type: none"> <li>a. Kegagalan dalam mengidentifikasi tren teknologi baru dan penting.</li> <li>b. Kegagalan dalam menghargai <i>value</i> dan potensi teknologi baru.</li> <li>c. Kegagalan dalam menerapkan dan memanfaatkan teknologi baru sesuai waktu (fungsionalitas, optimalisasi proses, dan lain-lain).</li> <li>d. Kegagalan dalam menyediakan teknologi yang mendukung model bisnis.</li> </ul>
18	<i>Environmental</i>	Peralatan yang tidak ramah lingkungan (misal dalam konsumsi daya dan pengemasan).
19	<i>Data dan manajemen informasi</i>	<ul style="list-style-type: none"> <li>a. Adanya kebocoran informasi sensitif ke pihak tidak berwenang karena proses penyimpanan, pengarsipan, penghapusan informasi tidak efisien.</li> <li>b. Modifikasi data yang disengaja dan berbahaya.</li> <li>c. Pengungkapan informasi sensitif yang tidak sah melalui email ataupun media sosial.</li> <li>d. Hilangnya IP dan atau kebocoran informasi.</li> </ul>

4. *I&T-related issues*. Merupakan metode yang terkait dengan *I&T risk assessment* untuk melihat masalah IT mana yang saat ini sedang dihadapi.

Tabel 2.6. I&amp;T Related Issues Design Factor

<i>Reference</i>	<i>Risk Category</i>
A	Permasalahan antara entitas IT berbeda di dalam organisasi karena persepsi dari kontribusi yang rendah terhadap <i>business value</i> .
B	Permasalahan antara departemen bisnis (contoh IT <i>customer</i> ) dan departemen IT karena gagalnya inisiatif atau persepsi dari kontribusi yang rendah terhadap <i>business value</i> .
C	Adanya insiden IT yang signifikan, contoh kehilangan data, pelanggaran keamanan, kegagalan proyek, <i>error</i> aplikasi dan lainnya yang terkait dengan IT.
D	Masalah <i>service delivery</i> oleh IT <i>outsourcer</i> .
E	Kegagalan dalam memenuhi aturan atau kontrak yang terkait IT.
F	Temuan audit regular atau laporan lainnya tentang kinerja IT yang buruk atau adanya pelaporan tentang permasalahan IT <i>quality</i> dan <i>service</i> .
G	Pengeluaran IT yang tersembunyi yang ada di luar anggaran IT yang disetujui.

Tabel 2.6. I&amp;T Related Issues Design Factor (lanjutan)

Reference	Risk Category
H	Duplikasi atau overlap dari berbagai kebijakan sehingga menyebabkan pemborosan sumber daya.
I	Sumber daya IT tidak mencukupi, staf dengan keterampilan tidak memadai, ataupun staf yang lelah.
J	IT <i>enabled changes</i> sering kali gagal memenuhi kebutuhan bisnis, adanya keterlambatan, dan melebihi anggaran.
K	<i>Board members, executives</i> , ataupun senior manajemen tidak mau terlibat dengan IT, atau tidak adanya pihak <i>business sponsor</i> yang berkomitmen menggunakan IT.
L	Model operasi IT yang kompleks dan mekanisme keputusan yang tidak jelas untuk mengambil keputusan terkait IT.
M	Biaya IT yang terlalu tinggi.
N	Gagalnya implementasi inisiatif atau inovasi baru yang disebabkan sistem dan arsitektur IT saat ini.
O	Kesenjangan antara bisnis dan pengetahuan teknis yang mengarah ke <i>user IT</i> dan bisnis atau teknologi menggunakan bahasa yang berbeda.
P	Masalah regular dengan <i>data quality</i> dan integrasi data di berbagai sumber.
Q	Komputasi pengguna akhir tingkat tinggi menyebabkan kurangnya pengawasan dan <i>quality control</i> aplikasi yang dikembangkan dan dioperasikan.
R	Business department menciptakan solusi informasi sendiri dengan sedikit atau tanpa keterlibatan dari departemen IT.
S	Ketidaktahuan dan atau ketidakpatuhan pada regulasi <i>security</i> dan <i>privacy</i> .
T	Ketidakmampuan memanfaatkan teknologi baru atau berinovasi menggunakan I&T.

5. *Threat landscape*. Landscape ancaman ditunjukkan Tabel 2.7.

Tabel 2.7. Threat Landscape Design Factor

Threat Landscape	Explanation
Normal	Perusahaan berjalan pada tingkat ancaman yang dianggap normal.
High	Karena situasi geopolitik, sektor industri atau tertentu, perusahaan berjalan di lingkungan dengan tingkat risiko ancaman yang tinggi.

6. *Compliance requirement*. Persyaratan kepatuhan dapat dilihat di Tabel 2.8.

Tabel 2.8. Compliance Requirement Design Factor

Regulatory Environment	Explanation
Low compliance requirement	Perusahaan patuh pada regular <i>compliance requirement</i> yang lebih rendah dari rata-rata.
Normal compliance requirement	Perusahaan patuh pada regular <i>compliance requirement</i> yang umum digunakan pada sektor industri lainnya.
High compliance requirement	Perusahaan patuh pada regular <i>compliance requirement</i> yang lebih tinggi dari rata-rata, terkait dengan sektor industri atau kondisi geopolitik.

7. *Role of IT*. Peran IT di dalam organisasi dapat diklasifikasikan ke dalam beberapa role diantaranya *support*, *factory*, *turnaround*, dan *strategic*.

Tabel 2.9. Role of IT Design Factor

<i>Role of IT</i>	<i>Explanation</i>
<i>Support</i>	IT bukan hal krusial dalam keberlangsungan proses bisnis dan servis, maupun untuk inovasi.
<i>Factory</i>	Ketika IT gagal akan berdampak langsung pada keberlangsungan proses bisnis dan servis. Namun IT tidak terlihat sebagai pendorong dalam inovasi proses bisnis dan servis.
<i>Turnaround</i>	IT terlihat sebagai pendorong dalam inovasi proses bisnis dan servis. Tidak ada <i>critical dependency</i> dalam IT untuk keberlangsungan proses bisnis dan servis saat ini.
<i>Strategic</i>	IT sangat penting untuk menjalankan dan berinovasi dalam proses bisnis dan servis.

8. *Sourcing model for IT*. Sourcing model dalam perusahaan dapat diklasifikasikan menjadi model *outsourcing*, *cloud*, *insourced*, dan *hybrid*.

Tabel 2.10. Sourcing Model for IT Design Factor

<i>Sourcing Model</i>	<i>Explanation</i>
<i>Outsourcing</i>	Perusahaan meminta servis ke pihak ketiga untuk menyediakan IT servis.
<i>Cloud</i>	Perusahaan memaksimalkan penggunaan <i>cloud</i> untuk menyediakan IT servis ke <i>user</i> .
<i>Insourced</i>	Perusahaan menyediakan sendiri staf IT dan IT servis.
<i>Hybrid</i>	Penerapan model campuran dengan menggabungkan ketiga model diatas.

9. *IT implementation methods*. Metode yang diterapkan perusahaan dapat diklasifikasikan dalam beberapa model implementasi IT.

Tabel 2.11. IT Implementation Method

<i>IT Implementation Model</i>	<i>Explanation</i>
<i>Agile</i>	Perusahaan menggunakan metode Agile untuk mengembangkan <i>software</i> .
<i>DevOps</i>	Perusahaan menggunakan metode DevOps untuk pembuatan, penerapan, dan pengoperasian <i>software</i> .
<i>Traditional</i>	Perusahaan menggunakan pedekatan klasik dalam pengembangan <i>software</i> ( <i>waterfall</i> ) dan memisahkan antara pengembangan dan pengoperasian <i>software</i> .
<i>Hybrid</i>	Perusahaan menerapkan campuran model implementasi IT tradisional dan modern, sering disebut juga bimodal IT.



10. *Technology adoption strategy*. Strategi penerapan teknologi dapat diterapkan dalam strategi *first mover*, *follower*, dan *slow adopter*.

Tabel 2.12. Technology Adoption Strategy Design Factor

<i>Technology Adoption Strategy</i>	<i>Explanation</i>
<i>First mover</i>	Perusahaan umumnya menerapkan teknologi baru sedini mungkin dan mencoba mendapatkan keuntungan sebagai <i>first-mover</i> .
<i>Follower</i>	Perusahaan biasanya menunggu adanya teknologi baru yang akan <i>mainstream</i> dan terbukti sebelum menerapkannya.
<i>Slow adopter</i>	Perusahaan terlambat dalam menerapkan teknologi baru.

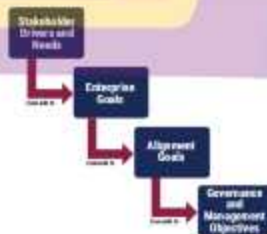
11. *Enterprise size*. Pembagian sistem tata kelola perusahaan menurut ukuran perusahaan itu dapat dibagi menjadi perusahaan besar, serta perusahaan kecil dan sedang.

Tabel 2.13. Enterprise Size Design Factor

<i>Enterprise Size</i>	<i>Explanation</i>
Perusahaan besar ( <i>default</i> )	Perusahaan dengan lebih dari 250 pekerja <i>full-time</i>
Perusahaan kecil dan sedang	Perusahaan dengan 50-250 pekerja <i>full-time</i>

#### 2.3.4.6.5. Goal Cascade

*Goal cascade* pada Gambar 2.8 menerjemahkan tujuan perusahaan menjadi prioritas dalam tujuan penyelarasan.



Gambar 2.8. Goal Cascade

(Sumber : ISACA 2020)



*Stakeholder needs* harus ditransformasikan menjadi strategi perusahaan yang kemudian ditransformasi dalam bentuk *enterprise goals*. *Enterprise goals* kemudian akan ditransformasikan menjadi *alignment goals*, yang selanjutnya akan *mensupport governance* dan *management objectives*.

### 2.3.4.6.5.1. Enterprise Goals

*Stakeholder need* dapat diturunkan dalam bentuk *enterprise goal* seperti ditunjukkan pada Tabel 2.14.

Tabel 2.14. Goals Cascade: Enterprise Goals and Metrics

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG01	Financial	Portofolio produk dan servis yang kompetitif	<ul style="list-style-type: none"> <li>a. Persentase produk dan servis memenuhi atau melampaui target pendapatan dan atau market share.</li> <li>b. Persentase produk dan servis memenuhi atau melampaui target kepuasan pelanggan.</li> <li>c. Persentase produk dan servis memberi keunggulan kompetitif.</li> <li>d. <i>Time-to-market</i> produk dan servis baru.</li> </ul>
EG02	Financial	Manage business risk	<ul style="list-style-type: none"> <li>a. Persentase tujuan dan servis bisnis yang penting dapat dicover <i>risk assessment</i>.</li> <li>b. Rasio insiden signifikan yang tidak teridentifikasi dalam <i>risk assesment</i> vs total insiden.</li> <li>c. Kesesuaian frekuensi dalam <i>update risk profile</i> yang tepat.</li> </ul>
EG03	Financial	Kepatuhan terhadap hukum dan regulasi eksternal	<ul style="list-style-type: none"> <li>a. Biaya karena ketidakpatuhan terhadap regulasi, termasuk <i>settlements</i> dan denda.</li> <li>b. Jumlah masalah ketidakpatuhan terhadap regulasi yang menimbulkan <i>public comment</i> atau publikasi negatif.</li> <li>c. Jumlah masalah ketidakpatuhan yang dicatat regulator ataupun <i>supervisor authorities</i>.</li> <li>d. Jumlah masalah ketidakpatuhan terhadap regulasi yang berkaitan dengan perjanjian kontrak dengan partner bisnis.</li> </ul>

Tabel 2.14. Goals Cascade: Enterprise Goals and Metrics (lanjutan)

<i>Reference</i>	<i>BSC Dimension</i>	<i>Enterprise Goal</i>	<i>Example Metrics</i>
EG04	<i>Financial</i>	Kualitas dari informasi finansial	<ul style="list-style-type: none"> <li>a. Survei kepuasan <i>stakeholder</i> utama tentang transparansi, pemahaman, dan keakuratan informasi finansial perusahaan.</li> <li>b. Biaya dari ketidakpatuhan terhadap regulasi dengan regulasi yang terkait dengan keuangan.</li> </ul>
EG05	<i>Customer</i>	Budaya layanan yang berorientasi pelanggan	<ul style="list-style-type: none"> <li>a. Jumlah gangguan dalam pelayanan pelanggan.</li> <li>b. Persentase <i>business stakeholder</i> yang puas dengan pelayanan pelanggan yang memenuhi level yang disetujui.</li> <li>c. Jumlah komplain pelanggan.</li> <li>d. Tren hasil survei kepuasan pelanggan.</li> </ul>
EG06	<i>Customer</i>	Kontinuitas dan ketersediaan <i>business service</i>	<ul style="list-style-type: none"> <li>a. Jumlah <i>customer service</i> atau proses bisnis yang mengalami gangguan dan menyebabkan insiden signifikan.</li> <li>b. <i>Business cost</i> dari insiden.</li> <li>c. Jumlah waktu pemrosesan bisnis yang hilang karena adanya gangguan layanan tidak terencana.</li> <li>d. Persentase komplain sebagai fungsi ketersediaan target servis.</li> </ul>
EG07	<i>Customer</i>	Kualitas dari manajemen informasi	<ul style="list-style-type: none"> <li>a. Tingkat kepuasan <i>board</i> dan manajemen eksekutif dengan informasi pengambilan keputusan.</li> <li>b. Jumlah insiden yang disebabkan keputusan bisnis yang tidak tepat karena informasi tidak akurat.</li> <li>c. Waktu yang dipersiapkan dalam memberi informasi untuk mendapatkan keefektifan dalam pengambilan keputusan.</li> <li>d. Ketepatan waktu dalam manajemen informasi.</li> </ul>
EG08	<i>Internal</i>	Optimalisasi fungsionalitas proses bisnis internal	<ul style="list-style-type: none"> <li>a. Tingkat kepuasan <i>board</i> dan manajemen eksekutif dengan kapabilitas proses bisnis.</li> <li>b. Tingkat kepuasan <i>customer</i> dengan kemampuan penyampaian servis.</li> <li>c. Tingkat kepuasan <i>supplier</i> dengan kemampuan <i>supply chain</i>.</li> </ul>
EG09	<i>Internal</i>	Optimalisasi biaya proses bisnis	<ul style="list-style-type: none"> <li>a. Rasio biaya vs pencapaian servis level.</li> <li>b. Tingkat kepuasan <i>board</i> dan manajemen eksekutif dengan biaya proses bisnis.</li> </ul>

Tabel 2.14. Goals Cascade: Enterprise Goals and Metrics (lanjutan)

<i>Reference</i>	<i>BSC Dimension</i>	<i>Enterprise Goal</i>	<i>Example Metrics</i>
EG10	<i>Internal</i>	Skill, motivasi, dan produktivitas staff	<ul style="list-style-type: none"> <li>a. Produktivitas staf dibandingkan dengan <i>benchmarks</i>.</li> <li>b. Tingkat kepuasan <i>stakeholder</i> dengan keahlian dan skill staf.</li> <li>c. Persentase staf yang memiliki keterampilan kurang dibandingkan kompetensi yang dibutuhkan untuk <i>role</i> mereka.</li> <li>d. Persentase kepuasan staf.</li> </ul>
EG11	<i>Internal</i>	Kepatuhan dengan kebijakan internal	<ul style="list-style-type: none"> <li>a. Jumlah insiden yang terkait ketidakpatuhan pada kebijakan</li> <li>b. Persentase <i>stakeholder</i> yang mengerti kebijakan yang ada.</li> <li>c. Persentase kebijakan yang disupport oleh standar dan praktik kerja yang efektif.</li> </ul>
EG12	<i>Growth</i>	Memanager program transformasi digital	<ul style="list-style-type: none"> <li>a. Jumlah program yang tepat waktu dan sesuai dengan anggaran.</li> <li>b. Persentase <i>stakeholder</i> yang puas dengan pelaksanaan program.</li> <li>c. Persentase program transformasi bisnis yang dihentikan.</li> <li>d. Persentase status <i>update</i> dari program transformasi bisnis yang dilaporkan secara teratur.</li> </ul>
EG13	<i>Growth</i>	Produk dan inovasi bisnis	<ul style="list-style-type: none"> <li>a. Tingkat kesadaran dan pemahaman tentang peluang inovasi bisnis.</li> <li>b. Kepuasan <i>stakeholder</i> terhadap level produk dan ide serta keahlian dalam berinovasi.</li> <li>c. Jumlah inisiatif produk dan servis yang disetujui yang didapat dari ide yang inovatif.</li> </ul>

#### 2.3.4.6.5.2. Alignment Goals

Dari *Enterprise Goals* kemudian diturunkan dalam bentuk *alignment goal* seperti ditunjukkan pada Tabel 2.15.

Tabel 2.15. Goals Cascade: Alignment Goals and Metrics

Reference	IT Dimension	BSC Alignment Goal	Metrics
AG01	Financial	Kepatuhan dan dukungan I&T dalam kepatuhan bisnis terhadap hukum eksternal dan regulasi	<ul style="list-style-type: none"> <li>a. Biaya ketidakpatuhan terhadap IT, termasuk settlement dan denda, yang berdampak pada hilangnya reputasi.</li> <li>b. Jumlah masalah ketidakpatuhan terkait IT yang dilaporkan pada <i>board</i> atau menyebabkan komentar publik dan aib.</li> <li>c. Jumlah masalah ketidakpatuhan berkaitan dengan perjanjian kontrak dengan IT servis provider.</li> </ul>
AG02	Financial	Memanage risiko terkait I&T	<ul style="list-style-type: none"> <li>a. Frekuensi yang tepat dalam <i>update risk profile</i>.</li> <li>b. Persentase <i>risk assessment</i> perusahaan termasuk risiko terkait I&amp;T.</li> <li>c. Jumlah insiden signifikan terkait I&amp;T yang tidak teridentifikasi dalam <i>risk assessment</i>.</li> </ul>
AG03	Financial	Realisasi <i>benefit</i> dari investasi dan servis portofolio I&T	<ul style="list-style-type: none"> <li>a. Persentase investasi I&amp;T yang <i>benefitnya</i> dapat diklaim dalam <i>business case</i> yang terpenuhi atau terdampak.</li> <li>b. Persentase I&amp;T servis yang <i>benefitnya</i> diharapkan (seperti yang ada dalam SLA) untuk direalisasikan.</li> </ul>
AG04	Financial	Kualitas dari teknologi yang terkait dengan informasi finansial	<ul style="list-style-type: none"> <li>a. Kepuasan <i>stakeholder</i> utama dengan level dari transparansi, pemahaman dan keakuratan dari informasi finansial IT.</li> <li>b. Persentase I&amp;T servis dengan biaya operasional yang ditetapkan dan disetujui serta <i>benefit</i> yang diharapkan.</li> </ul>
AG05	Customer	<i>Delivery</i> dalam I&T servis sesuai dengan bisnis <i>requirement</i>	<ul style="list-style-type: none"> <li>a. Persentase <i>stakeholder</i> bisnis yang puas dengan IT <i>service delivery</i> yang memenuhi level servis yang disepakati.</li> <li>b. Jumlah gangguan bisnis karena insiden dalam IT servis.</li> <li>c. Persentase user yang puas dengan kualitas IT servis <i>delivery</i>.</li> </ul>
AG06	Customer	Keluhan dalam mengubah <i>business requirement</i> menjadi operasional	<ul style="list-style-type: none"> <li>a. Tingkat kepuasan eksekutif bisnis dengan IT <i>responsive</i> terhadap <i>requirement</i> baru.</li> <li>b. Rata-rata <i>time-to-market</i> servis dan aplikasi baru terkait I&amp;T.</li> <li>c. Waktu rata-rata untuk mengubah strategi I&amp;T <i>objective</i> menjadi inisiatif yang disepakati dan disetujui.</li> <li>d. Jumlah kritikal proses bisnis yang disupport infrastruktur dan aplikasi yang <i>up-to-date</i>.</li> </ul>



Tabel 2.15. Goals Cascade: Alignment Goals and Metrics (lanjutan)

Reference	IT Dimension	BSC Alignment Goal	Metrics
AG07	Internal	Keamanan informasi, infrastruktur pemrosesan dan aplikasi, serta <i>privacy</i>	<ul style="list-style-type: none"> <li>a. Jumlah insiden rahasia yang membuat kerugian finansial, gangguan bisnis, dan aib publik.</li> <li>b. Jumlah insiden yang ada yang menyebabkan kerugian finansial gangguan bisnis, dan aib publik.</li> <li>c. Jumlah insiden integritas yang ada yang menyebabkan kerugian finansial gangguan bisnis, dan aib publik.</li> </ul>
AG08	Internal	Mengaktifkan dan mensupport proses bisnis dengan melakukan integrasi aplikasi dan teknologi	<ul style="list-style-type: none"> <li>a. Waktu untuk mengeksekusi bisnis servis atau proses.</li> <li>b. Jumlah program bisnis I&amp;T yang tertunda atau menimbulkan biaya tambahan karena masalah integrasi teknologi.</li> <li>c. Jumlah perubahan bisnis proses yang perlu ditunda atau dikerjakan kembali karena masalah integrasi teknologi.</li> <li>d. Jumlah aplikasi atau kritikal infrastruktur yang beroperasi dalam silo dan tidak terintegrasi.</li> </ul>
AG09	Internal	Penyampaian program yang tepat waktu, sesuai budget, dan memenuhi persyaratan serta standar kualitas	<ul style="list-style-type: none"> <li>a. Jumlah program atau proyek yang <i>on time</i> dan sesuai dengan <i>budget</i>.</li> <li>b. Jumlah program yang membutuhkan pengerjaan ulang secara signifikan karena cacat kualitas.</li> <li>c. Persentase <i>stakeholder</i> yang puas dengan kualitas program atau proyek.</li> </ul>
AG10	Internal	Kualitas manajemen informasi I&T	<ul style="list-style-type: none"> <li>a. Tingkat kepuasan user dengan kualitas dan ketepatan waktu serta ketersediaan informasi manajemen terkait I&amp;T, dengan mempertimbangkan sumber daya yang tersedia.</li> <li>b. Rasio dan tingkat keputusan bisnis yang salah dimana informasi terkait I&amp;T yang salah atau tidak tersedia merupakan suatu <i>key factor</i>.</li> <li>c. Persentase informasi yang memenuhi kriteria kualitas.</li> </ul>



Tabel 2.15. Goals Cascade: Alignment Goals and Metrics (lanjutan)

Reference	IT BSC Dimension	Alignment Goal	Metrics
AG11	Internal	Kepatuhan I&T dengan kebijakan internal	<ul style="list-style-type: none"> <li>a. Jumlah insiden terkait ketidakpatuhan terhadap kebijakan terkait IT.</li> <li>b. Jumlah pengecualian untuk kebijakan internal.</li> <li>c. Frekuensi dari peninjauan dan pembaruan kebijakan.</li> </ul>
AG12	Internal	Staf yang kompeten dan termotivasi dengan pemahaman yang baik mengenai teknologi dan bisnis	<ul style="list-style-type: none"> <li>a. Persentase pelaku bisnis yang memahami I&amp;T (yaitu mereka yang memiliki pengetahuan dan pemahaman yang diperlukan mengenai I&amp;T sebagai panduan, arahan, inovasi dan peluang I&amp;T untuk bidang keahlian mereka).</li> <li>b. Persentase orang IT yang memahami bisnis (yaitu mereka yang memiliki pengetahuan dan pemahaman yang diperlukan tentang domain bisnis yang relevan untuk memandu, mengarahkan, berinovasi, dan melihat peluang I&amp;T dalam domain bisnis).</li> <li>c. Jumlah atau persentase pebisnis dengan pengalaman dalam manajemen teknologi.</li> </ul>
AG13	Internal	Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis	<ul style="list-style-type: none"> <li>a. Tingkat kesadaran eksekutif bisnis dan pemahaman tentang kemungkinan inovasi I&amp;T.</li> <li>b. Jumlah inisiatif yang disetujui yang dihasilkan dari ide I&amp;T yang inovatif.</li> <li>c. Jumlah inovasi hebat yang diakui.</li> </ul>

### 2.3.4.6.5.3. Purpose

Tujuan dari 40 *governance* dan *management objective* yang ada dalam COBIT *Core Model* pada COBIT 2019 ditunjukkan pada Tabel 2.16.

Tabel 2.16. Governance and Management Objective and Purpose

Reference	Name	Purpose
EDM01	<i>Ensured governance framework setting and maintenance</i>	Memberi pendekatan konsisten, terintegrasi, dan sejalan dengan pendekatan tata kelola perusahaan. I&T <i>related decision</i> harus dibuat sejalan dengan strategi dan tujuan perusahaan serta terwujudnya <i>value</i> yang diharapkan. Karena itu proses terkait I&T harus diawasi dengan efektif dan transparan; harus ada kepatuhan pada legal, kontrak, dan peraturan; serta perlu ada pemenuhan persyaratan sistem tata kelola pada <i>board</i> .

Tabel 2.16. Governance and Management Objective and Purpose (lanjutan)

<i>Reference</i>	<i>Name</i>	<i>Purpose</i>
EDM02	<i>Ensured benefits delivery</i>	Mengamankan optimal <i>value</i> dari <i>IT enabled initiatives</i> , aset dan layanan, solusi dan <i>service</i> pengiriman yang hemat biaya, serta gambaran yang handal dan akurat mengenai biaya dan benefit yang dibutuhkan dan disupport oleh kebutuhan bisnis secara efektif dan efisien.
EDM03	<i>Ensured risk optimization</i>	Memastikan bahwa risiko perusahaan terkait I&T tidak melebihi <i>risk appetite</i> dan <i>risk tolerance</i> , melakukan identifikasi dan <i>manage</i> dampak dari I&T <i>risk</i> ke <i>value</i> perusahaan, serta meminimalisasi potensi kegagalan.
EDM04	<i>Ensured resource optimization</i>	Memastikan terpenuhinya kebutuhan sumber daya perusahaan secara optimal, pengoptimalan biaya I&T, dan kemungkinan peningkatan realisasi <i>benefit</i> dan persiapan terhadap perubahan di masa depan.
EDM05	<i>Ensured stakeholder engagement</i>	Memastikan <i>stakeholder</i> mendukung I&T <i>strategy</i> dan <i>roadmap</i> ; memastikan komunikasi ke <i>stakeholder</i> yang efektif dan tepat waktu; dan memastikan pada dasar pelaporan yang ditetapkan terdapat peningkatan performa. Mengidentifikasi area perbaikan dan mengkonfirmasi I&T <i>relative objective</i> dan <i>strategy</i> yang sejalan dengan strategi perusahaan.
APO01	<i>Managed I&amp;T management framework</i>	Mengimplementasikan secara konsisten pendekatan manajemen yang memenuhi persyaratan tata kelola perusahaan, mencakup komponen tata kelola seperti manajemen proses, <i>role</i> dan tanggungjawab, kegiatan yang handal dan berulang, item informasi, kebijakan dan prosedur, <i>skill</i> dan kompetensi, budaya dan perilaku, serta servis, infrastruktur dan aplikasi.
APO02	<i>Managed strategy</i>	Mensupport strategi digital transformasi dan memberi <i>value</i> sesuai harapan melalui <i>roadmap</i> dari tahapan perubahan. Penggunaan pendekatan I&T yang holistik, memastikan setiap inisiatif terhubung dengan jelas ke strategi secara menyeluruh. Mengaktifkan perubahan pada semua aspek yang berbeda, mulai dari <i>channel</i> dan proses sampai ke data, budaya, <i>skill</i> , model operasi, serta insentif.
APO03	<i>Managed enterprise architecture</i>	Merepresentasikan <i>different building blocks</i> yang membentuk perusahaan dan berbagai relasinya, serta prinsip yang membimbing dalam mendesain dan mengevaluasi setiap waktu untuk memungkinkan standar, respon dan keefisienan dalam pencapaian tujuan operasional dan strategis.
APO04	<i>Managed innovation</i>	Mendapatkan keunggulan kompetitif, inovasi bisnis, peningkatan <i>customer experience</i> , dan peningkatan efektifitas dan efisiensi dalam operasional dengan memanfaatkan I&T <i>development</i> dan teknologi yang muncul.
APO05	<i>Managed portfolio</i>	Mengoptimasi performa portofolio program secara menyeluruh dengan merespon individual program, produk dan servis performa, dan perubahan dalam prioritas serta permintaan di perusahaan.

Tabel 2.16. Governance and Management Objective and Purpose (lanjutan)

<i>Reference</i>	<i>Name</i>	<i>Purpose</i>
APO06	<i>Managed budget and costs</i>	Membina hubungan antara IT dan stakeholder perusahaan untuk memungkinkan penggunaan sumber daya terkait IT yang efektif dan efisien, serta memberi transparansi dan akuntabilitas biaya dan bisnis <i>value</i> dari solusi dan servis. Memungkinkan perusahaan untuk membuat keputusan berdasar informasi dari penggunaan IT solusi dan servis.
APO07	<i>Managed human resources</i>	Mengoptimalisasi kemampuan sumber daya manusia dalam memenuhi tujuan perusahaan.
APO08	<i>Managed relationships</i>	Memungkinkan pengetahuan, <i>skill</i> , dan perilaku yang tepat untuk menciptakan <i>outcome</i> yang lebih baik, meningkatkan percaya diri, <i>mutual trust</i> , dan penggunaan <i>resource</i> yang efektif untuk menstimulasi hubungan yang produktif dengan <i>stakeholder</i> bisnis.
APO09	<i>Managed service agreements</i>	Memastikan produk, servis, dan servis level I&T memenuhi kebutuhan perusahaan saat ini dan di masa depan.
APO10	<i>Managed vendors</i>	Mengoptimalisasi kemampuan I&T yang tersedia untuk mensupport I&T <i>strategy</i> dan <i>roadmap</i> , meminimalisasi risiko yang terkait dengan vendor yang tidak berperforma atau tidak patuh, serta memastikan harga yang ditawarkan kompetitif.
APO11	<i>Managed quality</i>	Memastikan konsistensi dalam pengiriman solusi dan servis sesuai dengan kualitas <i>requirement</i> dari perusahaan dan kepentingan stakeholder.
APO12	<i>Managed risk</i>	Melakukan integrasi manajemen risiko perusahaan yang terkait IT dengan <i>enterprise risk management</i> (ERM) serta menyeimbangkan <i>cost</i> dan <i>benefit</i> dari pengelolaan risiko perusahaan terkait I&T.
APO13	<i>Managed security</i>	Menjaga dampak dan insiden keamanan yang terjadi di perusahaan sesuai dengan level <i>risk appetite</i> .
APO14	<i>Managed data</i>	Memastikan efektifnya pemanfaatan aset data penting untuk mencapai <i>enterprise goal</i> dan objektif.
BAI01	<i>Managed programs</i>	Mewujudkan <i>business value</i> yang diinginkan dan mengurangi risiko <i>delay</i> , biaya dan <i>erosi value</i> . Untuk itu perlu adanya peningkatan komunikasi serta keterlibatan antara perusahaan dan <i>end user</i> , memastikan <i>value</i> dan kualitas dari program serta melakukan <i>follow up</i> proyek dalam program, dan memaksimalkan kontribusi program pada portofolio investasi.
BAI02	<i>Managed requirements definition</i>	Menciptakan solusi optimal untuk memenuhi kebutuhan perusahaan dengan meminimalkan risiko.
BAI03	<i>Managed solutions identification and build</i>	Memastikan pengiriman produk dan layanan digital yang lincah dan terukur. Menetapkan solusi tepat waktu dan hemat biaya (teknologi, proses bisnis, dan <i>workflow</i> ) yang mampu mendukung <i>enterprise strategic</i> dan operasional perusahaan.



Tabel 2.16. Governance and Management Objective and Purpose (lanjutan)

<i>Reference</i>	<i>Name</i>	<i>Purpose</i>
BAI04	<i>Managed availability and capacity</i>	Menjaga ketersediaan layanan, manajemen sumber daya yang efisien, optimalisasi kinerja sistem melalui prediksi kinerja di masa depan dan <i>capacity requirement</i> .
BAI05	<i>Managed organizational change</i>	Mempersiapkan komitmen stakeholder untuk perubahan bisnis dan mengurangi risiko kegagalan.
BAI06	<i>Managed IT changes</i>	Memungkinkan kecepatan dan kehandalan dalam penyampaian perubahan pada bisnis. Mengurangi risiko negatif terhadap stabilitas atau integritas lingkungan yang berubah.
BAI07	<i>Managed IT change acceptance and transitioning</i>	Mencraapkan solusi yang aman dan sesuai dengan harapan dan hasil yang disepakati.
BAI08	<i>Managed knowledge</i>	Memberi pengetahuan dan informasi manajemen yang diperlukan untuk mendukung semua staf dalam tata kelola dan manajemen I&T perusahaan dan memungkinkan pengambilan keputusan yang terinformasi.
BAI09	<i>Managed assets</i>	Memperhitungkan semua aset I&T dan mengoptimalkan nilai yang diberikan oleh pengguna.
BAI10	<i>Managed configuration</i>	Memberi informasi yang cukup tentang aset layanan untuk memungkinkan pengelolaan secara efektif. Menilai dampak perubahan dan memahami servis insiden.
BAI11	<i>Managed projects</i>	Mewujudkan hasil proyek yang ditentukan dan mengurangi risiko penundaan yang tidak terduga, biaya, dan pengurangan nilai dengan meningkatkan komunikasi dan keterlibatan bisnis dan end user. Memastikan nilai dan kualitas hasil proyek dan memaksimalkan kontribusinya pada program dan portofolio investasi yang ditentukan.
DSS01	<i>Managed operations</i>	Memberi hasil produk dan servis operasional I&T sesuai dengan yang direncanakan.
DSS02	<i>Managed service requests and incidents</i>	Meraih peningkatan dalam produktivitas dan meminimalisir gangguan dengan melakukan penyelesaian dari pertanyaan dan insiden user. Menilai dampak perubahan dan menangani insiden dari servis. Menyelesaikan permintaan user dan <i>restore service</i> sebagai respon dari insiden.
DSS03	<i>Managed problems</i>	Meningkatkan ketersediaan, meningkatkan servis level, mengurangi <i>cost</i> , meningkatkan kenyamanan dan kepuasan <i>customer</i> dengan mengurangi masalah operasional, dan mengidentifikasi akar penyebab sebagai bagian dari resolusi masalah.
DSS04	<i>Managed continuity</i>	Beradaptasi secara cepat, melanjutkan operasi bisnis, dan memaintain ketersediaan <i>resource</i> dan informasi di tingkat yang dapat diterima perusahaan bila terjadi gangguan signifikan (seperti ancaman, peluang, permintaan).

Tabel 2.16. Governance and Management Objective and Purpose (lanjutan)

<i>Reference</i>	<i>Name</i>	<i>Purpose</i>
DSS05	<i>Managed security services</i>	Meminimalkan dampak bisnis dari kerentanan serta insiden keamanan operasional informasi.
DSS06	<i>Managed business process controls</i>	Memastikan integritas informasi dan keamanan aset informasi yang ditangani dalam proses bisnis perusahaan atau operasi <i>outsourced</i> .
MEA01	<i>Managed performance and conformance monitoring</i>	Memberi transparansi performa dan kesesuaian serta mendorong pencapaian goals.
MEA02	<i>Managed system of internal control</i>	Memperoleh transparansi bagi <i>stakeholder</i> kunci tentang cukupnya sistem pengendalian internal dan memberikan kepercayaan dalam beroperasi, keyakinan dalam pencapaian <i>enterprise objective</i> , dan pemahaman memadai mengenai risiko residual.
MEA03	<i>Managed compliance with external requirements</i>	Memastikan perusahaan mematuhi semua <i>requirement external</i> yang berlaku.
MEA04	<i>Managed assurance</i>	Memungkinkan organisasi mendesain dan mengembangkan inisiatif asuransi yang efisien dan efektif, memberi panduan dalam <i>planning, scoping, execute</i> , dan tindak lanjut review asuransi, dengan menggunakan <i>roadmap</i> yang berdasar pada asuransi yang dapat diterima dengan baik.

#### 2.3.4.7. Performa Management

COBIT *Performance Management* (CPM) merujuk pada seberapa baik sistem tata kelola serta manajemen dan seluruh komponen pekerjaan pada perusahaan, serta bagaimana perusahaan dapat naik ke tingkat level yang diperlukan. CPM mencakup konsep dan metode seperti *capability level* dan *maturity level* (ISACA, 2020).



### 2.3.4.7.1. COBIT Capability Levels

Proses dalam *Capability Maturity Model Integration* (CMMI) terbagi dalam berbagai tingkat kapabilitas yang terukur mulai dari 0 hingga 5 (ISACA,2020).



Gambar 2.9. Capability Level Proses

(Sumber : ISACA 2020)

*Capability* level proses pada Gambar 2.9 menunjukkan tingkat kemampuan perusahaan dalam pengukuran performa tata kelola dan tujuan manajemen. *Capability* level mengukur seberapa baik suatu proses diimplementasi dan dilakukan. Setiap aktivitas proses dikaitkan dengan tingkat kemampuan.

Berikut keterangan dari *capability* level tiap tingkat proses (ISACA, 2020):

- 0 : Kurangnya kemampuan dasar apapun. Pendekatan yang tidak lengkap untuk mengatasi tujuan tata kelola dan manajemen. Mungkin atau mungkin tidak memenuhi maksud dari praktik proses apapun.

- 1 : Proses tersebut kurang lebih mencapai tujuannya melalui penerapan serangkaian kegiatan yang tidak lengkap yang dapat dicirikan sebagai awal atau intuitif-tidak terlalu terorganisir.
- 2 : Proses mencapai tujuannya melalui penerapan serangkaian kegiatan dasar, namun lengkap, yang dapat dicirikan sebagai dilakukan.
- 3 : Proses mencapai tujuannya dengan cara jauh lebih terorganisir menggunakan aset organisasi. Proses biasanya didefinisikan dengan baik.
- 4 : Proses mencapai tujuannya, didefinisikan dengan baik, dan kinerjanya (secara kuantitatif) terukur.
- 5 : Proses mencapai tujuannya, didefinisikan dengan baik, kinerjanya diukur untuk meningkatkan kinerja dan perbaikan terus-menerus dilakukan.

Pada penilaian aktivitas proses dapat diberikan peringkat skor dengan menggunakan metode formal yang mengarah ke serangkaian peringkat biner yang mendeskripsikan lulus atau gagal; sedangkan untuk metode kurang formal dengan menggunakan rentang nilai 1-5 (ISACA, 2020).

#### **2.3.5. Skala Guttman**

Skala Guttman merupakan skala kumulatif yang memberikan jawaban tegas, seperti jawaban benar-salah, ya-tidak, dan seterusnya[19]. Selain dalam bentuk pilihan ganda, skala Guttman dapat dibuat dalam bentuk daftar *checklist*. Untuk jawaban positif, bernilai 1; sedangkan untuk jawaban negatif bernilai 0.

### 2.3.6. Politeknik Negeri Sriwijaya

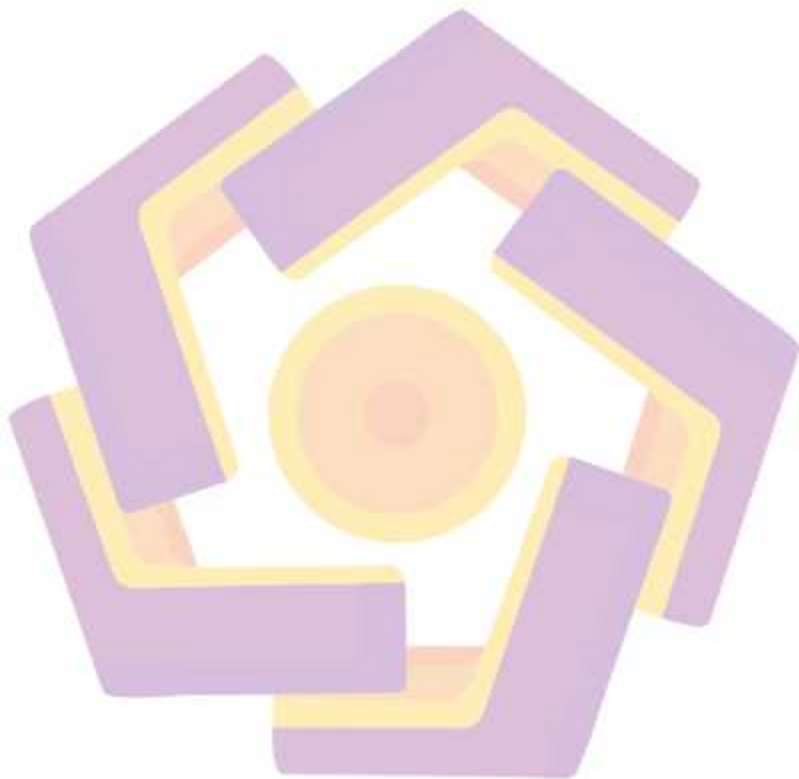
Politeknik Negeri Sriwijaya awalnya bernama Politeknik Universitas Sriwijaya yang dibuka secara resmi pada 20 September 1982. Pendirian ini bersama dengan enam PTN pertama di Indonesia sesuai dengan surat Keputusan Dirjen DIKTI Nomor 03/DJ/Kep/1979.

Pada awal pendirian Polstri hanya memiliki dua jurusan yaitu Teknik Sipil dan Teknik Mesin. Pada tahun 1986 dibukalah program studi Akuntansi dan Kesekretariatan. Sedangkan di tahun 1987 dibuka jurusan Teknik Kimia Industri dan Teknik Elektro, yang kemudian dikembangkan menjadi Teknik Listrik, Teknik Elektronika, dan Teknik Telekomunikasi. Di tahun 1992 dibukalah jurusan Akuntansi dan Administrasi Niaga.

Berdasar Keputusan Menteri Pendidikan dan Kebudayaan No. 235/O/1998 tanggal 21 September 1998 Politeknik Negeri Sriwijaya menjadi lembaga pendidikan mandiri. Selanjutnya di tahun 2002 dibuka jurusan baru yaitu Teknik Komputer dan Manajemen Informatika. Politeknik Negeri Sriwijaya saat ini sudah memiliki 9 jurusan dengan 11 program studi DIII dan 11 program studi DIV.

Struktur organisasi utama Politeknik Negeri Sriwijaya terdiri atas Direktur dan Wakil Direktur, Senat Polstri, Jurusan/Program Studi, Bagian dan Unit Penunjang lainnya. Bagian terdiri atas Bagian Akademik dan Kemahasiswaan serta Bagian Umum di bidang umum, keuangan, dan kepegawaian. Sedangkan Unsur Penunjang terdiri atas Pusat Penelitian dan Pengabdian Masyarakat (PPPM), Badan Penjaminan Mutu (BPM), Pusat Pengembangan Pendidikan dan Aktivitas Intruksional (P3AI), Satuan Pengawasan Internal (SIP), Unit Penunjang

lainnya yaitu Unit Pelaksana Teknis (UPT) yang terdiri dari tiga bagian yaitu UPT Perpustakaan, UPT Pemeliharaan dan Perbaikan, dan Unit Pelaksana Teknis TIK. Pengembangan struktur organisasi dan tata kerja akan terus dilakukan sesuai dengan kebutuhan.



## **BAB III**

### **METODE PENELITIAN**

#### **3.1. Jenis, Sifat, dan Pendekatan Penelitian**

Penelitian yang mengambil judul “Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya” ini termasuk dalam jenis penelitian studi kasus. Studi kasus yang dilakukan menggunakan sampel di Politeknik Negeri Sriwijaya.

Penelitian ini bersifat deskriptif merupakan penelitian yang mendeskripsikan atau menjelaskan mengenai objek tertentu dan menggambarkan fakta-fakta tertentu. Selain itu, penelitian ini menggunakan pendekatan kualitatif yaitu dengan melakukan pengamatan, wawancara, serta studi literatur.

#### **3.2. Metode Pengumpulan Data**

Pembagian jenis data menurut sumbernya dapat diklasifikasikan menjadi data primer dan data sekunder. Data primer merupakan data yang diperoleh dari sumber data dengan mengumpulkan secara langsung, baik melalui observasi, wawancara, dan *survey*. Sedangkan data sekunder merupakan data yang didapat dari penelitian sebelumnya.

Pada penelitian ini menggunakan jenis data primer dan data sekunder. Data primer yang didapat dari Politeknik Negeri Sriwijaya dengan melakukan wawancara dan kuisioner. Sedangkan data sekunder didapat dari literatur review terhadap penelitian-penelitian baik dari jurnal, buku, laporan, dan lain sebagainya.



### 3.3. Metode Analisis Data

Metode analisis data merupakan suatu bagian proses analisa dimana data yang ada di dalam penelitian diproses untuk mendapatkan kesimpulan dalam suatu pengambilan keputusan. Data yang digunakan pada penelitian ini berasal dari data hasil wawancara, *survey* kuisisioner, dan literatur review. Kuisisioner yang dipergunakan pada penelitian ini dapat dilihat di lampiran 2 sampai dengan lampiran 5. Sedangkan hasil data kuisisioner dapat dilihat pada lampiran 6 sampai dengan lampiran 8.

Tahapan analisis pada penelitian ini berada di tahap ketiga yang terdiri atas analisis risiko, penyusunan profil risiko, evaluasi risiko, validasi data, serta penyusunan rekomendasi di dalam *risk treatment*.

#### 1. Analisis Risiko

Analisis ini mencakup pembuatan RACI *Chart* dengan menentukan target audien atau responden yang digunakan dalam wawancara dan pengisian kuisisioner. RACI *Chart* dibuat sesuai dengan peran dan tanggung jawab yang ada di dalam RACI serta struktur jabatan.

#### Penentuan Responden

Pada COBIT 2019 penentuan RACI *Chart* terbagi dalam bagian *Responsible, Accountable, Consulted, dan Informed*[26]. Deskripsi peran dari masing-masing *role* ditunjukkan pada Tabel 3.1.

Tabel 3.1. Deskripsi role menurut COBIT 2019

No.	Role COBIT 2019	Deskripsi
1.	<i>Board</i>	Eksekutif senior dan atau direktur non-eksekutif yang bertanggungjawab terhadap tata kelola perusahaan dan mengontrol keseluruhan sumber daya perusahaan.
2.	<i>Executive Committee</i>	Sekelompok eksekutif senior yang ditunjuk dewan untuk memastikan bahwa dewan terlibat dan terus mendapat informasi tentang keputusan-keputusan besar. Bertanggungjawab mengelola portofolio investasi yang mendukung I&T, layanan I&T dan I&T aktiva, memastikan adanya penyampaian <i>value</i> , dan mengelola risiko. Biasanya diketuai seorang anggota dewan.
3.	<i>Chief Executive Officer (CEO)</i>	Petugas berpangkat tinggi yang bertanggungjawab terhadap total manajemen perusahaan.
4.	<i>Chief Financial Officer (CFO)</i>	Pejabat senior yang bertanggungjawab di semua aspek manajemen finansial termasuk risiko dan kontrol keuangan.
5.	<i>Chief Operating Officer (COO)</i>	Pejabat paling senior yang bertanggungjawab terhadap operasional perusahaan.
6.	<i>Chief Risk Officer (CRO)</i>	Pejabat paling senior yang bertanggungjawab atas semua aspek manajemen risiko di dalam perusahaan (dibentuk untuk mengawasi risiko terkait I&T).
7.	<i>Chief Information Officer (CIO)</i>	Pejabat paling senior yang bertanggungjawab menyalurkan IT dengan strategi bisnis dan bertanggungjawab dalam <i>planning, resourcing, dan manage</i> pengiriman layanan dan solusi I&T.
8.	<i>Chief Technology Officer</i>	Sebagian besar pejabat senior yang ditugaskan dalam aspek teknis I&T termasuk mengelola dan memantau keputusan terkait layanan I&T, solusi, dan infrastruktur ( <i>role</i> ini dapat diambil CIO).
9.	<i>Chief Digital Officer</i>	Sebagian besar pejabat senior yang ditugaskan untuk mempraktikkan <i>digital ambition</i> dalam perusahaan atau unit bisnis ( <i>role</i> ini dapat diambil CIO atau anggota dalam <i>executive committee</i> ).
10.	<i>I&amp;T Governance Board</i>	Sekelompok <i>stakeholder</i> dan pakar yang bertanggungjawab memandu dalam masalah dan keputusan terkait I&T termasuk mengelola investasi yang mendukung I&T, memberi <i>value</i> , dan memantau risiko.
11.	<i>Architecture Board</i>	Sekelompok <i>stakeholder</i> dan pakar yang bertanggungjawab memandu dalam keputusan terkait arsitektur perusahaan serta menetapkan kebijakan dan standar arsitektur.
12.	<i>Enterprise Risk Committee</i>	Kelompok eksekutif yang bertanggungjawab dalam kolaborasi dan konsensus di level perusahaan yang diperlukan untuk mendukung aktivitas dan keputusan <i>Enterprise Risk Management (ERM)</i> . ( <i>I&amp;T risk council</i> dapat dibentuk untuk mempertimbangkan risiko I&T secara lebih rinci dan memberi saran pada <i>Enterprise Risk Committee</i> ).

Tabel 3.1. Deskripsi role menurut COBIT 2019 (lanjutan)

No.	Role COBIT 2019	Deskripsi
13.	<i>Chief Information Security Officer</i>	Pejabat paling senior yang bertanggungjawab atas semua aspek manajemen keamanan di dalam perusahaan.
14.	<i>Business Process Owner</i>	Individu yang bertanggungjawab melakukan proses dan atau mewujudkan tujuan proses, mendorong peningkatan proses, dan menyetujui perubahan proses.
15.	<i>Portfolio Manager</i>	Individu yang bertanggungjawab memandu manajemen portofolio, memastikan pemilihan program dan proyek yang benar, mengelola program dan proyek untuk mendapatkan optimal <i>value</i> , dan mewujudkan tujuan strategis jangka panjang secara efektif dan efisien.
16.	<i>Steering (Programs/Projects) Committee</i>	Kelompok stakeholder dan ahli yang bertanggungjawab memandu program dan proyek, termasuk mengelola dan memantau rencana, mengalokasikan sumber daya, memberikan <i>benefit</i> dan <i>value</i> , dan mengelola program dan risiko proyek.
17.	<i>Program Manager</i>	Individu yang bertanggungjawab memandu program tertentu, termasuk mengartikulasi dan mendaklanjuti tujuan dan sasaran program serta mengelola risiko dan dampak pada bisnis.
18.	<i>Project Manager</i>	Individu yang bertanggungjawab memandu proyek tertentu, termasuk mengkoordinasi dan mendelegasi waktu, anggaran, sumber daya, dan tugas di seluruh tim proyek.
19.	<i>Project Management Office</i>	Bertanggungjawab mendukung program dan manajer proyek untuk mengumpulkan, menilai dan melaporkan informasi tentang pelaksanaan program dan proyek konstituen.
20.	<i>Data Management Function</i>	Bertanggungjawab mensupport aset data perusahaan di seluruh siklus hidup data dan mengelola strategi data, infrastruktur, dan repositori.
21.	<i>Head Human Resources</i>	Pejabat paling senior yang bertanggungjawab atas perencanaan dan kebijakan mengenai sumber daya manusia di perusahaan.
22.	<i>Relationship Manager</i>	Individu senior yang bertanggungjawab mengawasi dan mengelola antarmuka internal dan komunikasi antara bisnis dan fungsi I&T.
23.	<i>Head Architect</i>	Individu senior yang bertanggungjawab dalam proses arsitektur perusahaan.
24.	<i>Head Development</i>	Individu senior yang bertanggungjawab dalam proses pengembangan solusi terkait I&T.
25.	<i>Head IT Operations</i>	Individu senior yang bertanggungjawab dalam operasional TI di lingkungan dan infrastruktur.
26.	<i>Head IT Administration</i>	Individu senior yang bertanggungjawab dalam pencatatan terkait I&T dan bertanggungjawab mendukung masalah administrasi terkait I&T.

Tabel 3.1. Deskripsi role menurut COBIT 2019 (lanjutan)

No.	Role COBIT 2019	Deskripsi
27.	<i>Service Manager</i>	Individu yang mengelola pengembangan, implementasi, evaluasi dan pemeliharaan berkelanjutan produk dan layanan baru dan yang sudah ada untuk <i>user</i> tertentu atau kelompok <i>user</i> .
28.	<i>Information Security Manager</i>	Individu yang mengelola, mendesain, mengawasi dan atau menilai keamanan informasi perusahaan.
29.	<i>Business Continuity Manager</i>	Individu yang mengelola, merancang, mengawasi dan atau menilai kemampuan kelangsungan bisnis perusahaan, untuk memastikan bahwa fungsi penting perusahaan terus beroperasi setelah adanya peristiwa yang mengganggu.
30.	<i>Privacy Officer</i>	Individu yang bertanggungjawab memantau risiko dan dampak bisnis dari undang-undang privasi serta membimbing dan mengoordinasi penerapan kebijakan dan aktivitas yang memastikan kepatuhan terhadap arahan privasi (Posisinya dapat dirujuk sebagai data <i>protection officer</i> ).
31.	<i>Legal Counsel</i>	Bertanggungjawab dalam panduan tentang masalah hukum dan peraturan.
32.	<i>Compliance</i>	Bertanggungjawab atas semua panduan tentang kepatuhan eksternal.
33.	<i>Audit</i>	Bertanggungjawab dalam penyediaan audit internal.

(Sumber : ISACA 2020)

Mengacu dari Tabel 3.1 masing-masing *role* memiliki tugas dan tanggungjawab masing-masing. Langkah berikutnya adalah dengan memetakan keseluruhan *role* menggunakan *toolkit* COBIT 2019 dengan menggunakan proses BAI06, BAI10, DSS01 dan DSS02 yang didapat dari identifikasi DF sebelumnya. Terdapat beberapa *role* yang bertanggungjawab terhadap proses tersebut dan disesuaikan dengan struktur yang ada dalam Politeknik Negeri Sriwijaya. Penempatan *role* bisa saja diisi oleh jabatan yang sama karena fungsi dan tugasnya yang sesuai. Penempatan *role* ini dilakukan bersama dengan pihak Politeknik Negeri Sriwijaya.

## 2. Penyusunan Profil Risiko



Tahap penyusunan profil risiko dimulai dengan melakukan identifikasi hasil audit menggunakan metode wawancara dan kuisioner. Pengukuran kuisioner dibuat dengan menggunakan skala guttman, responden bisa menjawab dengan pernyataan ya atau tidak di setiap aktivitas pada setiap proses yang ada. Setiap aktivitas di dalam proses memiliki *capability* level masing-masing yang sudah diatur dalam COBIT 2019. Apabila responden menjawab Ya di suatu aktivitas yang memenuhi *capability* level tertentu dan sudah sesuai dengan bukti data yang ada di lapangan, hal ini berarti sudah memenuhi *capability* level tersebut.

### 3. Evaluasi Risiko (*Risk Evaluation*)

Evaluasi risiko dilakukan dengan melakukan penilaian gap antara level pada kondisi saat ini dengan level target yang diharapkan terhadap domain proses tersebut. Level target pada COBIT 2019 merupakan level yang setingkat diatas level yang ada pada kondisi saat ini.

### 4. Validasi Data

Proses validasi data dilakukan agar hasil audit tepat dan dapat dipertanggungjawabkan. Proses ini dilakukan untuk memastikan bahwa data yang dipergunakan sudah sesuai dan akurat dengan kenyataan di lapangan.

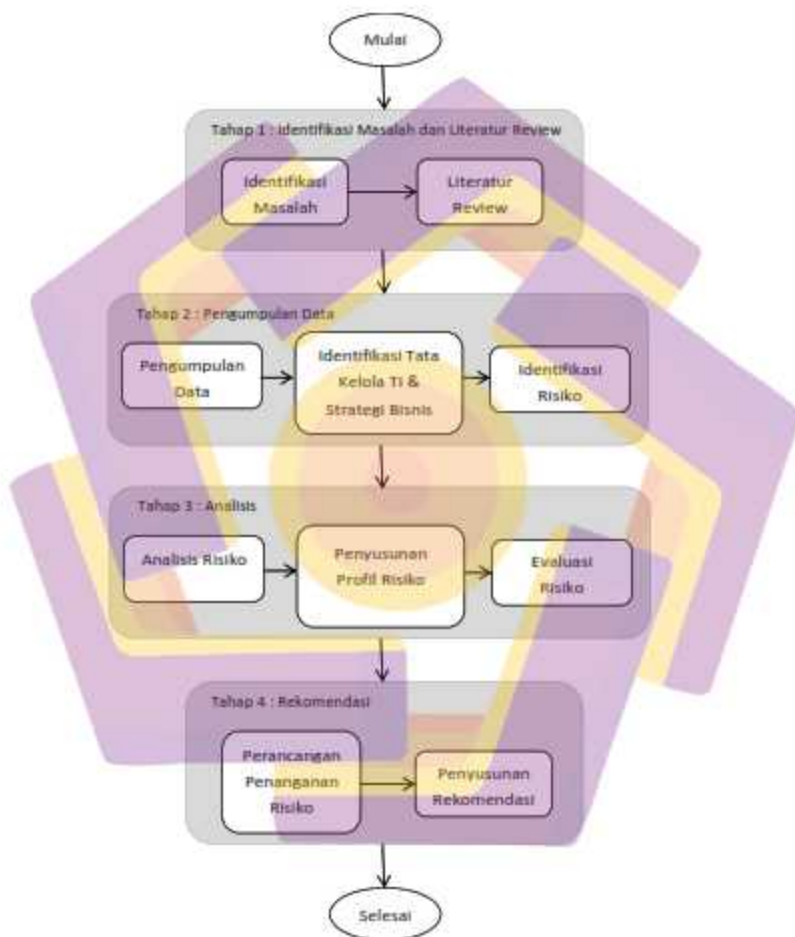
### 5. Risk Treatment

*Risk treatment* dilakukan dengan melakukan perencanaan atau rekomendasi dalam penanganan risiko serta pelaksanaannya.



### 3.4. Alur Penelitian

Alur penelitian yang dipergunakan pada penelitian ini ditunjukkan pada Gambar 3.1.



Gambar 3.1. Alur Penelitian

Berikut penjelasan singkat mengenai alur penelitian di atas:

#### 1. Tahap 1 : Identifikasi Masalah dan Literatur Review

Dalam tahap pertama dimulai dengan melakukan identifikasi masalah pada domain dan melakukan sistematik literatur review. Sistematik Literatur Review dilakukan dengan mengumpulkan dan mengevaluasi berbagai studi penelitian yang berkaitan dengan penelitian.

#### 2. Tahap 2 : Pengumpulan Data

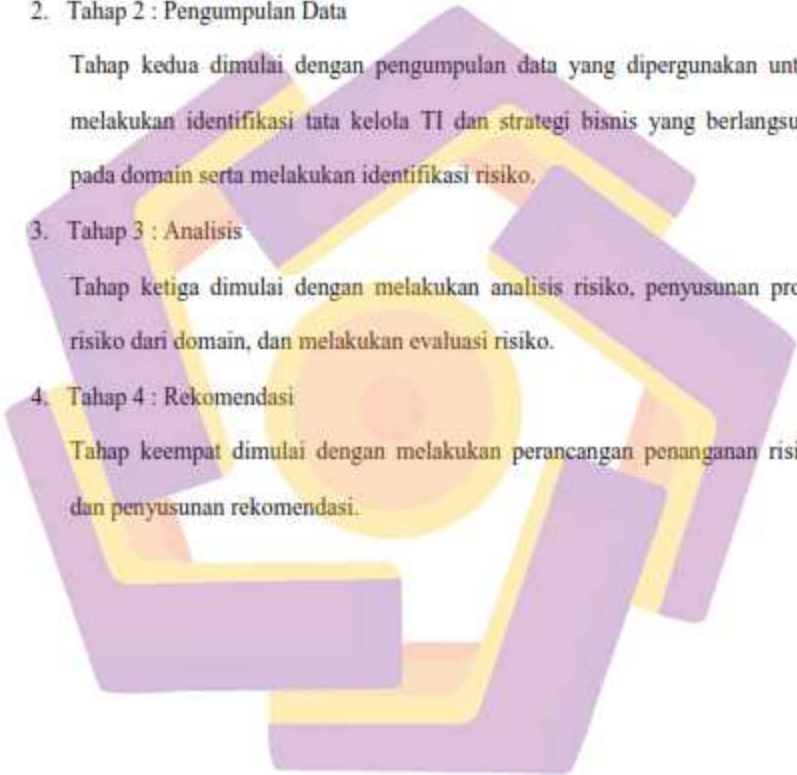
Tahap kedua dimulai dengan pengumpulan data yang dipergunakan untuk melakukan identifikasi tata kelola TI dan strategi bisnis yang berlangsung pada domain serta melakukan identifikasi risiko.

#### 3. Tahap 3 : Analisis

Tahap ketiga dimulai dengan melakukan analisis risiko, penyusunan profil risiko dari domain, dan melakukan evaluasi risiko.

#### 4. Tahap 4 : Rekomendasi

Tahap keempat dimulai dengan melakukan perancangan penanganan risiko dan penyusunan rekomendasi.



## BAB IV

### HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menjelaskan mengenai hasil penelitian dan pembahasan penelitian dengan judul “Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya” yang terdiri dari empat tahapan meliputi Tahap Identifikasi Masalah dan Literatur Review, Tahap Pengumpulan Data, Tahap Analisis, dan Tahap Rekomendasi.

#### 4.1. Tahap Identifikasi Masalah dan Literatur Review

Pada bagian ini dilakukan identifikasi awal masalah dan identifikasi business value mana yang ingin dicapai oleh Polsri. Selain itu dilakukan juga proses analisa dokumen, peneliti akan melakukan wawancara dengan pihak terkait. Dokumen yang dipergunakan dalam penelitian ini adalah dokumen Rencana Strategis Politeknik yang memuat visi, misi, tujuan, arah kebijakan pengembangan, analisa situasional, dan informasi lainnya yang berkaitan dengan penelitian.

#### 4.2. Tahap Pengumpulan Data

Pada tahap pengumpulan data dilakukan dengan menggunakan metode wawancara dan penyebaran kuisioner. Hasil dokumentasi pada tahap pengumpulan data terlihat pada Gambar 4.1.

1. Wawancara awal dilakukan dengan Wakil Direktur I, Bapak Carlos RS, S.T., M.T. untuk membahas mengenai agenda kegiatan penelitian yang dilakukan dan selanjutnya untuk membahas pemetaan RACI *role*. Selain itu terdapat juga wawancara awal dengan Kepala UPT Teknologi Informasi dan Komunikasi (TIK), Bapak Ir.Zulkarnaini, M.T., untuk membahas mengenai lingkup penelitian yang akan dilakukan.



Gambar 4.1. Dokumentasi wawancara

2. Kuisisioner dilakukan dengan menggunakan CMMI untuk melihat tingkat kemampuan Polsri dan skala pengukuran guttman.



Gambar 4.2. Dokumentasi pengisian kuisisioner

#### 4.2.1. Kustomisasi COBIT di Dunia Pendidikan

Langkah kustomisasi COBIT di dunia pendidikan adalah dengan menyelaraskan sistem yang berjalan di perguruan tinggi tersebut dengan *Design Factor* (DF) pada COBIT 2019. Gambar 4.3 menunjukkan diagram *default* dari DF pada COBIT 2019.



Gambar 4.3. COBIT Design Factor 1-4

Gambar 4.3 menunjukkan *default* awal dari COBIT *Design Factor* yang dipergunakan dalam penelitian ini, yaitu DF1 sampai dengan DF4. Dalam hal ini untuk melihat sistem tata kelola pendidikan di Politeknik Negeri Sriwijaya yang berjalan, dapat dilakukan dengan menggunakan DF1 sampai dengan DF4 seperti pada Gambar 4.4.



Gambar 4.4. Kustomisasi COBIT 2019 di Dunia Pendidikan

Gambar 4.4 menjelaskan mengenai kustomisasi COBIT 2019 di dunia pendidikan. Langkah pertama yang dilakukan adalah dengan mengetahui apakah



sasaran strategis dari perguruan tinggi tersebut yang kemudian diselaraskan ke dalam DF1 *enterprise strategy*. Langkah kedua adalah dengan mengetahui apakah tujuan dari perguruan tinggi tersebut, baik tujuan utama maupun tujuan luaran yang kemudian diselaraskan dalam DF2 *enterprise goals*. Langkah ketiga adalah dengan melakukan pengamatan mengenai profil risiko yang dihadapi oleh perguruan tinggi tersebut yang diselaraskan dalam DF3 *risk profile*. Profil risiko pada tiap perguruan tinggi bisa berbeda, bergantung pada risiko yang sedang dihadapi oleh perguruan tinggi tersebut. Langkah keempat adalah dengan mengetahui isu terkait IT di perguruan tinggi tersebut yang kemudian diselaraskan dalam DF4 *IT related issues*.

#### **4.2.2. Pembuatan Design Factor Polsri**

Matriks DF dibuat berdasarkan hasil wawancara dan studi literatur pada dokumen Rencana Strategis Politeknik Negeri Sriwijaya. Matriks design factor ini dibuat disesuaikan dengan kebutuhan penelitian dan kebutuhan Polsri. Penentuan ruang lingkup awal dari sistem tata kelola yang berjalan di Polsri dapat dianalisis dengan menggunakan DF1 sampai dengan DF4.

#### **Design Factor 1 : Enterprise Strategy**

Hasil identifikasi *enterprise strategy* dapat dilihat pada Tabel 4.1.

Tabel 4.1. Design factor 1 enterprise strategy

<i>Value</i>	<i>Importance (1-5)</i>	Keterangan / Deskripsi
<i>Growth/Acquisition</i>	1	Tidak relevan dengan tujuan organisasi.
<i>Innovation/Differentiation</i>	1	Tidak relevan dengan tujuan organisasi.
<i>Cost Leadership</i>	1	Tidak relevan dengan tujuan organisasi.
<i>Client Service/Stability</i>	5	Sasaran strategi polsri tertuang dalam Rencana Strategis Politeknik Negeri Sriwijaya tahun 2020-2024, diantaranya terdapat tujuh sasaran strategis sebagai penjabaran dari Tri Dharma Perguruan Tinggi dan pendukung Tri Dharma Perguruan Tinggi.

Tabel 4.1 menunjukkan fokus utama Polsri terkait pada penyediaan layanan yang stabil dan berorientasi *client* dengan nilai tertinggi 5. Penyediaan layanan yang stabil dan orientasi pada *client* ini dapat dilihat dengan adanya sasaran strategi Polsri terutama pada bidang layanan akademik.

#### Design Factor 2 : Enterprise Goals

Tabel 4.2 menunjukkan penyesuaian antara 5 tujuan utama dari Polsri yang diselaraskan dengan *Enterprise Goals* dalam DF2.

Tabel 4.2. Penyesuaian dengan design factor 2 stakeholder needs

Tujuan Politeknik	Dimensi Balance Scorecard (BSC)	Enterprise Goals
Tujuan utama: 1. Melaksanakan tugas dan fungsi Tri Dharma Perguruan Tinggi (pendidikan dan pengajaran, penelitian dan pengembangan, serta pengabdian kepada masyarakat).	<i>Customer</i>	EG05 – <i>Customer-Oriented Service Culture</i>
Tujuan luaran dari pelaksanaan tujuan utama: 2. Meningkatnya lulusan yang berkualitas, berdisiplin, bermoral, berjiwa wirausaha, berwawasan lingkungan, dan relevan dengan perkembangan industri.	<i>Customer</i>	EG05 – <i>Customer-Oriented Service Culture</i>

Tabel 4.2. Penyelarasan dengan design factor 2 stakeholder needs (lanjutan)

Tujuan Politeknik	Dimensi Balance Scorecard (BSC)	Enterprise Goals
3. Meningkatnya penyebaran ilmu pengetahuan, teknologi, dan seni serta hasil penelitian terapan bermutu untuk dimanfaatkan dalam kegiatan produktif dan peningkatan kualitas kehidupan masyarakat.	Customer	EG07 – <i>Quality of management information</i>
4. Meningkatnya mutu manajemen melalui pemberdayaan dan pengembangan organisasi berdasarkan prinsip tata kelola yang baik ( <i>good governance</i> ) dan mampu menghadapi tantangan masa depan.	Internal	EG10 – <i>Staff skills, motivation and productivity</i>
5. Meningkatnya mutu dan efisiensi pelayanan dalam bidang penyelenggaraan pendidikan.	Customer	EG05 – <i>Customer-Oriented Service Culture</i>

Dari penyelarasan tersebut kemudian dilakukan perincian dalam *enterprise goals* pada Polstri dapat dilihat pada Tabel 4.3.

Tabel 4.3. Design factor 2 enterprise goals

Value	Importance (1-5)
EG01 – <i>Portfolio of competition products and services</i>	1
EG02 – <i>Managed business risk</i>	1
EG03 – <i>Compliance with external laws and regulations</i>	1
EG04 – <i>Quality of financial information</i>	1
EG05 – <i>Customer-oriented service culture</i>	5
EG06 – <i>Business-service continuity and availability</i>	1
EG07 – <i>Quality of management information</i>	5
EG08 – <i>Optimization of internal business process functionality</i>	1
EG09 – <i>Optimization of business process costs</i>	1
EG10 – <i>Staff skills, motivation and productivity</i>	5
EG11 – <i>Compliance with internal policies</i>	1
EG12 – <i>Managed digital transformation programs</i>	1
EG13 – <i>Product and business innovation</i>	1

Dari Tabel 4.2 dan Tabel 4.3 dibatasi hanya pada 5 tujuan utama saja. Berdasar tabel tersebut diketahui bahwa EG05 *Customer-oriented service culture*, EG07 *Quality of management information*, dan EG10 *Staff skills, motivation, and productivity* menjadi *enterprise goals* utama di Polstri sehingga mendapat nilai

tertinggi. Dari *enterprise goals* dilakukan *mapping* ke *alignment goals* dan didapat *alignment goals* seperti pada Tabel 4.4.

Tabel 4.4. Alignment goals

<i>References</i>	<i>Alignment Goals</i>
AG08	<i>Enablement and support of business processes by Integrating applications and technology.</i>
AG12	<i>Competent and motivated staff with mutual understanding of technology and business.</i>

### Design Factor 3 : Risk Profile

Hasil penilaian terkait *Risk Profile* ditunjukkan pada Tabel 4.5.

Tabel 4.5. Design factor 3 risk profile

<i>Risk Scenario Category</i>	<i>Impact</i>	<i>Like- lihood</i>	<i>Risk Rating</i>	Keterangan/Deskripsi
<i>IT investment decision making, portfolio definition and maintenance</i>	1	1	1	Setiap program yang dipilih untuk diimplementasi di Polsri sudah dilakukan penyesuaian terlebih dahulu terhadap prioritas dan kebutuhan yang diperlukan Polsri.
<i>Program and projects life cycle management</i>	1	1	1	Proses bisnis Polsri masih tetap dapat berjalan meskipun program dan proyek IT mengalami hambatan ataupun kegagalan.
<i>IT cost and oversight</i>	1	1	1	Polsri selalu menyediakan biaya anggaran dan investasi yang disesuaikan dengan kebutuhan.
<i>IT expertise, skills, and behaviour</i>	4	4	16	Sudah adanya pembagian unit pelaksana teknik TIK di Polsri dan meskipun terjadi masalah pada unit ini, proses layanan akademik masih tetap bisa berjalan sebagaimana mestinya.
<i>Enterprise/IT architecture</i>	1	1	1	Proses layanan akademik masih tetap bisa berjalan meskipun arsitektur IT tidak dimanfaatkan secara tepat waktu.
<i>IT operational infrastructure incidents</i>	5	5	25	Polsri memiliki banyak SIM yang digunakan untuk penyimpanan data, bila terjadi kerusakan infrastruktur IT maka berisiko cukup besar.



Tabel 4.5. Design factor 3 risk profile (lanjutan)

<i>Risk Scenario Category</i>	<i>Impact</i>	<i>Likelihood</i>	<i>Risk Rating</i>	Keterangan/Deskripsi
<i>Unauthorized actions</i>	5	5	25	Bila ada gangguan pada software yang dipergunakan atau adanya manipulasi baik disengaja atau tidak disengaja akan berpengaruh besar pada layanan akademik.
<i>Software adoption/usage problems</i>	1	1	1	Skenario ini bukan merupakan masalah besar bagi Polsri
<i>Hardware incidents</i>	5	5	25	Insiden <i>hardware</i> memiliki <i>impact</i> besar terhadap jalannya sistem di Polsri dan memiliki <i>likelihood</i> yang besar juga.
<i>Software failures</i>	5	5	25	<i>Software failures</i> memiliki <i>impact</i> besar terhadap jalannya layanan sistem akademik di Polsri dan memiliki <i>likelihood</i> besar juga.
<i>Logical attacks (hacking, malware, etc)</i>	4	4	16	<i>Logical attacks</i> memiliki <i>impact</i> yang cukup tinggi terhadap sistem dan kerentanan data informasi yang terdapat di Polsri.
<i>Third-party/supplier incidents</i>	4	4	16	Polsri menggunakan layanan provider internet dan <i>cloud service</i> sehingga bila terjadi gangguan akan memiliki <i>impact</i> cukup besar.
<i>Non compliance</i>	1	1	1	Polsri tidak berada dalam bidang yang harus patuh pada regulasi nasional ataupun internasional.
<i>Geopolitical issues</i>	1	1	1	Polsri yang berada di wilayah kota Palembang sangat kecil kemungkinan terjadi isu geopolitik yang dapat mengganggu proses bisnis Polsri.
<i>Industrial action</i>	1	1	1	Aksi industri merupakan hal yang tidak pernah terjadi di Polsri.
<i>Acts of nature</i>	1	1	1	Posisi Polsri yang berada di kota Palembang memiliki risiko yang kecil mengalami gempa, tsunami, dan lainnya.
<i>Technology-based innovation</i>	1	1	1	Saat terjadi perubahan teknologi baru dan penting yang ada di luar sana tidak memiliki dampak yang besar terhadap Polsri.



Tabel 4.5. Design factor 3 risk profile (lanjutan)

<i>Risk Scenario Category</i>	<i>Impact</i>	<i>Likelihood</i>	<i>Risk Rating</i>	Keterangan/Deskripsi
<i>Environmental</i>	1	1	1	Meskipun Polsri memiliki program studi teknik kimia yang berhubungan dengan penggunaan laboratorium dan bahan kimia namun Polsri selalu berupaya mengutamakan keselamatan dan kesehatan kerja.
<i>Data and information management</i>	4	4	16	Data merupakan hal yang penting dan memiliki dampak cukup besar bagi Polsri.

#### Design Factor 4 : IT Related Issues

Permasalahan utama terkait IT yang terjadi di Polsri ditunjukkan pada

Tabel 4.6.

Tabel 4.6. Design factor 4 IT related issues

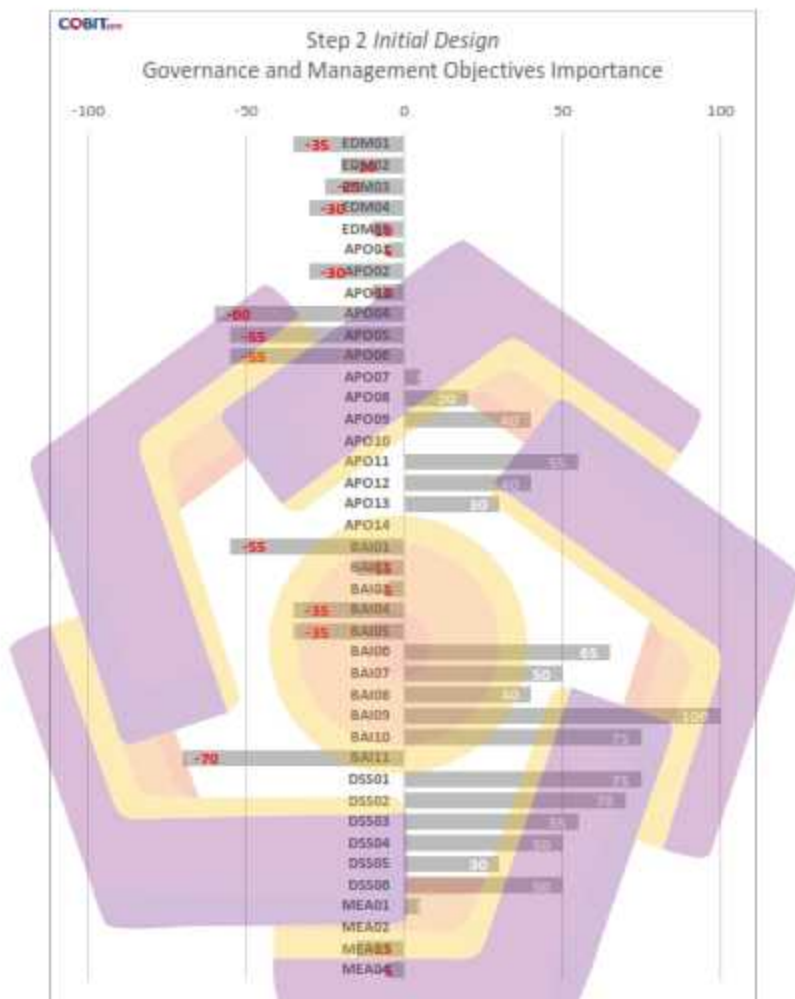
<i>IT Related Issues Category</i>	<i>Importance (1-3)</i>	Keterangan/Deskripsi
Permasalahan antara entitas IT berbeda di dalam organisasi karena persepsi dari kontribusi yang rendah terhadap <i>business value</i> .	1	Tidak ada masalah
Permasalahan antara departemen bisnis (contoh IT <i>customer</i> ) dan departemen IT karena gagalnya inisiatif atau persepsi dari kontribusi yang rendah terhadap <i>business value</i> .	1	Tidak ada masalah
Adanya insiden IT yang signifikan, contoh kehilangan data, pelanggaran keamanan, kegagalan proyek, error aplikasi dan lainnya yang terkait dengan IT.	2	Ada masalah
Masalah <i>service delivery</i> oleh IT <i>outsourc</i> e.	1	Tidak ada masalah
Kegagalan dalam memenuhi aturan atau kontrak yang terkait IT.	1	Tidak ada masalah
Temuan audit reguler atau laporan lainnya tentang kinerja IT yang buruk atau adanya pelaporan tentang permasalahan IT <i>quality</i> dan servis.	1	Tidak ada masalah
Pengeluaran IT yang tersembunyi yang ada di luar anggaran IT yang disetujui.	1	Tidak ada masalah
Duplikasi atau overlap dari berbagai kebijakan sehingga menyebabkan pemborosan sumber daya.	2	Ada masalah

Tabel 4.6. Design factor 4 IT related issues (lanjutan)

<i>IT Related Issues Category</i>	<i>Importance (1-3)</i>	<i>Keterangan/Deskripsi</i>
Sumber daya IT tidak mencukupi, staf dengan keterampilan tidak memadai, ataupun staf yang lelah.	2	Ada masalah
IT <i>enabled changes</i> sering kali gagal memenuhi kebutuhan bisnis, adanya keterlambatan, dan melebihi anggaran.	1	Tidak ada masalah.
<i>Board members, executives</i> , ataupun senior manajemen tidak mau terlibat dengan IT, atau tidak adanya pihak <i>business</i> sponsor yang berkomitmen menggunakan IT.	1	Tidak ada masalah.
Model operasi IT yang kompleks dan mekanisme keputusan yang tidak jelas untuk mengambil keputusan terkait IT.	1	Tidak ada masalah
Biaya IT yang terlalu tinggi.	1	Tidak ada masalah
Gagalnya implementasi inisiatif atau inovasi baru yang disebabkan sistem dan arsitektur IT saat ini.	2	Ada masalah
Kesenjangan antara bisnis dan pengetahuan teknis yang mengarah ke user IT dan bisnis atau teknologi menggunakan bahasa yang berbeda.	3	Ada masalah
Masalah regular dengan data <i>quality</i> dan integrasi data di berbagai sumber.	3	Ada masalah
Komputasi pengguna akhir tingkat tinggi menyebabkan kurangnya pengawasan dan <i>quality control</i> aplikasi yang dikembangkan dan dioperasikan.	1	Tidak ada masalah
<i>Business department</i> menerapkan solusi informasi sendiri dengan sedikit atau tanpa keterlibatan dari departemen IT.	1	Tidak ada masalah
Ketidaktahuan dan atau ketidakpatuhan pada regulasi <i>security</i> dan <i>privacy</i> .	1	Tidak ada masalah
Ketidakmampuan dalam memanfaatkan teknologi baru atau berinovasi menggunakan I&T.	1	Tidak ada masalah

### Identifikasi Design Factor

Gambar 4.5 menunjukkan hasil identifikasi domain berdasar DF1 sampai dengan DF4.



Gambar 4.5. Grafik identifikasi design factor

Berdasar identifikasi DF pada Gambar 4.5 didapat beberapa domain yang memiliki nilai mendekati 100 diantaranya yaitu BAI09 *Managed Assets*, BAI10 *Managed Configuration*, DSS01 *Managed Operation*, DSS02 *Managed Service Requests and Incidents*, dan BAI06 *Managed IT Changes*. Dari keempat domain

tersebut terdapat satu domain yang tidak diikutsertakan dalam penelitian karena adanya perbedaan ruang lingkup antara domain tersebut dengan penelitian yang dilakukan. Penelitian ini mengambil tema mengenai Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya, sedangkan domain BAI09 *Managed Assets* merupakan suatu domain yang melakukan analisis dan identifikasi aset, pencatatan keuangan, serta pembukuan yang tidak termasuk dalam lingkup layanan akademik di Poltri.

Berikut domain yang dipergunakan dalam penelitian ini (ISACA, 2020):

1. BAI06 *Managed IT Changes*. Domain BAI06 adalah domain proses yang mengelola semua perubahan secara terkendali, termasuk perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi, dan infrastruktur. Ini termasuk standar dan prosedur perubahan, penilaian dampak, prioritas dan otorisasi, perubahan darurat, pelacakan, pelaporan, penutupan, dan dokumentasi. Domain ini bertujuan memungkinkan pengiriman perubahan yang cepat dan andal ke bisnis. Mengurangi risiko dampak negatif terhadap stabilitas atau integritas lingkungan yang berubah.
2. BAI10 *Managed Configuration*. Domain BAI10 adalah domain yang digunakan untuk menetapkan dan mempertahankan deskripsi dan hubungan di antara sumber daya dan kemampuan utama yang diperlukan untuk memberikan layanan yang mendukung I&T. Termasuk mengumpulkan informasi konfigurasi, menetapkan *baseline*, memverifikasi dan mengaudit informasi konfigurasi, dan memperbarui repositori konfigurasi. Domain ini bertujuan memberikan informasi yang cukup tentang aset layanan untuk

memungkinkan layanan dikelola secara efektif. Menilai dampak perubahan dan menangani insiden layanan.

3. DSS01 *Managed Operation*. Domain DSS01 adalah domain untuk mengkoordinasikan dan melaksanakan kegiatan dan prosedur operasional yang diperlukan untuk memberikan layanan I&T internal dan *outsourcing*. Termasuk pelaksanaan prosedur operasi standar yang telah ditetapkan dan kegiatan pemantauan yang diperlukan. Domain ini bertujuan memberikan hasil produk dan layanan operasional I&T seperti yang direncanakan.
4. DSS02 *Managed Service Requests and Incidents*. Domain ini merupakan domain yang untuk memberikan tanggapan yang tepat waktu dan efektif terhadap permintaan pengguna dan penyelesaian semua jenis insiden. Pengembalian layanan normal; merekam dan memenuhi permintaan pengguna; dan merekam, menyelidiki, mendiagnosis, mengeskalisasi, dan menyelesaikan insiden. Domain ini bertujuan mencapai peningkatan produktivitas dan meminimalkan gangguan melalui penyelesaian cepat pertanyaan dan insiden pengguna. Menilai dampak perubahan dan menangani insiden layanan. Menyelesaikan permintaan pengguna dan memulihkan layanan sebagai tanggapan atas insiden.

#### 4.2.2. Penentuan Responden Penelitian

Responden pada penelitian dibuat berdasar RACI *Chart* COBIT 2019 yang disesuaikan dengan struktur organisasi di Politeknik Negeri Sriwijaya. Penelitian



ini berfokus pada domain yang terpilih yaitu BAI06, BAI10, DSS01 dan DSS02.

Hasil pemetaan RACI Chart COBIT 2019 terlihat pada Tabel 4.7.

Tabel 4.7. Hasil pemetaan RACI Chart COBIT 2019

Practice ID	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Process Owner	IT Governance Board	Steering Committee/Project Office	Project Management Office	Chief Information Security Officer	Architecture Board	Steering and Committee	Human Resource	Compliance	Legal	Chief Information Officer	Head of Block	Head of Department	Head of Applications	Head of Infrastructure	Service Manager	Information Security Manager	Business Continuity Manager	IT Strategy Office	Chief Legal Counsel	Executive Committee	Chief Technology Officer	Portfolio Manager	Program Manager	Project Manager	Legal Counsel	Relationship Manager
BAI06.01				R										A		R	R													
BAI06.02														A		R	R													
BAI06.03				R										A		R	R											R	R	
BAI06.04				R										A		R	R											R	R	
BAI10.01																R	R	R							A					
BAI10.02																R	R	R							A					
BAI10.03														A		R	R							R						
BAI10.04																R	R								A					
BAI10.05															R	R	R							A						
DSS01.01			R											A		R									R					
DSS01.02														A		R								R		R				
DSS01.03														R		R									A					
DSS01.04														R		R									A					
DSS01.05														R		R									A					
DSS02.01																A	R	R							A					
DSS02.02																R	R	R							A					
DSS02.03				R												R	R	R							A					
DSS02.04				R												R	R								A					
DSS02.05																R	R	R							A					
DSS02.06																R	R	R							A					
DSS02.07																R	R								A					

Pada Tabel 4.7 terlihat *role* yang memiliki peran sebagai R (*Responsible*) yang bertanggungjawab terhadap setiap domain proses yang ada. Dari Tabel 4.7 kemudian dilakukan pemetaan yang disesuaikan dengan struktur organisasi yang

ada di Politeknik Negeri Sriwijaya seperti pada Tabel 4.8, Tabel 4.9, Tabel 4.10, dan Tabel 4.11. Pemetaan ini dilakukan bersama dengan pihak Polsri.

Tabel 4.8. Pemetaan role domain BAI06

No.	RACI Chart COBIT 2019	Struktur Organisasi Polsri
1.	<i>Business Process Owner</i>	Wakil Direktur 1 Politeknik Negeri Sriwijaya Ketua UPT TIK/PIH
2.	<i>Chief Information Officer</i>	Ketua Koordinator Sistem Informasi
3.	<i>Head Development</i>	Ketua UPT TIK/PIH
4.	<i>Head IT Operations</i>	Ketua UPT TIK/PIH
5.	<i>Service Manager</i>	Ketua Koordinator Sistem Informasi
6.	<i>Information Security Manager</i>	Ketua Koordinator Infrastruktur dan Jaringan
7.	<i>Business Continuity Manager</i>	Tidak ada
8.	<i>Privacy Officer</i>	Tidak ada
9.	<i>Program Manager</i>	Ketua UPT TIK/PIH
10.	<i>Project Manager</i>	Ketua UPT TIK/PIH

Berdasar Tabel 4.8 dengan disesuaikan pada struktur organisasi di Polsri didapat 4 responden untuk domain BAI06 dari 10 peran yang direkomendasikan dalam COBIT 2019.

Tabel 4.9. Pemetaan role domain BAI10

No.	RACI Chart COBIT 2019	Struktur Organisasi Politeknik
1.	<i>Head Architect</i>	Tidak ada
2.	<i>Head Development</i>	Ketua UPT TIK/PIH
3.	<i>Head IT Operations</i>	Ketua UPT TIK/PIH
4.	<i>Head IT Administrations</i>	Tidak ada
5.	<i>Service Manager</i>	Ketua Koordinator Sistem Informasi
6.	<i>Information Security Manager</i>	Ketua Koordinator Infrastruktur dan Jaringan
7.	<i>Chief Technology Officer</i>	Ketua Koordinator Sistem Informasi

Berdasar Tabel 4.9 dengan disesuaikan pada struktur organisasi di Polsri didapat 3 responden untuk domain BAI10 dari 7 peran yang direkomendasikan dalam COBIT 2019.

Tabel 4.10. Pemetaan role domain DSS01

No.	RACI Chart COBIT 2019	Struktur Organisasi Politeknik
1.	<i>Chief Operation Officer</i>	Tidak ada
2.	<i>Chief Information Officer</i>	Ketua Koordinator Sistem Informasi
3.	<i>Head IT Operations</i>	Ketua UPT TIK/PIH
4.	<i>Information Security Manager</i>	Ketua Koordinator Infrastruktur dan Jaringan
5.	<i>Privacy Officer</i>	Tidak ada
6.	<i>Chief Technology Officer</i>	Ketua Koordinator Sistem Informasi

Berdasar Tabel 4.10 dengan disesuaikan pada struktur organisasi di Polstri didapat 3 responden untuk domain DSS01 dari 6 peran yang direkomendasikan dalam COBIT 2019.

Tabel 4.11. Pemetaan role domain DSS02

No.	RACI Chart COBIT 2019	Struktur Organisasi Politeknik
1.	<i>Business Process Owner</i>	Wakil Direktur 1 Politeknik Negeri Sriwijaya Ketua UPT TIK/PIH
2.	<i>Head Development</i>	Ketua UPT TIK/PIH
3.	<i>Head IT Operations</i>	Ketua UPT TIK/PIH
4.	<i>Service Manager</i>	Ketua Koordinator Sistem Informasi
5.	<i>Information Security Manager</i>	Ketua Koordinator Infrastruktur dan Jaringan

Berdasar Tabel 4.11 dengan disesuaikan pada struktur organisasi di Polstri didapat 4 responden untuk domain DSS02 dari 5 peran yang direkomendasikan dalam COBIT 2019.

#### 4.2.3. Persiapan dan Pengumpulan Data

Pada tahapan ini dilakukan persiapan yang mencakup penjelasan mengenai proses audit yang dilaksanakan di Politeknik Negeri Sriwijaya pada para responden. Tujuan dari tahapan ini agar responden memahami mengenai cara pengisian kuisioner, maksud dari setiap pertanyaan pada kuisioner, serta

mengetahui pelaksanaan audit yang dilaksanakan di Polsri. Audit berfokus pada domain BAI06, BAI10, DSS01 dan DSS02. Jadwal kegiatan yang dilaksanakan dapat dilihat pada Tabel 4.12.

Tabel 4.12. Jadwal kegiatan

No.	Kegiatan	Waktu Pelaksanaan
1.	Melakukan koordinasi dengan pihak Polsri	Januari 2022
2.	Menyiapkan dokumen	Januari 2022
3.	Melakukan sosialisasi dan persiapan dengan pihak Polsri	Januari 2022
4.	Mengumpulkan dokumen yang berkaitan dengan proses audit (Rencana Strategis, Dokumen Mutu yang terdiri dari Standar Mutu, Manual Mutu, Manual Prosedur, Standar Operasional Prosedur, dll)	Februari 2022
5.	Melakukan review dokumen	Februari 2022
6.	Melakukan pembagian <i>role</i> bersama Kepala Bidang Administrasi Umum dan Keuangan Politeknik Negeri Sriwijaya	Februari 2022
3.	Melakukan observasi ke Politeknik Negeri Sriwijaya	Maret 2022
4.	Melakukan pengumpulan data melalui survey baik melalui wawancara maupun kuisioner yang disebar	April 2022
5.	Melakukan penilaian <i>capability</i> level pada Politeknik Negeri Sriwijaya	April 2022
6.	Mengklarifikasi hasil audit untuk verifikasi data temuan audit	Mei 2022
7.	Membuat laporan hasil audit dan penyusunan rekomendasi untuk perbaikan	Mei-Juni 2022

#### 4.3. Tahap Analisis

Pada tahapan ini dilakukan analisis terhadap data yang ditemukan dengan menggunakan *Capability Maturity Model Integration* (CMMI) yang dapat diklasifikasi ke dalam 6 level (ISACA, 2020):

1. *Incomplete* (0) berarti belum ada kegiatan yang berkaitan dengan proses.
2. *Initial* (1) berarti kegiatan yang berkaitan dengan proses sudah dilakukan namun belum dilakukan secara berkala.



3. *Managed* (2) berarti kegiatan yang berkaitan dengan proses sudah dilakukan secara berkala.
4. *Defined* (3) berarti kegiatan yang berkaitan dengan proses sudah dilakukan dengan menggunakan SOP.
5. *Quantitative* (4) berarti kegiatan yang berkaitan dengan proses sudah dilakukan dengan menggunakan SOP dan dimonitor.
6. *Optimized* (5) berarti kegiatan yang berkaitan dengan proses sudah dilakukan, dimonitor, dan adanya pengembangan sistem yang terstandarisasi.

#### Hasil Audit Domain

Analisis domain dilakukan dengan melihat ketercapaian *capability* dari setiap aktivitas yang ada di setiap domain. Pada skala Guttman, bila seluruh responden menjawab Ya (1) pada aktivitas tertentu berarti memenuhi *capability* pada level tersebut. Untuk level *capability* telah diatur di dalam COBIT 2019 *Governance and Management Objective*.

Daftar dokumen yang dipergunakan dalam penelitian beserta penjelasan mengenai isi dokumen tersaji didalam Tabel 4.13. Daftar dokumen ini akan dipergunakan sebagai justifikasi bahwa proses pengisian data di dalam kuisisioner sudah benar sesuai dengan bukti dokumen yang ditunjukkan.

Tabel 4.13. Dokumen pendukung penelitian

No	Nama Dokumen	Keterangan
1	Peraturan Akademik Politeknik Negeri Sriwijaya	Perangkat aturan yang harus dipatuhi dan dilaksanakan di Polsri.
2	Peta Proses Bisnis Polsri	Dokumen ini memuat seluruh proses bisnis yang terjadi di Polsri.



Tabel 4.13. Dokumen pendukung penelitian (lanjutan)

No	Nama Dokumen	Keterangan
3	SOP Tingkat Institusi Politeknik Negeri Sriwijaya	Dokumen Standar Operasional Prosedur mengenai Instruksi Kerja di Polsri.
4	SOP Penanganan Gangguan Jaringan Lokal	Dokumen penanganan gangguan jaringan local di lingkungan Polsri.
5	SOP Penanganan Gangguan Server (PGS)	Dokumen penanganan gangguan server di lingkungan Polsri.
6	SOP Pembuatan Sub Domain dan Hosting (PSDH)	Dokumen pembuatan sub domain dan hosting Polsri.
7	SOP Pembuatan Website	Dokumen pembuatan website Polsri.
8	SOP Pembuatan Sistem Informasi	Dokumen pembuatan sistem informasi Polsri.
9	SOP Pembuatan Email	Dokumen pembuatan email Polsri.
10	Panduan Penggantian Kerusakan Bahan Peralatan	Dokumen panduan penggantian kerusakan bahan atau peralatan
11	Form Laporan Kerusakan / Kehilangan	Form ini digunakan untuk pengajuan laporan kerusakan atau kehilangan alat.
12	Form Pengambilan / Peminjaman Barang	Form ini digunakan untuk pengambilan atau peminjaman barang.
13	Form Peminjaman Alat	Form ini digunakan untuk peminjaman alat.
14	Form Permintaan Layanan PIH	Form ini digunakan untuk mengajukan layanan PIH.
15	Standar Sarana dan Prasarana Pembelajaran Politeknik Negeri Sriwijaya	Dokumen berisi standard dari Sarana dan Prasarana Pembelajaran.
16	Modul Bantuan Lainnya	Terdiri atas Modul Backup Reset Restore, Modul E-Learning Dosen, Modul E-Learning Mahasiswa, Modul Enrollment Key, Modul Pembuatan Cover MK, Modul Request MK.

Dokumen-dokumen yang disebutkan diatas dipergunakan dalam audit dari setiap domain yang terpilih.

#### 4.3.1. Hasil Audit BAI06 Managed IT Changes

Pengukuran kapabilitas Polsri berdasar domain BAI06 ditunjukkan pada Tabel 4.14, 4.15, 4.16, dan 4.17 dengan memberikan nilai 1 pada jawaban Ya dan nilai 0 pada jawaban Tidak.

### BAI06.01 Evaluate, prioritize and authorize change requests

Pada *key management practice* BAI06.01 dari 7 *role* dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.14.

Tabel 4.14. Hasil kuisioner domain BAI06.01

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Memastikan bahwa otorisasi perubahan formal dalam IT hanya muncul melalui permintaan perubahan secara formal.		1	1	1	Peraturan Akademik Politeknik Negeri Sriwijaya Bagian ke-2 mengenai Sarana dan Prasarana Pasal 32 bahwa sarana dan prasarana disediakan Polsri dan penggunaannya diatur Pimpinan Polsri.
2	Mengategorikan semua perubahan yang diminta dan menghubungkan item konfigurasi yang terpengaruh.		1	1	1	Pada Form Permintaan Layanan terdapat deskripsi layanan dengan mengelompokkan layanan berdasar kategori.
3	Memprioritas semua perubahan berdasar kebutuhan bisnis dan teknis; sumber daya yang dibutuhkan; dan alasan hukum, peraturan, dan kontraktual untuk perubahan yang diminta.	2	1	1	1	Pada Peta Proses Bisnis Polsri Bab VI terdapat pemrioritasan berdasar kebutuhan seperti layanan informasi, jaringan, website dan database, laboratorium komputer.
4	Melakukan persetujuan secara resmi dalam setiap perubahan. Perubahan yang berisiko rendah dan relatif sering harus disetujui terlebih dahulu sebagai perubahan standar.		1	1	1	Aktivitas 4 berkaitan dengan aktivitas 1.
5	Merencanakan dan menjadwalkan semua perubahan yang disetujui.		1	1	1	Ada surat tugas atau surat pengantar kepada pihak terkait yang diberikan oleh Pimpinan Polsri untuk melaksanakan kegiatan.

Tabel 4.14. Hasil kuisisioner domain BAI06.01 (lanjutan)

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
6	Merencanakan dan mengevaluasi semua permintaan secara terstruktur.	3	1	1	0	Kedua aktivitas ini berkaitan dengan aktivitas 1 namun masih belum ada perencanaan dan pengevaluasian secara terstruktur dan belum ada pertimbangan lebih lanjut mengenai pemilihan penyedia layanan yang dikontrak terhadap proses manajemen. Kegiatan evaluasi masih dilakukan secara individual.
7	Mempertimbangkan dampak penyedia layanan yang dikontrak pada proses manajemen perubahan.		1	1	0	

Berdasar keterangan pada Tabel 4.14 dapat dijustifikasi bahwa penilaian responden terhadap proses BAI06.01 sudah benar dan sesuai. Responden pada proses BAI06.01 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi.

5. Component: Process	
Management Practice	Example Metrics
<b>BAI06.01 Evaluate, prioritize and authorize change requests</b> Evaluate all requests for change to determine the impact on business processes and ICT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Prioritize changes on logical, provisioned, categorized, assessed, authorized, planned and scheduled.	a. Amount of requests caused by failed changes b. Percent of unsuccessful changes due to inadequate impact assessments
Activities	Capability Level
1. Use formal change requests to enable business process owners and IT to request changes to business processes, infrastructure systems or applications. Make sure that all such changes arise only through the change request management process.	2
2. Categorize all requested changes (e.g. business process, infrastructure, operating systems, networks, application systems, patches, firewalls, application software) and relate affected configuration items.	
3. Prioritize all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.	
4. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.	
5. Plan and schedule all approved changes.	
6. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, privacy, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies among changes. Involve business process owners in the assessment process, as appropriate.	
7. Consider the impact of contractual service providers (e.g. outsourced business processes, infrastructure, application development and shared services) on the change management process. Include integration of organizational change management processes with change management processes of service providers and the impact on contractual terms and SLAs.	

Gambar 4.6. Nilai capability level per aktivitas proses BAI06.01

(Sumber : ISACA 2020)

Gambar 4.6 dalam COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 5 berada di *capability* level 2, sedangkan aktivitas 6 dan 7 berada di *capability* level 3 ditunjukkan pada Gambar 4.4. Berdasarkan hasil penilaian dari responden, seluruh responden menjawab Ya

(1) pada aktivitas nomor 1 sampai dengan nomor 5, hal ini berarti Polsri sudah mencapai *capability level* 2. Sedangkan pada aktivitas nomor 6 dan nomor 7 bernilai 0, hal ini berarti bahwa Polsri belum mencapai *capability level* 3.

Kesimpulan dari penelitian ini Polsri sudah mencapai *capability level* 2 pada BAI06.01, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI06.01 *Evaluate, prioritize and authorize change requests* sudah dilakukan secara berkala.

#### **BAI06.02 Manage emergency changes**

Pada *key management practice* BAI06.02 dari 5 role dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.15.

Tabel 4.15. Hasil kuisioner domain BAI06.02

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Menjelaskan apa yang dimaksud dengan perubahan darurat.	2	1	1	1	Pada Peta Proses Bisnis Polsri disebutkan mengenai pembagian perubahan darurat berdasarkan jenisnya apakah rusak sedang, rusak ringan, atau masuk kategori rusak berat.
2	Memastikan adanya prosedur dokumentasi untuk menyatakan, menilai, menyetujui sebelumnya, mengesahkan setelah perubahan dan mencatat perubahan darurat.		1	1	0	
3	Memverifikasi semua pengaturan akses darurat untuk perubahan diotorisasi, didokumentasikan, dan dicabut dengan tepat setelah perubahan diterapkan.	3	0	0	0	



Tabel 4.15. Hasil kuisioner domain BAI06.02 (lanjutan)

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
4	Memantau semua perubahan darurat (akar penyebab masalah, pengembangan dan pemeliharaan sistem aplikasi, dokumentasi dan manual, dan integritas data).	4	0	0	0	

Berdasar keterangan pada Tabel 4.15 dapat dijustifikasi bahwa penilaian responden terhadap proses BAI06.02 sudah benar dan sesuai. Responden pada proses BAI06.02 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 dan 2 berada di *capability* level 2, aktivitas nomor 3 berada di level 3, sedangkan aktivitas nomor 4 berada di level 4. Berdasar data hasil kuisioner terlihat bahwa seluruh responden menjawab Ya (1) pada aktivitas nomor 1, meskipun di aktivitas nomor 2 masih ada yg menjawab Tidak (0) namun masih dapat memenuhi *capability* level 2 karena pada aktivitas nomor 1 terpenuhi. Sedangkan pada aktivitas nomor 3 dan 4 seluruh responden menjawab Tidak (0), berarti Polsri tidak memenuhi *capability* level 3 dan 4.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 2 pada BAI06.02, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI06.02 *Manage emergency changes* sudah dilakukan secara berkala.



### BAI06.03 Track and report change status

Pada *key management practice* BAI06.03 dari 6 role dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.16.

Tabel 4.16. Hasil kuisioner domain BAI06.03

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Mengategorikan permintaan perubahan dalam proses pelacakan perubahan IT (misal disetujui, ditolak, ditutup).	4	0	0	0	Berkaitan erat dengan proses BAI06.02 aktivitas 4, dimana Polri belum memiliki dokumentasi manual dari setiap hasil testing perubahan IT yang terjadi.
2	Menerapkan laporan status perubahan dengan metrik kinerja yang membentuk jejak audit.		0	0	0	Belum ada kegiatan pengujian atau testing secara formal.
3	Memantau perubahan terbuka untuk memastikan semua perubahan IT yang disetujui tepat waktu dan bergantung pada prioritas.		1	1	0	Belum ada kegiatan pengujian atau testing secara formal.
4	Melacak dan melapor untuk semua permintaan perubahan IT.		1	0	1	Belum ada kegiatan pengujian atau testing secara formal.

Berdasar keterangan pada Tabel 4.16 dapat dijustifikasi bahwa penilaian responden terhadap proses BAI06.03 sudah benar dan sesuai. Responden pada proses BAI06.03 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 4 berada di *capability* level 4. Berdasar hasil penilaian, setiap responden menjawab Tidak (0) untuk proses BAI06.03 aktivitas 1 dan 2, sedangkan pada aktivitas 3

dan 4 masih ada responden yang menjawab Tidak (0). Ini berarti Polsri belum memenuhi *capability level 4* pada proses BAI06.03.

Kesimpulannya pada BAI06.03 Polsri sudah mencapai *capability level 1*, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI06.03 *Track and report change status* namun belum dilakukan secara berkala.

#### **BAI06.04 Close and document the changes**

Pada *key management practice* BAI06.04 dari *6 role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.17.

Tabel 4.17. Hasil kuisioner domain BAI06.04

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Mendokumentasikan prosedur layanan IT, kelangsungan IT, kelangsungan pemulihan, konfigurasi item, dokumentasi aplikasi layar, layar bantuan, dan materi pelatihan.	2	1	1	Adanya SOP Penanganan Gangguan Lokal, SOP Penanganan Gangguan Server (PGS), SOP Pembuatan Sub Domain dan Hosting (PSDH), SOP Pembuatan Website, SOP Pembuatan Sistem Informasi, SOP Pembuatan Email, selain itu terdapat juga berbagai modul dokumentasi (untuk membantu pengguna dalam menggunakan layanan), contoh modul dokumentasi yang ada diantaranya Terdiri atas Modul Backup Reset Restore, Modul E-Learning Dosen, Modul E-Learning Mahasiswa, Modul Enrollment Key, Modul Pembuatan Cover MK, Modul Request MK.
2	Menentukan periode penyimpanan untuk dokumentasi perubahan sistem sebelum dan sesudah perubahan.	3	1	1	Pengarsipan dokumen dilakukan sesuai dengan SOP Tingkat Institusi yang tertuang dalam Instruksi Kerja Pengarsipan Dokumen. Di dalam instruksi kerja tersebut disebutkan mengenai pengarsipan dokumen kadaluarsa, dimana dokumen tersebut akan disimpan ke dalam ordner.

Tabel 4.17. Hasil kuisisioner domain BAI06.04 (lanjutan)

No	Aktivitas	Cap. Level	R1	R2	Keterangan
3	Mendokumentasikan subyek ke tingkat tinjauan yang sama.		0	0	Belum ada pendokumentasian terkait.

Berdasar keterangan pada Tabel 4.17 dapat dijustifikasi bahwa penilaian responden terhadap proses BAI06.04 sudah benar dan sesuai. Responden pada proses BAI06.04 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 berada di *capability level 2*, sedangkan aktivitas nomor 2 dan 3 berada di *capability level 3*. Berdasar hasil penilaian dari responden, seluruh responden menjawab Ya (1) untuk proses BAI06.04 aktivitas 1 dan 2. Sedangkan pada aktivitas 3 menjawab Tidak (0). Hal ini berarti bahwa Polsri sudah mencapai *capability level 2* karena seluruh responden menjawab Ya pada aktivitas nomor 1, dan sudah mencapai *capability level 3* karena sudah memenuhi aktivitas nomor 2.

Kesimpulannya bahwa Polsri sudah mencapai *capability level 3* pada proses BAI06.04, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI06.04 *Close and document the changes*.

#### Hasil Analisis BAI06

Dari hasil analisis di atas, dapat disimpulkan hasil keseluruhan proses domain BAI06 *Managed IT Changes* ditunjukkan pada Tabel 4.18.

Tabel 4.18. Hasil keseluruhan proses domain BAI06

No	Domain	Tingkat Kapabilitas Saat Ini	Tingkat Kapabilitas Target
1	BAI06.01	2	3
2	BAI06.02	2	3
3	BAI06.03	1	2
4	BAI06.04	3	3
	Rata-rata	2	
	Rata-rata Capability	2	

Sedangkan hasil audit dari domain BAI06 ditunjukkan pada Gambar 4.7.



Gambar 4.7. Hasil audit BAI06

Kesimpulan dari hasil audit diatas adalah sebagai berikut:

1. Pada BAI06.01 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 2, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 3 dan sudah sesuai dengan level maksimal pada *capability* level di BAI06.01 sesuai COBIT 2019 *Governance and Management Objective*. Pada *capability* level 2 berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI06.01 *Evaluate, prioritize and authorize change requests* sudah dilakukan secara berkala.
2. Pada BAI06.02 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 2, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 3. Pada *capability* level 2 berarti

Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI06.02 *Manage emergency changes* sudah dilakukan secara berkala.

3. Pada BAI06.03 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 1, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 2. Pada *capability* level 1 berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI06.03 *Track and report change status* namun belum dilakukan secara berkala.
4. Sedangkan pada BAI06.04 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu 3 pada domain proses tersebut. Pada *capability* level 3 berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI06.04 *Close and document the changes*.
5. Berdasar level kapabilitas dari setiap proses domain tersebut kemudian di rata-rata untuk mendapatkan level *capability* pada domain BAI06. Diketahui bahwa level *capability* pada domain BAI06 berada di level 2 yang berarti kegiatan pada proses domain BAI06 *Managed IT Changes* sudah dilakukan secara berkala.

#### **4.3.2. Hasil Audit BAI10 Managed Configuration**

Pengukuran proses kapabilitas Polsri berdasar domain BAI10 ditunjukkan pada Tabel 4.19, 4.20, 4.21, 4.22, dan 4.23.



### BAI10.01 Establish and maintain a configuration model

Pada *key management practice* BAI10.01 dari 7 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.19.

Tabel 4.19. Hasil kuisioner domain BAI10.01

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Menetapkan dan menyetujui cakupan dan tingkat detail manajemen konfigurasi (layanan, aset, dan item terkait konfigurasi IT).	3	1	1	Model konfigurasi berkaitan dengan model logis dari setiap layanan di Polsri yang sudah disusun dalam Peta Proses Bisnis.
2	Menetapkan dan memelihara model logis untuk manajemen konfigurasi tentang tipe CI, atribut, status.		1	1	Configuration item merupakan komponen yang harus dikelola dalam pelayanan IT meliputi hardware, software, dokumen, dan servis.

Berdasar keterangan pada tabel 4.19 dapat dijustifikasi bahwa penilaian responden terhadap proses BAI10.01 sudah benar dan sesuai. Responden pada proses BAI10.01 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 dan 2 berada di *capability* level 3. Berdasar hasil penilaian dari responden, seluruh responden menjawab Ya (1) untuk proses BAI10.01 aktivitas 1 dan 2 yang termasuk dalam *capability* level 3.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 3 pada proses BAI10.01, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.01 *Establish and maintain a configuration model*.

### BAI10.02 Establish and maintain a configuration repository and baseline

Pada *key management practice* BAI10.02 dari 5 *role* dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.20.

Tabel 4.20. Hasil kuisioner domain BAI10.02

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Mengidentifikasi dan mengklasifikasi CI dan isi repository.	2	1	1	1	Klasifikasi CI dan isinya bisa dilihat secara umum pada Peta Proses Bisnis Polsri.
2	Membuat, meninjau, dan menyetujui konfigurasi layanan, aplikasi atau infrastruktur.	3	1	1	1	Konfigurasi layanan, aplikasi atau infrastruktur dibuat, ditinjau dan disetujui sesuai dengan kebutuhan Polsri.

Berdasar keterangan pada Tabel 4.20 dapat dijustifikasi bahwa penilaian responden terhadap proses BAI10.02 sudah benar dan sesuai. Responden pada proses BAI10.02 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 berada di *capability* level 2, sedangkan aktivitas nomor 2 berada di *capability* level 3. Berdasar hasil penilaian dari responden, seluruh responden menjawab Ya (1) untuk proses BAI10.02 aktivitas 1 yang termasuk dalam *capability* level 2. Begitu pula pada aktivitas 2 yang termasuk dalam *capability* level 3.

Kesimpulannya bahwa Polsri sudah memenuhi dan mencapai *capability* level 2 dan 3 pada BAI10.02, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.02 *Establish and maintain a configuration repository and baseline*.

### BAI10.03 Maintain and control configuration items

Pada *key management practice* BAI10.03 dari 4 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.21.

Tabel 4.21. Hasil kuisioner domain BAI10.03

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Mengidentifikasi secara teratur semua perubahan CI.		1	1	Terdapat pembagian job desk berdasar tupoksi di dalam Polsri sehingga memudahkan dalam pengidentifikasian bila terjadi perubahan CI.
2	Memastikan kelengkapan dan akurasi, untuk meninjau perubahan yang diusulkan pada CI (bila terjadi perubahan).	2	1	0	Belum ada perhitungan akurasi bila terjadi perubahan CI.
3	Memperbarui detail konfigurasi untuk perubahan yang disetujui pada CI.		1	1	Bila terjadi perubahan CI yang mencakup perubahan hardware, software, dokumen, ataupun servis, terdapat pembaruan detail konfigurasi. Salah satu contohnya adalah adanya dokumen SOP Pembuatan Sub Domain dan Hosting (PSDH).
4	Membuat, meninjau, dan menyetujui perubahan konfigurasi layanan, aplikasi atau infrastruktur.	3	1	1	Pembuatan serta penyetujuan perubahan CI berdasar keputusan Pimpinan Polsri yang dibuktikan dengan munculnya surat tugas.

Berdasar keterangan pada tabel 4.21, dapat dijustifikasi bahwa penilaian responden terhadap proses BAI10.03 sudah benar dan sesuai. Responden pada proses BAI10.03 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 3 berada di *capability level* 2, sedangkan aktivitas nomor 4 berada di *capability level* 3.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses BAI10.03 aktivitas 1, 3, dan 4. Sedangkan pada aktivitas 2 meskipun masih ada responden yang menjawab Tidak (0) namun masih memenuhi *capability* level 2 karena ditunjang oleh aktivitas 1 dan 3. Hal ini berarti bahwa Polstri sudah mencapai *capability* level 2 dan 3 pada BAI10.03.

Kesimpulannya bahwa Polstri sudah mencapai *capability* level 3 pada BAI10.03, dimana berarti Polstri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.03 *Maintain and control configuration items*.

#### **BAI10.04 Produce status and configuration reports**

Pada *key management practice* BAI10.04 dari 2 *role* dalam COBIT 2019 didapat 1 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.22.

Tabel 4.22. Hasil kuisioner domain BAI10.04

No	Aktivitas	Cap. Level	RI	Keterangan
1	Mengidentifikasi perubahan status pada CI dan melaporkan.	2	1	Belum ada pelaporan secara resmi mengenai perubahan status pada item yang akan dikonfigurasi ini apakah masih dalam status menunggu dikonfigurasi ataupun sudah selesai. Pelaporan hanya dilakukan sesuai kebutuhan dengan menginfokan bahwa item sudah selesai dikonfigurasi.
2	Mencocokkan semua perubahan konfigurasi serta melaporkan perubahan yang tidak sah.	3	1	Mencocokkan semua perubahan konfigurasi berdasar permintaan yang dapat dibuat melalui Form Permintaan Layanan, bila ada perubahan yang tidak sesuai akan dibahas selanjutnya didalam rapat.



Tabel 4.22. Hasil kuisioner domain BAI10.04 (lanjutan)

No	Aktivitas	Cap. Level	RI	Keterangan
3	Mengidentifikasi persyaratan pelaporan dari semua pemangku kepentingan, mengenai konten, frekuensi, dan media yang digunakan.		1	Identifikasi ini dilakukan bersama dengan Pimpinan Polsri sehingga bisa menyesuaikan kebutuhan Polsri.

Berdasar keterangan pada Tabel 4.22 dapat dijustifikasi bahwa penilaian responden terhadap proses BAI10.04 sudah benar dan sesuai. Responden pada proses BAI10.04 yaitu Ketua UPT TIK/PIH. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 berada pada *capability* level 2, sedangkan aktivitas nomor 2 dan 3 berada di *capability* level 3.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses BAI10.04 aktivitas 1 yang artinya memenuhi *capability* level 2. Sedangkan untuk aktivitas 2 dan 3 juga sudah memenuhi *capability* level 3 pada BAI10.04.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 3 pada BAI10.04, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.4 *Produce status and configuration reports*.

#### **BAI10.05 Verify and review integrity of the configuration repository**

Pada *key management practice* BAI10.05 dari 4 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.23.



Tabel 4.23. Hasil kuisioner domain BAI10.05

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Mengadakan kegiatan verifikasi CI langsung secara berkala.	4	0	0	Belum ada kegiatan verifikasi secara berkala.
2	Melaporkan dan meninjau semua penyimpangan.		1	1	Sudah ada kegiatan pelaporan dengan mengumpulkan semua penyimpangan dan membahas dengan Pimpinan Polstri.
3	Memverifikasi secara berkala semua CI fisik dan melaporkan penyimpangan.		1	1	Belum ada kegiatan verifikasi secara berkala. Namun sudah ada kegiatan pelaporan penyimpangan.
4	Menetapkan dan meninjau target kelengkapan repository konfigurasi secara berkala.		0	0	Belum ada kegiatan tersebut.
5	Secara berkala membandingkan tingkat kelengkapan dan akurasi terhadap akurasi untuk meningkatkan kualitas repository.		5	0	0

Berdasar keterangan pada Tabel 4.23 dapat dijustifikasi bahwa penilaian responden terhadap proses BAI10.05 sudah benar dan sesuai. Responden pada proses BAI10.05 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 4 berada di *capability* level 4, sedangkan pada aktivitas nomor 5 berada di *capability* level 5.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses BAI10.05 aktivitas 2 dan 3, meskipun pada aktivitas 1 dan 4 responden menjawab Tidak (0). Hal ini karena masih belum ada kegiatan yang dilakukan secara berkala. Ini berarti bahwa pada aktivitas nomor 1 sampai dengan

4 sudah memenuhi *capability* level 4. Sedangkan pada aktivitas nomor 5 seluruh responden menjawab Tidak (0) sehingga belum memenuhi *capability* level 5.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 4 pada BAI10.05, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.05 *Verify and review integrity of the configuration repository* sudah dilakukan dan dimonitor.

### Hasil Analisis BAI10

Dari hasil analisis di atas, dapat disimpulkan hasil keseluruhan proses domain BAI10 *Managed Configuration* ditunjukkan pada Tabel 4.24.

Tabel 4.24. Hasil keseluruhan proses domain BAI10

No	Domain	Tingkat Kapabilitas Saat Ini	Tingkat Kapabilitas Target
1	BAI10.01	3	3
2	BAI10.02	3	3
3	BAI10.03	3	3
4	BAI10.04	3	3
5	BAI10.05	4	5
	Rata-rata	3,2	
	Rata-rata Capability	3	

Sedangkan hasil audit dari domain BAI10 ditunjukkan pada Gambar 4.8.



Gambar 4.8. Hasil audit BAI10

Kesimpulan dari hasil audit diatas adalah sebagai berikut:

1. Pada BAI10.01 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu level 3 pada domain proses BAI10.01 sesuai COBIT 2019 *Governance and Management Objective*. Pada *capability* level 3 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.01 *Establish and maintain a configuration*.
2. Pada BAI10.02 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu level 3 pada domain proses BAI10.02 sesuai COBIT 2019 *Governance and Management Objective*. Pada *capability* level 3 berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.02 *Establish and maintain a configuration repository and baseline*.
3. Pada BAI10.03 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu level 3 pada domain proses BAI10.03 sesuai COBIT 2019 *Governance and Management Objective*. Pada *capability* level 3 berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.03 *Maintain and control configuration items*.
4. Pada BAI10.04 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu level 3 pada domain proses BAI10.04 sesuai COBIT 2019 *Governance and Management Objective*. Pada *capability* level 3 berarti Polsri

sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.4 *Produce status and configuration reports*.

5. Pada BAI10.05 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 4, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 5 dan sudah sesuai dengan level maksimal pada *capability* level di BAI10.05 sesuai COBIT 2019 *Governance and Management Objective*. Pada *capability* level 4 berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses BAI10.05 *Verify and review integrity of the configuration repository* sudah dilakukan dan dimonitor.
6. Berdasar level kapabilitas dari setiap proses domain tersebut kemudian di rata-rata untuk mendapatkan level *capability* pada domain BAI10. Diketahui bahwa level *capability* pada domain BAI10 yaitu berada di level 3 berarti kegiatan yang berkaitan dengan proses BAI10 *Managed Configuration* sudah dilakukan dengan menggunakan SOP.

#### **4.3.3. Hasil Audit DSS01 Managed Operations**

Pengukuran kapabilitas Polsri berdasar domain DSS01 ditunjukkan pada Tabel 4.25, 4.26, 4.27, 4.28, dan 4.29.

##### **DSS01.01 Perform operational procedures**

Pada *key management practice* DSS01.01 dari 3 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.25.



Tabel 4.25. Hasil kuisioner domain DSS01.01

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Mengembangkan dan memelihara prosedur operasional dan kegiatan terkait untuk mendukung layanan.	2	1	1	Polsri memiliki jadwal operasional untuk mendukung pelayanan IT sesuai dengan jam kerja berdasar Surat Edaran Normor 8003/PL.6.4.2/SE/2017 yaitu hari Senin sampai dengan Kamis pukul 07.00 sampai dengan pukul 15.30. Serta hari Jumat pukul 07.00 sampai dengan 16.00.
2	Menjadwalkan kegiatan operasional.		1	1	
3	Memverifikasi data yang diterima dan diproses lengkap akurat dan tepat waktu.	3	0	0	Belum ada kegiatan terkait.
4	Mengelola kinerja dan hasil kegiatan yang dijadwalkan.	4	0	0	Belum ada kegiatan terkait.
5	Memantau insiden dan masalah yang berhubungan dengan prosedur operasional.	5	1	1	Adanya pemantauan insiden dan masalah berhubungan prosedur operasional namun tidak ada dokumentasi spesifik mengenai pemantauan insiden dan masalah tersebut.

Berdasar keterangan pada Tabel 4.25 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS01.01 sudah benar dan sesuai. Responden pada proses DSS01.01 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 dan 2 berada di *capability* level 2, aktivitas nomor 3 berada di level 3, aktivitas nomor 4 berada di level 4, dan aktivitas nomor 5 berada di level 5.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS01.01 aktivitas 1 dan 2 yang termasuk dalam *capability* level 2. Sedangkan pada aktivitas 3 dan 4 seluruh responden menjawab Tidak (0).



Meskipun pada aktivitas 5 seluruh responden menjawab Ya (1), namun belum bisa disebut memenuhi *capability* level 5, karena pada aktivitas 3 dan 4 yang berada di level 3 dan 4 belum terpenuhi.

Kesimpulannya bahwa Polsri mencapai *capability* level 2 pada DSS01.01, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS01.01 *Perform operational procedures* sudah dilakukan secara berkala.

#### DSS01.02 Manage outsourced I&T services

Pada *key management practice* DSS01.02 dari 4 *role* dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.26.

Tabel 4.26. Hasil kuisioner domain DSS01.02

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Memastikan persyaratan Polsri untuk keamanan informasi mematuhi kontrak dan SLA dengan pihak ketiga.		0	0	0	Belum ada kegiatan terkait.
2	Memastikan bisnis operasional dan persyaratan pemrosesan TI memenuhi kontrak dan SLA.	3	0	0	0	Belum ada kegiatan terkait.
3	Mengintegrasikan proses manajemen TI internal dengan penyedia layanan.		1	1	1	Salah satu bentuk integrasi yang dilakukan adalah dengan menerapkan sistem informasi di Polsri serta melakukan kerjasama dengan provider telekomunikasi.
4	Merencanakan audit independen terkait pengelolaan outsource layanan IT.	4	0	0	0	Belum ada kegiatan terkait.

Berdasar keterangan pada Tabel 4.26 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS01.02 sudah benar dan sesuai. Responden pada proses DSS01.02 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 3 berada di *capability* level 3, sedangkan aktivitas 4 berada di *capability* level 4.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Tidak (0) untuk proses DSS01.02 aktivitas 1, 2, dan 4. Meskipun aktivitas 3 pada *capability* level 3 bernilai Ya (1), namun Polsri belum mencapai *capability* level 3 pada DSS01.02 karena ada dua aktivitas sebelumnya di level *capability* yang sama belum memenuhi. Berarti dalam hal ini Polsri belum memenuhi *capability* level 3, dan berada pada *capability* level 1.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 1 pada DSS01.02, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS01.02 *Managed Outsourced I&T Services* namun belum dilakukan secara berkala.

#### **DSS01.03 Monitor I&T Infrastructure**

Pada *key management practice* DSS01.03 dari 3 *role* dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.27.

Tabel 4.27. Hasil kuisioner domain DSS01.03

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Mencatat event berdasar pertimbangan risiko dan kinerja.	2	1	1	1	Sudah ada pencatatan event dilakukan dengan pertimbangan risiko seperti yang tertera pada Peta Proses Bisnis Polsri (ringan, sedang, dan berat), namun belum dilakukan secara terstruktur.
2	Mengidentifikasi dan memelihara daftar aset infrastruktur yang perlu dipantau.	3	1	1	1	Pemeliharaan aset infrastruktur dilakukan bekerjasama dengan Layanan Perawatan dan Perbaikan Polsri, hal ini tertera dalam Peta Proses Bisnis Polsri.
3	Menetapkan aturan yang mengidentifikasi dan mengelola pencatatan pelanggaran sesuai ambang batas.		1	0	1	Belum ada kegiatan yang terstruktur.
4	Melaporkan log peristiwa dan penyimpanan dalam infrastruktur IT.		1	1	1	Sudah ada pelaporan log yang dilakukan saat terjadi event tertentu (segera diatasi), namun tidak terdapat dokumentasi secara terstruktur.
5	Membuat tiket insiden sehingga bisa dilakukan penyelesaian secara tepat waktu.	4	0	0	0	Tiket insiden dibuat dalam bentuk Form Permintaan Layanan, penyelesaian dilakukan sesuai dengan pertimbangan kebutuhan.
6	Menetapkan prosedur untuk penentuan log peristiwa secara berkala.		1	0	1	Belum ada prosedur terkait.

Berdasar keterangan pada Tabel 4.27 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS01.03 sudah benar dan sesuai. Responden pada proses DSS01.03 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 berada di *capability* level 2, aktivitas nomor 2 sampai dengan 5 berada di level 3, sedangkan aktivitas nomor 6 berada di level 4.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS01.03 aktivitas 1, dengan keterangan meskipun di Polsri sudah mengerjakan pencatatan *event* namun belum dilakukan secara terstruktur berdasarkan pertimbangan risiko dan kinerja, sehingga memenuhi *capability* level 2. Pada aktivitas 2 dan 4 bernilai Ya (1) sehingga memenuhi *capability* level 3, meskipun pada aktivitas 3 dan 6 masih ada responden yang menjawab Tidak (0). Sedangkan pada aktivitas 6 masih ada responden menjawab Tidak (0) dan belum ditemukan prosedur terkait.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 3 pada DSS01.03, dimana berarti Polsri sudah mengadakan kegiatan berkaitan dengan proses DSS01.03 *Monitor I&T Infrastructure* sudah dilakukan dengan menggunakan panduan pada Peta Proses Bisnis Polsri.

#### **DSS01.04 Manage the environment**

Pada *key management practice* DSS01.04 dari 3 *role* dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.28.

Tabel 4.28. Hasil kuisioner domain DSS01.04

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Mengidentifikasi terkait kemungkinan terjadinya bencana alam dan buatan manusia yang mempengaruhi di tempat fasilitas IT berada.	2	1	1	1	Sudah ada SOP Penanganan Gangguan Jaringan Lokal dan SOP Penanganan Gangguan Server (PGS) untuk kemungkinan terjadinya bencana.



Tabel 4.28. Hasil kuisioner domain DSS01.04 (lanjutan)

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
2	Mengidentifikasi untuk mengetahui bagaimana melindungi peralatan IT, serta lainnya yang menimbulkan bahaya kebakaran.		1	1	1	Belum ada SOP resmi mengenai ini namun sudah ada blueprint mengenai kerangka kerja kebijakan SOP IT per tahun 2020-2024 yang belum diajukan pada rapat senat.
3	Memastikan site IT dan ruang server bersih dan dalam kondisi aman.		1	1	1	Situs IT dan ruang server selalu diusahakan bersih dan aman.
4	Memastikan penempatan dan pembangunan fasilitas IT meminimalkan kerentanan terhadap ancaman lingkungan sekitar (pencurian, vandalisme, bahan peledak dan lain-lain).	3	1	1	1	Pencempatan dan pembangunan fasilitas IT sudah disesuaikan dengan kebijakan Polsri.
5	Merencanakan polis asuransi dan hasil laporan.		0	0	0	Belum ada perencanaan dan pelaporan terkait.
6	MerESPon notifikasi alarm bila terjadi kerentanan terhadap lingkungan dan pelatihan terhadap tim.		1	1	1	Pelatihan tim dilaksanakan berdasar surat tugas dari pimpinan Polsri.
7	Memelihara perangkat secara proaktif untuk mendeteksi ancaman lingkungan.	4	1	1	1	Perangkat dipelihara sesuai dengan prosedur.

Berdasar keterangan pada Tabel 4.28 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS01.04 sudah benar dan sesuai. Responden pada proses DSS01.04 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 3 berada di *capability* level 2, aktivitas nomor 4 sampai dengan 6



berada di *capability* level 3, sedangkan aktivitas nomor 7 berada di *capability* level 4.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS01.04 aktivitas nomor 1 sampai dengan 7. Kecuali pada aktivitas 5 seluruh responden menjawab Tidak (0). Hal ini berarti bahwa Polsri sudah mencapai *capability* level 2, 3, dan 4 pada DSS01.04.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 4 pada DSS01.04, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS01.04 *Manage the environment* sudah dilakukan dengan SOP (SOP Penanganan Gangguan Jaringan Lokal dan SOP Penanganan Gangguan Server) dan dimonitor.

#### DSS01.05 Manage facilities

Pada *key management practice* DSS01.05 dari 3 *role* dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.29.

Tabel 4.29. Hasil kuisioner domain DSS01.05

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Memeriksa persyaratan fasilitas IT untuk perlindungan terhadap fluktuasi dan pemadaman listrik.	2	1	1	1	Hal ini sudah tercantum dalam Rencana Kinerja Tahunan Polsri Tabel 2. Program Strategis dan Kegiatan bab VI mengenai Sarana dan Prasarana poin 4 Pembangunan unit utilitas (penjernihan air, energi, listrik, dan PABX/Private Automatic Branch eXchange). Selain itu tertuang juga dalam Standar Sarana dan Prasarana Pembelajaran Polsri.
2	Adanya pengalihan suplai catu daya.		1	1	1	
3	Adanya sumber utilitas lain (listrik, telekomunikasi cadangan) untuk sistem IT.		1	1	1	

Tabel 4.29. Hasil kuisioner domain DSS01.05 (lanjutan)

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
4	Pemasangan kabel eksternal ke arah IT sudah memiliki saluran yang aman dan terlindungi.		1	1	1	
5	Mendokumentasikan pemasangan struktur kabel dan saluran.		1	1	0	Belum ada dokumentasi spesifik mengenai pemasangan struktur kabel dan saluran.
6	Adanya pendidikan tim tentang undang-undang kesehatan, keselamatan, peraturan, dan perundangan yang relevan seandainya terjadi insiden (contoh kebakaran).		1	1	0	Adanya kegiatan Pelatihan Keselamatan dan Kesehatan Kerja (K3) di Polsri.
7	Pemeliharaan lokasi dan peralatan IT oleh personel yang berwenang.		1	1	1	Pemeliharaan dilakukan sesuai tupoksi dari setiap personel Polsri yang terkait.
8	Menganalisis ketersediaan kabel yang redundan atau fail over.	3	1	1	1	Analisis dibuat berdasar laporan mengenai insiden yang terjadi apabila terdapat kabel yang redundan.
9	Site dan fasilitas IT sudah mematuhi peraturan, pedoman terkait kesehatan dan keselamatan.		1	1	1	Site dan fasilitas IT dibuat sesuai arahan dari Pimpinan Polsri yang disesuaikan dengan Pedoman Keselamatan dan Kesehatan Kerja (K3) di Polsri.
10	Mencatat, memantau, mengelola, dan menyelesaikan insiden fasilitas yang sejalan dengan proses manajemen insiden IT.		1	0	1	Belum ada proses manajemen insiden IT terkait.
11	Menganalisis proses perubahan fisik atau bangunan IT untuk menilai risiko lingkungan (misal kerusakan akibat kebakaran atau air).	4	1	1	0	Belum ada kegiatan terkait.

Berdasar keterangan pada Tabel 4.29 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS01.05 sudah benar dan sesuai. Responden pada proses DSS01.05 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 6 berada di *capability* level 2, aktivitas nomor 7 sampai dengan 9 berada di level 3, sedangkan aktivitas nomor 10 dan 11 berada di level 4.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS01.05 aktivitas 1 sampai dengan 4, berarti Polstri sudah memenuhi *capability* level 2. Pada aktivitas 7 sampai 9 setiap responden menjawab Ya (1). Sedangkan pada aktivitas 10 dan 11 masih ada responden yang menjawab Tidak (0) karena kegiatan tersebut belum terealisasi secara baik.

Kesimpulannya bahwa Polstri sudah mencapai *capability* level 3 pada DSS01.05, dimana berarti Polstri sudah mengadakan kegiatan yang berkaitan dengan proses DSS01.05 *Manage facilities* dengan panduan dari Rencana Kinerja Tahunan Polstri, Standar Sarana dan Prasarana Pembelajaran Polstri, kegiatan Pelatihan Keselamatan dan Kesehatan Kerja (K3).

#### **Hasil Analisis DSS01**

Dari hasil analisis di atas, dapat disimpulkan hasil keseluruhan proses domain DSS01 *Managed Operations* ditunjukkan pada Tabel 4.30.

Tabel 4.30. Hasil keseluruhan proses domain DSS01

No	Domain	Tingkat Kapabilitas Saat Ini	Tingkat Kapabilitas Target
1	DSS01.01	2	3
2	DSS01.02	1	2
3	DSS01.03	3	4
4	DSS01.04	4	4
5	DSS01.05	3	4
	Rata-rata	2,6	
	Rata-rata Capability	3	

Sedangkan hasil audit dari domain DSS01 ditunjukkan pada Gambar 4.9.



Gambar 4.9. Hasil audit DSS01

Kesimpulan dari hasil audit diatas adalah sebagai berikut:

1. Pada DSS01.01 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 2, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 3. Pada *capability* level 2 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS01.01 *Perform operational procedures* sudah dilakukan secara berkala.
2. Pada DSS01.02 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 1, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 3. Pada *capability* level 1 berarti

bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS01.02 *Managed Outsourced I&T Services* namun belum dilakukan secara berkala.

3. Pada DSS01.03 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 4. Pada *capability* level 3 berarti bahwa Polsri sudah mengadakan kegiatan berkaitan dengan proses DSS01.03 *Monitor I&T Infrastructure* sudah dilakukan dengan menggunakan panduan pada Peta Proses Bisnis Polsri.
4. Pada DSS01.04 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 4, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu level 4 pada domain proses tersebut. Pada *capability* level 4 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS01.04 *Manage the environment* sudah dilakukan dengan SOP (SOP Penanganan Gangguan Jaringan Lokal dan SOP Penanganan Gangguan Server) dan dimonitor.
5. Sedangkan pada DSS01.05 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 4. Pada *capability* level 3 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS01.05 *Manage facilities* dengan panduan dari Rencana Kinerja Tahunan Polsri, Standar Sarana dan Prasarana Pembelajaran Polsri, kegiatan Pelatihan Keselamatan dan Kesehatan Kerja (K3).



6. Berdasar level kapabilitas dari setiap proses domain tersebut kemudian di rata-rata untuk mendapatkan level *capability* pada domain DSS01. Diketahui bahwa level *capability* pada domain DSS01 yaitu berada di level 3, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan DSS01 *Managed Operations* sudah dilakukan dengan SOP dan panduan terkait.

#### 4.3.4. Hasil Audit DSS02 Managed Service Requests and Incident

Pengukuran proses kapabilitas Polsri berdasar domain DSS02 ditunjukkan pada Tabel 4.31, 4.32, 4.33, 4.34, 4.35, 4.36, dan 4.37.

##### DSS02.01 Define classification schemes for incidents and service requests

Pada *key management practice* DSS02.01 dari 3 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.31.

Tabel 4.31. Hasil kuisioner domain DSS02.01

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Menentukan klasifikasi service request dan insiden untuk melakukan analisis tren service request dan insiden.	3	0	0	Penentuan klasifikasi pelayanan diidentifikasi berdasar jenis dan kebutuhan servis dengan menggunakan Form Permintaan Layanan yang bisa diakses secara online. Namun Polsri belum melakukan analisis lebih lanjut mengenai tren servis request dan insiden.
2	Menentukan model insiden untuk memungkinkan penyelesaian yang efektif dan efisien.		1	1	Model insiden yang terjadi di klasifikasi berdasar kebutuhan. Berdasar Peta Proses Bisnis Polsri diketahui bahwa klasifikasi dibuat dengan melihat apakah insiden tersebut termasuk tingkat ringan, sedang atau berat.

Tabel 4.31. Hasil kuisioner domain DSS02.01 (lanjutan)

No	Aktivitas	Cap. Level	R1	R2	Keterangan
3	Menentukan model service request dan insiden untuk mengaktifkan layanan yang swadaya dan efisien.		0	0	Adanya beberapa SOP yang terkait diantaranya SOP Penanganan Gangguan Jaringan Lokal, SOP Penanganan Gangguan Server (PGS). Serta adanya Panduan Pelayanan Informasi yang dijelaskan di dalam Peta Proses Bisnis Polsri.
4	Menetapkan aturan dan prosedur eskalasi insiden.		1	0	
5	Menentukan sumber pengetahuan (dokumen) tentang service request dan insiden serta penjelasan cara menggunakannya.		1	1	

Berdasar keterangan pada Tabel 4.31 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS02.01 sudah benar dan sesuai. Responden pada proses DSS02.01 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 5 berada di *capability* level 3.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS02.01 aktivitas 2 dan 5. Setelah dilakukan penelusuran dokumen terkait aktivitas 1, 3, dan 4, meskipun responden masih ada yang menjawab 0, namun kelengkapan dokumen Polsri untuk aktivitas tersebut sudah mencukupi dan lengkap.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 3 pada DSS02.01, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.01 *Define classification schemes for incidents and service requests* sudah dilakukan dengan menggunakan SOP Penanganan Gangguan

Jaringan Lokal, SOP Penanganan Gangguan Server (PGS), dan Panduan Pelayanan Informasi yang dijelaskan dalam Peta Proses Bisnis Polsri.

### DSS02.02 Record, classify and prioritize requests and incidents

Pada *key management practice* DSS02.02 dari 2 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.32.

Tabel 4.32. Hasil kuisioner domain DSS02.02

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Mencatat service request dan insiden.	2	1	1	Sudah adanya Form Permintaan Layanan yang disediakan secara online untuk mencatat service request dan insiden.
2	Mengklasifikasi service request dan insiden.		0	0	Aktivitas berkaitan dengan proses DSS02.01 aktivitas nomor 1. Belum ada pengklasifikasian servis request dan insiden.
3	Melakukan pemrioritasan service request dan insiden.		1	0	Pemrioritasan servis request dan insiden belum dilakukan secara formal namun berdasar kebutuhan (pemrioritasan ini disebutkan di dalam Peta Proses Bisnis Polsri) yang dibedakan menjadi ringan, sedang, dan berat.

Berdasar keterangan pada Tabel 4.32 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS02.02 sudah benar dan sesuai. Responden pada proses DSS02.02 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 3 berada di *capability* level 2.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS02.02 aktivitas 1. Sedangkan pada aktivitas 2 setiap responden

menjawab Tidak (0) karena belum ada klasifikasi rinci mengenai servis *request* dan insiden.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 2 pada DSS02.02, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.02 *Record, classify and prioritize requests and incidents* secara berkala.

### DSS02.03 Verify, approve and fulfill service request

Pada *key management practice* DSS02.03 dari 4 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.33.

Tabel 4.33. Hasil kuisioner domain DSS02.03

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Memverifikasi hak untuk service request dan insiden.	2	1	1	Hak penggunaan servis request dan insiden adalah dengan menggunakan Form Permintaan Layanan. Alur proses lebih lanjut dijelaskan pada Peta Proses Bisnis Polsri pada Bab VI poin a mengenai Layanan Informasi.
2	Melakukan persetujuan finansial dan fungsional service request dan insiden.		1	0	Persetujuan finansial dan fungsional disesuaikan dengan servis request dan insiden yang diminta. Bila membutuhkan persetujuan formal (tanda tangan) maka akan diteruskan ke Pimpinan Polsri untuk kemudian ditindaklanjuti ke bagian terkait.
3	Adanya menu otomatis bantuan mandiri saat melakukan prosedur permintaan service request dan insiden.	3	1	1	Sudah terdapat menu otomatis bantuan mandiri dengan melakukan pengisian form terkait serta modul-modul yang biasa dibutuhkan.

Berdasar keterangan pada Tabel 4.33 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS02.03 sudah benar dan sesuai. Responden pada



proses DSS02.03 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 dan 2 berada di *capability* level 2, sedangkan pada aktivitas nomor 3 berada di level 3.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS02.03 aktivitas 1 dan 3 yang berarti sudah memenuhi *capability* level 2 dan 3 pada DSS02.03.

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 3 pada DSS02.03, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.03 *Verify, approve and fulfill service request* sudah dilakukan dengan menggunakan panduan alur proses pada Peta Proses Bisnis Polsri Bab VI Poin a mengenai Layanan Informasi.

#### **DSS02.04 Investigate, diagnose and allocate incidents**

Pada *key management practice* DSS02.04 dari 3 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.34.

Tabel 4.34. Hasil kuisioner domain DSS02.04

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Mengidentifikasi dan menjelaskan gejala untuk menetapkan penyebab service request dan insiden.	2	1	1	Identifikasi mengenai akar penyebab servis request dan insiden masih dilakukan secara manual tanpa pencatatan. Namun sudah ada SOP dan modul yang menunjang untuk menangani servis request dan insiden.
2	Membuat service request dan insiden untuk service request dan insiden baru.		1	1	Bila terjadi permintaan servis request dan insiden yang baru bisa langsung mengisi pada Form Permintaan Layanan.



Tabel 4.34. Hasil kuisioner domain DSS02.04 (lanjutan)

No	Aktivitas	Cap. Level	R1	R2	Keterangan
3	Adanya service request dan insiden yang memerlukan keahlian yang lebih dalam sehingga melibatkan unit lain yang sesuai.		1	1	Pada Peta Proses Bisnis Polsri disebutkan mengenai penetapan sumber data/informasi apabila membutuhkan layanan tertentu akan dibuatkan Surat Pengantar yang dapat dipergunakan untuk menyampaikan instruksi lebih lanjut ke unit/bidang relevan.

Berdasar keterangan pada Tabel 4.34 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS02.04 sudah benar dan sesuai. Responden pada proses DSS02.04 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 3 *capability level 2*.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS02.04 aktivitas nomor 1 sampai dengan 3.

Kesimpulannya bahwa Polsri sudah mencapai *capability level 2* pada DSS02.04, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.04 *Investigate, diagnose and allocate incidents* sudah dilakukan secara berkala.

#### **DSS02.05 Resolve and recover from Incident**

Pada *key management practice* DSS02.05 dari 4 *role* dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.35.

Tabel 4.35. Hasil kuisioner domain DSS02.05

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Memilih dan menerapkan resolusi service request dan insiden sementara atau permanen.	2	1	1	0	Belum ada penetapan solusi apakah solusi tersebut sementara atau permanen, solusi dibuat berdasar kebutuhan.
2	Mencatat dari setiap solusi dari service request dan insiden.		1	1	1	Pencatatan dilakukan secara manual dan dilanjutkan secara langsung untuk penanganan servis.
3	Melakukan tindakan pemulihan dari setiap service request dan insiden.		1	1	1	Tindakan pemulihan dilakukan apabila dibutuhkan.
4	Mendokumentasi dan menilai dari service request dan insiden.		1	1	1	Dokumentasi dan penilaian dilakukan secara individual. Belum ada dokumentasi resmi.

Berdasar keterangan pada Tabel 4.35 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS02.05 sudah benar dan sesuai. Responden pada proses DSS02.05 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi. Berdasar buku COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 sampai dengan 4 berada di *capability level 2*.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS02.05 aktivitas nomor 1 sampai dengan 4.

Kesimpulannya bahwa Polsri sudah mencapai *capability level 2* pada DSS02.05, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.05 *Resolve and recover from incident* sudah dilakukan secara berkala.

### DSS02.06 Close service requests and incident

Pada *key management practice* DSS02.06 dari 3 *role* dalam COBIT 2019 didapat 3 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.36.

Tabel 4.36. Hasil kuisioner domain DSS02.06

No	Aktivitas	Cap. Level	R1	R2	R3	Keterangan
1	Memverifikasi dengan pengguna yang terpengaruh bahwa service request dan insiden sebelumnya telah diselesaikan.	2	1	1	1	Melakukan review kepada pengguna terpengaruh apakah permintaan servis request dan insiden sudah selesai ataukah belum.
2	Menutup service request dan insiden.		1	1	0	Belum ada penutupan resmi serta pencatatan dalam dokumen terkait.

Berdasar keterangan pada Tabel 4.36 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS02.06 sudah benar dan sesuai. Responden pada proses DSS02.06 yaitu Ketua UPT TIK/PIH, Ketua Koordinator Infrastruktur dan Jaringan, dan Ketua Koordinator Sistem Informasi. Berdasar COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 dan 2 berada di *capability* level 2.

Pada data hasil kuisioner terlihat bahwa setiap responden menjawab Ya (1) untuk proses DSS02.06 aktivitas 1. Sedangkan pada aktivitas nomor 2 masih menjawab Tidak (0).

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 2 pada DSS02.06, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.06 *Close service requests and incident* sudah dilakukan secara berkala.

### DSS02.07 Track status and produce reports

Pada *key management practice* DSS02.07 dari 2 *role* dalam COBIT 2019 didapat 2 responden dengan hasil kuisioner ditunjukkan pada Tabel 4.37.

Tabel 4.37. Hasil kuisioner domain DSS02.07

No	Aktivitas	Cap. Level	R1	R2	Keterangan
1	Memantau dan melacak laporan service request dan insiden untuk meningkatkan solusi penyelesaian.	2	1	1	Aktivitas ini berkaitan dengan DSS02.06 aktivitas nomor 1.
2	Mengidentifikasi frekuensi dan media laporan dari service request dan insiden.	3	1	1	Belum ada identifikasi mengenai frekuensi servis request dan insiden. Namun sudah ada pengetahuan mengenai media laporan yang dipergunakan yaitu melalui Form Permintaan Layanan.
3	Mencetak dan melaporkan service request dan insiden secara tepat waktu.	4	1	0	Sudah ada pelaporan melalui Form Permintaan Layanan namun penanganan masih disesuaikan dengan kebutuhan.
4	Menganalisis dan membuat permintaan layanan berdasar kategori dan jenisnya.		0	1	Sudah ada pembuatan permintaan layanan berdasar kategori namun belum ada analisis lebih lanjut.
5	Menggunakan informasi dalam service request dan insiden yang digunakan untuk masukan perencanaan perbaikan berkelanjutan.	5	0	1	Belum ada pencatatan informasi servis request dan insiden.

Berdasar keterangan pada Tabel 4.37 dapat dijustifikasi bahwa penilaian responden terhadap proses DSS02.07 sudah benar dan sesuai. Responden pada proses DSS02.07 yaitu Ketua UPT TIK/PIH dan Ketua Koordinator Sistem Informasi. Berdasar COBIT 2019 *Governance and Management Objective* diketahui bahwa aktivitas nomor 1 berada di *capability* level 2, aktivitas nomor 2

berada di level 3, aktivitas nomor 3 dan 4 berada di level 4, sedangkan aktivitas nomor 5 berada di level 5.

Pada data hasil kuisioner terlihat bahwa untuk aktivitas 1 seluruh responden menjawab Ya (1) berarti memenuhi *capability* level 2. Pada aktivitas 2 seluruh responden menjawab Ya (1) berarti memenuhi level 3. Sedangkan pada aktivitas 3 sampai dengan 5 masih ada responden yang menjawab Tidak (0).

Kesimpulannya bahwa Polsri sudah mencapai *capability* level 3 pada DSS02.07, dimana berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.07 *Track status and produce reports* sudah dilakukan dengan menggunakan Form Permintaan Layanan, namun belum ada pencatatan lebih lanjut dari informasi *servis request* dan insiden.

#### Hasil Analisis DSS02

Dari hasil analisis di atas, dapat disimpulkan hasil keseluruhan proses domain DSS02 *Managed Service Requests and Incidents* ditunjukkan pada Tabel 4.38.

Tabel 4.38. Hasil keseluruhan proses domain DSS02

No	Domain	Tingkat Kapabilitas Saat Ini	Tingkat Kapabilitas Target
1	DSS02.01	3	3
2	DSS02.02	2	2
3	DSS02.03	3	3
4	DSS02.04	2	2
5	DSS02.05	2	2
6	DSS02.06	2	2
7	DSS02.07	3	4
	Rata-rata	2,42	
	Rata-rata Capability	2	

Sedangkan hasil audit dari domain DSS02 ditunjukkan pada Gambar 4.10.





Gambar 4.10. Hasil audit DSS02

Kesimpulan dari hasil audit diatas adalah sebagai berikut:

1. Pada DSS02.01 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu 3 pada domain proses tersebut. Pada *capability* level 3 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.01 *Define classification schemes for incidents and service requests* sudah dilakukan dengan menggunakan SOP Penanganan Gangguan Jaringan Lokal, SOP Penanganan Gangguan Server (PGS), dan Panduan Pelayanan Informasi yang dijelaskan dalam Peta Proses Bisnis Polsri.
2. Pada DSS02.02 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 2, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu 2 pada domain proses tersebut. Pada *capability* level 2 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.02 *Record, classify and prioritize requests and incidents* sudah dilakukan secara berkala.

3. Pada DSS02.03 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 2, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu 2 pada domain proses tersebut. Pada *capability* level 2 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.03 *Verify, approve and fulfill service request* sudah dilakukan dengan menggunakan panduan alur proses pada Peta Proses Bisnis Polsri Bab VI Poin a mengenai Layanan Informasi.
4. Pada DSS02.04 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 2, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu 2 pada domain proses tersebut. Pada *capability* level 2 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.04 *Investigate, diagnose and allocate incidents* sudah dilakukan secara berkala.
5. Pada DSS02.05 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 2, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu 2 pada domain proses tersebut. Pada *capability* level 2 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.05 *Resolve and recover from incident* sudah dilakukan secara berkala.
6. Pada DSS02.06 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 2, dengan tingkat kapabilitas sudah memenuhi level kapabilitas maksimal yaitu 2 pada domain proses tersebut. Pada *capability* level 2 berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses

DSS02.06 *Close service requests and incident* sudah dilakukan secara berkala.

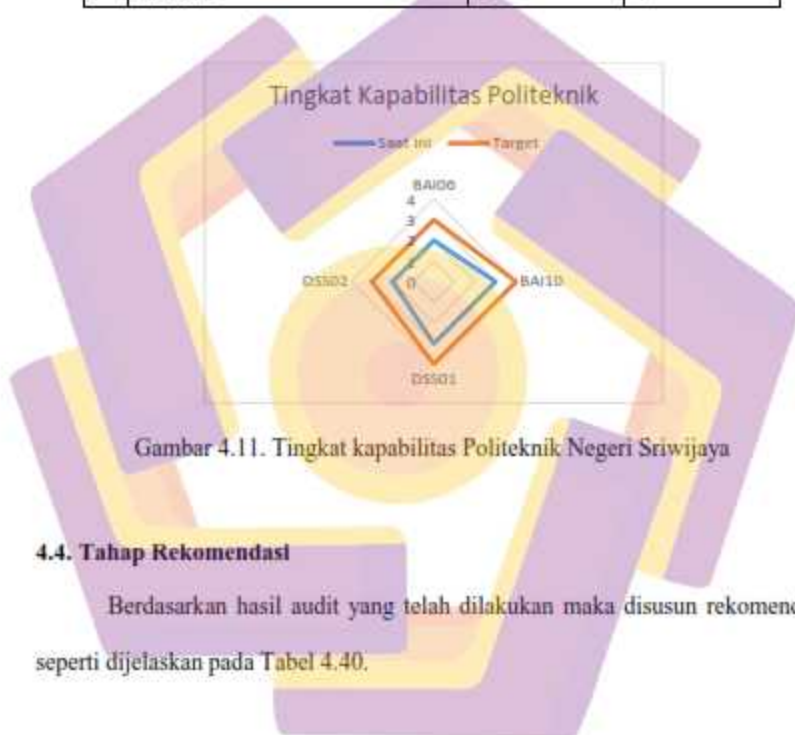
7. Pada DSS02.07 diketahui bahwa tingkat kapabilitas Polsri saat ini berada di level 3, dengan tingkat kapabilitas target berada 1 tingkat di atas level kapabilitas saat ini yaitu berada di level 4. Pada *capability level 3* berarti bahwa Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02.07 *Track status and produce reports* sudah dilakukan dengan menggunakan Form Permintaan Layanan, namun belum ada pencatatan lebih lanjut dari informasi servis *request* dan insiden.
8. Berdasar level kapabilitas dari setiap proses domain tersebut kemudian di rata-rata untuk mendapatkan level *capability* pada domain DSS02. Diketahui bahwa level *capability* pada domain DSS02 yaitu berada di level 2, yang berarti Polsri sudah mengadakan kegiatan yang berkaitan dengan proses DSS02 *Managed Service Requests and Incident* secara berkala.

#### **4.3.5. Rekapitulasi Hasil Audit Keseluruhan**

Berikut rekapitulasi hasil audit yang dilakukan pada Politeknik Negeri Sriwijaya menggunakan framework COBIT 2019 ditunjukkan pada Tabel 4.39, dari keseluruhan pengukuran terlihat bahwa rata-rata domain saat ini menunjukkan bahwa Polsri berada pada tingkat kapabilitas level 3. Gambar 4.11 menunjukkan kesenjangan dari setiap domain.

Tabel 4.39. Rekapitulasi hasil audit keseluruhan

No	Domain	Tingkat Kapabilitas Saat Ini	Tingkat Kapabilitas Target
1	BAI06	2	3
2	BAI10	3	4
3	DSS01	3	4
4	DSS02	2	3
	Rata-rata	3	4



Gambar 4.11. Tingkat kapabilitas Politeknik Negeri Sriwijaya

#### 4.4. Tahap Rekomendasi

Berdasarkan hasil audit yang telah dilakukan maka disusun rekomendasi seperti dijelaskan pada Tabel 4.40.

Tabel 4.40. Rekomendasi hasil audit

No	Domain	Temuan	Rekomendasi
1	BAI06.01	<p>a. Sudah ada Peraturan Akademik Politeknik mengenai otorisasi formal Sarana dan Prasarana.</p> <p>b. Sudah ada Form Permintaan Layanan untuk mengkategorikan layanan.</p> <p>c. Sudah ada Peta Proses Bisnis Polsri yang dijelaskan pada Bab VI mengenai pemrioritasan berdasar kebutuhan.</p> <p>d. Sudah ada surat tugas dalam pelaksanaan perubahan.</p> <p>e. Belum ada evaluasi permintaan layanan secara terstruktur dan pertimbangan dampak penyedia layanan yang dikontrak.</p>	Polsri perlu melakukan evaluasi permintaan layanan secara terstruktur dan pertimbangan dampak penyedia layanan yang dikontrak.
2	BAI06.02	<p>a. Sudah ada Peta Proses Bisnis Polsri mengenai pembagian perubahan darurat berdasar jenis kerusakan (sedang, ringan, atau berat).</p> <p>b. Polsri belum menggunakan proses dokumentasi manual dari setiap hasil testing perubahan IT yang terjadi.</p>	Polsri perlu membuat Panduan Standar Dokumentasi Manual Perubahan IT serta Form Panduan Dokumentasi Manual Perubahan IT yang terjadi.
3	BAI06.03	<p>a. Polsri belum menggunakan proses dokumentasi manual dari setiap hasil testing perubahan IT yang terjadi.</p> <p>b. Polsri belum menerapkan metric kinerja untuk membentuk jejak audit.</p>	Polsri perlu membuat Panduan Standar Dokumentasi Manual Perubahan IT serta Form Perubahan IT yang terjadi sehingga dapat membentuk jejak audit.
4	BAI06.04	<p>a. Sudah ada SOP Penanganan Gangguan Lokal, SOP Penanganan Gangguan Server (PGS), SOP Pembuatan Sub Domain dan Hosting (PSDH), SOP Pembuatan Website, SOP Pembuatan Sistem Informasi, SOP Pembuatan Email, dan berbagai modul dokumentasi.</p> <p>b. Sudah ada pengarsipan dokumen sesuai SOP Tingkat Institusi yang tertuang dalam Instruksi Kerja Pengarsipan Dokumen.</p>	Polsri perlu membuat Panduan Standar Dokumentasi Manual Perubahan IT serta Form Perubahan IT yang terjadi.



Tabel 4.40. Rekomendasi hasil audit (lanjutan)

No	Domain	Temuan	Rekomendasi
5	BAI10.01	Sudah adanya model logis dari setiap layanan di Polsri yang disusun dalam Peta Proses Bisnis Polsri.	Perlunya penyusunan prosedur lebih rinci di setiap Proses Bisnis Polsri sehingga dapat dipahami oleh setiap unit terkait.
6	BAI10.02	a. Klasifikasi configuration item bisa dilihat secara umum pada Peta Proses Bisnis Polsri. b. Konfigurasi layanan, aplikasi atau infrastruktur dibuat, ditinjau dan disetujui sesuai dengan kebutuhan Polsri.	Perlunya pembuatan configuration item yang lebih terperinci sehingga dapat dipahami oleh setiap unit terkait.
7	BAI10.03	a. Sudah terdapat pembagian job desk berdasar tupoksi di dalam Polsri sehingga memudahkan dalam pengidentifikasian bila terjadi perubahan CI. b. Belum ada perhitungan akurasi untuk meninjau perubahan CI.	Polsri perlu membuat Dokumentasi Manual Configuration Item.
8	BAI10.04	Belum ada identifikasi dan pelaporan perubahan status CI secara formal.	Polsri perlu membuat Form Laporan Perubahan Configuration Item.
9	BAI10.05	a. Belum ada kegiatan verifikasi CI secara berkala. b. Sudah ada kegiatan pelaporan dengan mengumpulkan semua penyimpangan dan membahas dengan Pimpinan Polsri. c. Belum ada kegiatan untuk meninjau dan membandingkan kelengkapan repository dan akurasi secara berkala untuk meningkatkan kualitas repository.	Polsri perlu mengadakan kegiatan untuk meninjau dan membandingkan kelengkapan repository dan akurasi secara berkala untuk meningkatkan kualitas repository.
10	DSS01.01	a. Sudah adanya jadwal operasional pelayanan IT. b. Belum ada kegiatan verifikasi data yang diproses secara lengkap akurat dan tepat waktu, pemrosesan sesuai kebutuhan. c. Sudah ada pemantauan insiden dan masalah, namun belum ada pengelolaan kinerja dan hasil dokumentasi kegiatan operasional.	a. Polsri perlu memastikan bahwa kegiatan verifikasi data diproses secara lengkap, akurat dan tepat waktu. b. Polsri perlu membuat Dokumentasi Kegiatan Operasional IT.

Tabel 4.40. Rekomendasi hasil audit (lanjutan)

No	Domain	Temuan	Rekomendasi
11	DSS01.02	Belum ada pengelolaan outsource layanan IT apakah sudah sesuai dengan kontrak dan SLA.	Polri perlu membuat Dokumen Pengelolaan Outsource Layanan IT sehingga bisa menilai apakah sudah sesuai dengan kontrak dan SLA.
12	DSS01.03	a. Sudah ada pencatatan event berdasar pertimbangan risiko dan kinerja namun belum dilakukan secara terstruktur. b. Belum ada pencatatan untuk mengidentifikasi dan mengelola pelanggaran IT infrastruktur sesuai ambang batas. c. Belum ada prosedur penentuan log peristiwa secara berkala.	Polri perlu membuat Form Penanganan Insiden untuk memonitor IT infrastruktur dan pembuatan log peristiwa secara berkala.
13	DSS01.04	a. Sudah ada SOP Penanganan Gangguan Jaringan Lokal dan SOP Penanganan Gangguan Server (PGS) untuk kemungkinan terjadinya bencana. b. Belum ada SOP Perlindungan Peralatan IT.	Perlu adanya pembuatan SOP Perlindungan Peralatan IT.
14	DSS01.05	a. Sudah ada RKT yang membahas mengenai Sarana dan Prasarana termasuk dalam fasilitas IT. b. Belum ada dokumentasi proses manajemen insiden IT yang dipergunakan untuk menilai risiko lingkungan.	Polri perlu membuat Dokumen Penanganan Insiden.
15	DSS02.01	a. Belum ada penentuan klasifikasi service request dan insiden serta analisis tren. b. Belum ada aturan dan prosedur eskalasi insiden.	Polri perlu membuat Aturan dan Prosedur Eskalasi Insiden serta analisis tren dari service request dan insiden.
16	DSS02.02	Belum ada pengklasifikasian service request dan insiden.	Polri perlu membuat Dokumen Service Request dan Insiden.
17	DSS02.03	Sudah adanya kegiatan verifikasi, approve, dan pemenuhan dalam service request.	Perlunya dokumentasi dalam kegiatan verifikasi, approve, dan pemenuhan service request.
18	DSS02.04	Sudah adanya kegiatan identifikasi, diagnose, dan alokasi insiden.	Perlunya dokumentasi dalam kegiatan identifikasi, diagnose, dan alokasi insiden.
19	DSS02.05	Belum ada penetapan apakah solusi yang dibuat dalam servis request dan insiden termasuk solusi sementara atau permanen.	Polri perlu membuat Dokumen Service Request dan Insiden.

Tabel 4.40. Rekomendasi hasil audit (lanjutan)

No	Domain	Temuan	Rekomendasi
20	DSS02.06	Sudah ada kegiatan verifikasi terhadap pengguna yang terpengaruh pada servis request dan insiden, namun belum ada penutupan resmi mengenai servis request dan insiden.	Polsri perlu melakukan tidak lanjut mengenai servis request dan insiden dengan melakukan penutupan resmi.
21	DSS02.07	Belum ada dokumentasi mengenai pencatatan informasi service request dan insiden untuk perbaikan berkelanjutan.	Perlu adanya dokumentasi mengenai Form Status Penanganan Service Request dan Insiden untuk perbaikan berkelanjutan.

Secara umum berikut rekomendasi perbaikan yang diperlukan pada Politeknik Negeri Sriwijaya:

1. Polsri perlu membuat Panduan Standar Dokumentasi Manual Perubahan IT serta Form Perubahan IT.
2. Polsri perlu membuat Dokumentasi Manual Configuration Item serta Form Laporan Perubahan Configuration Item.
3. Polsri perlu membuat Dokumen Kegiatan Operasional IT.
4. Polsri perlu membuat Dokumen Pengelolaan Outsource Layanan IT.
5. Polsri perlu membuat Form Penanganan Service Request dan Insiden serta Form Status Penanganan Service Request dan Insiden.
6. Polsri perlu membuat SOP Perlindungan Peralatan IT.
7. Polsri perlu membuat Aturan dan Prosedur Eskalasi Insiden serta analisis tren dari service request dan insiden.
8. Polsri perlu membuat Dokumen Service Request dan Insiden.

Sebelumnya pernah dilakukan audit di Politeknik Negeri Sriwijaya yang bekerjasama dengan NQA Indonesia sebagai penyelenggara ISO 9001:2015. Perbandingan antara audit Manajemen Mutu ISO 9001:2015 yang pernah

dilaksanakan di Politeknik Negeri Sriwijaya dengan penelitian yang saat ini dilakukan tersaji dalam Tabel 4.41.

Tabel 4.41. Perbandingan hasil audit iso 9001 dengan COBIT 2019

No	ISO 9001:2015	COBIT 2019
1.	Tujuan dari audit ini untuk mendapatkan sertifikasi sistem manajemen mutu dengan pelaksanaan audit di jurusan dan sub bagian Polsri.	Tujuan penelitian ini adalah mengetahui langkah pengelolaan risiko untuk meningkatkan layanan akademik di Polsri serta mengetahui bagaimana kustomisasi COBIT 2019 di sektor akademik.
2	Pengukuran dilakukan terhadap kinerja tim pengajar dan tim pendidik.	Penelitian dimulai dengan melihat bagaimana profil risiko Polsri melalui DF 1-4, setelah menemukan domain proses yang berpengaruh dilakukan penentuan responden berdasar rasi role dan struktur kerja Polsri. Penilaian pengukuran dilakukan berdasar hasil kuisioner yang telah dianalisis dan divalidasi.
3	Hasil audit adalah tidak ditemukan kesalahan mayor dan minor di Polsri, serta rekomendasi untuk memperoleh Sertifikat ISO 9001:2015.	Hasil audit ini berupa temuan dan rekomendasi yang sudah disusun dalam Tabel 4.40.

#### Justifikasi dari Rekomendasi yang Diusulkan

Tabel 4.42 menunjukkan perbandingan identifikasi kebutuhan SOP berdasarkan *best practice* COBIT 2019 dengan SOP yang sudah ada di Politeknik Negeri Sriwijaya berdasarkan kebutuhan Polsri saat ini.

Tabel 4.42. Perbandingan identifikasi kebutuhan SOP

No	Best Practice COBIT 2019	Identifikasi kebutuhan SOP berdasar best practice	SOP Polsri saat ini
1	BAI06 <i>Managed IT Changes</i>	SOP Manual Perubahan IT	Belum ada
2	BAI10 <i>Managed Configuration</i>	SOP Manual Configuration Item	SOP Pembuatan Sistem Informasi SOP Pembuatan Website
3	DSS01 <i>Managed Operations</i>	SOP Kegiatan Operasional IT	Form Permintaan Layanan PIH SOP Pembuatan Email SOP Pembuatan Sub Domain dan Hosting (PSDH)



Tabel 4.42. Perbandingan identifikasi kebutuhan SOP (lanjutan)

No	Best Practice COBIT 2019	Identifikasi kebutuhan SOP berdasar best practice	SOP Polsri saat ini
4	DSS01 <i>Managed Operations</i>	SOP Pengelolaan Outsource Layanan IT	Belum ada
5	DSS01 <i>Managed Operations</i>	SOP Service Request dan Insiden	Belum ada
6	DSS01 <i>Managed Operations</i>	SOP Perlindungan Peralatan IT	Belum ada
7	DSS02 <i>Managed Service Request and Incidents</i>	SOP Eskalasi Insiden	SOP Penanganan Gangguan Jaringan Lokal SOP Penanganan Gangguan Server (PGS)
8	DSS02 <i>Managed Service Request and Incidents</i>	SOP Service Request dan Insiden	Belum ada

Pada Tabel 4.42 menunjukkan SOP yang ada di Polsri dan disesuaikan dengan *best practice* di dalam COBIT 2019, meskipun masih ada beberapa SOP yang belum mencakup secara menyeluruh penggunaannya terhadap *best practice*. Tidak menutup kemungkinan akan ada SOP lain ke depannya sesuai dengan kebutuhan dan rencana Polsri ke depan dalam pengembangan organisasi berdasar prinsip tata kelola yang baik (*good governance*). Pelaksanaan rekomendasi audit tersebut bergantung kepada bagaimana Polsri menyikapi dan meyakini hasil audit.

Sebagai justifikasi tambahan dari rekomendasi penelitian ini, peneliti berdiskusi dengan Dr. Dra. Hj. Mikhriani, M.M selaku Lead Auditor AMI UIN Sunan Kalijaga dimana terdapat beberapa hal yang perlu diperhatikan didalam pemberian rekomendasi di antaranya sebagai berikut:

1. Perlu diperhatikan standar mutu pada organisasi ini mengacu pada standar apa. Dalam hal ini Politeknik Negeri Sriwijaya menggunakan Standar



Manajemen Mutu ISO 9001:2015, sedangkan penelitian yang dipergunakan mengacu pada standar COBIT 2019.

2. Perlu adanya penelitian lebih lanjut mengenai kaidah PLOR (*Problem, Location, Objective evidence, serta Reference*).
3. Perlu adanya klasifikasi rekomendasi sesuai Observasi (OB) maupun KeTidakSesuaian (KTS) baik minor dan mayor. Klasifikasi ini dibuat dalam bentuk Tabel 4.43 yang memuat mengenai Form Daftar Temuan Audit berdasar kaidah PLOR.

Berdasar Panduan Audit Mutu Internal diketahui beberapa KTS yang termasuk dalam kategori mayor diantaranya KTS tersebut mengancam akreditasi; memiliki pengaruh signifikan terhadap kualitas pelayanan; dan merupakan ancaman pelaksanaan kegiatan. Sedangkan KTS yang termasuk dalam kategori minor diantaranya yaitu KTS yang cepat dapat diperbaiki, tidak langsung mempengaruhi pelayanan, dan tidak menghambat dalam akreditasi.

Tabel 4.43. Form daftar temuan audit berdasar kaidah PLOR

No	Deskripsi / Uraian Temuan	Kategori Temuan (beri tanda v yang sesuai)			Referensi Standar
		OB	KTS Ma	KTS Mi	
1	Belum adanya standar dokumentasi manual perubahan IT serta form perubahan IT			v	BAI06
2	Belum adanya dokumentasi manual configuration item serta form laporan perubahan configuration item			v	BAI10
3	Belum ada dokumen kegiatan operasional IT		v		DSS01
4	Belum ada dokumen pengelolaan outsource layanan IT			v	DSS01
5	Belum ada form penanganan service request dan insiden serta form status penanganan service request dan insiden			v	DSS01

Tabel 4.43. Form daftar temuan audit berdasar kaidah PLOR (lanjutan)

No	Deskripsi / Uraian Temuan	Kategori Temuan (beri tanda v yang sesuai)			Referensi Standar
		OB	KTS Ma	KTS Mi	
6	Belum ada SOP perlindungan peralatan IT			v	DSS01
7	Belum ada aturan dan prosedur eskalasi insiden serta analisis tren dari service request dan insiden			v	DSS02
8	Belum ada dokumen service request dan insiden			v	DSS02

Dari Tabel 4.43 ditemukan KTS Mayor pada poin nomor 3 yaitu mengenai dokumen SOP kegiatan operasional IT. Dokumen ini dianggap masuk dalam KTS mayor karena dapat mempengaruhi terhadap kualitas pelayanan akademik Polstri. Rencana Tindakan Koreksi yang dilakukan terhadap KTS Mayor selanjutnya dijelaskan pada Tabel 4.44.

Tabel 4.44. Rencana tindakan koreksi

No	Unit Kerja Audit	Kriteria	Uraian Temuan	Rencana Tindakan Koreksi	Realisasi
1	Layanan Akademik	COBIT 2019	Masih adanya KTS Mayor dan KTS Minor dalam layanan akademik Polstri. Hal ini diketahui dari pemeriksaan berdasar panduan COBIT 2019.	Perlu melengkapi pembuatan dokumen SOP kegiatan operasional IT.	Melengkapi dokumen SOP kegiatan operasional IT

### Pembuatan Standar Operasional Prosedur

Berikut akan dijelaskan secara singkat mengenai pembuatan Standar Operasional Prosedur yang nantinya bisa disesuaikan kembali dengan kebutuhan Polstri. Gambar 4.12 menunjukkan halaman judul dari SOP yang dibuat.

POLITEKNIK NEGERI SRIWIJAYA (Identitas Instansi)
STANDAR OPERASIONAL PROSEDUR (SOP)
..... (Judul dari SOP)

Gambar 4.12. Halaman judul SOP

Gambar 4.13 menunjukkan SOP yang berisi rincian tanggal pembuatan, tanggal revisi, tanggal pengesahan, serta informasi lainnya.

	Identitas Politeknik							
<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Logo Poltri</div> <p>POLITEKNIK NEGERI SRIWIJAYA</p>	Nomor SOP:							
	Tanggal Pembuatan :	.....						
	Tanggal Revisi :	.....						
	Tanggal Pengesahan :	.....						
	Nama SOP :	.....						
<p><b>I. DESKRIPSI PROSES</b> Proses dideskripsikan menurut <i>Description</i> pada Buku COBIT 2019 Governance and Management objective berdasar proses yang mendasari SOP.</p>								
<p><b>II. MAKSUD PROSES</b> Maksud proses dideskripsikan menurut <i>Purpose</i> pada Buku COBIT 2019 Governance and Management objective berdasar proses yang mendasari SOP.</p>								
<p><b>III. TUJUAN DAN INDIKATOR KINERJA</b> Tujuan dan indikator kinerja dibuat menurut <i>goals</i> (tujuan) dari setiap <i>component process</i> terkait SOP dan <i>example metrics</i> (indikator kinerja) dengan mengisi tabel sebagai berikut:</p> <table border="1" style="margin-left: auto; margin-right: auto; text-align: center;"> <thead> <tr> <th style="width: 50%;">Tujuan</th> <th style="width: 50%;">Indikator Kinerja</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>			Tujuan	Indikator Kinerja				
Tujuan	Indikator Kinerja							
<p><b>IV. KETERKAITAN</b> Keterkaitan dengan SOP lain atau standar lain</p>								
<p><b>V. KUALIFIKASI DAFTAR PELAKSANA</b> Berdasar <i>component</i> : <i>people, skill, and competencies</i>.</p>								
<p><b>VI. PERLENGKAPAN / PERSYARATAN</b> Berdasar <i>component</i> : <i>services, infrastructure, and application</i></p>								

Gambar 4.13. Standar informasi prosedur

Sedangkan pada Gambar 4.14 menjelaskan mengenai diagram alir proses yang terjadi untuk menjalankan SOP.

NO	SUB AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		.....	.....	.....	.....	
1. Proses .....						
1.1	(deskripsi aktivitas)					
1.2						
....						
1.n						

Gambar 4.14. Diagram alir prosedur

### Simulasi Standar Operasional Prosedur

Simulasi SOP dibuat berdasar simulasi dari prosedur tertentu dan tidak mencakup keseluruhan SOP yang direkomendasikan. Skenario dari simulasi yang dilakukan selanjutnya dijelaskan dalam Tabel 4.45.

Tabel 4.45. Skenario Simulasi SOP

No	SOP	Skenario Simulasi	Tanggal Pelaksanaan Simulasi	Keterangan
1	SOP Service Request dan Insiden	Tenaga kependidikan salah satu jurusan meminta penanganan request untuk merubah data jumlah jam/minggu pada SISAK Dosen Eksternal dimana tersetting default 4.	11 Juli 2022	Simulasi dilakukan dengan melakukan perubahan jadwal ajar pada system SISAK tenaga kependidikan sehingga default tidak tersetting 4.

Berdasar hasil simulasi dengan pihak UPT TIK dari SOP Service Request dan Insiden pada Lampiran 10 terdapat beberapa perubahan yang harus diperhatikan peneliti bila SOP tersebut dibuat:

1. SOP yang dibuat harus disesuaikan kembali dengan kebutuhan Polsri (pengesahan harus dilakukan secara formal kepada Pimpinan Polsri terlebih dahulu).
2. Pada lembar judul perlu ditambahkan logo dari Politeknik Negeri Sriwijaya serta pengesahan dari Badan Penjamin Mutu Polsri. Selain itu perlu ditambahkan tahun pembuatan SOP di bagian bawah.
3. Perlu adanya lembar pengesahan yang disahkan oleh Direktur serta diperiksa oleh Pembantu Direktur I.
4. Pada bagian isi perlu ditambahkan Lingkup Kerja dan Penanggung jawab.
5. Pada bagian alur tahapan 1.4 perlu pengkategorian apakah servis request dan insiden ini termasuk servis ringan, sedang, atau berat.
6. Setelah permintaan servis request dan insiden selesai perlu menginformasikan juga kepada Kepala BAUK/Ketua UPT terkait.

Dari diskusi dengan pihak UPT TIK, SOP Servis Request dan Insiden ini dinilai cukup efektif dalam melakukan pencatatan mengenai servis request dan insiden yang terjadi, tetapi kembali lagi pembuatan SOP bergantung kepada keputusan rapat dengan Pimpinan Polsri.



## **BAB V**

### **PENUTUP**

#### **5.1. Kesimpulan**

Berdasarkan hasil audit yang telah dilakukan pada Politeknik Negeri Sriwijaya, maka dapat ditarik kesimpulan sebagai berikut:

1. Berdasarkan hasil pengukuran penilaian profil risiko menurut COBIT 2019 di Politeknik Negeri Sriwijaya didapat bahwa Polsri berada pada tingkat capability level 3 untuk domain BAI10 *Managed Configuration* dan DSS01 *Managed Operation* yang berarti kegiatan yang berkaitan dengan domain proses tersebut sudah dilakukan dengan menggunakan SOP. Sedangkan pada domain BAI06 *Managed IT Changes* dan DSS02 *Managed Service Request and Incidents* berada pada tingkat capability level 2 berarti kegiatan yang berkaitan dengan proses sudah dilakukan secara berkala.
2. Di dalam penelitian, kustomisasi COBIT pada sektor pendidikan dilakukan dengan cara menyelaraskan kebutuhan perguruan tinggi dalam penelitian ini Polsri dengan DF pada COBIT 2019. Langkah pertama yang dilakukan adalah dengan mengetahui apakah sasaran strategis dari perguruan tinggi tersebut yang kemudian diselaraskan ke dalam DF1 *enterprise strategy*. Langkah kedua adalah dengan mengetahui apakah tujuan dari perguruan tinggi tersebut, baik tujuan utama maupun tujuan luaran yang kemudian diselaraskan dalam DF2 *enterprise goals*. Langkah ketiga adalah dengan melakukan pengamatan mengenai profil risiko yang dihadapi oleh perguruan

tinggi tersebut yang diselaraskan dalam DF3 *risk profile*. Profil risiko pada tiap perguruan tinggi bisa berbeda, bergantung pada risiko yang sedang dihadapi oleh perguruan tinggi tersebut. Langkah keempat adalah dengan mengetahui isu terkait IT di perguruan tinggi tersebut yang kemudian diselaraskan dalam DF4 *IT related issues*.

3. Langkah melakukan analisis pengelolaan risiko dengan menggunakan COBIT 2019 dilakukan dengan terlebih dahulu melakukan pengukuran profil risiko pada Politeknik Negeri Sriwijaya. Pengukuran risiko akan memunculkan proses domain dengan nilai tertinggi mendekati 100 di antaranya yaitu BAI06, BAI10, DSS01, dan DSS02 beserta aktivitas yang ada di dalamnya. Dari setiap proses tersebut dilakukan pengukuran menggunakan Skala Guttman dengan melihat respon dari setiap responden penelitian. Bila dalam aktivitas yang terukur dalam capability level tertentu terpenuhi maka dapat disimpulkan bahwa Polsri memenuhi capability level tersebut. Sedangkan pengelolaan risiko dibuat dengan melihat fakta temuan dari setiap proses yang diukur dan dibuat rekomendasi dari setiap temuan proses tersebut.

## 5.2. Saran

Saran yang dapat dilakukan Politeknik Negeri Sriwijaya yaitu:

1. Polsri perlu membuat Panduan Standar Dokumentasi Manual Perubahan IT, Form Perubahan IT, Dokumentasi Manual Configuration, Form Laporan Perubahan Configuration Item, Dokumen Kegiatan Operasional IT, Dokumen Pengelolaan Outsource Layanan IT, Form Penanganan Service Request dan

Insiden, Form Status Penanganan Service Request dan Insiden, SOP Perlindungan Peralatan IT, Aturan dan Prosedur Eskalasi Insiden, dan Dokumen Service Request dan Insiden.

2. Polsri perlu membuat kegiatan untuk memonitor IT infrastruktur secara rutin.

Saran untuk penelitian selanjutnya berdasar hasil kegiatan audit yang dilakukan di Politeknik Negeri Sriwijaya adalah sebagai berikut:

1. Perlunya dilakukan kegiatan audit pada setiap perguruan tinggi terutama pada layanan akademik.
2. Perlunya penelitian lanjutan mengenai pelaksanaan rekomendasi di Polsri.
3. Perlunya audit dengan menggunakan framework lain di Polsri.



## DAFTAR PUSTAKA

### PUSTAKA BUKU

- I. P. A. Swastika; I. G. L. A. R. Putra, 2016, *Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus*, 1st ed, ANDI, Yogyakarta.
- C. Kymal, 2016, *How to audit ISO 9001:2015: a handbook for auditors*. ASQ Quality Press, Wisconsin.
- D. M. Burwick, 2008, *How to Implement the CMMI: Real Process Improvement Using Proven Solutions*, Business & Personal Solutions Publishing, Pittsburgh.
- Great Britain, Ed., 2007, *The Official Introduction to The ITIL Service Lifecycle*, Stationary Office, London.
- H. Djaali, M. Pudji, and Y.B. Sudarmanto, 2008, *Pengukuran dalam Bidang Pendidikan*. Jakarta: Grasindo.
- H. Umar, 2002, *Metode riset bisnis: panduan mahasiswa untuk melaksanakan riset dilengkapi contoh proposal dan hasil riset bidang manajemen dan akuntansi*. Jakarta: Gramedia Pustaka Utama.
- I. P. A. Swastika, and I. G. L. A. R. Putra, 2016, *Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus*, 1st ed. Yogyakarta: ANDI.
- ISACA, 2019, *COBIT 2019 Framework: Governance and Management Objectives*, ISACA, USA.
- ISACA, 2019, *COBIT 2019 Framework: Introduction and Methodology*, ISACA, USA.
- M. G. Saragih, L. Saragih, J. W. P. Purba, and P. D. Panjaitan, 2021, *Metode Penelitian Kuantitatif: Dasar-dasar Memulai Penelitian*, vol. 1. Yayasan Kita Menulis.
- M. N. Freed, R. K. Hess, and J. M. Ryan, 2022, *The educator's desk reference (EDR): a sourcebook of educational information and research*, 2nd ed. Westport, CT: Praeger.
- R. F. Smallwood, 2014, *Information governance: concepts, strategies, and best practices*. Wiley, New Jersey.



- R. M. Kaplan and D. P. Saccuzzo, 2009, *Psychological testing: principles, applications, and issues*, 7th ed. Belmont, CA: Wadsworth Cengage Learning.
- R. R. Moeller, 2014, *Executive's guide to COSO internal controls: understanding and implementing the new framework*, John Wiley and Sons, Inc, New Jersey.
- S. D. Haes, 2015, *Enterprise governance of information technology: achieving alignment and value, featuring Cobit 5*, 2nd edition. Springer Science+Business Media, New York.
- The Open Group, Ed., 2010, *TOGAF Version 9*, 9. ed. [Nachdr.], Van Haren Publishing, Zaltbommel.
- TSO, 2005. *Introduction to ITIL*. TSO, London.

#### **PUSTAKA MAJALAH, JURNAL ILMIAH ATAU PROSIDING**

- A. Dewi; Y. Latief; L. Sagita, 2020, Activity and risk identification in audit process on integrated management system to increase performance efficiency of construction services organization in Indonesia, *IOP Conf. Ser. Earth Environ. Sci.*, vol. 426, p. 012014, Mar. 2020, doi: 10.1088/1755-1315/426/1/012014.
- F. Veerankutty; T. Ramayah; N. Ali, 2018, Information Technology Governance on Audit Technology Performance among Malaysian Public Sector Auditors, *Soc. Sci.*, vol. 7, no. 8, p. 124, Jul. 2018, doi: 10.3390/socsci7080124.
- G. Hardy, 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges, *Inf. Secur. Tech. Rep.*, vol. 11, no. 1, pp. 55–61, 2006, doi: 10.1016/j.istr.2005.12.004.
- J. van Wyk; R. Rudman, 2019, COBIT 5 compliance: best practices cognitive computing risk assessment and control checklist, *Meditari Account. Res.*, vol. 27, no. 5, pp. 761–788, Oct. 2019, doi: 10.1108/MEDAR-04-2018-0325.
- P. Mulgund; P. Pahwa; G. Chaudhari, 2019, Strengthening IT Governance and Controls Using COBIT: A Systematic Literature Review, *Int. J. Risk Conting. Manag.*, vol. 8, no. 4, pp. 66–90, Oct. 2019, doi: 10.4018/IJRCM.2019100104.

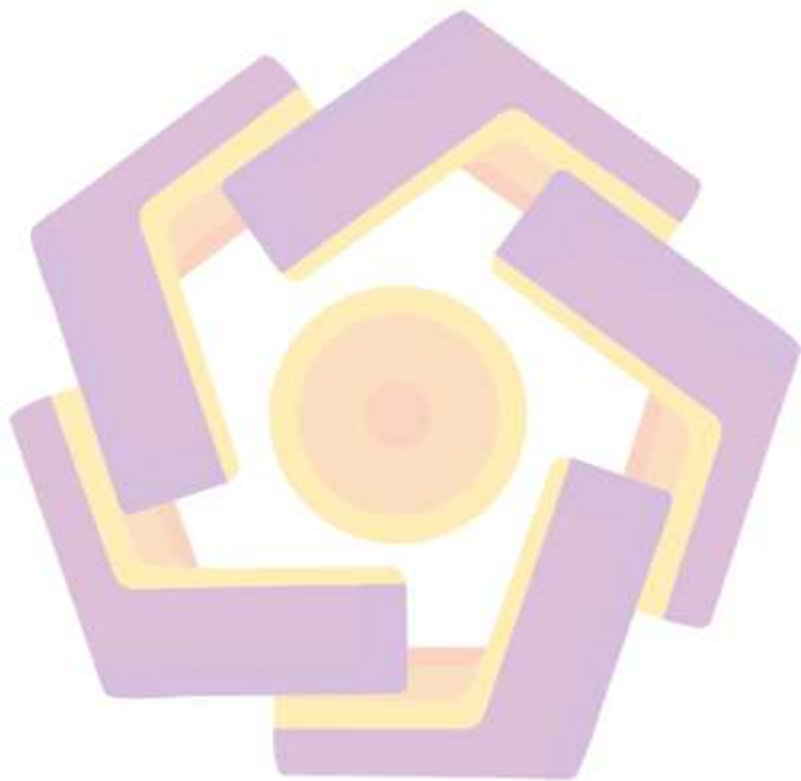


- S. Gantman and J. Fedorowicz, 2016, Communication and control in outsourced IS development projects: Mapping to COBIT domains, *Int. J. Account. Inf. Syst.*, vol. 21, pp. 63–83, Jun. 2016, doi: 10.1016/j.accinf.2016.05.001.
- X. Wang; T. Zhao; C.T. Chang, 2021, An integrated FAHP-MCGP approach to project selection and resource allocation in risk-based internal audit planning: A case study, *Comput. Ind. Eng.*, vol. 152, p. 107012, Feb. 2021, doi: 10.1016/j.cie.2020.107012.

#### **PUSTAKA ELEKTRONIK**

- Elue, Emeka, 27 Juli 2020, Effective Capability and Maturity Assessment Using COBIT 2019, <https://www.isaca.org/resources/news-and-trends/industry-news/2020/effective-capability-and-maturity-assessment-using-cobit-2019>
- Rafeq, Abdul; Elangovan, Narasimhan, 26 Mei 2021, A Systematic Approach to Implementing a Governance System Using COBIT 2019: A COVID-19 Case Study, <https://www.isaca.org/resources/news-and-trends/industry-news/2021/a-systematic-approach-to-implementing-a-governance-system-using-cobit-2019>

## LAMPIRAN



## LAMPIRAN 1

### Surat Izin Penelitian



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,  
RISET, DAN TEKNOLOGI  
**POLITEKNIK NEGERI SRIWIJAYA**

Jalan Srijaya Negara Bukit Besar - Palembang 30139 Telepon (0711) 353414  
Laman : <http://poltri.ac.id>, Pos El : [info@poltri.ac.id](mailto:info@poltri.ac.id)

Nomor : 061/SPEA.4.28/P/2022  
Perihal : Izin Penelitian

24 Januari 2022

Yth. Direktur Program Pascasarjana  
Universitas AMIKOM Yogyakarta  
di Yogyakarta.

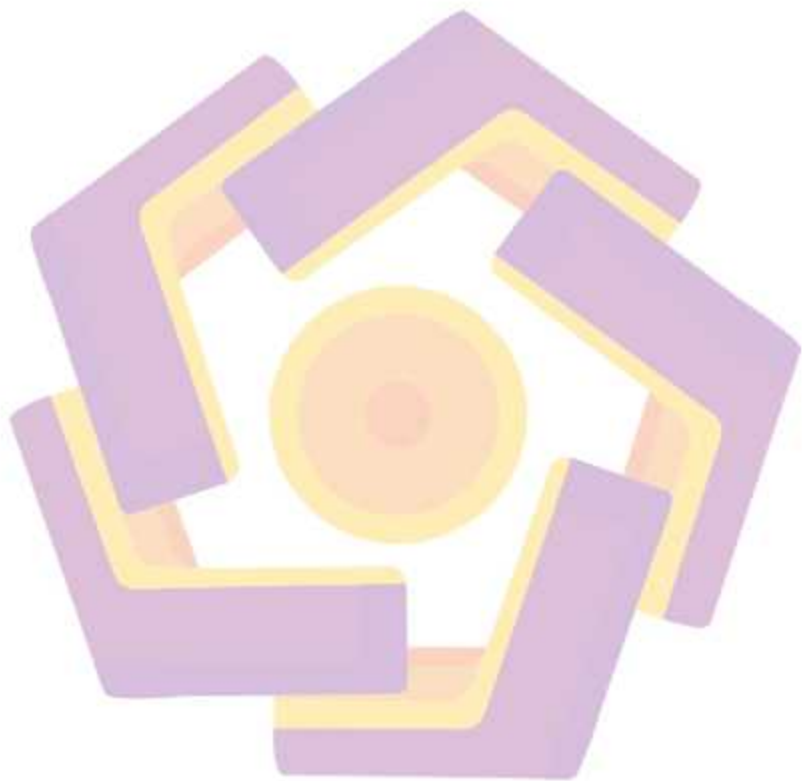
Sehubungan dengan surat dari Direktur Program Pascasarjana Universitas AMIKOM Yogyakarta Nomor : 230/PASCASARJANA/AMIKOM/XII/2021 tanggal 16 Desember 2021 perihal permohonan Penelitian, maka kami sampaikan bahwa pada prinsipnya tidak keberatan menerbitkan izin kepada Saudara Nurul Husein Usman Komar untuk mengadakan penelitian dan pengabdian masyarakat terkait dengan judul tesis yang bersangkutan, dengan ketentuan yang bersangkutan harus mengikuti semua aturan yang berlaku di Politeknik Negeri Sriwijaya.

Demikian atas perhatian dan kerjasamanya kami ucapkan terima kasih.

Yogyakarta, 24 Januari 2022  
Wakil Direktur I,  
  
Carlos R.S., S.T., M.T.  
NIP. 196402011980031803

Ditandatangani,  
1. Direktur,  
2. Ka. UPT SHU





## LAMPIRAN 2

### KUESIONER SURVEY

#### Penilaian Capability Level BAI06 Cobit 2019

Perkenalkan nama saya Nurul Ilma Hasana Kunio mahasiswa Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **BAI06 Managed IT Changes**. Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut:

- Ya jika aktivitas sudah dilaksanakan.
- Tidak jika aktivitas belum dilaksanakan.

Kuesioner diberikan secara bertahap, sesuai dengan tingkat aktivitas yang dinilai. Pada kuesioner ini, penilaian dilakukan sesuai dengan aktivitas yang ada pada setiap sub domain BAI06.

Identitas Responden	
Nama Responden	
NIP	
Unit Kerja	
Jabatan	



**BAI06.01 Mengevaluasi, memprioritaskan, dan mengotorisasi permintaan perubahan**

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Menggunakan permintaan perubahan formal untuk memungkinkan pemilik proses bisnis dan TI meminta perubahan pada proses bisnis, infrastruktur, sistem, atau aplikasi. Memastikan bahwa semua perubahan tersebut hanya muncul melalui proses manajemen permintaan perubahan.		
2	Mengkategorikan semua perubahan yang diminta (misalnya, proses bisnis, infrastruktur, sistem operasi, jaringan, sistem aplikasi, perangkat lunak aplikasi yang dibeli/dikemas) dan menghubungkan item konfigurasi yang terpengaruh.		
3	Memprioritaskan semua perubahan yang diminta berdasarkan kebutuhan bisnis dan teknis; sumber daya yang dibutuhkan; dan alasan hukum, peraturan, dan kontraktual untuk perubahan yang diminta.		
4	Secara resmi menyetujui setiap perubahan oleh pemilik proses bisnis, manajer layanan, dan pemangku kepentingan teknis TI, sebagaimana mestinya. Perubahan yang berisiko rendah dan relatif sering harus disetujui terlebih dahulu sebagai perubahan standar.		
5	Merencanakan dan menjadwalkan semua perubahan yang disetujui.		
6	Merencanakan dan mengevaluasi semua permintaan secara terstruktur. Menyertakan analisis dampak pada proses bisnis, infrastruktur, sistem dan aplikasi, rencana kelangsungan bisnis (BCP) dan penyedia layanan untuk memastikan bahwa semua komponen yang terpengaruh telah diidentifikasi. Menilai kemungkinan dampak negatif terhadap lingkungan operasional dan risiko penerapan perubahan. Mempertimbangkan implikasi keamanan, privasi, hukum, kontrak, dan kepatuhan dari perubahan yang diminta. Mempertimbangkan juga ketergantungan antar perubahan. Libatkan pemilik proses bisnis dalam proses penilaian, sebagaimana mestinya.		

7	Mempertimbangkan dampak penyedia layanan yang dikontrak (misal pemrosesan bisnis yang dialihdayakan, infrastruktur, aplikasi pengembangan dan layanan bersama) pada proses manajemen perubahan. Menyertakan integrasi manajemen proses perubahan organisasi dengan proses manajemen perubahan penyedia layanan dan dampaknya pada persyaratan kontrak dan SLA.		
---	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

BAI06.02 Mengelola perubahan darurat			
No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Menjelaskan apa yang dimaksud dengan perubahan darurat.		
2	Memastikan bahwa ada prosedur terdokumentasi untuk menyatakan, menilai, menyetujui sebelumnya, mengesahkan setelah perubahan dan mencatat perubahan darurat.		
3	Memverifikasi bahwa semua pengaturan akses darurat untuk perubahan diotorisasi, didokumentasikan, dan dicabut dengan tepat setelah perubahan diterapkan.		
4	Memantau semua perubahan darurat dan melakukan tinjauan pasca implementasi yang melibatkan semua pihak terkait. Tinjauan harus mempertimbangkan dan memulai tindakan korektif berdasarkan akar penyebab seperti masalah dengan proses bisnis, pengembangan dan pemeliharaan sistem aplikasi, lingkungan pengembangan dan pengujian, dokumentasi dan manual, dan integritas data.		

BAI06.03 Melacak dan melaporkan status perubahan			
No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak

1	Mengategorikan permintaan perubahan dalam proses pelacakan (misalnya, ditolak, disetujui tetapi belum dimulai, disetujui dan dalam proses, dan ditutup).		
2	Menerapkan laporan status perubahan dengan metrik kinerja untuk memungkinkan tinjauan manajemen dan pemantauan status rinci perubahan dan keadaan keseluruhan (misalnya, analisis lama permintaan perubahan). Memastikan bahwa laporan status membentuk jejak audit sehingga perubahan selanjutnya dapat dilacak dari awal hingga disposisi akhirnya.		
3	Memantau perubahan terbuka untuk memastikan bahwa semua perubahan yang disetujui ditutup tepat waktu, tergantung pada prioritas.		
4	Mempertahankan sistem pelacakan dan pelaporan untuk semua permintaan perubahan.		

#### BAI06.04 Menutup dan mendokumentasikan perubahan

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Menyertakan perubahan dalam dokumentasi dalam prosedur manajemen. Contoh dokumentasi termasuk prosedur operasional bisnis dan TI, kelangsungan bisnis dan dokumentasi pemulihan bencana, informasi konfigurasi, dokumentasi aplikasi, layar bantuan, dan materi pelatihan.		
2	Menentukan periode penyimpanan yang tepat untuk dokumentasi perubahan dan sistem sebelum dan sesudah perubahan dan dokumentasi pengguna.		
3	Mendokumentasikan subjek ke tingkat tinjauan yang sama dengan perubahan yang sebenarnya.		

### LAMPIRAN 3

## KUESIONER SURVEY

### Penilaian Capability Level BAI10 Cobit 2019

Perkenalkan nama saya Nurul Ilma Hasana Kunio mahasiswa Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **BAI10 Managed Configuration**. Kuesioner dibuat berdasarkan buku Cobit 2019 - *Governance & Management Objectives*.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut:

- Ya jika aktivitas sudah dilaksanakan.
- Tidak jika aktivitas belum dilaksanakan.

Kuesioner diberikan secara bertahap, sesuai dengan tingkat aktivitas yang dinilai. Pada kuesioner ini, penilaian dilakukan sesuai dengan aktivitas yang ada pada setiap sub domain BAI10.

#### Identitas Responden

Nama Responden	
NIP	
Unit Kerja	
Jabatan	



**BAI10.01 Menetapkan dan memelihara model konfigurasi**

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Menetapkan dan menyetujui cakupan dan tingkat detail untuk manajemen konfigurasi (yaitu, layahan, aset, dan item yang dapat dikonfigurasi infrastruktur mana yang akan disertakan).		
2	Menetapkan dan memelihara model logis untuk manajemen konfigurasi, termasuk informasi tentang tipe CI, atribut, tipe hubungan, atribut hubungan, dan kode status.		

**BAI10.02 Membangun dan memelihara repositori konfigurasi dan baseline**

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Mengidentifikasi dan mengklasifikasikan CI dan isi repositori.		
2	Membuat, meninjau, dan menyetujui secara formal baseline konfigurasi layanan, aplikasi, atau infrastruktur.		

**BAI10.03 Memelihara dan mengontrol item konfigurasi**

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Identifikasi secara teratur semua perubahan pada CI.		
2	Memastikan kelengkapan dan akurasi, meninjau perubahan yang diusulkan pada CI terhadap baseline.		
3	Memperbarui detail konfigurasi untuk perubahan yang disetujui pada CI.		



4	Membuat, meninjau, dan menyetujui secara formal perubahan pada baseline konfigurasi kapan pun diperlukan.		
---	-----------------------------------------------------------------------------------------------------------	--	--

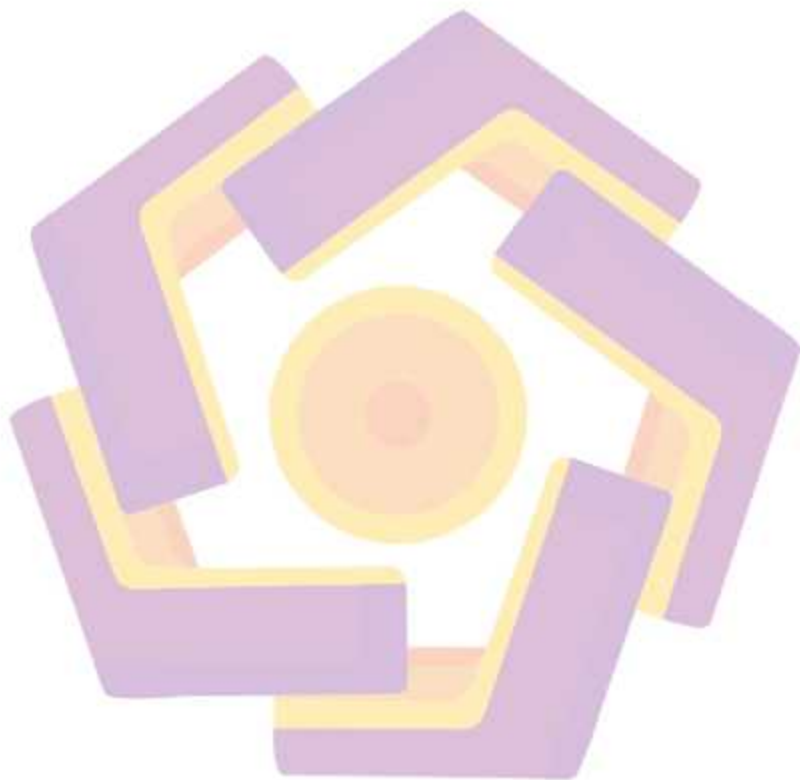
#### BAI10.04 Menghasilkan status dan laporan konfigurasi

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Mengidentifikasi perubahan status CI dan laporkan terhadap baseline.		
2	Mencocokkan semua perubahan konfigurasi dengan permintaan perubahan yang disetujui untuk mengidentifikasi perubahan yang tidak sah. Melaporkan perubahan yang tidak sah ke manajemen perubahan.		
3	Mengidentifikasi persyaratan pelaporan dari semua pemangku kepentingan, termasuk konten, frekuensi, dan media. Menghasilkan laporan sesuai dengan persyaratan yang diidentifikasi.		

#### BAI10.05 Memverifikasi dan meninjau integritas repositori konfigurasi

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Memverifikasi item konfigurasi langsung secara berkala terhadap repositori konfigurasi dengan membandingkan konfigurasi fisik dan logis dan menggunakan alat penemuan yang sesuai, sesuai kebutuhan.		
2	Melaporkan dan meninjau semua penyimpangan untuk koreksi yang disetujui atau tindakan untuk menghapus aset yang tidak sah.		
3	Memverifikasi secara berkala bahwa semua item konfigurasi fisik, sebagaimana didefinisikan dalam repositori, ada secara fisik. Laporkan setiap penyimpangan kepada manajemen		
4	Menetapkan dan meninjau target kelengkapan repositori konfigurasi secara berkala berdasarkan kebutuhan bisnis		

5	Secara berkala membandingkan tingkat kelengkapan dan akurasi terhadap target dan mengambil tindakan perbaikan, jika perlu, untuk meningkatkan kualitas data repositori.		
---	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--



#### LAMPIRAN 4

## KUESIONER SURVEY

### Penilaian Capability Level DSS01 Cobit 2019

Perkenalkan nama saya Nurul Ilma Hasana Kunio mahasiswa Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **DSS01 *Managed Operations***. Kuesioner dibuat berdasarkan buku Cobit 2019 - *Governance & Management Objectives*.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut:

- Ya jika aktivitas sudah dilaksanakan.
- Tidak jika aktivitas belum dilaksanakan.

Kuesioner diberikan secara bertahap, sesuai dengan tingkat aktivitas yang dinilai. Pada kuesioner ini, penilaian dilakukan sesuai dengan aktivitas yang ada pada setiap sub domain DSS01.

#### Identitas Responden

Nama Responden	
NIP	
Unit Kerja	
Jabatan	

**DSS01.01 Melakukan prosedur operasional**

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Mengembangkan dan memelihara prosedur operasional dan kegiatan terkait untuk mendukung semua layanan yang diberikan.		
2	Menjaga jadwal kegiatan operasional dan melakukan kegiatan.		
3	Memverifikasi bahwa semua data yang diharapkan untuk diproses diterima dan diproses secara lengkap, akurat dan tepat waktu. Memberikan output sesuai dengan kebutuhan perusahaan. Mendukung kebutuhan restart dan pemrosesan ulang. Memastikan bahwa pengguna menerima output yang tepat dengan cara yang aman dan tepat waktu.		
4	Mengelola kinerja dan hasil kegiatan yang dijadwalkan.		
5	Memantau insiden dan masalah yang berhubungan dengan prosedur operasional dan mengambil tindakan yang tepat untuk meningkatkan keandalan tugas operasional yang dilakukan.		

**DSS01.02 Mengelola outsource layanan I&T**

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Memastikan bahwa persyaratan perusahaan untuk keamanan proses informasi mematuhi kontrak dan SLA dengan hosting atau penyedia layanan pihak ketiga.		
2	Memastikan bahwa bisnis operasional perusahaan dan persyaratan pemrosesan TI dan prioritas untuk pemberian layanan mematuhi kontrak dan SLA dengan pihak ketiga yang menyediakan hosting atau layanan.		

3	Mengintegrasikan proses manajemen TI internal yang penting dengan proses dari penyedia layanan outsource. Yang mencakup, kinerja dan perencanaan kapasitas, manajemen perubahan, manajemen konfigurasi, permintaan layanan dan manajemen insiden, manajemen masalah, manajemen keamanan, kelangsungan bisnis, dan pemantauan kinerja proses dan pelaporan.		
4	Merencanakan audit independen dan jaminan lingkungan operasional penyedia outsourcing untuk mengonfirmasi bahwa persyaratan yang disepakati telah ditangani secara memadai.		

DSS01.03 Memantau infrastruktur I&T			
No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Mencatat acara. Mengidentifikasi tingkat informasi yang akan dicatat, berdasarkan pertimbangan risiko dan kinerja.		
2	Mengidentifikasi dan memelihara daftar aset infrastruktur yang perlu dipantau, berdasarkan kekritisan layanan dan hubungan antara item konfigurasi dan layanan yang bergantung padanya.		
3	Menetapkan dan menerapkan aturan yang mengidentifikasi dan mencatat pelanggaran ambang batas dan kondisi peristiwa. Menemukan keseimbangan antara menghasilkan peristiwa kecil palsu dan peristiwa penting sehingga log peristiwa tidak dibebani dengan informasi yang tidak perlu.		
4	Menghasilkan log peristiwa dan menyimpannya untuk jangka waktu yang tepat untuk membantu penyelidikan di masa mendatang.		
5	Memastikan bahwa tiket insiden dibuat tepat waktu saat memantau penyimpangan yang teridentifikasi dari ambang batas yang ditentukan.		
6	Menetapkan prosedur untuk memantau log peristiwa. Melakukan review secara berkala.		

DSS01.04 Mengelola lingkungan		
No	Aktivitas Tata Kelola	Temuan



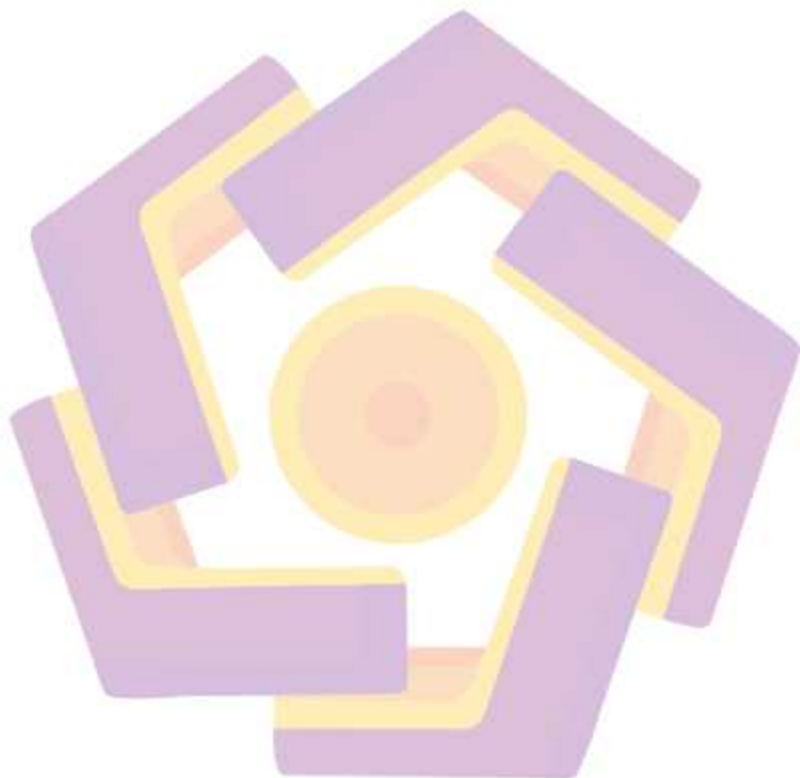
		Ya	Tidak
1	Mengidentifikasi bencana alam dan buatan manusia yang mungkin terjadi di daerah di mana fasilitas TI berada. Menilai efek potensial pada fasilitas TI.		
2	Mengidentifikasi bagaimana peralatan I&T, termasuk peralatan mobile dan off-site, dilindungi dari ancaman lingkungan. Memastikan bahwa kebijakan membatasi atau mengecualikan makan, minum, dan merokok di area sensitif, dan melarang penyimpanan alat tulis dan persediaan lain yang menimbulkan bahaya kebakaran di dalam ruang komputer.		
3	Menjaga situs IT dan ruang server bersih dan dalam kondisi aman setiap saat (yaitu, tidak berantakan, tidak ada kertas atau kotak kardus, tidak ada tempat sampah yang terisi, tidak ada bahan kimia atau bahan yang mudah terbakar).		
4	Menempatkan dan membangun fasilitas TI untuk meminimalkan dan mengurangi kerentanan terhadap ancaman lingkungan (misalnya, pencurian, udara, api, asap, air, getaran, teror, vandalisme, bahan kimia, bahan peledak). Mempertimbangkan zona keamanan tertentu dan/atau sel tahan api (misalnya, menempatkan lingkungan/server produksi dan pengembangan berjauhan).		
5	Membandingkan langkah-langkah dan rencana kontinjensi terhadap persyaratan polis asuransi dan hasil laporan. Mengatasi poin ketidakpatuhan pada waktu yang tepat.		
6	Menanggapi alarm lingkungan dan pemberitahuan lainnya. Mendokumentasikan dan melakukan prosedur pengujian, yang harus mencakup prioritas alarm dan kontak dengan otoritas tanggap darurat setempat. Melatih personel dalam prosedur ini.		
7	Secara teratur memantau dan memelihara perangkat yang secara proaktif mendeteksi ancaman lingkungan (misalnya, api, air, asap, kelembaban).		

#### DSS01.05 Mengelola fasilitas

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak

1	Memeriksa persyaratan fasilitas TI untuk perlindungan terhadap fluktuasi dan pemadaman listrik, bersama dengan persyaratan perencanaan kesinambungan bisnis lainnya. Memastikan pengadaan peralatan pasokan yang sesuai tak terputus (misalnya, baterai, generator) untuk mendukung perencanaan kesinambungan bisnis.		
2	Secara teratur menguji mekanisme catu daya yang tidak pernah terputus. Memastikan daya dapat dialihkan ke suplai tanpa ada efek signifikan pada operasi bisnis		
3	Memastikan fasilitas yang menampung sistem I&T memiliki lebih dari satu sumber untuk utilitas yang bergantung (misalnya, listrik, telekomunikasi, air, gas). Memisahkan pintu masuk fisik setiap utilitas.		
4	Mengkonfirmasi bahwa pemasangan kabel eksternal ke IT site terletak di bawah tanah atau memiliki perlindungan alternatif yang sesuai. Menentukan bahwa pemasangan kabel di dalam situs TI berada di dalam saluran yang aman, dan akses ke lemari kabel dibatasi untuk personel yang berwenang. Melindungi kabel dengan benar dari kerusakan yang disebabkan oleh api, asap, air, intersepsi, dan interferensi.		
5	Memastikan bahwa pemasangan kabel dan penambalan fisik (data dan telepon) terstruktur dan terorganisir. Mendokumentasikan struktur kabel dan saluran harus (misalnya, denah bangunan cetak biru dan diagram pengkabelan).		
6	Secara teratur, mendidik personel tentang undang-undang kesehatan dan keselamatan, peraturan, dan pedoman yang relevan. Mendidik personel tentang latihan kebakaran dan penyelamatan untuk memastikan pengetahuan dan tindakan yang diambil jika terjadi kebakaran atau insiden serupa.		
7	Memastikan bahwa lokasi dan peralatan TI dipelihara sesuai dengan interval dan spesifikasi servis yang direkomendasikan pemasok. Memastikan bahwa pemeliharaan hanya dilakukan oleh personel yang berwenang.		
8	Menganalisis sistem ketersediaan tinggi perumahan fasilitas untuk persyaratan kabel redundansi dan fail-over (eksternal dan internal).		
9	Memastikan bahwa situs dan fasilitas TI terus mematuhi undang-undang, peraturan, pedoman, dan spesifikasi vendor terkait kesehatan dan keselamatan.		
10	Mencatat, memantau, mengelola, dan menyelesaikan insiden fasilitas sejalan dengan proses manajemen insiden I&T. Menyediakan laporan tentang insiden fasilitas yang pengungkapannya diwajibkan oleh undang-undang dan peraturan.		

11	Menganalisis perubahan fisik pada situs atau bangunan TI untuk menilai kembali risiko lingkungan (misal kerusakan akibat kebakaran atau air). Melaporkan hasil analisis ini kepada business continuity dan manajemen fasilitas.		
----	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--



## LAMPIRAN 5

### KUESIONER SURVEY

#### Penilaian Capability Level DSS02 Cobit 2019

Perkenalkan nama saya Nurul Ilma Hasana Kunio mahasiswa Universitas AMIKOM Yogyakarta yang melakukan penelitian tentang Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sriwijaya.

Kuesioner survey ini disampaikan untuk mengetahui tingkat kemampuan / *Capability Level* proses **DSS02 Managed Service Requests and Incidents**. Kuesioner dibuat berdasarkan buku Cobit 2019 - Governance & Management Objectives.

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada tempat yang tersedia. Penilaian didasarkan atas kondisi berikut:

- Ya jika aktivitas sudah dilaksanakan.
- Tidak jika aktivitas belum dilaksanakan.

Kuesioner diberikan secara bertahap, sesuai dengan tingkat aktivitas yang dinilai. Pada kuesioner ini, penilaian dilakukan sesuai dengan aktivitas yang ada pada setiap sub domain DSS02.

Identitas Responden	
Nama Responden	
NIP	
Unit Kerja	
Jabatan	



**DSS02.01 Menentukan skema klasifikasi insiden dan permintaan layanan**

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Menentukan klasifikasi insiden dan permintaan layanan dan skema prioritas, serta kriteria untuk pendaftaran masalah. Menggunakan informasi ini untuk memastikan pendekatan yang konsisten untuk menangani dan menginformasikan pengguna tentang masalah dan melakukan analisis tren.		
2	Menentukan model insiden untuk kesalahan yang diketahui untuk memungkinkan penyelesaian yang efisien dan efektif.		
3	Menentukan model permintaan layanan sesuai dengan jenis permintaan layanan untuk mengaktifkan layanan swadaya dan layanan yang efisien untuk permintaan standar.		
4	Menetapkan aturan dan prosedur eskalasi insiden, terutama untuk insiden besar dan insiden keamanan.		
5	Menentukan sumber pengetahuan tentang insiden dan permintaan dan menjelaskan cara menggunakannya.		

**DSS02.02 Mencatat, mengklasifikasikan, dan memprioritaskan permintaan dan insiden**

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Mencatat semua permintaan dan insiden layanan, mencatat semua informasi yang relevan, sehingga dapat ditangani secara efektif dan pencatatan sejarah lengkap dapat dipertahankan.		
2	Mengaktifkan analisis tren dengan cara mengklasifikasikan permintaan dan insiden layanan dengan mengidentifikasi jenis dan kategori.		
3	Memprioritaskan permintaan dan insiden layanan berdasarkan definisi layanan SLA tentang dampak dan urgensi bisnis.		



DSS02.03 Memverifikasi, menyetujui, dan memenuhi permintaan layanan			
No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Memverifikasi hak untuk permintaan layanan menggunakan, jika memungkinkan, memeriksa aliran proses yang telah ditentukan sebelumnya dan perubahan standar		
2	Mendapatkan persetujuan finansial dan fungsional atau tanda tangan, jika diperlukan, atau persetujuan yang telah ditentukan sebelumnya untuk perubahan standar yang disepakati.		
3	Memenuhi permintaan dengan melakukan prosedur permintaan yang dipilih. Jika memungkinkan, menggunakan menu otomatis bantuan mandiri dan model permintaan yang telah ditentukan sebelumnya untuk item yang sering diminta.		

DSS02.04 Menyelidiki, mendiagnosa, dan mengalokasikan insiden			
No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Mengidentifikasi dan menjelaskan gejala yang relevan untuk menetapkan penyebab insiden yang paling mungkin. Merefereksi sumber pengetahuan yang tersedia (termasuk kesalahan dan masalah yang diketahui) untuk mengidentifikasi kemungkinan resolusi insiden (solusi sementara dan/atau solusi permanen).		
2	Jika masalah terkait atau kesalahan yang diketahui belum ada dan jika insiden memenuhi kriteria yang disepakati untuk pendaftaran masalah, membuat log masalah baru.		

3	Menetapkan insiden ke fungsi spesialis jika diperlukan keahlian yang lebih dalam. Melibatkan tingkat manajemen yang sesuai, di mana dan jika diperlukan.		
---	----------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

#### DSS02.05 Menyelesaikan dan memulihkan dari insiden

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Memilih dan menerapkan resolusi insiden yang paling tepat (solusi sementara dan/atau solusi permanen)		
2	Mencatat apakah solusi dapat digunakan untuk resolusi insiden.		
3	Melakukan tindakan pemulihan, jika diperlukan.		
4	Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat digunakan sebagai sumber pengetahuan di masa depan.		

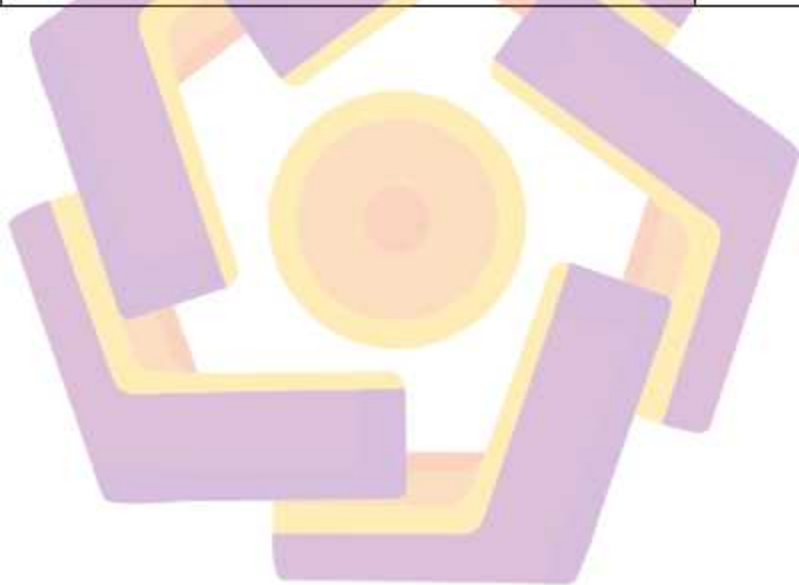
#### DSS02.06 Menutup permintaan layanan dan insiden

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak
1	Memverifikasi dengan pengguna yang terpengaruh bahwa permintaan layanan telah dipenuhi dengan memuaskan atau insiden telah diselesaikan dengan memuaskan dan dalam jangka waktu yang disepakati/dapat diterima.		
2	Menutup permintaan dan insiden layanan.		

#### DSS02.07 Melacak status dan membuat laporan

No	Aktivitas Tata Kelola	Temuan	
		Ya	Tidak

1	Memantau dan melacak eskalasi dan resolusi insiden dan meminta prosedur penanganan untuk kemajuan menuju resolusi atau penyelesaian.		
2	Mengidentifikasi pemangku kepentingan informasi dan kebutuhan mereka akan data atau laporan. Mengidentifikasi frekuensi dan media pelaporan.		
3	Menghasilkan dan mendistribusikan laporan tepat waktu atau menyediakan akses terkontrol ke data online.		
4	Menganalisis insiden dan permintaan layanan berdasarkan kategori dan jenis. Menetapkan tren dan identifikasi pola masalah berulang, pelanggaran SLA atau inefisiensi.		
5	Menggunakan informasi tersebut sebagai masukan untuk perencanaan perbaikan berkelanjutan.		



## LAMPIRAN 6

### DATA KUISIONER KETUA UPT TIK/PIH

The image shows two pages of a questionnaire. The left page is the cover page with the title "KUISIONER SURVEY" and a subtitle "Berkas: C:\panti\11111111\11111111\11111111". It contains introductory text in Indonesian and a table for respondent information. The right page contains several numbered questions (1-10) regarding the use of information systems in the organization, with a Likert scale from 1 to 5 for each response.

**COVER PAGE:**

**KUISIONER SURVEY**  
Berkas: C:\panti\11111111\11111111\11111111

Sebelumnya, kami ucapkan terima kasih yang sebesar-besarnya atas partisipasi, kontribusi, dan kerendahan hati Anda dalam mengisi kuisioner ini. Kami berharap kuisioner ini dapat memberikan informasi yang bermanfaat bagi kami dalam meningkatkan kualitas pelayanan kami kepada Anda.

Informasi yang kami butuhkan meliputi:

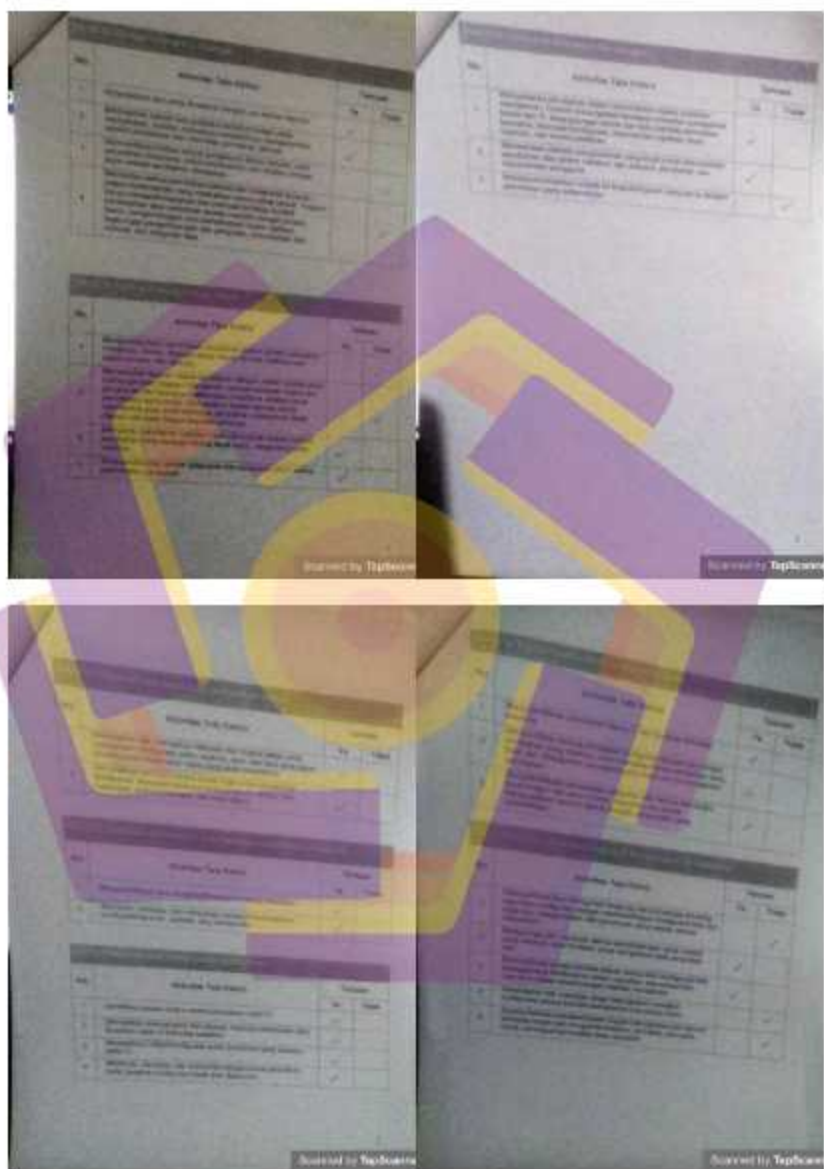
- 1. Bagaimana tanggapan Anda terhadap pernyataan-pernyataan yang tertera di bagian bawah kuisioner ini?
- 2. Apakah ada hal-hal yang perlu diperhatikan oleh kami dalam meningkatkan kualitas pelayanan kami kepada Anda?
- 3. Bagaimana tanggapan Anda terhadap pernyataan-pernyataan yang tertera di bagian bawah kuisioner ini?

Untuk menjawab kuisioner ini, mohon mengisi kuisioner ini dengan jujur dan objektif. Jawaban Anda akan kami gunakan untuk meningkatkan kualitas pelayanan kami kepada Anda.

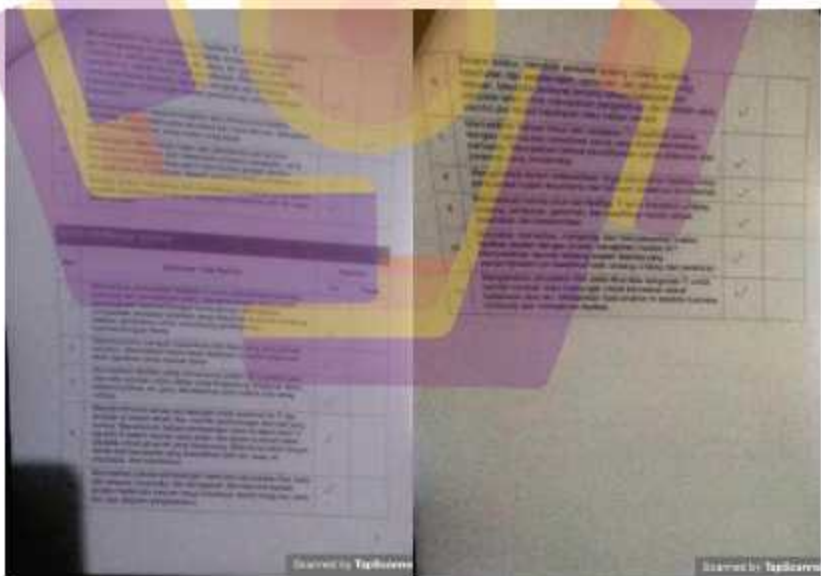
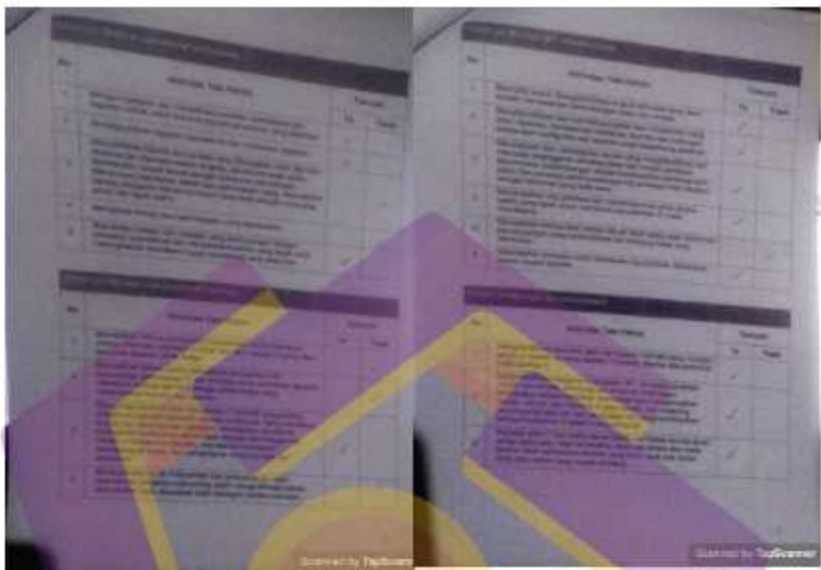
Terima kasih banyak atas partisipasi dan kerendahan hati Anda dalam mengisi kuisioner ini.

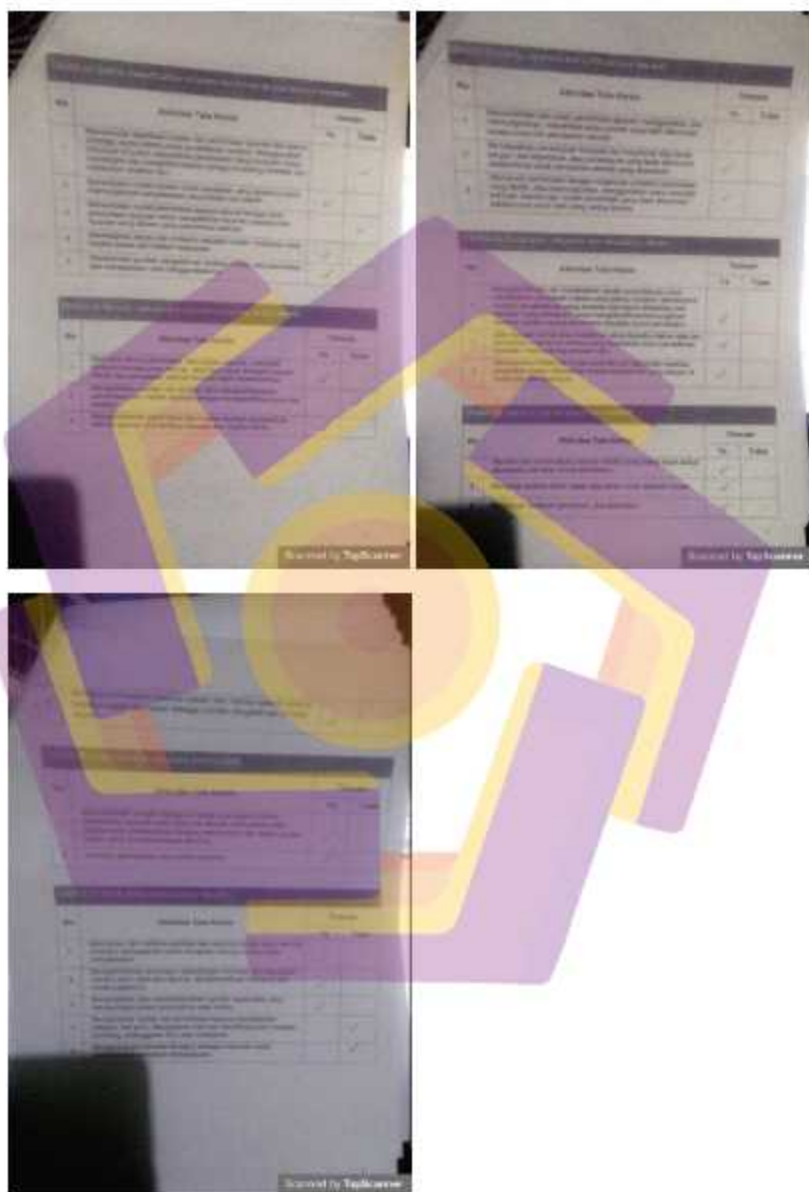
No	Nama	Jabatan

Scanned by TeckSource

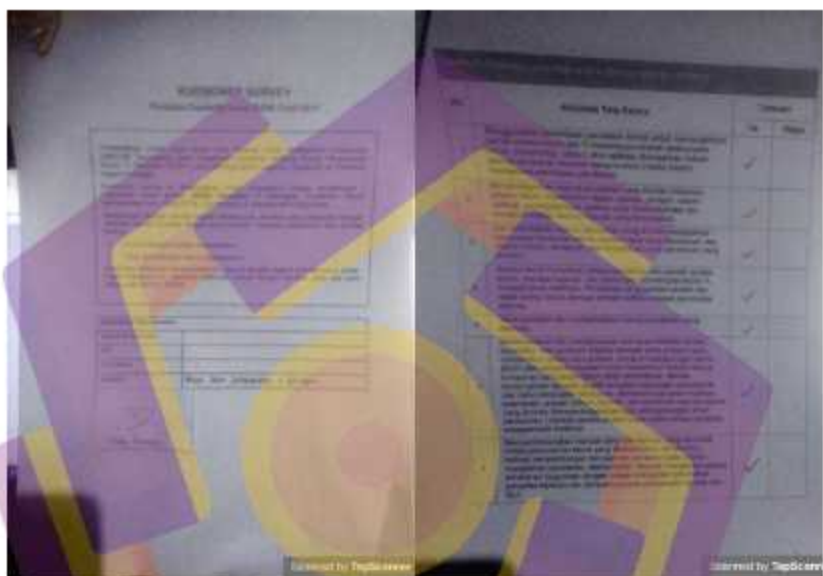


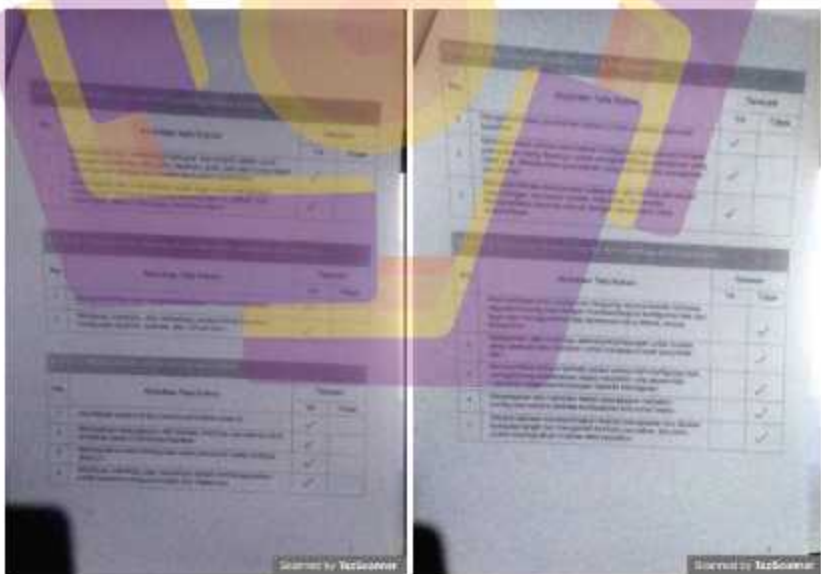
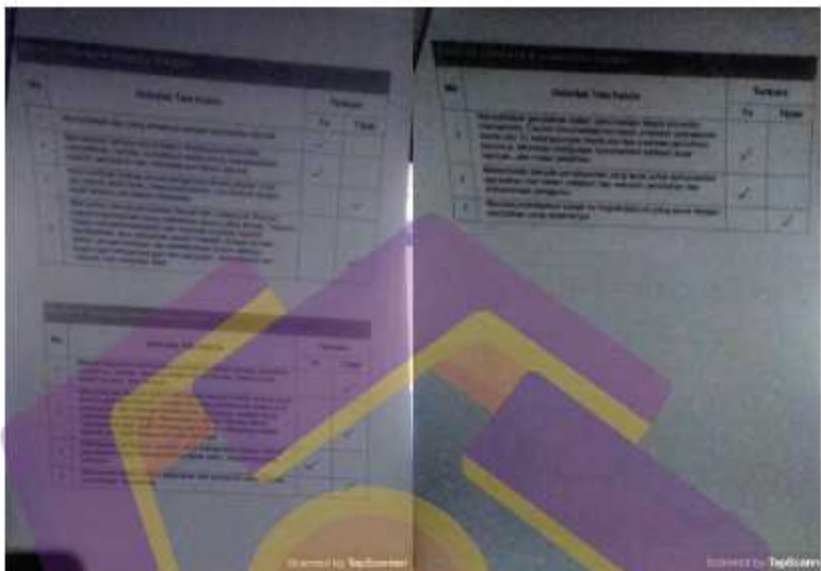


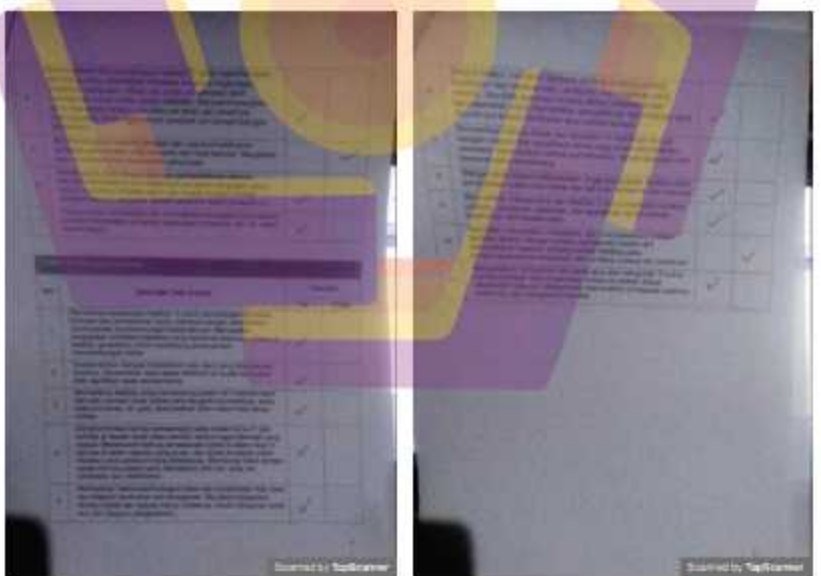
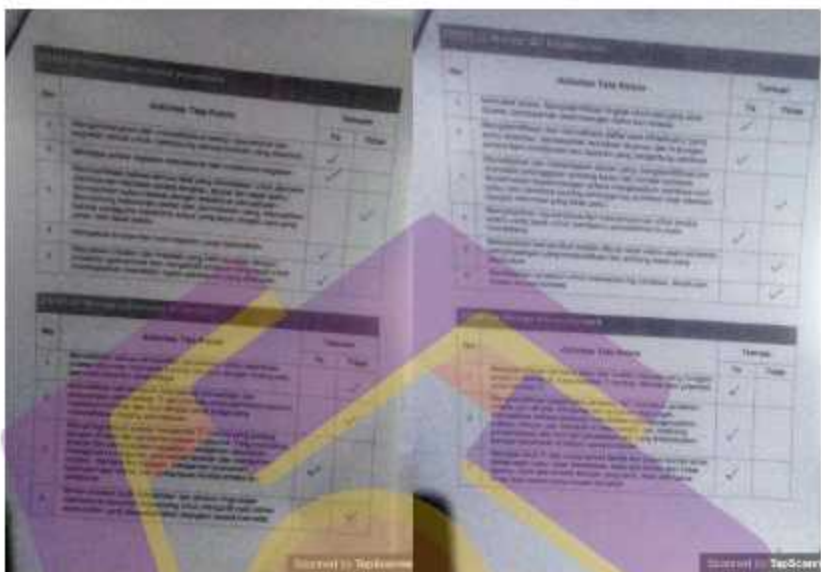




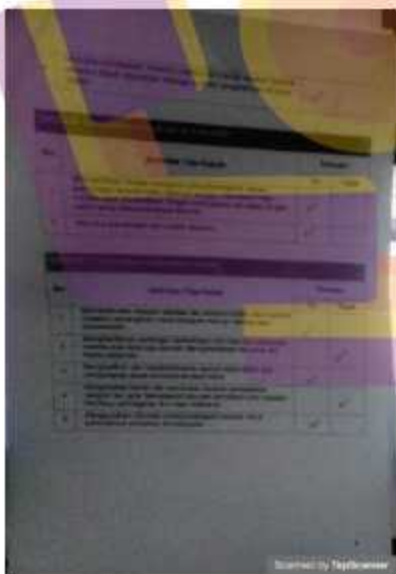
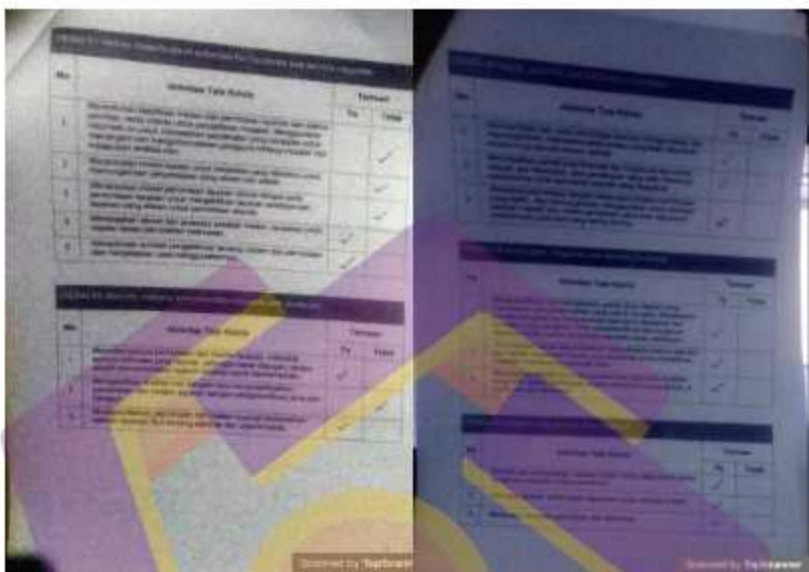
**LAMPIRAN 7**  
**DATA KUISIONER**  
**KETUA KOORDINATOR INFRASTRUKTUR DAN JARINGAN**











## LAMPIRAN 8

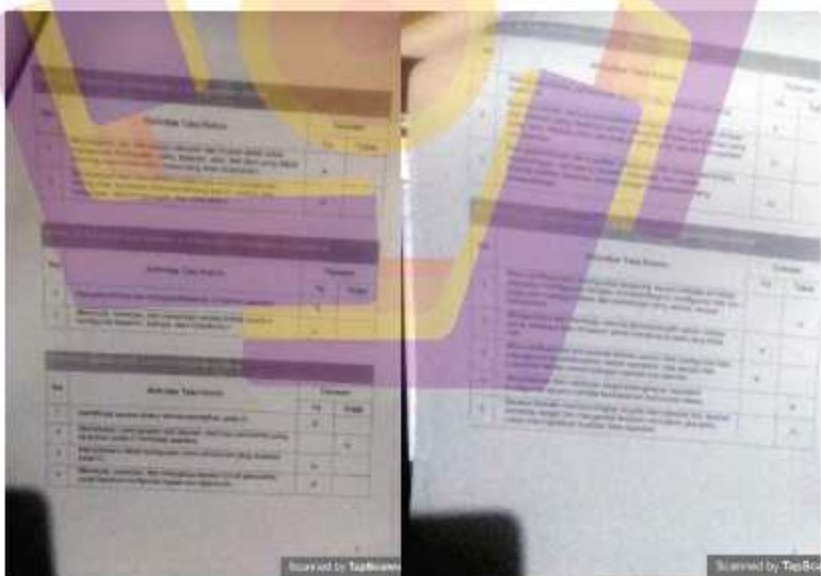
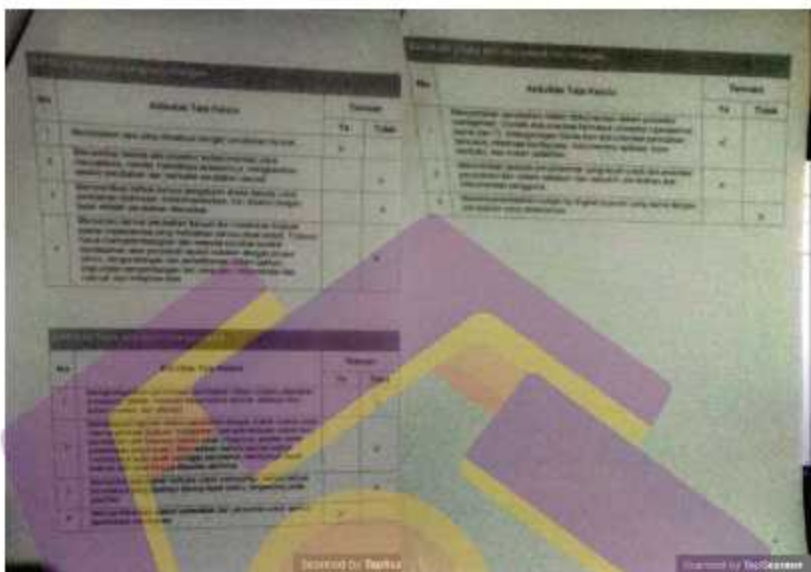
### DATA KUISIONER

#### KETUA KOORDINATOR SISTEM INFORMASI

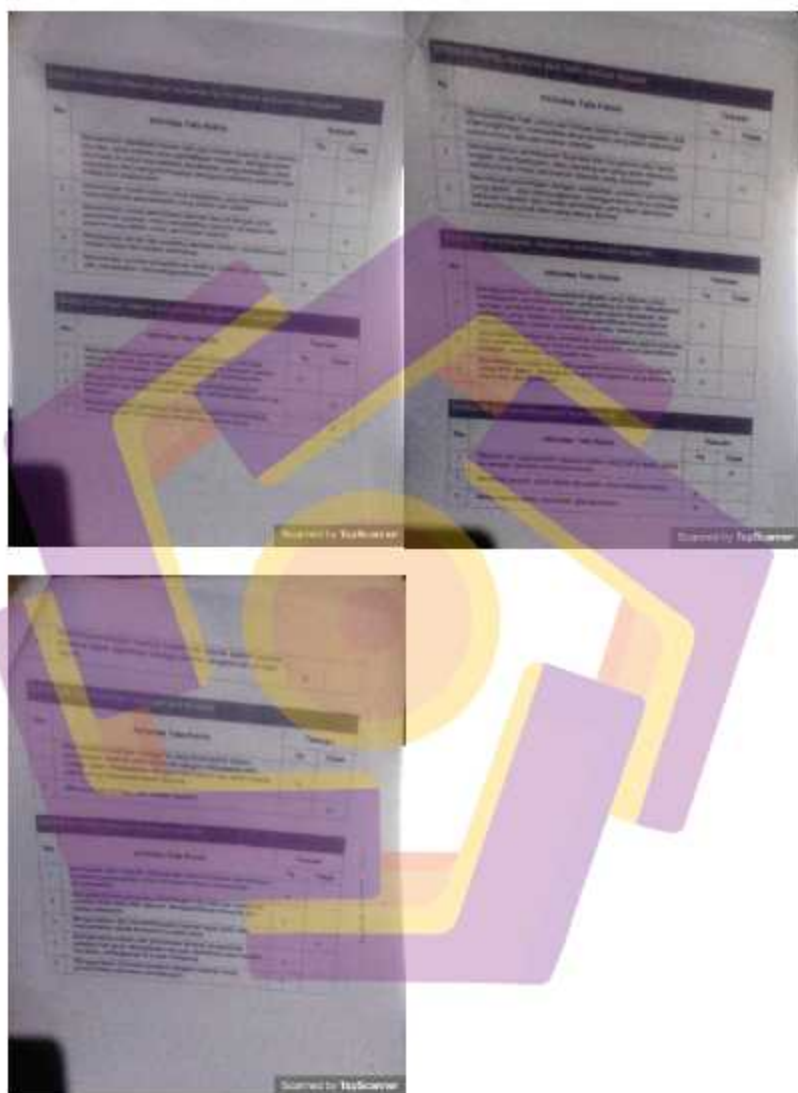
**KUESIONER KEPALA**  
Tujuan: Untuk mengetahui pendapat Kepala Sekolah tentang...

**KUESIONER TATA PELAKSANA**  
Tujuan: Untuk mengetahui pendapat Kepala Sekolah tentang...

No	Ya	Tidak
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		
36		
37		
38		
39		
40		
41		
42		
43		
44		
45		
46		
47		
48		
49		
50		









## LAMPIRAN 9

### Lembar Catatan Revisi Ujian Tes

PROGRAM STUDI S2 TEKNIK INFORMATIKA  
UNIVERSITAS AMKOM YOGYAKARTA

#### CATATAN REVISI UJIAN TESIS

NIM	20.51.1327
Nama mahasiswa	Nurul Ima Hasang Kiria
Pembimbing I	Prof. Dr. Ema Utami, S.Si, M.Kom.
Pembimbing II	Aba Haidi Muhammad, S.T., M.Eng., Ph.D.
Judul Tesis	Model Pengelolaan Risiko TI Berbasis COBIT untuk Meningkatkan Layanan Akademik di Politeknik Negeri Sleman
Kegiatan	Ujian Tesis
Hari, tanggal	Selasa, 5 Juli 2022
Pengaji I	Dr. Andi Sunyoto, M.Kom.
Revisi	- Jika memungkinkan ditambahkan mekanisme pengukuran seberapa efektif model (rekomendasi) yang diusulkan jika diterapkan. - Pada pertengahan dengan penelitian sebelumnya jika bisa tidak hanya berbeda, tetapi menambahkan apa signifikansi hasil dari penelitian sebelumnya.
Rekomendasi	- LULUS dengan revisi.
Pengaji II	Dhoni Ariyanto, M.Eng., Ph.D.
Revisi	1. Persilakan sumber yang terletak dibawah table pada bab 4 sebanyak 6-8 halaman saja 2. terkait dengan kontribusi apa yang diberikan dari hasil penelitian yang telah anda lakukan apakah ada penjelasan yang detail dan bisa digambarkan frame work terkait implementasi cobit untuk penelitian
Rekomendasi	- Lulus dengan revisi
Pengaji III	Prof. Dr. Ema Utami, S.Si, M.Kom.
Revisi	1). perlu menambahkan mekanisme justifikasi terhadap rekomendasi yang dihasilkan dari model yang diusulkan untuk mengukur seberapa efektif model yang diusulkan ini dalam meningkatkan pelayanan bila nantinya diterapkan. 2). setelah melakukan ulasan maka perlu untuk menyajikan ilustrasi supaya mempermudah maknanya
Rekomendasi	- lulus dengan catatan revisi.

Perhatian atas revisi ujian tesis adalah tanggung jawab Dosen Pengaji yang bersangkutan.

## LAMPIRAN 10

### SOP SERVICE REQUEST DAN INSIDEN

POLITEKNIK NEGERI SURABAYA

STANDAR OPERASIONAL PROSEDUR (SOP)  
SARUKER (SERVICE REQUEST DAN INSIDEN)

Formulir Request / Insiden	
No. Form	Formulir Request / Insiden
Dibuat Oleh	XXXXXXXXXX
Revisi	XXXXXXXXXX
Disetujui Oleh	XXXXXXXXXX
Tgl. Disetujui	XXXXXXXXXX

**I. TUJUAN PROSEDUR**  
Menjelaskan prosedur yang harus diikuti oleh staf untuk mengelola permintaan layanan dan masalah teknis yang dihadapi pengguna sistem, memastikan masalah tersebut dapat diselesaikan dengan cepat, akurat, dan efisien, sehingga meningkatkan kepuasan pengguna.

**II. RUANG LINGKUP**  
Prosedur ini berlaku untuk semua pengguna sistem yang melaporkan masalah teknis atau permintaan layanan. Tidak berlaku untuk masalah yang berkaitan dengan kebijakan organisasi atau masalah yang memerlukan tindakan hukum.

**III. TUGAS DAN FUNGSI KELOMPOK**

Posisi	Tugas
Manajemen	Mengetahui, menyetujui, dan memantau pelaksanaan SOP.
Staf	Menerima, mencatat, dan menyelesaikan masalah teknis atau permintaan layanan.

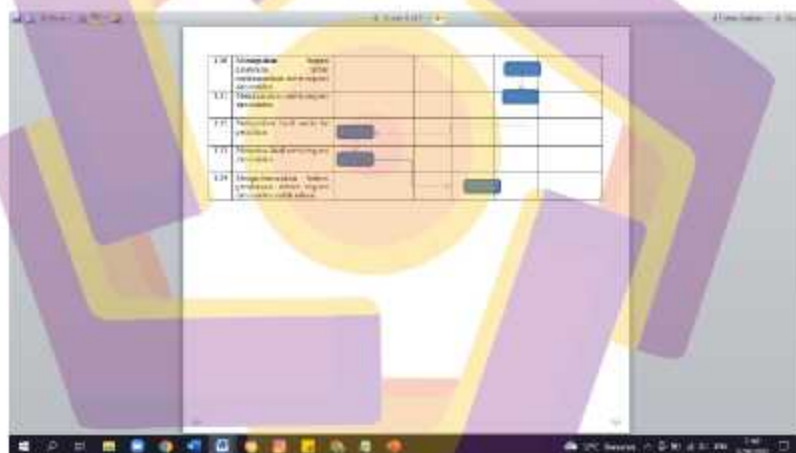
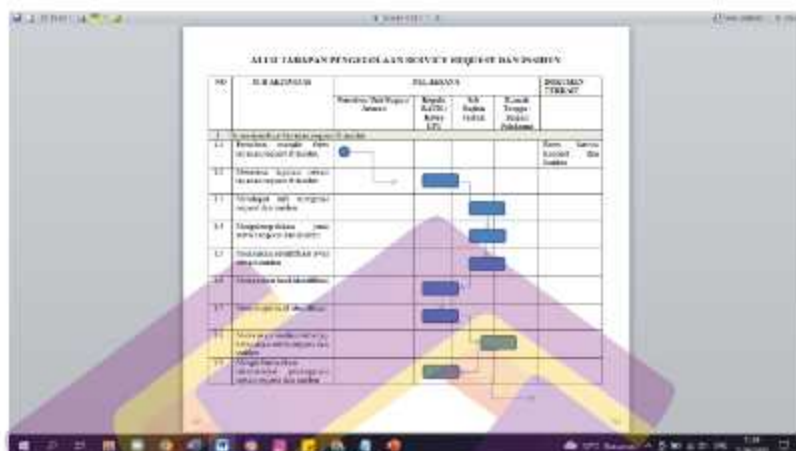
**IV. ALUR PROSEDUR**  
SOP ini menjelaskan alur proses yang harus diikuti oleh staf untuk mengelola permintaan layanan dan masalah teknis.

**V. REFERENSI DAN CATATAN**

- Manajemen Sistem Informasi
- Manajemen Sistem Jaringan
- Manajemen Sistem Aplikasi
- Manajemen Sistem Keamanan

**VI. PENYIMPANAN DAN REVISI**  
SOP ini disimpan di bagian IT dan harus direvisi jika ditemukan perubahan yang signifikan.

**VII. PENYIMPANAN**  
SOP ini harus disimpan di bagian IT dan harus direvisi jika ditemukan perubahan yang signifikan.



FORMULIR PENYANGANAN KEPUTUSAN DAN TAMPILAN  
 Politeknik Negeri Sriwijaya

NO. FORMULIR	TANGGAL
190-1002-70-100-1001/19	14.08.2019

**AGUNG/IBRIS:**

Nama	
Tempat/Tgl. Lahir	
Id. Email	

**KEPUTUSAN/KEPUTUSAN/KEPUTUSAN:**

**KEPUTUSAN/KEPUTUSAN:**

MENGETARI      DIREKTORAN GURU

       
 JCF        
     

