TUGAS AKHIR – KS141501

PEMBUATAN PERANGKAT AUDIT BERBASIS RISIKO BERDASARKAN COBIT 5 DAN SERVICE DESK STANDARD PADA SERVICE DESK (STUDI KASUS: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

DESIGNING A RISK BASED AUDIT PROGRAM BASED ON COBIT 5 AND SERVICE DESK STANDARD IN SERVICE DESK (STUDY CASE: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

SARAH PUTRI RAMADHANI
NRP 5213 100 185

Dosen Pembimbing
Hanim Maria Astuti, S.Kom., M.Sc.
Anisah Herdiyanti, S.Kom., M.Sc.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS141501

PEMBUATAN PERANGKAT AUDIT BERBASIS RISIKO BERDASARKAN COBIT 5 DAN SERVICE DESK STANDARD PADA SERVICE DESK (STUDI KASUS: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

SARAH PUTRI RAMADHANI
NRP 5213 100 185

Dosen Pembimbing

Hanim Maria Astuti, S.Kom., M.Sc.
Anisah Herdiyanti, S.Kom, M.Sc.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS 141501

DESIGNING A RISK BASED AUDIT PROGRAM BASED ON COBIT 5 AND SERVICE DESK STANDARD IN SERVICE DESK (STUDY CASE: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

SARAH PUTRI RAMADHANI
NRP 5213 100 185

Supervisor

Hanim Maria Astuti, S.Kom., M.Sc.
Anisah Herdiyanti, S.Kom, M.Sc.

INFORMATION SYSTEMS DEPARTMENT
Information Technology Faculty
Sepuluh Nopember Institut of Technology
Surabaya 2017

PEMBUATAN PERANGKAT AUDIT BERBASIS RISIKO BERDASARKAN COBIT 5 DAN SERVICE DESK STANDARD PADA SERVICE DESK (STUDI KASUS: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

SARAH PUTRI RAMADHANI
5213 100 185

Surabaya, Januari 2017

KETUA
JURUSAN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom.
NIP 19650310 199102 1 001

PEMBUATAN PERANGKAT AUDIT BERBASIS RISIKO BERDASARKAN COBIT 5 DAN SERVICE DESK STANDARD PADA SERVICE DESK (STUDI KASUS: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

SARAH PUTRI RAMADHANI
5213 100 185

Disetujui Tim Penguji : Tanggal Ujian : 9 Januari 2017
Periode Wisuda : Maret 2017

Hanim Maria Astuti, S.Kom., M.Sc. **(Pembimbing1)**

Anisah Herdiyanti, S.Kom., M.Sc. **(Pembimbing 2)**

Sholiq, S.T., M.Kom., M.SA. **(Penguji 1)**

Feby Artwodini Muqtadiroh, S.Kom., M.T. **(Penguji 2)**

PEMBUATAN PERANGKAT AUDIT BERBASIS RISIKO BERDASARKAN COBIT 5 DAN SERVICE DESK STANDARD PADA SERVICE DESK (STUDI KASUS: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

Nama Mahasiswa	**: SARAH PUTRI RAMADHANI**
NRP	**: 5213100185**
Jurusan	**: Sistem Informasi**
Dosen Pembimbing 1	**: Hanim Maria Astuti, S.Kom, M.Sc.**
Dosen Pembimbing 2	**: Anisah Herdiyanti, S.Kom., M.Sc.**

ABSTRAK

SubDirektorat Layanan Teknologi dan Sistem Informasi pada DPTSI sebagai penyedia layanan TI di lingkungan Institut Teknologi Sepuluh Nopember (ITS) tidak sedikit mengalami gangguan atau insiden yang mengakibatkan menurunnya kualitas pelayanan yang diberikan. Oleh karena itu terdapat unit service desk yang bertugas menangani berbagai macam keluhan insiden dan memenuhi permintaan layanan TI. Namun DPTSI belum pernah mengadakan pengendalian internal terhadap prosesnya. Untuk memastikan pengelolaan telah diterapkan dalam kontrolnya maka perlu sebuah metode yaitu audit teknologi informasi. Salah satu hal yang perlu disiapkan dalam melaksanakan audit adalah perangkat audit. Suatu perangkat audit penting untuk dibuat karena menyediakan serangkaian instruksi dari proses yang harus dilakukan service desk sehingga membantu seorang auditor dalam menjalankan audit sesuai dengan tujuan dan memastikan seluruh proses telah dilakukan.

Penelitian ini bertujuan untuk membuat perangkat audit pengelolaan permintaan layanan dan insiden pada service desk DPTSI yang dibuat berdasarkan control objective pada Service Desk Standard yang dipetakan dengan proses pada best practice COBIT 5 domain DSS02. Ruang lingkup

perangkat audit juga ditetapkan melalui control objective yang dipetakan dengan risiko TI pada service desk yang dianalisis menggunakan pendekatan best practice COBIT 5 for Risk APO12 Manage Risk. Langkah terakhir adalah melakukan verifikasi dokumen perangkat audit dan persetujuan perangkat audit.

Hasil dari tugas akhir ini adalah sebuah dokumen perangkat audit beserta panduan penggunaannya, yang nantinya diharapkan dapat membantu DPTSI untuk melakukan audit pengelolaan permintaan layanan dan insiden pada service desk sesuai acuan best practice COBIT 5 dan standar kontrol Service Desk Standard.

Kata Kunci**: **Perangkat Audit, Service Desk, Permintaan Layanan, Insiden, COBIT 5, COBIT 5 for Risk, Service Desk Standard.

DESIGNING A RISK BASED AUDIT PROGRAM BASED ON COBIT 5 AND SERVICE DESK STANDARD IN SERVICE DESK (STUDY CASE: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

Name	**: SARAH PUTRI RAMADHANI**
NRP	**: 5213100185**
Department	**: Sistem Informasi**
Supervisor 1	**: Hanim Maria Astuti, S.Kom, M.Sc.**
Supervisor 2	**: Anisah Herdiyanti, S.Kom., M.Sc.**

ABSTRACT

Sub-Directorat of Technology and Information Systems Services at DPTSI as a provider of IT services in Institut Teknologi Sepuluh Nopember (ITS) frequently can cause disturbance or incident that resulted in a decreased quality of services provided. Therefore, there is a service desk who has responsible for handling a variety of complaints of incidents and meet the demand for IT services. However DPTSI has never held internal control over processes. To ensure the management has been applied in the control it needs a method that is information technology auditing. One of the things that need to be prepared to carry out an audit is an audit program. An audit program necessary to be made because it provides a set of instructions on the process to be followed service desk that helps an auditor in performing the audit in accordance with the objectives and ensure the entire process has been conducted.

This study aims to design a risk based service requests and incident management audit program based on audit control objectives in Service Desk Standard mapped with processes in COBIT 5 DSS02 domain. The scope of the audit also determined through the control objectives are mapped to IT risks at the service desk were analyzed using best practice approaches

COBIT 5 for Risk APO12 Manage Risk. The last step is to verify the documents audit and approval of the audit.

The results of this research is a document of audit program and its user guide, that later is expected to be able to help DPTSI on performing audit of service requests and incidents management on the service desk based on the reference best practice of COBIT 5 and standard of Service Desk Standard.

Keyword**: **Audit Program, Service Desk, Service Requests, Incidents, COBIT 5, COBIT 5 for Risk, Service Desk Standard.

KATA PENGANTAR

Syukur Alhamdulillah atas segala petunjuk, pertolongan, dan kekuatan yang diberikan oleh Allah SWT. Hanya karena ridho-Nya, peneliti dapat menyelesaikan laporan Tugas Akhir dengan judul:

PEMBUATAN PERANGKAT AUDIT BERBASIS RISIKO BERDASARKAN COBIT 5 DAN SERVICE DESK STANDARD PADA SERVICE DESK (STUDI KASUS: DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI ITS)

yang merupakan salah satu syarat kelulusan dalam rangka mendapat gelar sarjana pada Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya.

Terima kasih yang teramat besar penulis ucapkan pada semua pihak yang telah membantu dalam menyelesaikan tugas akhir ini, yaitu:

1. Allah SWT yang telah memberikan kesempatan, petunjuk, kekuatan, kasih sayang, kesehatan dan waktu yang cukup dalam mengerjakan dan menyelesaikan tugas akhir ini.
2. Alm. Bapak Andri Atomoko dan Ibu Nuri Mashitah selaku orang tua penulis yang tiada henti selalu memberikan doa, semangat, segala bentuk dukungan, mengajarkan arti berjuang, kerendahan hati dan selalu mengingatkan untuk beribadan serta bersyukur kepada Allah SWT. Terima kasih, Inshaa Allah kerja keras papa dan mama tidak akan pernah sia-sia.
3. Mas Novan Anggara Putra dan Mbak Elsa Btari Andani selaku saudara kandung penulis yang membimbing penulis dari kecil hingga dewasa dan selalu memberi nasihat untuk kebaikan.

4. Bapak Dr. Ir. Aris Tjahyanto, M.Kom. selaku Ketua Jurusan Sistem Informasi.
5. Bapak Ibu Hanim Maria Astuti dan Ibu Anisah Herdiyanti selaku dosen pembimbing yang telah memberikan bimbingan, dukungan, semangat dan motivasi dalam menyelesaikan tugas akhir ini.
6. Bapak Feby Artwodini Muqtadiroh selaku dosen wali yang telah memberikan pengarahan dan semangat bagi penulis dalam menempuh masa perkuliahan dan pengerjaan tugas akhir
7. Pak Hermono, selaku admin laboratorium MSI yang senantiasa membantu penulis dalam hal administrasi penyelesaian tugas akhir dan memberikan kenyamanan pada laboratorium selama pengerjaan tugas akhir.
8. Para Bapak dan Ibu dosen Jurusan Sistem Informasi
9. Pak Jainul Arifin, Ibu Widiyaningsih, dan Ibu Mudjiatin, sebagai Staf *Service desk* DPTSI ITS Surabaya yang telah bersedia memberikan waktunya untuk memberikan kemudahan dan arahan bagi penulis dalam pengambilan data tugas akhir.
10. Sahabat-sahabat terbaik penulis An Nisa' aka Yurah, Bos Fian, Sherly aka acid, Firzah aka zuya, Itak aka suitaq, Mahesti aka etik, Niswa aka wawa, Orie, Rr, Selina aka kucluk, dan Visha aka shuya dari Keong Club atas semangat, dukungan, dan kebersamaannya selama perkuliahan.
11. Sahabat-sahabat terbaik penulis Arum, Fara, Shasa, Diana, Arizta, Denisa, Feby, Fira, Harizka, Indik, Trysa, dan Rosa atas semangat yang diberikan untuk penulis agar dapat menyelesaikan tugas akhir ini.
12. Teman-teman seperjuangan laboratorium MSI dan geng penelitian DPTSI Chitra, Hemas, Mega, dan lainnya yang tidak bisa disebutkan satu persatu terima kasih selalu ada menemani, memberikan semangat dan bantuan dalam mengerjakan tugas akhir ini.
13. Andika Aji Siswoyo yang selalu memberi semangat penulis dalam menyelesaikan tugas akhir, meluangkan

waktu untuk memberikan dukungan, serta mengingatkan penulis untuk menjadi lebih baik.

14. Galuh Satya Nugraha yang selalu mengingatkan bahwa sebuah hasil tidak akan membohongi sebuah perjuangan, serta meyakinkan bahwa penulis pasti dapat menyelesaikan tugas akhir ini dengan baik dan sesuai target waktu.
15. Teman-teman angkatan 2013, BELTRANIS yang telah menjadi keluarga bagi penulis selama empat tahun ini.
16. Mas dan Mbak BASILISK dan SOLARIS yang telah memberikan semangat dan inspirasi bagi penulis.
17. Seluruh staf dan karyawan di Jurusan Sistem Informasi, terima kasih telah bekerja dengan baik dan membantu penulis dalam menyelesaiakan urusan akademik selama penulis ada dalam masa perkuliahan.

Penelitian ini diharapkan dapat menjadi bahan acuan dalam melakukan evaluasi bagi perusahaan dalam meningkatkan performa dalam melakukan pengelolaan tugas akhir. Penulis menyadari masih terdapat banyak kekurangan dalam pengerjaan dan pembuatan buku tugas akhir ini, oleh karena itu penulis masih sangat terbuka dalam menerima kritik dan saran yang membangun untuk dapat menyempurnakan tugas akhir ini. Semoga dengan terselesaikannya tugas akhir ini dapat membawa manfaat bagi banyak pihak.

Surabaya, Januari 2017

Penulis

Halaman ini sengaja dikosongkan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

Pada bab ini akan dijelaskan latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat yang diperoleh, target luaran, dan sistematika penulisan yang ingin dicapai dalam pengerjaan Tugas Akhir.

1.1 Latar Belakang

DPTSI (Direktorat Pengembangan Teknologi dan Sistem Infromasi) sebagai salah satu unit pada Institut Teknologi Sepuluh Nopember (ITS) Surabaya membantu organisasi dalam memberikan layanan prima bagi civitas akademik melalui pengelolaan teknologi dan sistem informasi secara terpadu [1]. *Service desk* sebagai unit fungsional pada DPTSI berfungsi menghubungkan antara unit teknologi sistem informasi dengan semua pengguna layanan TI yang ada pada ITS Surabaya. Suatu unit *service desk* harus memberikan respon yang tepat waktu dan efektif untuk memenuhi permintaan pengguna dan resolusi dari semua jenis insiden dengan cepat dan tepat [2].

Dalam aktivitas operasional pemberian layanan TI kepada pengguna, tidak jarang *service desk* mengalami gangguan dan risiko dalam melakukan aktivitas pengelolaan insiden, pemenuhan permintaan layanan di luar insiden, maupun penerimaan permintaan akses [3]. Begitu juga dengan *service desk* DPTSI yang selama ini hanya sebatas pada melakukan pencatatan dan penanganan tanpa memberikan prioritas dan klasifikasi terhadap permintaan layanan dan insiden sehingga dapat menyebabkan kesalahan mengambil keputusan dalam penanganannya. Gangguan dan risiko ini mengakibatkan kualitas performa pada *service desk* menjadi berkurang. Oleh karena itu *service desk* membutuhkan suatu kontrol untuk memastikan bahwa proses pengelolaan permintaan layanan dan insiden pada *service desk* dilaksanakan dengan baik, serta untuk memitigasi risiko pada proses. Salah satu upaya kontrol

terhadap proses pada *service desk* yang belum dilakukan oleh DPTSI adalah pengendalian internal.

Audit internal sebagai upaya pengendalian perlu dilakukan untuk memastikan bahwa tingkat layanan terhadap pengelolaan permintaan layanan dan insiden yang diberikan oleh *service desk* DPTSI telah memenuhi standar yang diinginkan dan sesuai dengan *best practice*. Dalam melakukan audit, ada banyak hal yang harus dipersiapkan seperti salah satunya dengan mempersiapkan perangkat audit. Perangkat audit sebagai alat atau *tools* yang di dalamnya berisi dokumen-dokumen kerja terstandar dapat digunakan para auditor internal DPTSI dalam membantu proses audit agar lebih efektif dan efisien. Suatu perangkat audit penting untuk dibuat karena menyediakan serangkaian instruksi dari proses yang harus dilakukan *service desk* sehingga membantu seorang auditor dalam menjalankan audit sesuai dengan tujuan dan memastikan seluruh proses telah dilakukan [4].

Berdasarkan refleksi terhadap permasalahan dari kondisi kekinian yang dialami oleh DPTSI, penelitian tugas akhir ini bertujuan untuk menghasilkan dokumen perangkat audit berbasis risiko yang disesuaikan dengan prosedur operasional layanan pada unit *service desk*. Dalam pembuatan perangkat audit berbasis risiko ini, langkah pertama penulis melakukan pemetaan *control objective* pada *Service Desk Standard* dengan proses pengelolaan permintaan layanan dan insiden berdasarkan *best practice* COBIT 5 domain DSS02. Selanjutnya dilakukan analisis risiko teknologi informasi berbasis proses pada *service desk* menggunakan kerangka kerja COBIT 5 *for Risk* domain APO12 dan pemetaan risiko dengan *control objecive* untuk mitigasi risiko yang akan digunakan dalam pembuatan perangkat audit. Pada langkah akhir, penulis melakukan verifikasi berdasarkan *best practice* dan persetujuan perangkat audit. Dengan adanya perangkat audit untuk pengelolaan permintaan layanan dan insiden diharapkan Direktorat Pengembangan Teknologi dan Sistem Informasi ITS

Surabaya dapat meningkatkan performa kualitas layanan terhadap pemberian layanan TI dan mengurangi permasalahan layanan TI sehingga layanan tersebut dapat memberikan nilai secara prima bagi setiap pengguna layanan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka berikut perumusan masalah yang akan diselesaikan pada tugas akhir ini:

1. Apa sajakah risiko teknologi informasi yang terdapat pada *service desk* Direktorat Pengembangan Teknologi dan Sistem Informasi?
2. Bagaimana hasil penilaian risiko teknologi informasi?
3. Apa sajakah *control objective* yang dapat memitigasi risiko yang ada?
4. Bagaimana bentuk perangkat audit untuk *control objective* yang dibuat?

1.3 Batasan Masalah

Tugas akhir ini memiliki batasan pengendalian pengerjaan untuk fokus pada permasalahan yang dibahas. Maka berikut batasan masalah dalam tugas akhir ini:

1. Perangkat audit yang akan dibuat ditujukan untuk manajemen layanan pada *service desk* Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember.
2. Perangkat audit yang akan dibuat mengacu pada pemetaan proses COBIT 5 dan *control objective* menggunakan acuan *Service Desk Standard*.
3. Perangkat audit yang akan dibuat berdasarkan ruang lingkup *control objective* terhadap risiko teknologi informasi yang teridentifikasi berdasarkan hasil wawancara untuk setiap proses pada *service desk* DPTSI.
4. Dokumen yang akan dihasilkan dari penulisan ini berupa perangkat audit yang didalamnya terdapat

prosedur pelaksanaan audit, daftar cek untuk setiap prosedur, Laporan Temuan Audit, dan panduan penggunaan perangkat audit.

1.4 Tujuan Penulisan

Berdasarkan latar belakang permasalahan yang telah dijelaskan, penulisan tugas akhir ini bertujuan untuk:

1. Mengetahui risiko teknologi informasi yang terdapat pada *service desk* Direktorat Pengembangan Teknologi dan Sistem Informasi.
2. Mengetahui hasil penilaian risiko yang akan terjadi untuk setiap proses pada *service desk* DPTSI.
3. Mengetahui *control objective* yang dapat memitigasi risiko yang akan digunakan dalam pembuatan perangkat audit.
4. Menghasilkan perangkat audit untuk *control objective* yang digunakan dalam melakukan audit pengelolaan permintaan layanan dan insiden pada *service desk* Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember.

1.5 Manfaat Penulisan

Manfaat yang diberikan dari pengerjaan tugas akhir ini adalah sebagai berikut:

1. Bagi dunia akademis dan auditor, sebagai referensi untuk penelitian dalam bidang audit teknologi informasi/sistem informasi khususnya pada pembuatan perangkat audit.
2. Bagi DPTSI ITS Surabaya, sebagai referensi perangkat organisasi dalam melakukan audit internal terhadap pengelolaan permintaan layanan dan insiden pada *service desk* secara tepat agar meningkatkan kualitas manajemen layanan TI dan mencapai kepuasan pengguna layanan.

1.6 Relevansi Tugas Akhir

Penelitian tugas akhir ini memiliki relevansi dengan mata kuliah yang diajarkan di Jurusan Sistem Informasi ITS yaitu mata kuliah Manajemen Layanan Teknologi Informasi, Tata Kelola Teknologi Informasi, Manajemen Risiko Teknologi Informasi, dan Audit.

1.7 Target Luaran

Target luaran dari pengerjaan tugas akhir ini adalah sebagai berikut :

1. Dokumen perangkat audit pengelolaan permintaan layanan dan insiden pada *service desk* DPTSI ITS beserta dokumen panduan penggunaannya.
2. Dokumentasi pengerjaan Tugas Akhir berupa buku Tugas Akhir dan Paper atau Jurnal Ilmiah.

Halaman ini sengaja dikosongkan

BAB II
TINJAUAN PUSTAKA

Pada bab ini akan menjelaskan mengenai penelitian sebelumnya dan dasar teori pendukung yang akan dijadikan acuan atau landasan dalam pengerjaan tugas akhir ini.

2.1 Studi Sebelumnya

Penelitian Sebelumnya memaparkan acuan yang digunakan oleh penulis dalam melakukan penulisannya. Acuan yang digunakan berupa teori maupun penulisan yang sejenis dengan penulisan yang dilakukan, berikut ditunjukkan pada Tabel 2.1 Penelitian Sebelumnya.

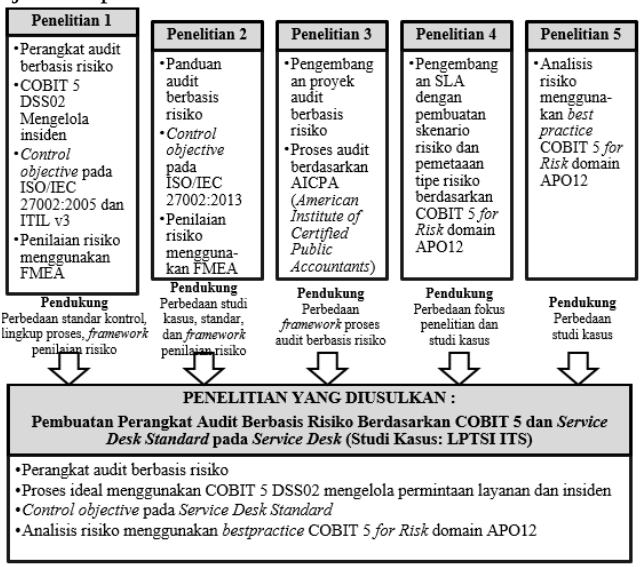
Tabel 2.1 Penelitian Sebelumnya

Penelitian 1	
Penulis	Dyah Retnani Sulistyaningrum
Judul	Pembuatan Perangkat Audit Berbasis Risiko untuk Manajemen Insiden pada Service Desk Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya [5]
Metodologi	- Memetakan proses ideal berdasarkan COBIT 5 DSS02 - Menentukan kontrol perangkat audit berdasarkan ISO/IEC 27002:2005 dan ITIL V3 *Service Operation* - Mengidentifikasi risiko setiap kontrol berbasis aset kritis - Melakukan penilaian risiko dengan *framework* FMEA
Relevansi Penelitian	Penelitian ini sebagai acuan penulis dalam mengerjakan Tugas Akhir dalam hal pembuatan perangkat audit berbasis risiko untuk *service desk*, termasuk sebagai acuan pembuatan *protocol interview* dan daftar risiko pada proses *service desk*. Relevansi penelitian dalam penggunaan proses ideal sesuai *best practice* COBIT 5 DSS02. Namun penulis melengkapi proses pada *service desk*, yaitu

	pengelolaan permintaan layanan dan insiden. Kemudian penulis menggunakan *control objective* pada *service desk standard* di mana lebih spesifik dan detail untuk *service desk*.
Penelitian 2	
Penulis	Stephen Christian
Judul	Pembuatan Panduan Audit Keamanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 pada Direktorat Sistem Informasi Universitas Airlangga [6]
Metodologi	- Mengidentifikasi risiko berbasis aset informasis - Melakukan penilaian risiko dengan *framework* FMEA - Memetakan risiko ke dalam *control objective* berdasarkan standar ISO/IEC 27002:2013 klausul keamanan fisik dan lingkungan
Relevansi Penelitian	Penelitian ini membuat perangkat audit audit berbasis risiko sehingga menjadi acuan penulis dalam menyusun metodologi penelitian. Namun penelitian ini juga termasuk melakukan perencanaan audit, sedangkan penulis hanya membuat perangkat audit.
Penelitian 3	
Penulis	Wiliam F. Messier Jr.
Judul	*An Approach to Learning Risk-Based Auditing* [7]
Metodologi	Mengembangkan proyek audit dan penilaian menggunakan proses audit berbasis risiko pada AICPA (*American Institute of Certified Public Accountants*)
Relevansi Penelitian	Relevansi penelitian ini adalah penggunaan proses audit berbasis risiko sehingga menjadi referensi bagi penulis untuk menyusun metodologi penelitian.
Penelitian 4	
Penulis	Onyeka Illoh, Shaun Aghili, dan Sergey Butakov
Judul	*Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates* [8]
Metodologi	Membuat template SLA melalui pemetaan skenario risiko dan tipe risiko berdasarkan *framework*

	COBIT 5 *for Risk* domain APO12 dengan komponen SLA.
Relevansi Penelitian	Penelitian ini menggunakan COBIT 5 *for Risk* domain APO12 untuk mengidentifikasi, membuat skenario, dan memetakan tipe risiko seperti yang dilakukan penulis dalam menganalisis risiko.
Penelitian 5	
Penulis	Dwi Rosa Indah, Halili, Mgs. Afriyan Firdaus
Judul	*Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk* [9]
Metodologi	Menilai ERP menggunakan ERP *post-implementation success* dan CSF. Lalu melakukan analisis (mengidentifikasi dan menilai) risiko menggunakan COBIT 5 *for Risk* domain APO12
Relevansi Penelitian	Relevansi penelitian ini adalah penggunaan justifikasi penilaian risiko berdasarkan COBIT 5 *for Risk* APO12.

Berikut analisis gap dari keempat penelitian terdahulu ditunjukkan pada Gambar 2.1.



Gambar 2.1 Analisis Gap Penelitian Sebelumnya

2.2 Dasar Teori

Pada bagian ini dipaparkan beberapa teori yang digunakan dalam pengerjaan tugas akhir ini.

2.2.1 Audit SI/TI

2.2.1.1 Pengertian Audit SI/TI

Terdapat beberapa pengertian audit menurut beberapa ahli, berikut diataranya.

1. Menurut Dan M. Guy, C. Wayne Alderman, dan Allan J. Winters, Proses audit atau dikenal sebagai auditing adalah suatu proses sistematis yang secara objektif memperoleh dan mengevaluasi bukti yang terkait dengan pernyataan mengenai tindakan atau kejadian ekonomi untuk menilai tingkat kesesuaian antara pernyataan tersebut dengan kriteria yang telah ditetapkan serta menghormati hasilnya kepada pihak-pihak berkepentingan [10].
2. Menurut Arens dan Loebbecke, Audit adalah akumulasi dan evaluasi dari bukti mengenai informasi untuk menentukan dan melaporkan derajat kesesuaian antara informasi dan kriteria yang telah ditentukan. Aktivitas audit harus dilakukan oleh seseorang yang berkompeten dan independen [11].
3. Menurut Spicer dan Pegler, proses audit adalah pemeriksaan pembukuan akuntansi dan bisnis, yang akan memungkinkan auditor untuk memastikan bahwa neraca bisnis yang dibuat telah benar sehingga memberi pandangan bahwa laba/rugi pada periode finansial perusahaan telah sesuai dengan informasi dan fakta pada buku yang diterima [4].

Dapat disimpulkan dari ketiga pendapat di atas, bahwa audit merupakan suatu proses sistematik yang dilakukan untuk memastikan dan mengevaluasi bukti yang dilakukan oleh seorang auditor.

Menurut James A. Hall, suatu aktivitas audit yang melibatkan elemen komputerisasi dari sebuah akuntansi sistem informasi disebut dengan Audit Teknologi Informasi [12]. Sedangkan menurut Riananto Sarno dalam bukunya yang berjudul "Audit Sistem/Teknologi Informasi", Audit Sistem Informasi merupakan aktivitas audit yang dilakukan untuk memastikan pengelolaan sistem informasi sehingga terarah dalam kerangka perbaikan berkelanjutan dan penyesuaian terhadap kepatutan apakah sistem berjalan sesuai dengan standard yang berlaku [13].

Berdasarkan pengertian audit sistem informasi dan teknologi informasi menurut para ahli di atas, maka dapat disimpulkan bahwa audit sistem informasi/teknologi informasi merupakan aktivitas pemeriksaan, pengawasan, dan pengendalian suatu sistem informasi apakah berjalan sesuai suatu standar yang telah ditetapkan dengan bantuan elemen komputerisasi.

2.2.1.2 Pengertian Audit Berbasis Risiko

Aktivitas audit yang dilakukan oleh auditor bertujuan untuk mendukung pencapaian tujuan organisasi yang telah ditetapkan dengan memperhatikan seluruh aspek penting, termasuk segala sesuatu yang dapat menghambat pencapaian tujuan tersebut, atau disebut dengan risiko. Memahami penilaian risiko dapat sangat membantu auditor dalam merencanakan aktivitas audit dengan cara memeriksa praktik-praktik dalam perusahaan, toleransinya terhadap suatu risiko, serta kendali operasional dan internal yang dimiliki.

Menurut Lawrence B. Sawyer, *risk-based auditing* atau audit berbasis risiko merupakan observasi dan analisis kontrol yang kemudian berlanjut ke penentuan risiko terkait operasional dan akhirnya menentukan apakah suatu aktivitas sesuai dengan tujuan organisasi. Tidak dapat terhindarnya risiko di seluruh aktivitas operasional menjadikan konsep manajemen risiko semakin diterima dalam aktivitas audit [14]. Kelebihan dari audit berbasis risiko adalah penentuan lingkup target audit yang

lebih jelas sehingga auditor tidak perlu mengevaluasi keseluruhan kondisi organisasi yang akan membutuhkan waktu dan biaya yang tinggi dalam prosesnya [15].

2.2.1.3 Jenis Audit

Menurut Abdul Halim, dilihat dari sisi luas pemeriksaan dan untuk siapa audit dilaksanakan, audit dapat dikelompokkan menjadi tiga jenis golongan, berikut diantaranya [16]:

1. Audit Eksternal – merupakan suatu kontrol sosial yang memberikan jasa untuk memenuhi kebutuhan informasi untuk pihak luar perusahaan yang diaudit. Pelaksana audit eksternal adalah auditor dari pihak luar perusahaan yang independen dan telah diakui oleh pihak berwenang untuk melaksanakan tugas tersebut. Auditor eksternal pada umumnya dibayar oleh manajemen perusahaan yang diaudit.
2. Audit Internal – merupakan suatu kontrol organisasi yang mengukur dan mengevaluasi efektivitas organisasi. Informasi yang dihasilkan, ditujukan untuk manajemen organisasi itu sendiri. Pelaksana audit internal adalah auditor internal dan merupakan karyawan organisasi tersebut. Berfungsi membantu meningkatkan efisiensi dan efektivitas kegiatan perusahaan.
3. Audit Sektor Publik – suatu kontrol atas organisasi pemerintah yang memberikan jasanya pada masyarakat, seperti pemerintah pusat maupun pemerintah daerah. Audit dapat mencakup audit laporan keuangan, audit kepatuhan, maupun audit operasional. Pelaksana audit sektor publik disebut dengan auditor pemerintah dan dibayar oleh pemerintah.

Pada penelitian ini, pembuatan perangkat audit ditujukan untuk audit internal di mana proses pelaksanaan pemeriksaan atau audit dilakukan oleh auditor internal organisasi.

2.2.1.4 Tipe Audit

Terdapat beberapa jenis audit yang banyak dilakukan pada suatu perusahaan atau instansi, seperti [15]:

1. *Administrative Audit* – merupakan aktivitas audit yang berfokus pada proses operasional
2. *Financial Audit* – merupakan aktivitas audit yang berhubungan dengan pencarian kebenaran laporan keuangan suatu organisasi. Audit tipe ini termasuk dalam pengujian substantif.
3. *Forensic Audit* – merupakan aktivitas audit yang berfokus pada pemulihan informasi yang dapat megungkap sebuah penipuan atau kejahatan seperti pengubahan informasi dan angka-angka keuangan sebuah organisasi, yang mana pemulihan informas melalui audit forensik ini ditinjau oleh penegak hukum.
4. *Information System Audit* – merupakan aktivitas audit yang dilakukan untuk verifikasi mekanisme perlindungan terhadap integritas, kerahasiaan, penjaminanan data, dan informasi elektronik yang disediakan oleh sistem informasi dan sistem-sistem pendukung lain yang terkait.
5. *Operational Audit* – merupakan aktivitas audit yang dirancang untuk memeriksa strukur pengendalian internal suatu proses atau area tertentu.
6. Audit lainnya – merupakan pemeriksaan kepatuhan yang digunakan untuk melakukan verifikasi bahwa sebuah layanan organisasi telah melalui proses audit terhadap aktivitas pengendalian. Contoh dari audit kepatuhan antara lain Sarbanes-Oxley, *Health Insurance Portability and Accountability Act* (HIPAA), atau *Statement on Auditing Standards* (SAS) 70.

Tipe audit yang dapat dilakukan oleh auditor terkait pengelolaan permintaan layanan dan insiden pada *service desk* adalah *operational audit* dan *information system audit*.

2.2.1.5 Tujuan Audit

Menurut TYBCom Accountancy Auditing, terdapat dua tujuan dari proses audit, yaitu diantaranya tujuan utama dan sekunder [4].

1. Tujuan Utama (*Primary Objective*)
   Tujuan utama dari proses audit adalah untuk melaporkan pemilik perusahaan apakah neraca keuangan merepresentasikan kebenaran dan keadilan atas kondisi laba/rugi dari keuangan tahunan yang sesungguhnya.
2. Tujuan Sekunder (*Secondary Objective*)
   Tujuan sekunder ini juga disebut tujuan insidental, yaitu bersifat opsional terhadap kepuasan dari tujuan utama. Proses audit bertujuan untuk mendeteksi dan mencegah adanya penipuan dan kesalahan. Sebagaimana pernyataan dari *Institute of Chartered Accountants of India States* mengenai isu praktik audit, seorang auditor sebaiknya mempertimbangkan adanya kemungkinan penipuan atau kesalahan dalam proses pencatatan/pembukuan.

Selain itu, fungsi audit juga bertujuan untuk menyediakan sebuah evaluasi independen dari suatu kontrol internal dengan rekomendasi yang tepat untuk mitigasi risiko yang terdeteksi apabila terjadi [15].

2.2.1.6 Faktor Penting Audit

Informasi yang didapatkan dan digunakan selama proses audit harus dijaga kerahasiaannya karena hanya akan diserahkan kepada pihak penting perusahaan. Oleh karena itu, proses audit harus dilakukan oleh auditor yang berkompeten, bersifat independen, dan melaporkan hasil audit kepada pengguna informasi yang terkait. Auditor mempertanggungjawabkan hasil audit hanya kepada manajemen senior pada fokus masalah tertentu dengan melaporkan hasil temuannya kepada manajemen [15]. Bukti yang dimiliki auditor setidaknya harus memiliki sifat berikut untuk dapat mencapai tujuan audit [15] :

1. *Sufficient*

2. *Usable*
3. *Reliable*
4. *Relevant*
5. *Effective*

Berikut beberapa hal yang harus diperhatikan oleh auditor dalam melakukan audit SI/TI [17]:

1. Perlengkapan keamanan yang akan berguna untuk melindungi perlengkapan komputer, program, komunikasi, dan data dari akses yang tidak sah, modifikasi, atau penghancuran.
2. Pengembangan dan perolehan program dilaksanakan sesuai dengan otorisasi khusus dan umum dari pihak manajemen.
3. Modifikasi program dilaksanakan dengan otorisasi dan persetujuan dari pihak manajemen.
4. Pemrosesan transaksi, file laporan, dan catatan komputer lainnya telah bersifat akurat dan lengkap.
5. Data sumber yang tidak akurat atau yang tidak memiliki otorisasi yang tepat diidentifikasi dan ditangani sesuai dengan kebijakan manajerial yang telah ditetapkan.
6. File data komputer telah akurat, lengkap dan dijaga kerahasiaannya.

2.2.1.7 Proses Audit

Menurut James A. Hall, struktur sebuah audit TI meliputi tiga tahap, yaitu [12]:

1. **Perencanaan audit**

   Tahap perencanaan ini memungkinkan auditor untuk memperoleh pemahaman menyeluruh terhadap proses bisnis organisasi melalui kebijakan, praktik, dan struktur organisasi. Selanjutnya auditor memahami pengendalian umum dan pengendalian aplikasi yang dimiliki organisasi. Auditor juga harus mengidentifikasi ancaman yang kemungkinan dialami organisasi dan menentukan pengendalian yang tepat untuk mengurangi ancaman tersebut. Maka

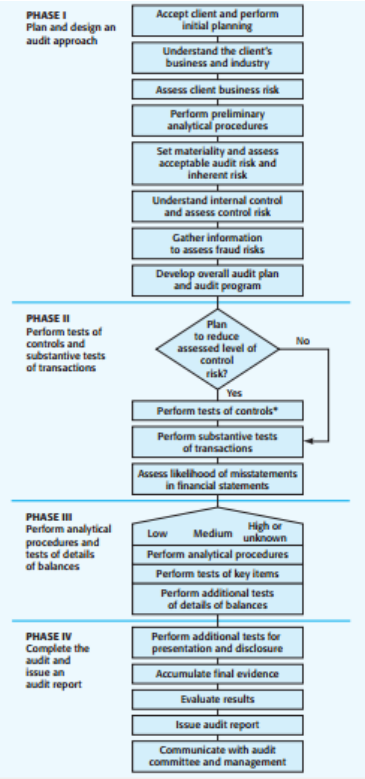
bagian utama pada tahap ini adalah analisis risiko audit, yang didapatkan melalui wawancara dengan pihak manajemen, penyebaran kuesioner, pengkajian dokumentasi sistem, dan observasi seluruh aktivitas.

2. **Pengujian terhadap pengendalian sistem**
   Tujuan pengujian pengendalian sistem adalah untuk mengetahui apakah pengendalian internal telah memadai dan berjalan dengan baik. Untuk melaksanakan tahap ini, auditor dapat menggunakan teknik pengumpulan bukti secara manual maupun dibantu teknik audit komputer.

3. **Pengujian substantif terhadap data dalam sebuah sistem.**

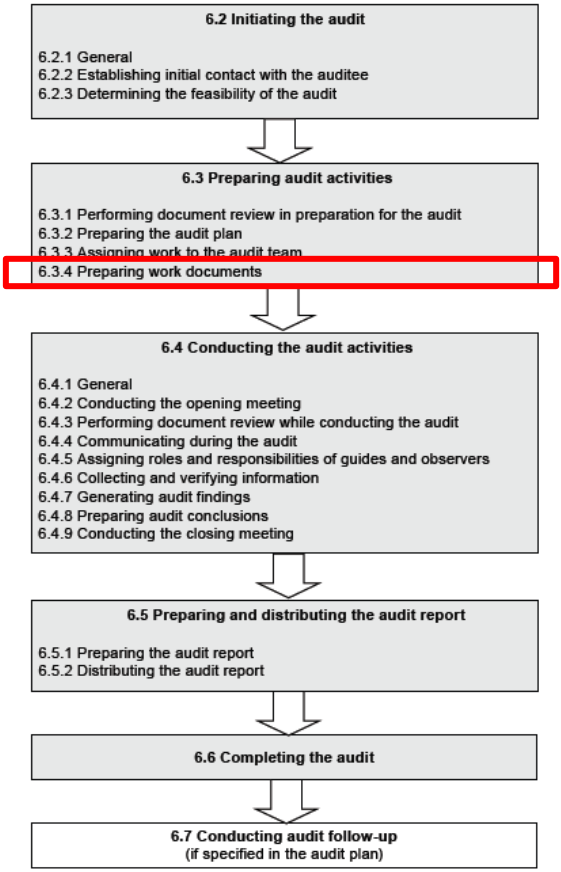
   Tahap terakhir berfokus pada data yang bersifat sangat penting, yaitu data keuangan. Informasi yang digunakan pada pengujian substantif antara lain saldo akun dan identitas pelanggan.

Menurut Alvin A. Arens, Randal J. Elder, dan Marks S. Beasley, proses audit terbagi menjadi empat tahap yang dapat dilihat pada Gambar 2.2 Proses Audit [11].



Gambar 2.2 Proses Audit (Sumber:Auditing and Assurance Services [11])

Sedangkan proses audit berdasarkan IS/ISO 19011:2011 memiliki enam tahapan proses seperti yang terdapat pada Gambar 2.3 Proses Pembuatan Perangkat [18].



Gambar 2.3 Proses Pembuatan Perangkat (Book: IS/ISO 19011:2011) [18]

Pada Gambar 2.3 terdapat pada *phase Preparing Audit Activities* yaitu *preparing Work Document* yaitu fase di mana sebuah perangkat audit dibuat. Berikut penjelasan proses pembuatan perangkat audit menurut IS/ISO 19011:2011 [18]:

1. *Initiating the Audit*

Ketika sebuah audit dimulai, tanggung jawab atas terselenggaranya audit ada pada ketua tim audit yang ditugaskan hingga audit tersebut telah selesai (tahap ke enam

pada Gambar 2.3 bagian 6.6). Langkah-langkah audit seperti pada Gambar 2.3 perlu diperhatikan, namun langkah-langkah tersebut dapat berbeda tergantung pada *auditee* dan ruang lingkup serta keadaan audit. Dalam tahap awal memulai audit terdapat 2 hal yang perlu diperhatikan, yaitu:

1.1. Pertemuan awal dengan *auditee*

Pertemuan awal ini dapat diadakan secara formal atau informal. Tujuan dari pertemuan ini adalah untuk membicarakan segala hal mengenai audit yang akan dilakukan, termasuk jadwal, tim audit, ruang lingkup audit, *auditee*, dan penyerahan tanggung jawab kepada ketua tim auditor.

1.2. Menentukan kemungkinan audit

Kemungkinan audit harus ditentukan untuk dapat memastikan tujuan dari audit dapat dicapai dengan baik. Ketika audit yang akan dilaksanakan terlihat tidak memungkinkan, auditor harus mengajukan perubahan pada klien, tentunya dengan persetujuan *auditee*.

2. *Preparing audit activities*

Hal yang perlu diperhatikan dalam tahap persiapan aktivitas audit antara lain:

2.1. Meninjau dokumen sistem manajemen untuk persiapan audit

Tahap ini dilakukan agar auditor dapat mengumpulkan informasi untuk dapat digunakan pada audit selanjutnya. Dokumen yang harus diulas antara lain dokumen sistem manajemen dan catatan-catatannya serta laporan audit sebelumnya.

2.2. Menyiapkan dokumen *audit plan*

Ketua tim audit harus menyiapkan *audit plan* berdasarkan informasi yang ada pada audit program dan pada dokumen yang telah disediakan oleh *auditee*. Detil yang ada pada *audit plan* harus

berdasarkan pada ruang lingkup dan kompleksitas audit yang dilaksanakan. *Audit plan* harus sedapat mungkin fleksibel terhadap perubahan yang mungkin diperlukan saat aktivitas audit berlangsung. *Audit plan* harus mencakup atau merujuk hal-hal berikut ini:

- Tujuan audit
- Ruang lingkup audit
- Kriteria audit
- Lokasi, tanggal, waktu yang direncanakan dan durasi audit dilaksanakan, termasuk rapat dengan pihak manajemen *auditee*
- Metode audit yang akan digunakan
- Peran dan tanggung jawab anggota tim audit

Audit plan harus dipresentasikan pada *auditee*. Kerancuan terhadap apa yang ada di *audit plan* haruslah diselesaikan antara *auditee*, audit client, dan auditor.

2.3. Pemberian tugas pada tim audit

Ketua tim audit berhak memberikan tanggung jawab kepada setiap anggota tim audit untuk mengaudit proses, aktivitas fungsi, atau lokasi tertentu. Perubahan terhadap tugas yang diberikan dapat dilakukan saat proses audit berlangsung untuk memastikan tujuan audit terpenuhi.

2.4. Menyiapkan dokumen kerja

Anggota tim audit harus mengumpulkan dan meninjau ulang informasi yang berkaitan dengan tugas audit masing-masing anggota dan menyiapkan dokumen kerja. Dalam pembuatan perangkat audit terdapat beberapa dokumen kerja yang dapat dibuat yaitu dokumen prosedur audit, daftar cek berdasarkan prosedur dan dokumen tambahan seperti *audit report* yang dapat dibuat sesuai dengan kebutuhan seperti pencatatan daftar temuan, hasil evaluasi, data

penanggung jawab, data auditor, solusi, catatan dari manajemen perusahaan, dan laporan-laporan lainnya.

3. *Conducting the audit activities*

Aktivitas audit umumnya dilaksanakan seperti yang tertera pada Gambar 2.3 yaitu:

a. Melakukan *kick-off meeting*
b. Melakukan *review* dokumen saat audit berlangsung
c. Berkomunikasi dengan tim saat audit
d. Pemberian tugas dan tanggung jawab pada pemantau audit
e. Mengumpulkan dan memverifikasi informasi
f. Membuat temuan audit
g. Menyiapkan simpulan audit
h. Melakukan *closing meeting*

4. *Preparing and distributing the audit report*

Ketua tim audit harus melaporkan hasil audit yang dilakanakan berdasarkan audit program. Laporan audit juga harus dikeluarkan dalam kurun waktu yang disetujui. Jika waktu tidak sesuai, auditor harus mengomunikasikan alasan keterlambatan kepada *auditee*. Selain itu laporan audit juga harus di beri tanggal dan disetujui oleh pihak *auditee*.

5. *Completing the audit*

Audit telah selesai ketika semua rencana aktivitas audit telah dilaksanakan dan diselesaikan, atau telah disetujui oleh *audit client* (hal in dapat terjadi ketika audit tidak dapat berjalan sesuai rencana).

Dokumen yang berkaitan dengan audit dapat disimpan atau dihancurkan sesuai dengan persetujuan pihak yang terlibat dalam audit program. Pembelajaran yang didapat saat audit harus dicatat dalam sistem manajemen organisasi yang diaudit.

6. *Conducting audit follow-up*

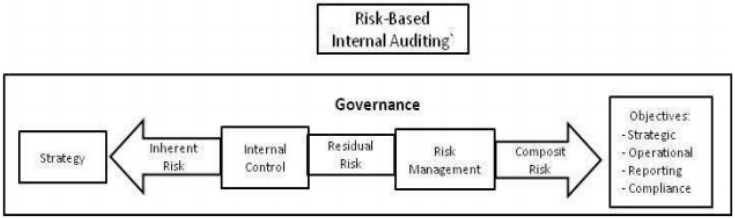
Kesimpulan dari audit yang dilakukan mungkin saja memerlukan perbaikan, baik itu aksi *corrective, preventive*,

atau *improvement*. Kegiatan tersebut biasanya dilakukan oleh *auditee* dalam kurun waktu tertentu yang sudah disetujui. *Auditee* juga harus menghubungi dan mengomunikasikan audit mengenai status kegiatan perbaikan yang dilakukan.

Berdasarkan alur proses audit dari tiga sumber berbeda, dalam penelitian ini menggunakan proses audit berdasarkan standar IS/ISO 19011:2011. Dari seluruh enam tahapan proses yang ada, dalam pengerjaan tugas akhir ini hanya akan digunakan tahap 1 dan 2 yaitu *initiating the audit* dan *preparing audit activities*. Pada tahap kedua, yaitu *preparing audit activities* yang digunakan hanya proses persiapan dokumen kerja. Pemilihan proses ini dikarenakan fokus penelitian adalah pembuatan perangkat audit, tanpa dilakukan perencanaan audit bersama tim audit. Sedangkan tahap 3 sampai 6 tidak akan dilakukan oleh penulis karena penelitian ini tidak sampai tahap melakukan proses audit.

2.2.1.8 Proses Audit Berbasis Risiko

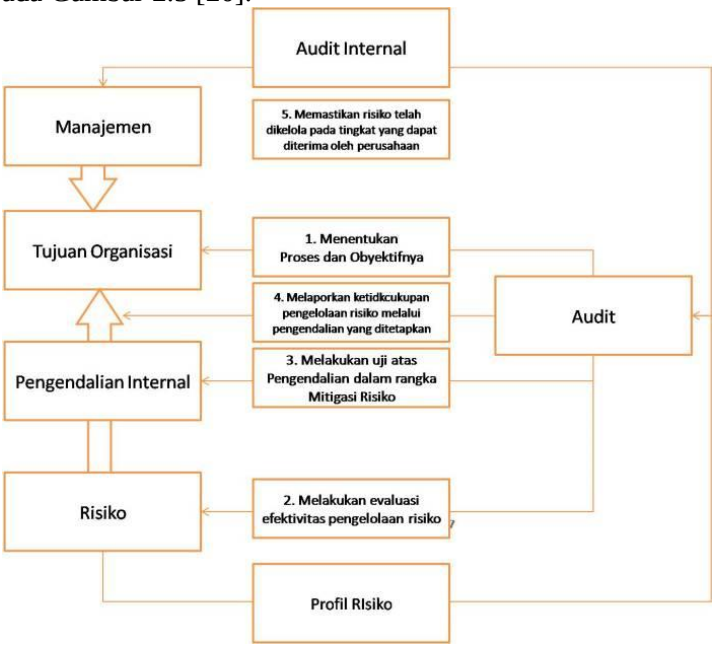
Berikut Gambar 2.4 Proses Risk-Based Auditing menjelaskan proses yang menunjukkan hubungan antara audit dan manajemen risiko [19].



Gambar 2.4 Proses Risk-Based Auditing (Book: Risk and System Based Internal Audit [19])

Melalui proses audit, auditor akan menemui risiko-risiko yang mungkin terjadi dalam organisasi sehingga risiko yang teridentifikasi akan menjadi dasar pertimbangan penentuan strategi organisasi. Risidual risk yang terjadi dari proses audit kemudian dapat diminimalisir dan ditangani melalui aktivitas manajemen risiko.

Berikut intisari dari proses audit berbasis risiko ditunjukkan pada Gambar 2.5 [20].



Gambar 2.5 Intisari Proses Audit Berbasis Risiko [20]

Proses audit berbasis risiko yang digambarkan pada alur di atas tidak mengakomodasi proses pembuatan perangkat audit, namun berelasi dengan proses audit pada acuan standar IS/ISO 19011:2011 yang digunakan dalam penelitian ini. Proses audit berbasis risiko yang dilakukan adalah proses pertama dan kedua, yaitu:

1. Menentukan proses dan obyektifnya.
2. Melakukan evaluasi efektivitas pengelolaan risiko.

2.2.2 Perangkat Audit

Menurut *TYBCom Accountancy Auditing*, sebuah program audit adalah daftar-daftar pemeriksaan dan langkah verifikasi yang harus diterapkan dan ditetapkan sedemikian hingga perancangan antar setiap langkah menunjukkan hubungan yang

jelas dan menjadi dasar penilaian terhadap suatu pelaporan/pembukuan. Dengan kata lain, program audit merupakan rincian pelaporan yang menerapkan prosedur audit berdasarkan instruksi dengan teknik yang tepat untuk mencapai tujuan audit. Hasil keluaran program audit adalah perangkat audit [4].

Perangkat audit merupakan sebuah alat atau *tools* yang dapat digunakan dalam membantu proses audit agar lebih efektif dan efisien. Dengan menggunakan sebuah perangkat audit, seorang auditor dapat menjalankan audit sesuai dengan tujuan dan selain itu juga memastikan seluruh proses audit telah dilakukan [4].

Dalam pembuatan perangkat audit pada penelitian ini mengacu pada standar IS/ISO 19011 : 2011 terkait pembuatan dokumen kerja yang akan digunakan oleh tim audit untuk mengumpulkan dan menganalisa relevansi informasi dan bukti-bukti yang nantinya akan dicatat pada *audit report* [18]. Pembuatan isi konten pada perangkat audit ini dapat berubah sewaktu-waktu sesuai dengan kebutuhan perubahan pada objek yang akan di audit. Perubahan pada objek ini dapat berupa pembaharuan pada aktivitas operasional organisasi, analisis risiko kondisi terkini organisasi, serta pembaharuan konten pada standar kontrol yang digunakan organisasi.

Berikut beberapa penjelasan singkat mengenai perangkat audit yang akan dibuat pada penulisan ini mengacu IS/ISO 19011:2011 [18]:

1. **Prosedur Audit**
   Dokumen prosedur atau skenario langkah-langkah untuk *control objective* yang telah dianalisis. Pada prosedur audit ini di dalamnya akan berisi langkah-langkah sesuai dengan *control objective* yang dilengkapi dengan *flow activity*.
2. **Daftar Cek**
   Daftar cek ini dibuat untuk mengetahui apakah aktivitas yang ada pada setiap prosedur sudah atau

belum berjalan. Dimana dalam daftar cek ini akan dilengkapi dengan tempat penulisan sebuah bukti (*evidence*) yang akan membantu auditor untuk membuat temuan dan dicatatkan pada *audit report*.

3. **Audit Report atau Laporan Temuan Audit**
   Dibuat sesuai dengan kebutuhan seperti pencatatan daftar temuan, hasil evaluasi, data penanggung jawab, data auditor, solusi, catatan dari manajemen organisasi, dan laporan-laporan lainnya.
4. **Panduan Penggunaan Perangkat Audit**
   Panduan ini dibuat untuk memudahkan tim audit internal untuk melakukan audit dan mengoperasikan perangkat yang telah dibuat. Panduan penggunaan perangkat audit ini nantinya akan berisi langkah-langkah dan tata-cara penggunaan perangkat audit yang telah dibuat pada tahapan sebelumnya.

Dalam penelitian ini akan menghasilkan dua dokumen, yaitu:

1. **Dokumen Perangkat Audit** – berisi Prosedur Audit, Daftar Cek, dan Laporan Temuan Audit.
2. **Dokumen Panduan Penggunaan Perangkat Audit** – berisi langkah-langkah dan tata-cara penggunaan dokumen perangkat audit

Dalam pembuatan perangkat audit terdapat beberapa hal yang harus diperhatikan seperti:

1. Mempunyai tujuan yang jelas dan lengkap
2. Bebas dari kesalahan, baik dalam penghitungan/ pengukuran maupun dalam penyajian data/informasi
3. Didasarkan atas fakta dan argumentasi yang rasional
4. Sistematis, mudah diikuti dan diatur rapi
5. Memuat hal-hal yang penting dan relevan dengan pekerjaan audit
6. Sedapat mungkin menghindari pekerjaan menyalin
7. Informasi dan pengguna perangkat audit ini juga harus didefinisikan dengan jelas

2.2.3 Analisis Risiko TI

Risiko merupakan pemaparan terhadap kemungkinan adanya kerugian, cedera, atau keadaan yang merugikan dan yang tidak diinginkan lainnya [21]; peristiwa yang tidak pasti atau kondisi yang, jika terjadi, memiliki efek pada setidaknya satu proyek tujuan [22]. Menurut Metinaro, Risiko Teknologi Informasi (TI) merupakan risiko yang berkaitan dengan teknologi informasi yang mana dari sudut pandang ilmu manajemen risiko secara umum dan industri finansial, merupakan bagian dari risiko operasional [23]. Sedangkan berdasarkan ISO (*International Standard Operation*), risiko SI/TI adalah suatu potensi yang mana ancaman yang ada akan mengeksploitasi kerentanan dari aset atau gabungan aset yang dapat menyebabkan bahaya bagi organisasi [24].

Risiko TI membutuhkan adanya suatu pengelolaan yang sistematik dari organisasi sehingga meminimalisir dampak atau bahkan meniadakan terjadinya risiko tersebut. Oleh karena itu, organisasi membutuhkan suatu manajemen risiko TI yang merupakan proses pengidentifikasian, penilaian, dan prioritas risiko dengan tujuan untuk lebih mengkoordinasi sumber daya perusahaan agar lebih tepat sasaran untuk meminimalkan, memantau, dan mengendalikan kemungkinan terjadinya sebuah risiko dan dampak yang dapat ditimbulkan oleh risiko tersebut [25]. Sedangkan menurut Hubbard, Manajemen Risiko TI merupakan proses pengidentifikasian, penilaian, dan prioritas risiko dengan tujuan untuk lebih mengkoordinasi sumber daya perusahaan agar lebih tepat sasaran untuk meminimalkan, memantau, dan mengendalikan kemungkinan terjadinya sebuah risiko dan dampak yang dapat ditimbulkan oleh risiko tersebut. Proses analisis risiko TI merupakan bagian dari aktivitas manajemen risiko TI, termasuk diantaranya tahap identifikasi, penilaian, dan prioritas risiko [26].

2.2.4 Kerangka Kerja Analisis Risiko

Keberhasilan analisis risiko risiko tergantung pada efektivitas kerangka manajemen risiko diimplementasikan pada sebuah

organisasi. Kerangka kerja membantu dalam menganalisis risiko secara efektif melalui penerapan proses manajemen risiko pada berbagai tingkat dan dalam konteks tertentu sebuah organisasi. Tujuan dari kerangka kerja manajemen risiko yaitu memastikan bahwa informasi tentang risiko yang berasal dari proses manajemen risiko secara memadai dilaporkan dan digunakan sebagai dasar pengambilan keputusan serta kerangka kerja membantu pemenuhan akuntabilitas di semua tingkat organisasi yang relevan [27]. Untuk dapat melakukan analisis risiko dengan baik, diperlukan kerangka kerja tersertifikasi dan metode-metode atau landasan-landasan yang dapat dijadikan sebagai dasar pedoman pengelolaan risiko yang sesuai dengan arahan dan permasalahan yang dihadapi organisasi tersebut.

Terdapat banyak *best practice* yang menyediakan kerangka kerja untuk melakukan analisis risiko dalam proses manajemen risiko, contoh diantaranya adalah OCTAVE, ISO 31000, COSO ERM, dan COBIT 5 *for Risk.* OCTAVE merupakan metode kerangka kerja manajemen risiko berbasis aset kritis di mana risiko dikelompokkan berdasarkan aset kritis organisasi, namun kelemahan dari metode ini adalah tidak adanya kerangka kerja penilaian risiko sehingga membutuhkan metode lain dalam penilaian [28]. Sedangkan ISO 31000, COSO ERM, dan COBIT 5 memiliki kerangka kerja penilaian risiko, namun kekurangan dari ISO 31000 dan COSO ERM adalah hanya mengidentifikasi risiko berdasarkan apa saja yang mempengaruhi pencapaian sasaran organisasi, bukan berbasis proses atau aktivitas dalam organisasi tersebut [29].

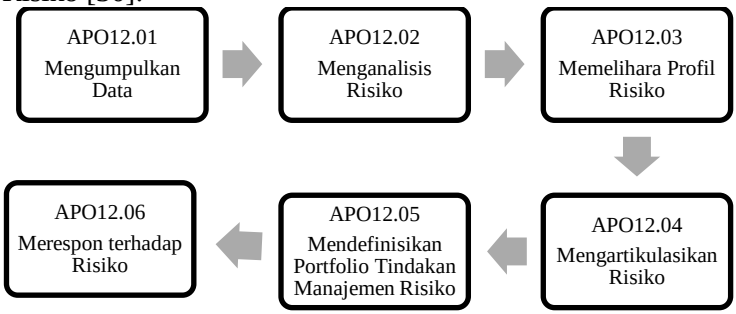
Best practice COBIT 5 dapat membantu organisasi dalam mengidentifikasi risiko berbasis proses terkait TI yang dilakukan oleh organisasi. Identifikasi risiko berbasis proses terkait TI bersifat komprehensif. Hal ini ditunjukkan oleh COBIT 5 *for Risk* yang menyediakan pemahaman tentang seberapa efektif dan efisien manajemen risiko TI dapat mengoptimalkan proses bisnis organisasi serta meningkatkan kualitas dan mengurangi kerugian [30]. Oleh karena itu, pada

penelitian ini dilakukan analisis risiko berdasarkan pendekatan COBIT 5 *for Risk*.

2.2.5 COBIT 5 for Risk

COBIT 5 *for Risk* merupakan panduan komprehensif atau kerangka kerja yang khusus dibuat untuk mengatur/mengelola risiko TI di dalam organisasi/perusahaan. COBIT 5 *for Risk* memiliki perspektif manajemen risiko yang mendeskripsikan bagaimana proses manajemen risiko utama dalam mengidentifikasi, menganalisis, dan merespon risiko. Perspektif ini membutuhkan proses risiko utama, yaitu COBIT 5 EDM03 *Ensure Risk Optimisation* dan APO12 *Manage Risk* [2]. Aktivitas manajemen risiko pada penelitian ini berfokus pada praktik terbaik sesuai kerangka kerja COBIT 5 *for Risk* domain APO12 *Manage Risk.*

The Process Risk Management APO12 dalam kerangka kerja COBIT 5 *for Risk* memiliki beberapa proses yang mendefinisikan pengelolaan risiko TI, berikut ditunjukkan alur proses mengelola risiko pada Gambar 2.6 Proses Mengelola Risiko [30]:



Gambar 2.6 Proses Mengelola Risiko

Pada pembuatan perangkat audit berbasis risiko, proses pengelolaan risiko berdasarkan COBIT 5 *for Risk* hanya dilakukan dari tahap pertama hingga kedua, yaitu mengumpulkan data dan menganalisis risiko. Berikut

penjelasan proses dan aktivitas pada tahap mengumpulkan data dan menganalisis risiko [30].

2.2.5.1 Mengumpulkan Data

2.2.5.1.1 Mengumpulkan Informasi terkait Risiko TI

Melakukan survei dan analisis data historis risiko TI dan pengalaman kerugian dari data yang tersedia secara eksternal dan tren, rekan-rekan industri melalui *event log* berbasis industri, database, dan kesepakatan industri (*industry agreement*) untuk pengungkapan peristiwa yang umum [30].

2.2.5.1.2 Membuat Daftar Risiko dan Menentukan Tipe Risiko

Pada proses ini dilakukan pembuatan daftar resiko yang didokumentasikan dalam *risk event* dan menentukan tipe risiko berdasarkan pada *type of risk event* dapat dibagi menjadi tiga kategori yaitu sebagai berikut [30].

a. ***IT benefit / value enablement risk***
Merupakan tipe risiko di mana dapat berkesempatan untuk menggunakan teknologi dalam meningkatkan efisiensi atau efektifitas bisnis proses atau sebagai enabler untuk inisiatif bisnis baru.

b. ***IT programme and project delivery risk***
Merupakan tipe risiko dimana kontribusi TI untuk memperbarui atau meningkatkan solusi bisnis, biasanya dalam bentuk proyek dan program.

c. ***IT operations and service delivery risk***
Merupakan tipe risiko dimana berhubungan dengan stabilitas operasional, ketersediaan, dan pemulihan layanan TI, yang dapat membawa kehancuran atau penurunan nilai perusahaan.

Pada setiap risiko yang sudah diidentifikasi dilakukan kategorisasi untuk setiap tipe risiko (*type of risk event*) berdasarkan kepentingan tipe skenario risiko tersebut. Tipe risiko dikategorisasikan dalam dua hal yaitu [30]:

- '**P**' untuk tipe skenario risiko yang menunjukkan primer atau menunjukkan tingkat yang lebih tinggi
- '**S**' untuk tipe skenario risiko menunjukkan sekunder atau menunjukkan tipe yang lebih rendah.

2.2.5.1.3 Menentukan Kategori Risiko

Berikut merupakan daftar 20 kategori risiko ditunjukkan pada Tabel 2.2 [30].

Tabel 2.2 Kategori Risiko

No.	Kategori
1	*Portfolio establishment and maintenance*
2	*Programme/ projects life cycle management (programme/ project initiation, economics, delivery, quality and termination)*
3	*IT investment decision making*
4	*IT expertise and skills*
5	*Staf operations (human error and malicious intent)*
6	*Information (data breach: damage, leakage and access)*
7	*Architectural (vision and design)*
8	*Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)*
9	*Software*
10	*Business ownership of IT*
11	*Supplier selection/performanse, contractual compliance, termination of service and transfer*
12	*Regulatory compliance*
13	*Geopolitical*
14	*Insfrastructure theft or destruction*
15	*Malware*
16	*Logical attacks*
17	*Industrial action*
18	*Environmental*
19	*Acts of Nature*
20	*Innovation*

2.2.5.1.4 Menentukan Faktor Risiko

Faktor risiko adalah suatu kondisi yang mempengaruhi frekuensi dan dampak bisnis terhadap skenario risiko. Faktor risiko dapat dibedakan menjadi dua, yaitu berdasarkan faktor kontekstual dan faktor kapabilitas [30]. Pada penelitian ini akan digunakan faktor risiko kontekstual. Faktor risiko kontekstual dibagi menjadi faktor internal dan eksternal [30].

- **Internal Contextual Factors** – sebagian besar berada di bawah kendali perusahaan meskipun tidak selalu mudah untuk diubah. Faktor internal meliputi berikut [30]:
  - *Enterprise goals and objectives* (tujuan perusahaan)
  - *Strategic importance of IT in the enterprise* (kepentingan strategis TI dalam perusahaan)
  - *Complexity of IT* (kompleksitas TI)
  - *Complexity of the enterprise* (kompleksitas perusahaan)
  - *Degree of change* (tingkat perubahan)
  - *Change management capability* (kapabilitas manajemen perubahan)
  - *The risk management philosopy* (filosofi manajemen risiko)
  - *Operating model* (model pengoperasian)
  - *Startegic priorities* (prioritas strategis)
  - *Culture of the enterprise* (budaya perusahaan)
  - *Financial capacity* (kapasitas finansial)
  -
- **External Contextual Factors** – sebagian besar di luar kendali perusahaan. Faktor eksternal meliputi [30]:
  - *Market/economic factors* (faktor pasar/ekonomi)
  - *Rate of change in the market in which the enterprise operates* (laju perubahan dalam pasar di mana perusahaan beroperasi)
  - *Competitive environment* (lingkungan kompetitif)
  - *Geopolitical situation* (situasi geopolitik)
  - *Regulatory environment* (lingkungan peraturan)
  - *Technology status and evolution* (evolusi dan status teknologi)

- *Threat landscape* (ancaman)

2.2.5.2 Menganalisis Risiko

2.2.5.2.1 Membuat Skenario Risiko

Selanjutnya dilakukan pembuatan dan pembaharuan skenario risiko TI secara teratur, termasuk skenario untuk risiko yang tidak terduga, dan dikembangkan menjadi aktivitas kontrol yang lebih spesifik. Pada tahap ini dilakukan pembuatan skenario berdasarkan dua jenis, yaitu skenario positif dan skenario negatif. Skenario positif menunjukkan apabila risiko TI tidak terjadi, maka peluang apa yang akan dimiliki organisasi. Sedangkan skenario negatif menunjukkan apabila risiko TI terjadi, maka kerugian apa yang dapat dialami oleh organisasi [30].

2.2.5.2.2 Melakukan Penilaian Risiko

Penilaian risiko menggunakan perkiraan frekuensi dan dampak (*magnitude*) untuk setiap risiko. Berdasarkan perkiraan frekuensi dan dampak ini, akan didapatkan hasil level setiap risiko [30].

a. Frekuensi

Frekuensi terjadinya risiko merupakan pengukuran tingkat seberapa sering suatu kejadian atau skenario risiko terjadi selama satu tahun. Berikut adalah ukuran parameter yang digunakan dalam menentukan tingkat frekuensi terjadinya risiko menggunakan skala angka 1 hingga 5 ditampilkan pada Tabel 2.3 [9] [30].

Tabel 2.3 Skala Penilaian Frekuensi Risiko

Peringkat Frekuensi	Frekuensi Skenario	Keterangan
1	$N \leq 0{,}1$	**Very Low** - Kemungkinan skenario risiko terjadi sangat rendah. - Ada kemungkinan terjadi dalam keadaan yang sangat khusus (kemungkinan kecil).

Peringkat Frekuensi	Frekuensi Skenario	Keterangan
		- Frekuensi kegagalan terjadi kurang dari sama dengan 0,1 kali dalam satu tahun.
2	$0{,}1 < N \leq 1$	**Low** - Kemungkinan skenario risiko terjadi rendah. - Mungkin terjadi dalam beberapa keadaan. - Frekuensi kegagalan terjadi lebih dari 0,1 kali dan kurang dari sama dengan 1 kali dalam satu tahun.
3	$1 < N \leq 10$	**Moderate** - Kemungkinan skenario risiko terjadi cukup tinggi. - Cenderung terjadi pada beberapa keadaan (kadang-kadang terjadi). - Frekuensi kegagalan terjadi lebih dari 1 dan kurang dari sama dengan 10 kali dalam satu tahun.
4	$10 < N \leq 100$	**High** - Kemungkinan skenario risiko terjadi tinggi. - Ada kemungkinan terjadi pada sebagian besar keadaan (mungkin terjadi). - Frekuensi kegagalan terjadi lebih dari 10 kali dan kurang dari sama dengan 100 kali dalam satu tahun.
5	$100 < N$	**Very High** - Skenario risiko sangat tidak mungkin untuk dihindari. - Cenderung terjadi pada sebagian besar keadaan (sering terjadi). - Frekuensi terjadinya kegagalan sangat tinggi, yaitu lebih dari 100 kali dalam satu tahun.

Keterangan : N adalah jumlah terjadinya skenario risiko setiap tahun

b. Dampak (*Magnitude*)

Magnitude atau dampak merupakan pengukuran tingkat keparahan potensi kerugian atau potensi keuntungan dari terjadinya skenario risiko terhadap bisnis. Terdapat empat dampak skenario pada bisnis, antara lain produktivitas (*productivity*), biaya tanggapan (*cost of response*), keunggulan kompetitif (*competitive advantage*), dan hukum (*legal*) di mana setiap dampak memiliki pengukuran parameter. Berikut adalah ukuran parameter yang digunakan dalam menentukan tingkat dampak akibat terjadinya skenario risiko menggunakan skala angka 1 hingga 5 ditampilkan pada Tabel 2.4 [9] [30]. Nilai mata uang yang digunakan adalah rupiah dengan ukuran parameter yang disesuaikan dengan kondisi DPTSI.

Tabel 2.4 Skala Penilaian Dampak Risiko

Peringkat Dampak	**Dampak**			
	Produktivitas	**Biaya Tanggapan**	**Keunggulan Kompetitif**	**Hukum**
	Rugi Pendapatan Selama Satu Tahun	Beban terkait dengan Mengelola Kejadian yang Merugikan	Penurunan Kepuasan Pengguna	Kepatuhan terhadap Peraturan - Denda
1	I≤1%	I≤Rp1juta	I ≤ 1	<Rp1 juta
2	1%<I≤3%	Rp1juta<I≤Rp10juta	1 < I ≤ 1,5	<Rp10 juta
3	3%<I≤5%	Rp10juta<I≤Rp100 juta	1,5 < I ≤ 2	<Rp100 juta
4	5%<I≤10%	Rp100juta<I≤Rp500 juta	2 < I ≤ 2,5	<Rp500 juta
5	10%<I	Rp500 juta<I	2,5 < I	>Rp500 juta

Keseluruhan peringkat dampak (empat dampak) kemudian dirata-rata sehingga memiliki satu penilaian peringkat dampak.

Justifikasi ukuran parameter serta keterangan peringkat frekuensi dan dampak akan dimodifikasi dan disesuaikan dengan kondisi organisasi DPTSI. Berikut pemaparan secara detail untuk justifikasi pengukuran parameter setiap dampak.

- Produktivitas

  Produktivitas dilihat dari dampak kerugian pendapatan yang dialami ITS selama kurun waktu satu tahun. Bentuk kerugian yang dialami ITS dapat dilihat dari beberapa aspek, antara lain:
  - Lambatnya kinerja staf DPTSI yang mengelola permintaan layanan dan insiden sehingga proses bisnis ITS terhambat
  - Kerugian finansial yang dialami ITS
  - Kerusakan terhadap aset milik DPTSI dan ITS sehingga tidak layak/tidak dapat digunakan.

  Setiap aspek kerugian dihitung berupa kerugian persentase (%) yang dialami ITS selama kurun waktu satu tahun. Berikut pemaparan justifikasi dampak produktivitas menggunakan skala angka 1 hingga 5 ditunjukkan pada Tabel 2.5.

Tabel 2.5 Skala Penilaian Dampak Produktivitas

Peringkat Dampak	**Produktivitas**	
	Rugi Pendapatan/th	Keterangan
1	I≤1%	**Very Low** - Kegagalan menimbulkan kerugian yang sangat rendah - Kerugian yang dialami melalui beberapa aspek sebesar kurang dari sama dengan 1% dalam satu tahun
2	1%<I≤3%	**Low** - Kegagalan menimbulkan kerugian yang rendah

Peringkat Dampak	Produktivitas	
	Rugi Pendapatan/th	Keterangan
		- Kerugian yang dialami melalui beberapa aspek sebesar lebih dari 1% dan kurang dari sama dengan 3% dalam satu tahun
3	3%<I≤5%	**Moderate** - Kegagalan menimbulkan kerugian yang cukup merugikan - Kerugian yang dialami melalui beberapa aspek sebesar lebih dari 3% dan kurang dari sama dengan 5% dalam satu tahun
4	5%<I≤10%	**High** - Kegagalan menimbulkan kerugian yang tinggi - Kerugian yang dialami melalui beberapa aspek sebesar lebih dari 5% dan kurang dari sama dengan 10% dalam satu tahun
5	10%<I	**Very High** - Kegagalan menimbulkan kerugian yang sangat tinggi - Kerugian yang dialami melalui beberapa aspek sebesar lebih dari 10%

- Biaya Tanggapan

  Biaya tanggapan (*cost of response*) merupakan biaya yang harus dikeluarkan oleh ITS dalam menangani kejadian yang merugikan dari setiap skenario risiko yang terjadi. Berikut pemaparan justifikasi dampak biaya tanggapan menggunakan skala angka 1 hingga 5 ditunjukkan pada Tabel 2.6.

Tabel 2.6 Skala Penilaian Dampak Biaya Tanggapan

Peringkat Dampak	Biaya Tanggapan	
	Beban terkait dengan Mengelola Kejadian yang Merugikan	Keterangan
1	I≤Rp1juta	**Very Low**

Peringkat Dampak	Biaya Tanggapan	
	Beban terkait dengan Mengelola Kejadian yang Merugikan	Keterangan
		Untuk menangani skenario risiko, organisasi mengeluarkan biaya yang sangat rendah, yaitu kurang dari sama dengan satu juta rupiah.
2	Rp1juta<I≤Rp10juta	**Low** Untuk menangani skenario risiko, organisasi mengeluarkan biaya yang rendah, yaitu lebih dari satu juta rupiah dan kurang dari sama dengan sepuluh juta rupiah.
3	Rp10juta<I≤Rp100 juta	**Moderate** Untuk menangani skenario risiko, organisasi mengeluarkan biaya yang cukup membebani, yaitu lebih dari sepuluh juta rupiah dan kurang dari sama dengan seratus juta rupiah.
4	Rp100juta<I≤Rp500 juta	**High** Untuk menangani skenario risiko, organisasi mengeluarkan biaya yang tinggi, yaitu lebih dari seratus juta rupiah dan kurang dari sama dengan lima ratus juta rupiah.
5	Rp500 juta<I	**Very High** Untuk menangani skenario risiko, organisasi mengeluarkan biaya yang sangat tinggi, yaitu lebih dari lima ratus juta rupiah.

- Keunggulan Kompetitif
  Merupakan dampak penurunan kepuasan pengguna layanan akibat terjadinya setiap skenario risiko. Indeks

penurunan kepuasan pengguna didapatkan dari hasil survei yang dilakukan oleh DPTSI kepada pengguna layanan *service desk*. Indeks penurunan kepuasan pengguna ini diberi angka skala likert 1-5. Semakin kecil angka indeks menunjukkan semakin rendah penurunan kepuasan pengguna, begitu juga sebaliknya. Berikut pemaparan justifikasi dampak keunggulan kompetitif menggunakan skala angka 1 hingga 5 ditunjukkan pada Tabel 2.7.

Tabel 2.7 Skala Penilaian Dampak Keunggulan Kompetitif

Peringkat Dampak	**Keunggulan Kompetitif**	
	Penurunan Kepuasan Pengguna	Keterangan
1	$I \leq 1$	**Very Low** Kegagalan menyebabkan penurunan yang sangat tidak signifikan (sangat rendah) terhadap kepuasan pengguna layanan
2	$1 < I \leq 1{,}5$	**Low** Kegagalan menyebabkan penurunan yang tidak signifikan (rendah) terhadap kepuasan pengguna layanan
3	$1{,}5 < I \leq 2$	**Moderate** Kegagalan menyebabkan penurunan yang cukup signifikan terhadap kepuasan pengguna layanan
4	$2 < I \leq 2{,}5$	**High** Kegagalan menyebabkan penurunan yang signifikan (tinggi) terhadap kepuasan pengguna layanan
5	$2{,}5 < I$	**Very High** Kegagalan menyebabkan penurunan yang sangat signifikan (sangat tinggi) terhadap kepuasan pengguna layanan

Keterangan : I adalah *impact* berupa indeks kepuasan pengguna.

- Hukum
  Merupakan dampak berupa biaya denda yang harus ditanggung oleh ITS akibat dari terjadinya risiko yang terkait dengan hukum. Nilai pengukuran berupa biaya (rupiah). Berikut pemaparan justifikasi dampak terkait hukum menggunakan skala angka 1 hingga 5 ditunjukkan pada Tabel 2.8.

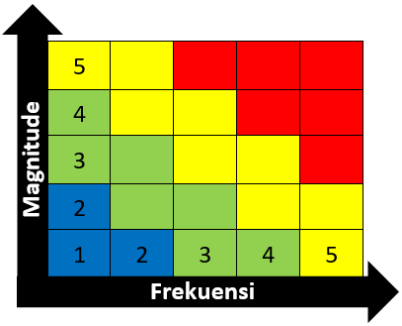
Tabel 2.8 Skala Penilaian Dampak Hukum

Peringkat Dampak	Hukum	
	Kepatuhan terhadap Peraturan - Denda	Keterangan
1	<Rp1 juta	Organisasi mengeluarkan biaya berupa denda atas terjadinya risiko terkait ketidakpatuhan terhadap peraturan hukum sejumlah kurang dari satu juta rupiah.
2	<Rp10 juta	Organisasi mengeluarkan biaya berupa denda atas terjadinya risiko terkait ketidakpatuhan terhadap peraturan hukum sejumlah kurang dari sepuluh juta rupiah.
3	<Rp100 juta	Organisasi mengeluarkan biaya berupa denda atas terjadinya risiko terkait ketidakpatuhan terhadap peraturan hukum sejumlah kurang dari seratus juta rupiah.
4	<Rp500 juta	Organisasi mengeluarkan biaya berupa denda atas terjadinya risiko terkait ketidakpatuhan terhadap peraturan hukum sejumlah kurang dari lima ratusjuta rupiah.
5	>Rp500 juta	Organisasi mengeluarkan biaya berupa denda atas terjadinya

Peringkat Dampak	Hukum	
	Kepatuhan terhadap Peraturan - Denda	Keterangan
		risiko terkait ketidakpatuhan terhadap peraturan hukum sejumlah lebih dari lima ratus juta rupiah.

c. Level Penilaian Risiko

Melalui penilaian risiko berdasarkan frekuensi dan dampak (*magnitude*) risiko TI, didapatkan prioritas risiko berdasarkan level penilaian risiko melalui pemetaan pada suatu peta risiko yang dibagi berdasarkan empat wilayah warna. Berikut penggambaran peta risiko ditampilkan pada Gambar 2.7 [30].



Gambar 2.7 Peta Frekuensi dan Magnitude

Pemetaan frekuensi dan *magnitude* berdasarkan empat wilayah warna kemudian diklasifikasikan berdasarkan level prioritas kegagalan yang memerlukan penanganan lanjut. Berikut pemetaan level prioritas risiko ditampilkan pada Tabel 2.9 [30].

Tabel 2.9 Level Prioritas Risiko

Pemetaan Warna	Level Prioritas
Merah	Very High
Kuning	High
Hijau	Medium
Biru	Low

2.2.6 Service Desk

2.2.6.1 Pengertian Service Desk

Service desk atau istilah lainnya *Help Desk, Support Desk,* atau *IT Service Center* adalah salah satu fungsi dalam operasi layanan (*Service Operation*) sebuah organisasi yang menjadi komunikator antara penyedia layanan dengan pengguna. *Service desk* merupakan suatu unit yang sangat penting bagi sebuah organisasi khususnya divisi teknologi informasi karena merupakan satu-satunya titik kontak antara pengguna TI dan divisi TI yang berhubungan dengan insiden dan semua permintaan (*request*) terhadap layanan [31].

2.2.6.2 Tujuan Service Desk

Tujuan utama adanya *service desk* ini adalah mengembalikan sebuah pelayanan dalam keadaan normal dengan secepat mungkin. Kebanyakan di dalam *service desk* yang diselesaikan adalah sejenis insiden seperti menyelesaikan kesalahan teknis, memenuhi permintaan layanan, dan menjawab pertanyaan [31]. Pada dasarnya *service desk* bertugas memilah panggilan/laporan yang masuk apakah sebagai sebuah laporan insiden, sebuah permintaan akses, atau sebuah permintaan lainnya di luar insiden dan akses. Selanjutnya semua panggilan/laporan tersebut dicoba untuk diselesaikan sesuai dengan SOP proses masing-masing [32].

2.2.6.3 Proses Mengelola Permintaan Layanan dan Insiden pada Service Desk

Proses yang dilakukan oleh *service desk* antara lain adalah manajemen insiden dan pemintaan layanan. Berikut definisi dan tujuan dari proses manajemen insiden dan permintaan layanan [32].

2.2.6.3.1 Manajemen Insiden

Menurut terminologi ITIL, sebuah insiden didefinisikan sebagai sebuah interupsi layanan TI yang tidak direncanakan sebelumnya atau penurunan dalam kualitas suatu layanan TI. Kegagalan dalam konfigurasi uang berdampak pada layanan

juga merupakan suatu insiden. Sedangkan definisi Manajemen Insiden adalah suatu rangkaian aktivitas untuk mengatasi seluruh insiden yang dapat berupa kegagalan, pertanyaan, atau pelaporan oleh pengguna layanan TI, staf teknis, atau secara otomatis terdeteksi dan terlapor oleh suatu tool pemantau kejadian [32].
Tujuan dari proses manajemen insiden adalah untuk mengembalikan operasional normal layanan TI secepat mungkin dan meminimalkan dampak buruk gangguan layanan TI sekecil mungkin agar kualitas layanan dapat selalu terjaga [32].

2.2.6.3.2 Permintaan Layanan (Service Request)

Permintaan layanan merupakan permintaan pengguna tentang informasi tertentu, pertanyaan atau permintaan saran, perubahan yang bersifat standar, maupun akses ke suatu layanan TI [33]. Permintaan layanan pada manajemen layanan TI yang umumnya dilakukan oleh *service desk* terdiri dari dua proses, yaitu pemenuhan permintaan (*request fulfillment*) dan manajemen akses (*access management*).

a. Pemenuhan Permintaan (*Request fulfillment*)

Dalam definisi ITIL, *request fulfillment* adalah sebuah proses yang bertanggung jawab untuk mengelola siklus hidup semua permintaan layanan TI. Proses pemenuhan permintaan pengguna layanan TI, di luar laporan terkait dengan insiden TI [32]. Pemenuhan permintaan adalah proses pemenuhan permintaan layanan (*service request*) dari pengguna. Tujuan dari proses ini antara lain [32] :

- Menerima layanan standar bagi pengguna dalam menyampaikan permintaan
- Untuk menyediakan informasi kepada pengguna dan pelanggan mengenai ketersediaan layanan dan prosedur
- Untuk menyediakan komponen layanan standar yang diminta
- Untuk membantu dengan informasi umum, keluhan, atau komentar

b. Manajemen Akses *(Access management)*

Manajemen akses merupakan proses pemberian hak akses kepada pengguna yang berwenang untuk menggunakan layanan, sementara mencegah akses ke pengguna yang tidak berwenang. Kebijakan hak akses telah ditetapkan dalam proses manajemen keamanan informasi dan manajemen ketersediaan di tahapan perancangan layanan (*service design*) [32]. Aktivitas proses manajemen akses dimulai dengan permintaan akses yang dapat disampaikan dalam bentuk sebuah permintaan permintaan layanan melalui sistem pemenuhan permintaan pada *service desk* [3]. Tujuan dari manajemen akses adalah menyediakan hak bagi pengguna untuk dapat menggunakan satu atau sejumlah layanan TI [32].

2.2.7 Kerangka Kerja Mengelola Permintaan Layanan dan Insiden pada Service Desk

Pada pembuatan perangkat audit, penting untuk memahami proses ideal yang dilakukan organisasi sesuai praktik terstandar untuk kelak akan dilakukan pemeriksaan berdasarkan *control objective* pada proses tersebut [18]. Suatu kerangka kerja digunakan oleh organisasi sebagai panduan yang lebih baik dalam melakukan proses mengelola permintaan layanan dan insiden. Kerangka kerja yang menjelaskan proses pengelolaan permintaan layanan dan insiden pada *service desk* diantaranya adalah ITIL (*Information Technology Infrastructure Library*) dan COBIT 5 domain DSS02 *Manage Service Requests and Incidents.*

ITIL merupakan kerangka kerja yang menyediakan pendekatan sistematis untuk mencapai kualitas layanan TI yang dibuat berdasarkan praktek terbaik. Salah satu tahap pada ITIL adalah *Service Operation* di mana tahap ini mendefinisikan proses yang dilakukan oleh *service desk*, antara lain manajemen insiden serta permintaan layanan termasuk proses pemenuhan permintaan (*request fulfilment*) dan manajemen akses [32].

Sedangkan COBIT 5 merupakan sebuah kerangka kerja yang dibuat untuk melakukan manajemen dan tata kelola perusahaan TI yang memiliki bahasa *high level objective* [2].

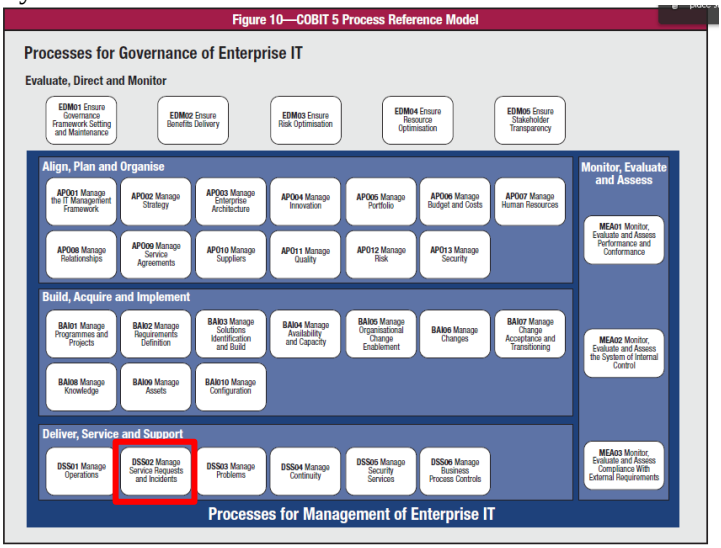
Pembuatan perangkat audit membutuhkan kontrol, di mana COBIT 5 mendetailkan proses dengan bahasa *high level objective* yang dapat mendefinisikan kontrol. Sedangkan hal tersebut tidak terdapat pada ITIL. Selain itu, ITIL lebih detail dalam memaparkan proses sedangkan COBIT 5 merangkum proses-proses besar yang ada. Hal ini menunjukkan bahwa COBIT 5 lebih efektif untuk digunakan dalam pemetaan dengan *control objective.* Oleh karena itu, penulisan tugas akhir ini menggunakan *best practice* COBIT 5 domain DSS02 *Manage Service Requests and Incidents* untuk memetakan kesesuaian proses.

2.2.8 COBIT 5 DSS02 Mengelola Permintaan Layanan dan Insiden

COBIT 5 merupakan sebuah kerangka kerja yang dibuat dengan 5 prinsip dasar dimana kerangka kerja ini dibuat lebih detail termasuk juga di dalamnya terdapat panduan yang lebih baik yang dapat digunakan untuk melakukan manajemen dan tata kelola perusahaan TI. COBIT 5 *Enabling Process* memiliki beberapa domain proses, salah satunya berkaitan dengan mengelola permintaan layanan dan insiden [2].

Mengelola permintaan layanan dan insiden pada COBIT 5 menjadi fokus pada domain *Deliver, Service, And Support* (DSS) yang ke dua yaitu *Manage Service Requests and Incidents*. Dimana dalam domain ini didefinisikan beberapa proses yang berjalan di dalamnya. *Service request* merupakan permintaan pengguna tentang informasi tertentu atau saran, perubahan yang bersfat standar, atau akses ke suatu layanan TI yang umumnya ditangani oleh *service desk* [32]. DSS02 sendiri menyediakan standarisasi respon yang efektif dan efisien untuk request dari pengguna dan memberikan resolusi untuk semua

jenis insiden. Sebagai upaya mengembalikan layanan pada kondisi normal, mencatat dan memenuhi kebutuhan user, dan melakukan investigasi, diagnosa, eskalasi, dan penanganan insiden [2]. Keseluruhan proses TI pada COBIT 5 *Enabling Process* ditunjukkan pada Gambar 2.8 Mengelola Permintaan Layanan dan Insiden.



Gambar 2.8 Mengelola Permintaan Layanan dan Insiden (ISACA, *COBIT 5: Enabling Process*) [2]

Terdapat tujuh proses (*key management practice*) yang ada di dalam DSS02 yang juga akan dijadikan sebagai proses ideal dalam pembuatan perangkat audit :

- DSS02.01 : Mendefinisikan skema klasifikasi insiden dan permintaan layanan
  - ✓ Mendefinisikan skema klasifikasi dan prioritisasi insiden dan permintaan layanan dan kriteria untuk pendaftaran masalah, untuk memastikan pendekatan yang konsisten dalam menangani, menginformasikan pengguna dan melakukan analisis tren

- ✓ Menetapkan model insiden terhadap error yang diketahui untuk meningkatkan efisiensi dan efektifitas resolusi penyelesaian masalah
- ✓ Mendefinisikan model permintaan layanan berdasarkan tipe permintaan layanan untuk meningkatkan layanan yang bersifat mandiri dan efisien untuk permintaan-permintaan yang standar
- ✓ Mendefinisikan aturan dan prosedur eskalasi insiden, khususnya pada insiden yang utama dan insiden keamanan
- ✓ Mendefinisikan sumber pengetahuan mengenai insiden dan permintaan dan cara penggunaannya

- DSS02.02 : Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden
  - ✓ Mencatat semua permintaan layanan dan insiden, serta merekam semua informasi yang relevan sehingga dapat ditangani secara efektif dan semua rekaman terdahulu yang ada dapat di kelola
  - ✓ Memungkinkan analisis tren, klasifikasi permintaan layanan dan insiden dengan mengidentifikasi tipe dan kategori
  - ✓ Memprioritaskan permintaan layanan dan insiden berdasarkan layanan SLA yang mendefinisikan pengaruh bisnis dan urgensi
- DSS02.03 : Memverifikasikan, menyetujui dan memenuhi permintaan layanan
  - ✓ Melakukan verifikasi terhadap hak untuk menggunakan permintaan layanan, jika dimungkinkan, alur proses yang telah didefinisikan dan perubahan standar
  - ✓ Memperoleh persetujuan finansial dan fungsional atau tanda tangan, jika dibutuhkan, atau persetujuan otomatis untuk persetujuan dalam perubahan yang standar
  - ✓ Memenuhi permintaan dengan cara memilih prosedur permintaan, jika memungkinkan menggunakan menu bantuan mandiri dan model permintaan yang telah

dibuat sebelumnya untuk item – item yang sering diminta

- DSS02.04 : Menginvestigasikan, mendiagnosis dan mengalokasikan insiden
  - ✓ Mengidentifikasi dan mendeskripsikan gejala yang relevan untuk menetapkan kemungkinan penyebab insiden. Mereferensikan sumber pengetahuan yang tersedia (termasuk eror dan permasalahan yang diketahui) untuk mengidentifikasikan penyelesaian insiden (baik secara sementara dan atau permanen)
  - ✓ Mencatat permasalahan baru jika masalah terkait atau kesalahan yang diketahui belum ada dan jika memenuhi kriteria insiden yang disetujui untuk pendaftaran masalah
  - ✓ Memberikan insiden kepada fungsi spesialis jika keahlian yang lebih dalam diperlukan, dan melibatkan level manajemen yang tepat jika dibutuhkan
- DSS02.05 : Menyelesaikan dan Memulihkan Insiden
  - ✓ Memilih dan menerapkan penyelesain insiden yang paling tepat (baik solusi secara sementara dan atau permanen)
  - ✓ Merekam apakah solusi digunakan untuk penyelesaian insiden sebelumnya
  - ✓ Melaksanankan aksi pemulihan jika dibutuhkan
  - ✓ Mendokumentasikan penyelesaian insiden dan menilai jika penyelasaian dapat digunakan untuk sumber pengetahuan kedepannya
- DSS02.06 : Menutup Permintaan Layanan dan Insiden
  - ✓ Melakukan verifikasi kepuasan dalam pemenuhan permintaan layanan dan penyelesaian insiden terhadap pengguna yang terlibat
  - ✓ Menutup permintaan layanan dan insiden
- DSS02.07 : Melacak Status dan Membuat Laporan
  - ✓ Memantau dan menelusuri peningkatan insiden, penyelesaian, dan prosedur permintaan pengelolaan untuk menuju penyelesain masalah

- ✓ Melakukan identifikasi informasi pemangku kepentingan (*stakeholders*) dan kebutuhan mereka terhadap data atau laporan serta mengidentifikasi frekuensi dan perantara laporan
- ✓ Menganalisis insiden dan permintaan layanan berdasarkan kategori dan tipe untuk menetapkan trend dan mengidentifikasi pola dari masalah yang berulang, pelanggaran atau ketidakefisiensian SLA. Kemudian menggunakan informasi tersebut sebagai input dalam perencanaan peningkatan berlanjut.
- ✓ Membuat dan mendistribusikan laporan secara tepat waktu atau menyediakan akses data yang dikontrol secara *online*.

2.2.9 Service Desk Standard

Service Desk Standard merupakan standar yang diterbitkan oleh *Service Desk Institute* (SDI) yang merepresentasikan standar kualitas untuk proses manajemen *service desk* dan komitmen untuk peningkatan pelayanan terus-menerus. *Service Desk Standard* telah dirancang untuk melihat secara dekat seluruh aspek operasi *service desk* dalam hal manajemen staf, sumber daya, peralatan, pelatihan dan pengiriman, strategi, perencanaan, dan peningkatan pelayanan terus-menerus. *Service Desk Standard* merupakan *best practice* yang menawarkan pengukuran yang jelas dan terukur untuk operasi *service desk*. *Service Desk Standard* terdiri dari sembilan konsep beserta sub-konsep di dalamnya. Pada sub-konsep terdapat kendali tujuan (*control objective*). Berikut sembilan konsep *Service Desk Standard* [34]:

- *Concept 1 – Leadership* mengenai bagaimana seluruh tingkat manajemen dan staf lain dalam peran tim kepemimpinan mendefinisikan kesuksesan, serta menginspirasi dan menyampaikan perbaikan terus-menerus.
- *Concept 2 – Policy & Strategy* mengenai manajemen *service desk* menggabungkan nilai-nilai organisasi ke

dalam definisi, komunikasi, ulasan, serta perbaikan kebijakan dan strategi *service desk.*

- *Concept 3 – People & Management* mengenai merealisasikan potensial sumber daya manusia secara menyeluruh.
- *Concept 4 – Partnership & Resources* mengenai akses untuk kebutuhan sumber daya dan *tools* untuk mencapai tujuan.
- *Concept 5 – Processes & Procedures* mengenai bagaimana operasi pendukung TI mengidentifikasi, mengulas, mendokumentasikan, dan merevisi proses dan prosedurnya dengan tujuan untuk mengoptimalkan tingkat dukungan.
- *Concept 6 – Managing People Satisfaction* mengenai staf pendukung menyampaikan kualitas layanan dan dukungan.
- *Concept 7 – Managing Customer Satisfaction* mengenai informasi kepuasan pengguna yang dicatat dan digunakan untuk mencapai tujuan organisasi dan ekspektasi pelanggan.
- *Concept 8 – Performance Results* mengenai hasil kinerja operasi pendukung TI diukur melalui kinerja yang telah direncanakan.
- *Concept 9 – Social Responsibility* mengenai *service desk* berusaha memahami dan menanggapi harapan pemangku kepentingan (*stakeholder*).

Pada penelitian ini, digunakan beberapa konsep dan sub-konsep sebagai kontrol untuk dipetakan pada proses terkait pengelolaan permintaan layanan dan insiden yang dilakukan oleh *service desk.* Pada **LAMPIRAN A** menjabarkan kontrol terkait manajemen insiden dan permintaan layanan pada standar.

2.2.10 Service Desk DPTSI

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) merupakan unit yang bertugas untuk menyediakan dan mengelola layanan Teknologi Informasi di lingkungan Institut

Teknologi Sepuluh Nopember (ITS) Kota Surabaya. Selain itu, DPTSI mempunyai tugas melaksanakan, mengkoordinasi, memonitor dan mengevaluasi kegiatan penelitian dan informasi berikut [1].

DPTSI memiliki tiga SubDirektorat, antara lain SubDirektorat Infrastruktur dan Keamanan Teknologi Informasi, SubDirektorat Pengembangan Sistem Informasi, serta SubDirektorat Layanan Teknologi dan Sistem Informasi [1]. SubDirektorat Layanan Teknologi dan Sistem Informasi memiliki tugas untuk menyediakan layanan TI kepada pengguna. Salah satu bentuk penyediaan layanan TI bagi pengguna, SubDirektorat Layanan Teknologi dan Sistem Informasi memiliki suatu unit fungsional *service desk* yang menangani berbagai macam keluhan dan permintaan layanan TI di lingkungan ITS. Permasalahan layanan TI yang ditangani oleh *service desk* sebagian besar terkait dengan insiden dan permintaan layanan TI seperti menyelesaikan kesalahan teknis, menjawab pertanyaan, memenuhi permintaan layanan, dan permintaan akses layanan [35].

DPTSI memiliki suatu alur penanangan permasalahan layanan TI. Mahasiswa, karyawan, dosen dan tamu dikategorikan sebagai pengguna layanan TI yang dapat melaporkan permasalahan layanan TI ke *service desk* DPTSI ITS dengan berbagai cara diantaranya melalui telepon, fax, email atau langsung mengunjungi kantor DPTSI ITS. *Service desk* DPTSI ITS mencatat permasalahan layanan TI yang dilaporkan pengguna kemudian mendistribusikannya ke setiap sub direktorat yang sesuai untuk menyelesaikan permasalahan layanan TI [35].

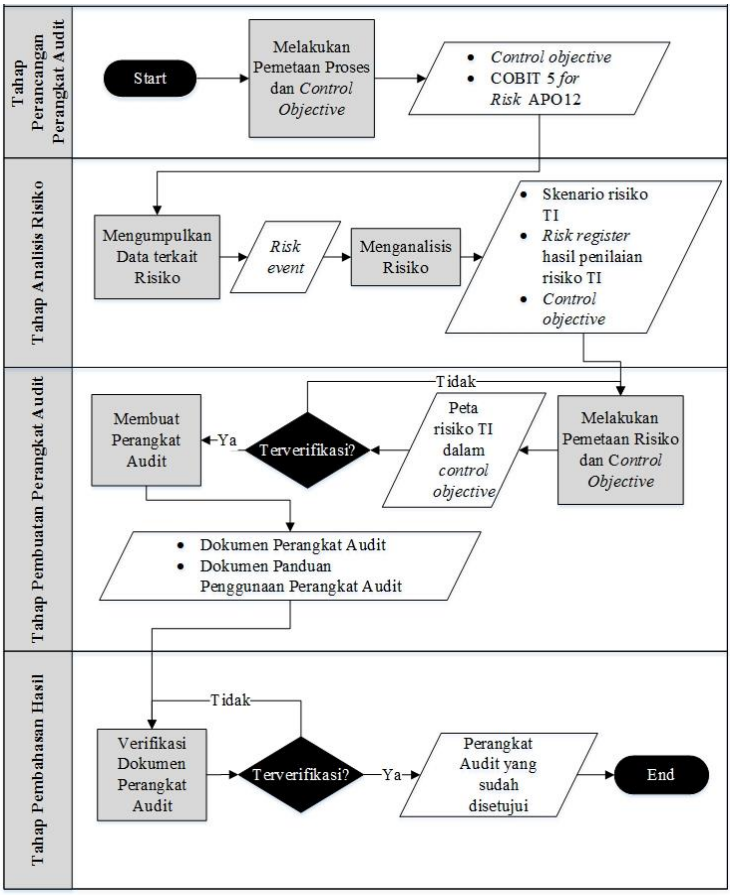
Keterkaitan antar dasar teori dalam penelitian ini digunakan untuk membuat perangkat audit berbasis risiko pada *service desk* terkait proses mengelola permintaan layanan dan insiden dengan studi kasus DPTSI ITS. Analisis risiko terkait proses

yang mengacu pada COBIT 5 DSS02 dilakukan berdasarkan kerangka kerja COBIT 5 *for Risk* APO12. Setiap risiko akan dipetakan dengan *control objective* sesuai *Service Desk Standard* yang kemudian setiap *control objective* dijadikan sebuah dokumen perangkat audit.

Halaman ini sengaja dikosongkan

BAB III
METODOLOGI PENELITIAN

Pada bab ini akan menggambarkan metodologi yang akan digunakan dalam melakukan penelitian. Metode penulisan merupakan suatu panduan dalam mengerjakan tugas akhir secara sistematis, terarah, dan jelas. Berikut Gambar 3.1 Metodologi Penelitian menunjukkan empat tahap penelitian yang disajikan dalam bentuk *flowchart*:



Gambar 3.1 Metodologi Penelitian

3.1 Tahapan Perancangan Perangkat Audit

Dalam penelitian ini, pada tahap perancangan perangkat audit merupakan tahap awal penulis melakukan aktivitas sebelum membuat perangkat audit berbasis risiko. Tahap ini harus dilakukan guna mendapat *control objective* yang akan digunakan untuk menyusun dokumen perangkat audit. Pada tahapan ini dilakukan satu tahap aktivitas, yaitu pemetaan proses dan *control objective*.

3.1.1 Melakukan Pemetaan Proses dan Control Objective

Pada tahapan ini dilakukan pemetaaan proses mengelola permintaan layanan dan insiden yang ideal pada *service desk* sesuai pendekatan *best practice* COBIT 5 DSS02 *Manage Service Requests and Incidents* dengan kontrol terkait yang harus dilakukan menggunakan standar kontrol *Service Desk Standard*. Aktivitas kontrol disebut *control objective* sebagai keluaran tahapan ini yang akan digunakan dalam kontrol mitigasi risiko TI untuk pembuatan perangkat audit.

3.2 Tahapan Analisis Risiko

Tahap kedua dalam pengerjaan penelitian ini adalah tahap analisis risiko. Pada tahap ini, penulis melakukan dua tahapan proses diantaranya adalah tahap mengumpulkan data terkait risiko dan tahap menganalisis risiko.

3.3.1 Mengumpulkan Data terkait Risiko

Pada tahapan ini dilakukan manajemen risiko berbasis proses berdasarkan *best practice* COBIT 5 *for Risk* domain APO12 *Manage Risk* pada tahap pertama, yaitu mengumpulkan data (*collect data*). Masukan pada tahap ini adalah informasi kondisi organisasi terkait risiko TI dan *best practice* COBIT 5 *for Risk* APO12. Hasil keluaran tahapan ini adalah berupa daftar risiko dalam bentuk *risk event* yang akan digunakan dalam tahap menganalisis risiko.

3.2.1.1 Mengumpulkan Informasi terkait Risiko TI

Tahap pertama dalam mengumpulkan informasi terkait risiko TI dalam proses pengelolaan permintaan layanan dan insiden. Pengumpulan data dan informasi terkait risiko TI dapat dilakukan dengan tiga cara, yaitu:

1. Wawancara
   Wawancara dilakukan secara langsung kepada bersama staf *service desk* yang bertugas secara langsung dalam operasional maupun teknis layanan teknologi informasi di DPTSI ITS. Metode ini untuk memperoleh informasi kondisi kekinian organisasi terkait proses pengelolaan layanan dan insiden pada unit *service desk* DPTSI. Informasi ini digunakan untuk menggali informasi terkait risiko TI pada prosesnya.
2. Survei
   Survei dilakukan untuk mengumpulkan data terkait dampak penurunan kepuasan pengguna layanan terhadap skenario risiko yang mungkin terjadi. Jumlah pengguna layanan *service desk* DPTSI di lingkungan ITS sangat besar sehingga ruang lingkup populasi akan dispesifikkan untuk pengguna layanan *service desk* DPTSI dari seluruh mahasiswa ITS Surabaya, yaitu 15.000 orang. Selanjutnya jumlah populasi ini akan dihitung menggunakan metode Slovin, yaitu metode yang digunakan untuk mencari jumlah sampel responden minimal. Rumus Slovin [36]:

$$n = \frac{\mathrm{N}}{1 + \mathrm{N}e^2}$$

   Keterangan :
   n = ukuran sampel;
   N = ukuran populasi;
   e = persentase toleransi kesalahan karena kesalahan pengambilan sampel.

Sehingga diperoleh :

$$n = \frac{15000}{1 + 15000\ (0{,}15)^2}$$

$$n = \frac{15000}{1 + 338{,}5}$$

$$n = 44 \text{ orang}$$

Berdasarkan perhitungan tersebut, dengan nilai e = 0,15 didapatkan sebanyak minimal 44 orang yang akan menjadi sampel dari populasi sebanyak 15.000 orang. Pada tahap ini akan digunakan metode *simple random sampling*. Selanjutnya dari tahapan ini akan dihasilkan suatu data kuesioner yang telah didapatkan dari 44 responden tersebut.

3. Studi Literatur (Dokumen)
   Studi literature dilakukan menggunakan berbagai sumber pustaka atau dokumen. Pada tahapan ini penulis mengumpulkan data terkait risiko TI pada *service desk* dari penelitian manajemen risiko TI pada manajemen layanan TI.

3.2.1.2 Membuat Daftar Risiko dan Menentukan Tipe Risiko

Setelah kita mengumpulkan data terkait risiko pada *service desk* DPTSI, yang harus dilakukan adalah mengembangkan data tersebut, maka kita lakukan aktivitas pencatatan data risiko TI yang sesuai atau relevan yang berperan signifikan dalam manajemen risiko TI yang dilakukan pada lingkungan operasional organisasi baik lingkungan internal maupun eksternal. Hasil keluaran pada tahap ini adalah tabel *risk event* yang telah dipetakan berdasarkan tipe risiko. Tipe risiko dapat dibedakan menjadi tiga, yaitu menentukan apakah risiko yang teridentifikasi termasuk dalam risiko manfaat atau pemberdayaan nilai TI (*IT benefit / value enablement risk*), risiko program dan proyek TI (*IT programme and project*

delivery risk), atau risiko operasional dan pemberian layanan TI (*IT operations and service delivery risk*).

3.2.1.3 Menentukan Kategori Risiko

Untuk daftar risiko yang telah dicatat pada tabel *risk event*, kemudian dilakukan pemetaan setiap risiko yang teridentifikasi dengan kategori risiko yang telah ditentukan berdasarkan COBIT 5 *for risk*. Tujuan dari tahap ini adalah untuk mengetahui pengelompokkan kategori risiko yang mungkin terjadi pada *service desk* DPTSI.

3.2.1.4 Menentukan Faktor Risiko

Setelah melakukan pengkategorian risiko, tahap terakhir pada pengumpulan data adalah menentukan faktor risiko yang mungkin terjadi pada *service desk* DPTSI. Faktor risiko kontekstual dapat dibedakan menjadi dua, yaitu berdasarkan lingkungan internal maupun eksternal.

3.3.2 Menganalisis Risiko

Tahap kedua adalah menganalisis risiko. Dalam menganalisis risiko, dilakukan pengelolaan daftar risiko yang telah diketahui beserta atribut dan sumber terkait, serta kapabilitas dan aktivitas kontrol saat ini. Masukkan pada tahap ini adalah tabel *risk event*. Pada tahap ini terdapat tiga aktivitas yang akan dilakukan, yaitu memetakan risiko terhadap proses *service desk*, membuat skenario risiko TI, dan melakukan penilaian risiko TI.

3.2.2.1 Melakukan Pemetaan Risiko terhadap Proses Service Desk

Aktivitas ini dilakukan untuk memetakan risiko yang teridentifikasi dengan setiap proses sesuai kerangka kerja COBIT 5 domain DSS02 terkait pengelolaan permintaan layanan dan insiden pada unit *service desk* DPTSI.

3.2.2.2 Membuat Skenario Risiko TI

Selanjutnya dilakukan pembuatan dan pembaharuan skenario risiko TI secara teratur, termasuk skenario untuk risiko yang

tidak terduga, dan dikembangkan menjadi aktivitas kontrol yang lebih spesifik. Pada tahap ini dilakukan pembuatan skenario berdasarkan dua jenis, yaitu skenario positif dan skenario negatif.

3.2.2.3 Melakukan penilaian Risiko TI

Penilaian risiko TI dilakukan berdasarkan perkiraan frekuensi dan besarnya keuntungan atau kerugian (*magnitude*) yang terkait dengan skenario risiko TI. Berdasarkan frekuensi dan besarnya keuntungan/kerugian (*magnitude*) ini, akan didapatkan hasil level setiap risiko untuk kemudian dikelompokkan menurut prioritas risiko TI. Keluaran pada tahapan ini adalah berupa *risk register* berisi hasil penilaian risiko TI berdasarkan prioritas risiko.

3.3 Tahapan Pembuatan Perangkat Audit

Tahap ketiga dalam pengerjaan penelitian ini adalah tahap pembuatan perangkat audit. Masukkan pada tahap ini adalah *control objective* dan tabel *risk register*. Pada tahap ini, penulis melakukan dua tahapan proses diantaranya adalah tahap pemetaan risiko dan *control objective* serta tahap pembuatan perangkat audit.

3.3.1 Melakukan Pemetaan Risiko dan Control Objective

Pada tahap ini dilakukan pemetaan hasil penilaian risiko TI pada *risk register* terhadap *control objective* yang dapat memitigasi risiko. Hasil keluaran pada tahap ini adalah *control objective* sebagai rekomendasi penanganan risiko berupa tindakan kontrol mitigasi risiko yang akan dibuatkan perangkat audit.

3.3.2 Membuat Perangkat Audit

Merupakan tahap penyusunan perangkat audit untuk *control objective* yang telah dipetakan terhadap risiko TI yang ada. Tahapan ini terbagi menjadi empat aktivitas, yaitu pembuatan Dokumen Perangkat Audit dan Dokumen Panduan Penggunaan Perangkat Audit.

3.3.2.1 Pembuatan Dokumen Perangkat Audit

Perangkat Audit yang dibuat berdasarkan prosedur audit pada setiap *control objective*. Dokumen Perangkat Audit yang dibuat terdiri dari:

- **Prosedur Audit**
  Berisikan prosedur-prosedur beserta skenario langkah-langkah untuk setiap aktivitas *control objectiv*e berdasarkan proses, aktivitas *control objective*, dan kemungkinan risiko beserta hasil penilaiannya untuk setiap proses. Prosedur audit ini terdapat pada setiap dokumen daftar cek perangkat audit.
- **Daftar Cek atau Checklist**
  Merupakan lanjutan dari prosedur yang telah dibuat. Daftar cek berguna untuk mengetahui apakah aktivitas pada setiap prosedur telah dijalankan sebagaimana mestinya. Keluaran dari tahapan ini adalah sebuah daftar cek dari *control objective* dan prosedur di dalamnya.
- **Laporan Temuan Audit**
  Laporan Temuan Audit yang akan dibuat yaitu berbentuk template *audit report* yang nantinya akan berisi pencatatan daftar temuan, hasil evaluasi, data penanggung jawab, data auditor, solusi, catatan dari manajemen perusahaan, dan laporan-laporan lainnya.

3.3.2.2 Pembuatan Dokumen Panduan Penggunaan Perangkat Audit

Panduan ini ditujukan untuk pengguna perangkat audit, yaitu tim audit internal untuk dimudahkan dalam menggunakan dan mengoperasikan perangkat yang telah dibuat. Panduan penggunaan perangkat audit berisikan langkah-langkah dan tata cara penggunaan sehingga sesuai dengan tujuan pembuatan perangkat audit. Keluaran pada tahapan ini adalah berupa dokumen panduan penggunaan perangkat audit.

3.4 Tahapan Pembahasan Hasil

Pada tahap terakhir dalam pengerjaan penelitian ini adalah tahap pembahasan hasil. Pada tahap ini, penulis telah berfokus pada verifikasi perangkat audit.

3.4.1 Verifikasi Perangkat Audit

Tahap verifikasi perangkat audit dilakukan ketika dokumen perangkat audit telah selesai dibuat. Verifikasi dilakukan oleh Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi dengan cara menyesuaikan perangkat audit yang dibuat oleh penulis dengan pendekatan *best practice* yang digunakan. Tahapan verifikasi berguna untuk memastikan kesesuaian, serta menemukan apabila adanya ketidaksesuaian untuk dilakukan perbaikan. Apabila terdapat ketidaksesuaian pada dokumen perangkat audit, maka akan dilakukan kembali proses verifikasi untuk perbaikan ketidaksesuaian yang ada.

Setelah perbaikan dilakukan dan perangkat audit telah sepenuhnya sesuai dengan pendekatan *best practice*, maka selanjutnya akan dilakukan persetujuan rilisnya perangkat audit. Persetujuan perangkat audit merupakan proses terakhir dari tahap verifikasi ini dan keseluruhan metodologi di mana penulis melakukan proses persetujuan terhadap dokumen panduan audit yang telah dibuat. Dokumen perangkat audit akan ditandatangani oleh Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi dan siap digunakan oleh Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI).

BAB IV
PERANCANGAN

Bagian ini menjelaskan mengenai perancangan penulisan tugas akhir yang dilakukan. Perancangan ini bertujuan untuk menjadi panduan dalam melakukan penulisan tugas akhir.

4.1 Perancangan Studi Kasus

4.1.1 Tujuan Studi Kasus

Penelitian ini bertujuan untuk membuat perangkat audit berbasis risiko pada *service desk* yang sesuai untuk diterapkan dalam suatu organisasi tertentu, yaitu studi kasus organisasi DPTSI ITS. Harapannya perangkat audit tersebut dapat digunakan oleh auditor internal organisasi dalam melakukan pengendalian internal. Penggunaan studi kasus merupakan suatu hal yang penting di dalam suatu penelitian untuk menggali data dan informasi yang diperlukan pada *service desk* suatu organisasi. Seperti sebagaimana yang diutarakan oleh beberapa ahli mengenai pengertian dan pentingnya penggunaan yang merepresentasikan tujuan sebuah studi kasus, diantaranya adalah:

1. Studi kasus dalam penulisan merupakan sebuah aktivitas pengamatan yang berfokus untuk mendeskripsikan, memahami, memprediksi ataupun mengontrol sebuah individu [37].
2. Sykes (1990) mengatakan bahwa tidak mudah dalam mendapatkan jenis-jenis informasi tertentu yang sulit bahkan tidak mungkin untuk didapatkan selain dengan menggunakan studi kasus [38].
3. Yin (2003) menawarkan suatu pengertian yang berbeda mengapa kita harus menggunakan studi kasus dalam melakukan penulisan, dikarenakan sebuah studi kasus adalah suatu metode unik untuk mengamati sebuah topik empiris yang dilakukan berdasarkan satu set prosedur yang telah dibuat sebelumnya. Penulisan studi kasus dikatakan

> metode unik karena hanya mengobservasi area geografis yang sangat kecil atau suatu objek menarik secara mendalam. Dalam sebuah penulisan, studi kasus merupakan hal yang sangat menguntungkan karena penulis mempunyai kesempatan untuk mengamati suatu proses secara menyeluruh, mempelajari berbagai aspek, menguji hubungan satu sama lain dengan menggunakan kapasitas penulis untuk memahami [39].

Di dalam melakukan sebuah penulisan penting dalam menentukan dan memilih sebuah studi kasus yang tepat. Dalam pemilihannya terdapat tiga kategori studi kasus yang dijelaskan oleh Yin [39], diantaranya adalah:

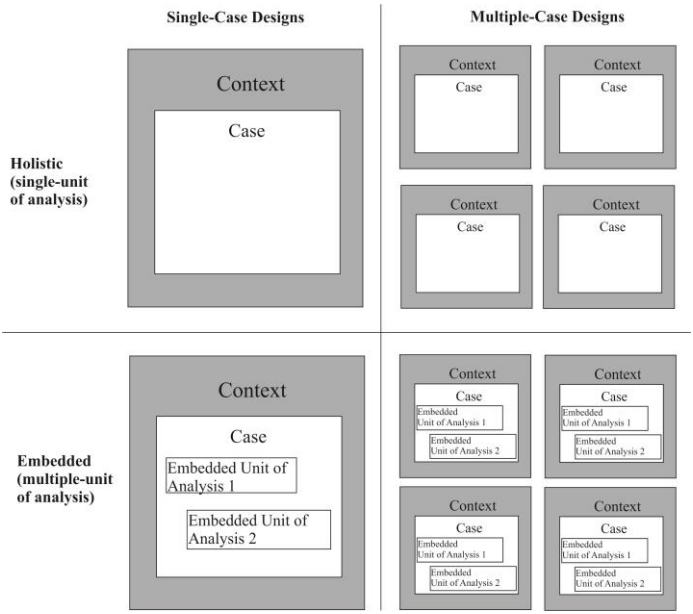
1. Studi kasus eksplorasi *(exploratory)* merupakan sebuah studi kasus yang bertujuan untuk melakukan eksplorasi secara mendalam terhadap fenomena apapun dalam subjek penulisan yang mengarah pada tujuan diadakannya penulisan.
2. Studi kasus deskriptif *(descriptive)* bertujuan untuk menggambarkan suatu fenomena yang biasanya berbentuk narasi, yang biasanya harus dimulai dengan mendeskripsikan teori untuk mendukung suatu fenomena tertentu.
3. Studi kasus *explanatory* bertujuan untuk menjelaskan fenomena dalam data secara jelas dan mendalam.

Tujuan penulis menggunakan studi kasus adalah agar penulis fokus dengan eksplorasi sehingga tujuan penelitian ini tercapai. Pertimbangan dengan pemilihan kategori eksplorasi ini adalah penulis ingin lebih melakukan eksplorasi lebih mendalam terkait risiko yang mungkin terjadi serta *control objective* yang harus ada pada proses pengelolaan permintaan layanan dan insiden pada unit *service desk* dengan studi kasus DPTSI ITS Surabaya. Oleh karena adanya studi kasus ini, penulis dapat mencapai tujuan penelitian dengan mengembangkan suatu

perangkat audit berbasis risiko pada *service desk* yang sesuai dengan DPTSI ITS.

Menurut Yin, langkah selanjutnya yang dapat dilakukan dalam melakukan penulisan adalah melakukan perancangan penulisan. Perancangan inilah yang nantinya akan membantu penulis dalam menentukan dan memahami tujuan pemilihan studi kasus, persiapan pengumpulan data untuk kebutuhan penulisan, menentukan metode pengolahan data hingga menentukan pendekatan untuk melakukan analisis mendalam mengenai data yang nantinya akan digunakan selama proses penulisan [39].

Dalam memilih studi kasus terdapat dua tipe yaitu *single-case design* dan *multiple-case design.* Terdapat perbedaan diantara kedua tipe tersebut jika digunakan dalam suatu penulisan, *Single-case design* merupakan tipe perancangan studi kasus dengan menggunakan pengujian pada satu studi kasus sehingga dapat mengeksplorasi lebih lanjut terhadap metode yang digunakan di dalamnya. *Single-case design* banyak digunakan pada penulisan dengan kasus yang unik, kritis, menguji kebenaran suatu teori, mengamati dan mengeksplorasi kondisi tertentu pada suatu kasus. Tipe yang kedua adalah *multiple-case design* dimana tipe ini menggunakan lebih dari satu studi kasus yang bertujuan untuk membandingkan beberapa studi kasus yang ada dan bertujuan untuk melakukan replikasi temuan di seluruh studi kasus. Perbedaan mendasar kedua tipe ini terletak pada jumlah *unit of analysis* yang digunakan seperti yang dapat terlihat pada Gambar 4.1 Type Unit Of Analysis [39].



Gambar 4.1 Type Unit Of Analysis (Book: A Case Study Methodology) [39]

Perancangan studi kasus pada penulisan tugas akhir ini menggunakan *single-case design* yang berarti penulisan ini menggunakan satu studi kasus dengan satu *unit of analysis.* Penulisan tugas akhir ini menggunakan satu studi kasus karena bertujuan untuk melakukan eksplorasi kondisi tertentu khususnya pada pembuatan perangkat audit berbasis risiko terkait proses pengelolaan permintaan layanan dan insiden yang ada pada *service desk* suatu organisasi, yaitu DPTSI ITS Surabaya.

4.1.2 *Unit of Analysis*

Berdasarkan pemaparan pentingnya studi kasus untuk mencapai tujuan penelitian, penulis memilih Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember menjadi studi kasus penulisan. Di mana *unit of analysis* yang ditentukan oleh penulis adalah analisis

pemetaan risiko dengan *control objective* yang berfokus pada layanan TI *service desk* meliputi proses pengelolaan permintaan layanan dan insiden di DPTSI.

4.2 Persiapan Pengumpulan Data

Pada tahap pengumpulan data dan informasi, peneliti membutuhkan data dan informasi untuk mengetahui kondisi kekinian dan kondisi harapan dari proses pengelolaan permintaan layanan dan insiden pada *service desk* DPTSI ITS. Di dalam bagian ini akan dibahas bagaimana metode yang akan digunakan dalam pengumpulan data pada studi kasus penulisan. Pada pengerjaan tugas akhir ini, penulis menggunakan beberapa metode untuk mengumpulkan data yang dibutuhkan, diantaranya adalah wawancara, observasi, survei, dan dokumen. Berikut penjelasan mengenai metode pengumpulan data yang digunakan oleh penulis:

1. **Wawancara**
   Wawancara merupakan aktivitas untuk menggali informasi dari seseorang untuk suatu tujuan tertentu. Penulis melakukan wawancara kepada orang-orang yang memegang kendali terhadap *service desk* DPTSI ITS, diantaranya adalah staf *service desk*. Di dalam melakukan teknik ini penulis akan mewawancarai staf *service desk* yang berkaitan langsung dengan pengelolaan permintaan layanan dan insiden. Wawancara ini dilakukan untuk mendapatkan informasi mengenai kondisi kekinian pengelolaan permintaan layanan dan insiden. Kondisi kekinian ini meliputi siapa saja yang memegang kendali dan tanggung jawab pada *service desk* dan proses pengelolaan permintan layanan dan insiden, bagiaman alur pengelolaannya mulai dari tahapan pencatatan, penanganan, hingga penutupan. Tujuan mengetahui kondisi kekinian ini adalah untuk memperoleh informasi terkait risiko TI pada proses pengelolaan

permintaan layanan dan insiden pada *service desk* DPTSI.

2. **Observasi**
   Observasi dilakukan terhadap keseluruhan teknik pelaporan mulai dari pencatatan manual, telepon, hingga *web application service desk* guna mengetahui alur dan proses pengelolaan permintaan layanan dan insiden. Observasi ini dilakukan untuk lebih mendapatkan data yang akurat mengenai pengelolaan permintaan layanan dan insiden dengan juga melihat kemungkinan risiko pada prosesnya.
3. **Survei**
   Survei dilakukan untuk mengumpulkan data terkait penurunan kepuasan pengguna layanan terhadap skenario risiko yang mungkin terjadi. Survei dilakukan dengan membagikan kuesioner kepada sampel pengguna layanan *service desk* DPTSI. Hasil pengumpulan data melalui survei penurunan kepuasan pengguna layanan digunakan untuk memberi penilaian salah satu jenis dampak risiko menurut *best practice* COBIT 5 *for Risk*, yaitu Keunggulan Kompetitif untuk aspek Penurunan Kepuasan Pengguna.
4. **Analisis Dokumen**
   Analisis terhadap beberapa dokumen yang dilakukan adalah melalui log insiden dan dokumen terkait risiko TI pada *service desk* dari penelitian manajemen risiko TI pada manajemen layanan TI. Dari beberapa teknik pengumpulan data yang akan dilakukan dalam penulisan ini, berikut beberapa detail data yang ingin di dapatkan selama proses penulisan:
   - Tugas pokok dan tanggung jawab utama *service desk* pada SubDirektorat Layanan Teknologi dan Sistem Informasi DPTSI.
   - Dokumen Log Insiden yang berasal dari sistem *e-ticket* dan *e-mail service desk.*
   - Dokumen penelitian terkait risiko TI pada manajemen layanan TI dari berbagai literatur.

- Dokumen pendukung lain untuk melengkapi bukti dalam pembuatan perangkat audit.
- Dokumen standar yang digunakan dalam melakukan penelitian yaitu dokumen standard COBIT 5 *Enabling Process, Service Desk Standard,* dan COBIT 5 *for Risk.*

Di dalam teknik pengumpulan data ini terdapat banyak informasi dan data yang harus di dapatkan. Dimana data dan informasi ini akan dipertanggung jawabkan pada pihak manajemen DPTSI ITS pada akhir penulisan dalam bentuk dokumen luaran berupa perangkat audit.

Berikut pemetaan keterkaitan antara metode pengumpulan data, tujuan pengumpulan data, *goals*, acuan sumber pertanyaan dan lampiran yang merepresentasikan setiap poin *interview protocol*, *checklist* observasi, kuesioner survei, dan analisis dokumen ditunjukkan pada Tabel 4.1.

Tabel 4.1 Pemetaan Metode Pengumpulan Data

Tujuan	Goals	Sumber	Lampiran
Metode : Wawancara			
Mengetahui kondisi implementasi layanan TI *service desk* pada SubDirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS.	• Permasalahan (insiden) layanan TI • Permintaan layanan TI oleh pengguna • Struktur organisasi • Tupoksi • Visi Misi • Layanan yang ditangani oleh *service desk* DPTSI	IS/ISO 19011:2011 [18] Dyah Retnani Sulistya-ningrum [5] Stephen Christian [6]	**B**

Tujuan	Goals	Sumber	Lampiran
Metode : Wawancara			
	• Kondisi kekinian proses pada *service desk*		
Mengetahui kondisi kekinian *service desk* dalam implementasi pengelolaan permintaan layanan dan insiden.	• Alur Pengelolaan Permintaan Layanan dan Insiden • Teknologi informasi (sistem aplikasi) yang digunakan	Dyah Retnani Sulistya-ningrum [5] ITIL [32]	
Mengetahui permasalahan atau risiko pada proses pengelolaan permintaan layanan dan insiden pada *service desk* DPTSI.	• Risiko TI pada proses pengelolaan permintaan layanan dan insiden • Kondisi sistem aplikasi yang digunakan	Dyah Retnani Sulistya-ningrum [5]	
Metode : Observasi			
Mengetahui alur dan proses pengelolaan permintaan layanan dan insiden secara detail	• Kelengkapan proses pengelolaan permintaan layanan dan insiden sesuai COBIT 5 *for Risk* untuk menggali lebih dalam	Dyah Retnani Sulistya-ningrum [5]	**B**

Tujuan	Goals	Sumber	Lampiran
Metode : Wawancara			
	risiko terkait proses		
Metode : Survei			
Mengetahui nilai indeks dampak skenario risiko terhadap penurunan kepuasan pengguna layanan *service desk*	• Nilai indeks penurunan kepuasan pengguna terhadap skenario risiko pada layanan *service desk*	Dwi Rosa Indah, Halili, Mgs. Afriyan Firdaus [9]	**C**
Metode : Analisis Dokumen			
Mengetahui kondisi kekinian *service desk* yang terdokumentasi	• Dokumen tupoksi *service desk* DPTSI • Dokumen log permintaan layanan dan insiden • Dokumen penelitian terkait risiko TI pada manajemen layanan TI	IS/ISO 19011:2011 [18] Dyah Retnani Sulistya-ningrum [5]	-

4.3 Metode Pengolahan Data

Metode pengolahan data pada penulisan ini terdapat dua metode yang digunakan. Metode pertama dilakukan agar penulis dapat dengan mudah melakukan analisis pada hasil wawancara dengan narasumber, yaitu data dari hasil wawancara yang telah direkam menggunakan bantuan alat perekam kemudian disalin pada aplikasi *Microsoft Word*. Setelah data disalin dan disimpan di aplikasi *Microsoft Word*, data akan lebih mudah

untuk diolah seperti melakukan *highlight text, underline point*, hingga menerjemahkan hasil wawancara narasumber dalam sebuah kalimat. Metode pengolahan data yang digunakan yaitu dengan cara melakukan analisis deskriptif dari data yang didapatkan dengan memaparkannya ke dalam tabel sehingga data menjadi lebih mudah untuk dipahami. Sedangkan data yang didapatkan melalui observasi dilakukan pencatatan terhadap hasil pengamatan tersebut.

Metode yang kedua adalah melakukan pengolahan data untuk memberikan penilaian-penilaian terhadap risiko proses pengelolaan permintaan layanan dan insiden. Penilaian-penilaian ini digunakan untuk melakukan prioritisasi terhadap risiko berdasarkan aspek frekuensi dan dampak (*magnitude*). Penilaian dan prioritisasi risiko menggunakan *Microsoft Excel* untuk memudahkan penulis dalam mendapatkan nilai dampak dengan menghitung rata-rata nilai empat dampak. Hasil dari pengolahan data terkait risiko ini dipaparkan dalam tabel prioritas risiko.

4.4 Pendekatan Analisis

Setelah data berhasil dikumpulkan, selanjutnya dilakukan pendekatan analisis. Analisis ini dilakukan untuk mengetahui hubungan antara data yang didapat dan akan menggunakannya pada tahapan pengerjaan penulisan. Beberapa analisis yang akan dilakukan antara lain adalah:

1. Analisis dengan pendekatan konseptual, yaitu dilakukan analisis tugas pokok dan fungsi (tupoksi) *service desk* DPTSI serta kondisi kekinian pengelolaan permintaan layanan dan insiden pada *service desk*. Analisis ini dilakukan untuk mengetahui bagaimana alur dan proses pengelolaan permintaan layanan dan insiden mulai dari tahap awal pendefinisian hingga akhir pentupan proses beserta penanggung jawab setiap proses sesuai tupoksi. Informasi kondisi kekinian ini

untuk membantu dalam penggalian risiko terkait proses.

2. Analisis pemetaan proses berdasarkan COBIT 5 DSS02 dengan penentuan *control objective* yang telah disesuaikan dengan *Service Desk Standard*.
3. Analisis pendekatan menganalisis risiko berdasarkan *best practice* COBIT 5 *for Risk* APO12 untuk mencari kemungkinan risiko yang akan terjadi pada proses pengelolaan permintaan layanan dan insiden.
4. Analisis penilaian risiko berdasarkan aspek frekuensi dan dampak terhadap risiko pada *risk event* berdasarkan *best practice* COBIT 5 *for Risk* APO12.
5. Analisis pemetaan risiko yang teridentifikasi dengan *control objective* yang telah ditentukan. *Control objective* untuk setiap risiko ini yang akan dianalisis untuk pembuatan perangkat audit.

4.5 Perancangan Kuesioner Survei

Kuesioner survei diperlukan untuk mengetahui respon dari pengguna layanan *service desk* DPTSI terkait penurunan kepuasan pengguna akibat adanya skenario risiko yang mungkin terjadi pada proses pengelolaan permintaan layanan dan insiden. Kuesioner yang akan disebarkan adalah kuesioner yang berjenis *online* melalui internet. Kuesioner ini dibuat dengan Google Forms. Setelah dibuat, link dari kuesioner *online* ini akan disebarkan kepada sampel pengguna layanan *service desk* yang dispesifikkan di ruang lingkup mahasiswa Insititut Teknologi Sepuluh Nopember (ITS) Kota Surabaya.

Kuesioner yang dirancang menggunakan pernyataan dengan jawaban berupa dari skala likert bernilai indeks 1-5 dimana jawaban pada kolom Penurunan Sangat Sedikit bernilai 1, Penurunan Sedikit bernilai 2, Netral bernilai 3, Penurunan Banyak bernilai 4, Penurunan Sangat Banyak bernilai 5. Perancangan kuesioner ditampilkan pada **LAMPIRAN C.**

4.6 Perancangan Analisis Risiko

Perancangan analisis risiko mengacu pada template *best practice* COBIT 5 *for Risk* domain APO12. Berikut template dokumen yang akan diisikan pada proses analisis antara lain perancangan *risk event*, pemetaan kategori risiko, pemetaan faktor risiko, pemetaan risiko terhadap proses, skenario risiko, dan penilaian risiko.

4.6.1 Perancangan Risk Event

Berikut perancangan template *risk event* dengan penentuan tipe risiko ditunjukkan pada Tabel 4.2.

Tabel 4.2 Perancangan Risk Event dan Tipe Risiko

No.	Risiko	Tipe Risiko		
		IT Benefit/Value Enablement	IT Programme and Project	IT operations and Service Delivery
1	Risiko 1	P	S	P
2	Risiko 2	S	S	P

4.6.2 Perancangan Pemetaan Kategori Risiko

Berikut perancangan template pemetaan kategori risiko ditunjukkan pada Tabel 4.3.

Tabel 4.3 Perancangan Kategori Risiko

No	Kategori Risiko	ID Risiko	Risiko
1	(ex. *IT expertise and skill*)	(ex. IT01)	Risiko 1
2	(ex. *Software*)	(ex. SW01)	Risiko 2

4.6.3 Perancangan Pemetaan Faktor Risiko

Berikut perancangan template pemetaan faktor risiko kontekstual ditunjukkan pada Tabel 4.4.

Tabel 4.4 Perancangan Faktor Kontekstual

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
(ex. IT01)	Risiko 1	(ex. ***Culture of the enterprise*** *penjelasan aspek faktor*)	(ex. ***Regulatory environment*** *penjelasan aspek faktor*)
(ex. SW01)	Risiko 2	(ex. ***Culture of the enterprise*** *penjelasan aspek faktor*)	(ex. ***Regulatory environment*** *penjelasan aspek faktor*)

4.6.4 Perancangan Pemetaan Risiko terhadap Proses

Pemetaan risiko yang teridentifikasi terhadap proses pengelolaan permintaan layanan dan insiden berdasarkan COBIT 5 domain DSS02. Berikut perancangan template pemetaan risiko terhadap proses ditunjukkan pada Tabel 4.5.

Tabel 4.5 Perancangan Pemetaan Risiko pada Proses

Kategori Risiko	ID Risiko	Risiko	Pemetaan Risiko Operasional
(ex. *IT expertise and skill*)	(ex. IT01)	Risiko 1	(ex. **DSS02.03** Memverifikasikan, menyetujui dan memenuhi permintaan layanan.)
(ex. *Software*)	(ex. SW01)	Risiko 2	(ex. **DSS02.05** Menyelesaikan dan Memulihkan Insiden.)

4.6.5 Perancangan Skenario Risiko

Berikut perancangan template skenario risiko ditunjukkan pada Tabel 4.6.

Tabel 4.6 Perancangan Skenario Risiko

ID Risiko	Risiko	Contoh Skenario	
		Skenario Negatif	Skenario Positif
(ex. IT01)	Risiko 1	Pemaparan skenario negatif	Pemaparan skenario positif

4.6.6 Perancangan Template Penilaian Risiko

Berikut perancangan template penilaian untuk mengisi peringkat frekuensi dan dampak untuk setiap skenario risiko, serta level penilaian risikonya ditunjukkan pada Tabel 4.7.

Tabel 4.7 Perancangan Template Penilaian Risiko

ID Risiko	Risiko	Peringkat Frekuensi	Peringkat Dampak					Level Penilaian Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Keseluruhan Peringkat Dampak	
(ex. IT01)	Risiko 1	(ex. 2)	(ex. 1)	(ex. 2)	(ex. 1)	(ex. 3)	(ex.2)	(ex. Medi-um)

Keseluruhan peringkat dampak merupakan nilai rata-rata dari empat peringkat dampak. Kemudian keseluruhan peringkat risiko adalah level nilai risiko yang didapatkan dari hasil pemetaan antara peringkat frekuensi dengan keseluruhan peringkat dampak.

4.7 Perancangan Perangkat Audit

4.7.1 Perancangan Dokumen Perangkat Audit

Berikut perancangan dokumen perangkat audit mengacu pada IS/ISO 19011:2011 ditunjukkan pada Tabel 4.8.

Tabel 4.8 Perancangan Dokumen Perangkat Audit

Struktur Bab	Deskripsi
Daftar Cek Audit (*Audit Checklist*)	*Checklist* yang digunakan pada proses audit untuk setiap *control objective*.
Laporan Temuan Audit	Template Laporan Temuan Audit yang digunakan untuk laporan hasil pemeriksaan

4.7.2 Perancangan Dokumen Panduan Penggunaan Perangkat Audit

Berikut perancangan dokumen panduan penggunaan perangkat audit mengacu pada IS/ISO 19011:2011 ditunjukkan pada Tabel 4.9.

Tabel 4.9 Perancangan Dokumen Panduan Penggunaan Perangkat Audit

Struktur Bab	Sub-Bab	Deskripsi
Pendahuluan	Tujuan	Tujuan penulisan dan pembuatan dokumen perangkat audit
	Ruang Lingkup Dokumen	Penjelasan ruang lingkup dokumen panduan penggunaan perangkat audit
	Definisi, Istilah, Singkatan	Penjabaran definisi, istilah, dan singkatan yang digunakan dalam perangkat audit
	Daftar Perangkat Audit	Daftar perangkat audit yang digunakan untuk melakukan pemeriksaan
	Daftar Penilaian Risiko	Daftar risiko beserta hasil penilaiannya sebagai acuan

Struktur Bab	Sub-Bab	Deskripsi
		dalam pengisian kolom "Risiko Terkait" pada Laporan Temuan Audit
	Ikhtisar Dokumen	Urutan atau format dari singkatan isi panduan penggunaan perangkat audit
Panduan Umum	Petunjuk Penggunaan Bagian Penilaian Risiko	Menjelaskan petunjuk dalam menggunakan tabel penilaian risiko
	Petunjuk Pengisian Daftar Cek Perangkat Audit	Petunjuk dalam mengisi daftar cek perangkat audit ketika proses audit dilaksanakan
	Petunjuk Pengisian Laporan Temuan Audit	Petunjuk dalam mengisi Laporan Temuan Audit sebagai laporan pemeriksaan
Panduan Khusus	Petunjuk Peninjauan Dokumen yang Dibutuhkan	Bahan-bahan dokumen dan pustaka yang dapat dikumpulkan oleh tim auditor dalam melakukan audit
	Pengecualian	Daftar pengecualian terkait kondisi yang terduga maupun tidak terduga dalam proses pelaksanaan audit

BAB V
IMPLEMENTASI

Bab ini menjelaskan mengenai hasil implementasi yang diperoleh dari proses perancangan pada bab IV yang telah dijabarkan sebelumnya. Hasil implementasi akan berupa data dan informasi mentah.

5.1 Proses Pelaksanaan Penulisan

Proses pelaksanaan penulisan membahas mengenai hasil perancangan studi kasus yang di dapatkan melalui wawancara, observasi, dan analisis dokumen yang di dapatkan guna memperoleh kondisi kekinian organisasi terkait risiko TI pada proses pengelolaan permintaan layanan dan insiden. Berdasarkan tahapan persiapan pengumpulan data pada bab perancangan studi kasus, maka narasumber yang diwawancara adalah Bapak Jainul Arifin, Ibu Widiyaningsih, dan Ibu Mudjiatin sebagai staf *service desk* layanan pada DPTSI Institut Teknologi Sepuluh Nopember (ITS) Kota Surabaya. Wawancara dan observasi mengenai kondisi kekinian serta risiko terkait proses pengelolaan permintaan layanan dan insiden pada *service desk* telah dilakukan satu kali yaitu pada tanggal 24 November 2016. Hasil wawancara tersebut secara singkat akan dijelaskan pada poin di bawah ini:

1. Pengelolaan *service desk* dilakukan dengan menggunakan *web application service desk* bernama sistem *e-ticket*.
2. Pelaporan permintaan layanan dan insiden oleh pengguna layanan menggunakan dua saluran yaitu *e-mail* dan sistem *e-ticket*.
3. Pengelolaan permintaan layanan dan insiden pada *service desk* DPTSI bertujuan untuk memenuhi permintaan pengguna layanan dan memulihkan insiden yang terjadi dimulai dengan melakukan proses pelaporan oleh pengguna, pencatatan pelaporan (melalui *e-mail* dan log pencatatan otomatis melalui sistem *e-ticket*), pemenuhan permintaan dan

penanganan insiden, penutupan pelaporan, hingga membuat layanan tersebut tetap dapat berjalan bagi para *user* (pengguna layanan).

4. *Service desk* dikelola oleh beberapa staf layanan yang telah diberikan *job desk* sesuai dengan pembagian masing-masing.

Untuk hasil wawancara dan observasi yang telah dilakukan secara lengkap telah terlampir pada **LAMPIRAN D**.

5.2 Analisis Kondisi Kekinian Organisasi

5.2.1 Gambaran Umum DPTSI

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) merupakan unit yang ada di dalam Institut Teknologi Sepuluh Nopember (ITS) Kota Surabaya. DPTSI bertugas untuk menyediakan dan mengelola layanan Teknologi Informasi di lingkungan ITS, antara lain melaksanakan penyiapan perumusan kebijakan pengembangan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan di bidang teknologi dan sistem informasi. Dalam melaksanakan tugas tersebut, DPTSI menyelenggarakan fungsi :

a. pengelolaan dan pengembangan infrastruktur dan keamanan informasi;
b. pengelolaan dan pengembangan sistem informasi; dan
c. pengelolaan dan pengembangan layanan sistem dan teknologi informasi.

Terkait peran, DPTSI berperan untuk mendukung aktivitas akademik, penelitian dan pengabdian masyarakat, serta manajerial di lingkungan ITS dalam rangka membantu ITS mencapai visi misinya. Berikut visi dan misi strategi DPTSI.

Visi

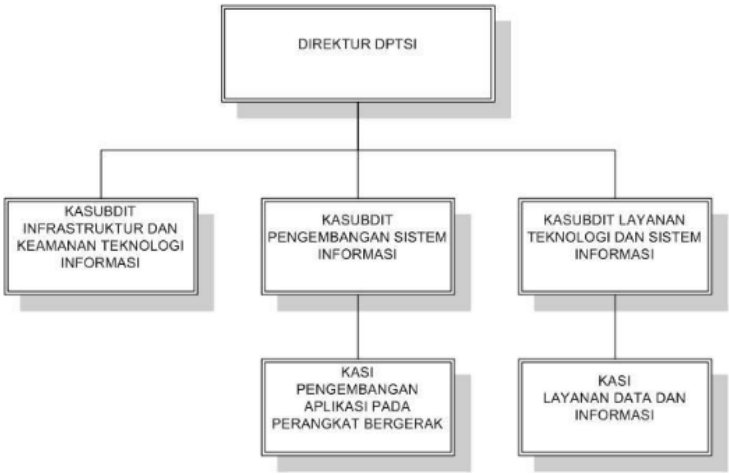
Mewujudkan ITS Smart Campus, ITS in one hand.

Misi

1. Menyediakan teknologi informasi dan komunikasi beserta pendukungnya.
2. Mengembangkan infrastruktur informasi kampus.
3. Menjalin kerjasama dan kemitraan baik di dalam maupun di luar kampus.

5.2.2 Struktur Organisasi DPTSI

Berikut struktur organisasi DPTSI digambarkan pada Gambar 5.1.



Gambar 5.1 Struktur Organisasi DPTSI [1]

DPTSI dipimpin oleh seorang direktur bernama Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom dan dibantu oleh tiga Kepala SubDirektorat (KaSubDit). DPTSI terdiri atas tiga SubDirektorat yang masing-masing dipimpin oleh KaSubDit, antara lain SubDirektorat Infrastruktur dan Keamanan Teknologi Informasi, SubDirektorat Pengembangan Sistem Informasi, serta SubDirektorat Layanan Teknologi dan Sistem Informasi. Pada SubDirektorat Pengembangan Sistem Informasi dibantu oleh Seksi Pengembangan Aplikasi pada

Perangkat Bergerak, sedangkan SubDirektorat Layanan TSI dibantu oleh Seksi Layanan Data dan informasi di mana setiap Seksi dipimpin oleh KaSi (Kepala Seksi). Penelitian ini berfokus pada unit *service desk* yang terdapat pada SubDirektorat Layanan Teknologi dan Sistem Informasi (Layanan TSI).

Untuk saat ini DPTSI belum memiliki tim auditor dalam struktur organisasi untuk melaksanakan audit internal pada *service desk* sehingga tanggung jawab terkait audit internal diserahkan kepada Kepala SubDirektorat (KaSubDit) Layanan TSI. Tim auditor nantinya akan dibentuk oleh KaSubDit Layanan TSI dengan penambahan tugas pokok dan fungsi pada staf/karyawan maupun manajemen (Direktur, KaSubDit, dan KaSi) DPTSI.

5.2.3 Tugas Pokok dan Fungsi SubDirektorat Layanan TSI

SubDirektorat Layanan TSI dipimpin oleh kepala SubDirektorat (KaSubDit) yaitu Hanim Maria Astuti, S.Kom., M.Sc. Berikut rincian informasi dasar dari SubDirektorat Layanan TSI terdapat pada Tabel 5.1.

Tabel 5.1 Informasi Dasar SubDirektorat Layanan TSI

Informasi Dasar	Uraian
Tugas Pokok	Melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, operasional layanan, pengawasan dan pemantauan, evaluasi, dan pelaporan untuk layanan teknologi dan sistem informasi.
Fungsi Dasar	a. penyiapan bahan perumusan kebijakan dan standar mutu layanan teknologi dan sistem informasi; b. pelaksanaan operasional layanan teknologi dan sistem informasi; c. pelaksanaan pengawasan dan pemantauan layanan teknologi dan sistem informasi; dan

Informasi Dasar	Uraian
	d. pelaksanaan evaluasi dan pelaporan layanan teknologi dan sistem informasi.
Staf	Terdiri dari lima staf layanan, antara lain: - Jainul Arifin - Mudjiatin, SE - Widiyaningsih, S.Kom - Wiwin Rochmawati, A.Md - Rizki Rinaldi

Pada Subdit Layanan TSI terdapat unit *service desk* atau *help desk* yang berfungsi untuk menangani berbagai macam keluhan dan permintaan layanan TI di lingkungan ITS. Berikut tugas pokok dan fungsi (tupoksi) dari staf layanan *service desk* dijabarkan pada Tabel 5.2.

Tabel 5.2 Tugas Pokok dan Fungsi Service Desk

No.	Tugas Pokok dan Fungsi
	Mengelola keluhan dari pengguna layanan DPTSI
1	Mempersiapkan *service desk* dan perlengkapannya
2	Menerima keluhan, melakukan pencatatan dan kategorisasi keluhan layanan
3	Melakukan troubleshoot atas keluhan yang diterima oleh subdit LTSI a. Troubleshoot terkait email b. Troubleshoot terkait penggunaan software berlisensi c. Troubleshoot terkait penggunaan software f/oss
4	Melakukan eskalasi keluhan ke subdit PSI atau IKTI apabila penanganan di luar kapasitas *service desk*
5	Memantau penanganan keluhan
6	Menginformasikan status keluhan kepada pengguna yang mengalami insiden/masalah
7	Mengupdate status keluhan

Mengelola *request* (permintaan layanan)	
1	Menerima dan mencatat *request* pengguna layanan
2	Melakukan eksekusi *request* pengguna layanan a. Mengelola proses pendaftaran email ITS baru - Melakukan verifikasi data pemohon - Melakukan verifikasi alamat email - Membuat email baru b. Membantu kesulitan user atas reset password email ITS c. Melaksanakan request migrasi email ITS ke gmail d. Mengelola proses pendaftaran domain - Melakukan verifikasi data pemohon

5.3 Hasil Survei

Proses survei melalui penyebaran kuesioner tingkat penurunan kepuasan pengguna kepada responden atau sampel pengguna terhadap layanan *service desk* DPTSI dimulai pada tanggal 28-31 Desember 2016. Hasil survei terlampir pada **LAMPIRAN E.** Setelah data terkumpul sebanyak 53 sampel, langkah selanjutnya adalah menghitung rata-rata nilai indeks skala likert pada setiap poin pernyataan kuesioner yang merepresentasikan dampak penurunan kepuasan pengguna layanan terhadap kemungkinan skenario risiko yang terjadi. Penulis menentukan rentang skala likert yang menunjukkan persepsi responden terhadap pertanyaan yang diberikan. Rentang skala likert kuesioner yang dipetakan dengan peringkat dampak keunggulan kompetitif ditunjukkan pada Tabel 5.3.

Tabel 5.3 Pemetaan Peringkat Dampak dan Skala Likert

Peringkat Dampak	Keunggulan Kompetitif		
	Penurunan Kepuasan Pengguna	Rentang Skala Likert	Keterangan
1	I ≤ 1	1,00-1,50	**Very Low** Kegagalan menyebabkan penurunan yang sangat tidak signifikan (sangat rendah)

			terhadap kepuasan pengguna layanan
2	1 < I ≤ 1,5	1,51-2,50	**Low** Kegagalan menyebabkan penurunan yang tidak signifikan (rendah) terhadap kepuasan pengguna layanan
3	1,5 < I ≤ 2	2,51-3,50	**Moderate** Kegagalan menyebabkan penurunan yang cukup signifikan terhadap kepuasan pengguna layanan
4	2 < I ≤ 2,5	3,51-4,50	**High** Kegagalan menyebabkan penurunan yang signifikan (tinggi) terhadap kepuasan pengguna layanan
5	2,5 < I	4,51-5,00	**Very High** Kegagalan menyebabkan penurunan yang sangat signifikan (sangat tinggi) terhadap kepuasan pengguna layanan

Berikut pada Tabel 5.4 menampilkan hasil perhitungan rata-rata setiap poin pernyataan kuesioner survei, peringkat dampak yaitu memasukkan nilai indeks pada skala 1-5 sesuai COBIT 5 *for Risk*, beserta pemetaan tiap poin pernyataan dengan risiko terkait.

Tabel 5.4 Hasil Kuesioner Survei

ID	Pernyataan	Rata-rata indeks	Peringkat Dampak	Risiko
K.01	Ketika *service desk* tidak memenuhi permintaan dan menangani keluhan sesuai harapan saya,	3.79	4	**IT02** - Kesalahan penanganan insiden dan pemenuhan permintaan layanan

ID	Pernyataan	Rata-rata indeks	Peringkat Dampak	Risiko
	maka kepuasan saya mengalami:			**IT03** - Kesalahan pemahaman permintaan pengguna layanan
				SO01 - Kesalahan pencatatan permintaan layanan dan insiden
				SO02 - Log permintaan layanan dan insiden tidak lengkap
				SO04 - Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan
K.02	Ketika *service desk* terlambat dalam merespon laporan keluhan dan permintaan saya, maka kepuasan saya mengalami :	3.58	4	**IT04** - Keterlambatan respon service desk
K.03	Ketika *service desk* mengabaikan	4.24	4	**SO03** - Pengabaian laporan insiden

ID	Pernyataan	Rata-rata indeks	Peringkat Dampak	Risiko
	laporan keluhan dan permintaan saya, maka kepuasan saya mengalami :			oleh teknisi/staf service desk
K.04	Ketika *service desk* selesai menangani laporan keluhan dan permintaan saya di luar batas waktu yang dijanjikan, maka kepuasan saya mengalami :	3.13	3	**IT01** - Penanganan insiden dan pemenuhan permintaan layanan overdue
K.05	Ketika *service desk* tidak melakukan verifikasi kepuasan saya untuk memastikan bahwa laporan keluhan dan permintaan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami :	2.87	3	**SO05** - Ketidakpuasan user dengan layanan
K.06	Ketika *service desk* tidak memberi keluhan dan permintaan informasi status	3.36	3	**SO06** - Ketidakjelasan status permintaan layanan dan insiden

ID	Pernyataan	Rata-rata indeks	Peringkat Dampak	Risiko
	laporan saya (sedang direspon / selesai ditangani / telah ditutup), maka kepuasan saya mengalami :			
K.07	Ketika *service desk* tidak menangani masalah yang berulang kali saya keluhkan hingga akar permasalahan, maka kepuasan saya mengalami:	3.79	4	**SO07** - Kesalahan pendefinisan tren pada laporan
K.08	Ketika *service desk* tidak mengalami peningkatan dalam melayani permintaan dan keluhan saya, maka kepuasan saya mengalami:	3.37	3	**SW02 -** Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan
K.09	Ketika sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak dapat saya akses, maka	3.23	3	**SW01** - Kegagalan akses sistem e-ticket

ID	Pernyataan	Rata-rata indeks	Peringkat Dampak	Risiko
	kepuasan saya mengalami :			
K.10	Ketika keamanan informasi pada sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak terlindungi, maka kepuasan saya mengalami:	3.87	4	**LA01** - Penyalahgunaan hak akses permintaan layanan secara sengaja

5.4 Pemetaan Control Objective

Control objective akan dihasilkan dari proses pemetaan antara proses ideal berdasarkan COBIT 5 dengan acuan standar lain yang digunakan oleh penulis yaitu kontrol pada *Service Desk Standard*. Dimana dalam penentuan pemetaan pada bagian ini, penulis menggunakan semua proses dan aktivitas pada COBIT 5 dengan pertimbangan perusahaan harus menggunakan dan mengikuti semua proses ideal pada standar ini.

Pemetaan dilakukan dengan mencari hubungan antara proses ideal berdasarkan COBIT 5 domain DSS02 *Manage Service Requests and Incidents* dengan kontrol yang dibutuhkan dalam setiap prosesnya sehingga didapatkan pemetaan *control objective*. Tabel 5.5 Pemetaan Control Objective di bawah ini menunjukkan gambaran besar hasil pemetaan *control objective* yang nantinya dapat digunakan dalam pembuatan perangkat audit.

Tabel 5.5 Pemetaan Control Objective

Proses COBIT 5	Service Desk Standard	Control Objective
DSS02.01 Mendefinisikan skema klasifikasi insiden dan permintaan layanan	*4.05 Stafing and scheduling* *4.13 Service catalogue management* *5.03 Service level management* *5.05 Incident and service request management*	Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian
DSS02.02 Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden	*4.06 IT service management system* *4.08 Remote access and control* *4.10 Self-service* *5.01 Pro-active incident detection and remediation* *5.04 Communication*	Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden
	4.02 Infrastructure *4.06 IT service management system* *4.07 IT service management system – product capability* *5.06 Incident and service request logging*	Memastikan Adanya Prosedur Pencatatan Permintaan Layanan dan Insiden
	5.07 Prioritization	Memastikan Adanya Prioritisasi Permintaan Layanan dan Insiden
	5.08 Categorization	Memastikan Adanya Klasifikasi Permintaan

Proses COBIT 5	Service Desk Standard	Control Objective
		Layanan dan Insiden

Pemetaan akan lebih terinci terlampir pada **LAMPIRAN F**. Berikut pada Tabel 5.6 Control Objective akan dijabarkan daftar dua belas *control objective* yang akan dipetakan dengan risiko terkait proses pengelolaan permintaan layanan dan insiden.

Tabel 5.6 Control Objective

No.	ID Control Objective	Control Objective
1	CO.01	Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian
2	CO.02	Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden
3	CO.03	Memastikan Adanya Prosedur Pencatatan Permintaan Layanan dan Insiden
4	CO.04	Memastikan Adanya Prioritisasi Permintaan Layanan dan Insiden
5	CO.05	Memastikan Adanya Klasifikasi Permintaan Layanan dan Insiden
6	CO.06	Memastikan Adanya Verifikasi Hak Penggunaan Permintaan Layanan
7	CO.07	Memastikan Adanya Persetujuan Pemenuhan Permintaan Layanan
8	CO.08	Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden
9	CO.09	Memastikan Adanya Penggunaan Informasi Pengelolaan Insiden
10	CO.10	Memastikan Adanya Penutupan Permintaan Layanan dan Insiden

No.	ID Control Objective	Control Objective
11	CO.11	Memastikan Adanya Laporan Pengelolaan Permintaan Layanan dan Insiden
12	CO.12	Memastikan Adanya Peningkatan Pengelolaan Permintaan Layanan dan Insiden

5.5 Analisis Risiko TI

Pada proses perancangan, salah satu pendekatan analisis yang dilakukan pada penelitian ini adalah menganalisis risiko berdasarkan *best practice* COBIT 5 *for Risk* APO12 untuk mencari kemungkinan risiko yang akan terjadi pada proses pengelolaan permintaan layanan dan insiden. Sebelum melakukan analisis risiko TI, dilakukan penggalian informasi terkait kemungkinan risiko yang akan terjadi pada setiap proses pengelolaan permintaan layanan dan insiden yang ada pada *service desk* DPTSI. Kemungkinan risiko yang dihasilkan melalui tahapan wawancara pada staf *service desk* DPTSI dijabarkan pada Tabel 5.7.

Tabel 5.7 Kemungkinan Risiko pada *Service Desk*

No	Risiko
1	Kesalahan pemahaman permintaan pengguna layanan
2	Keterlambatan respon *service desk*
3	Kesalahan pencatatan permintaan layanan dan insiden
4	Sistem aplikasi tidak dapat diakses
5	Log permintaan layanan dan insiden tidak lengkap
6	Penyalahgunaan hak akses permintaan layanan secara sengaja
7	Pengabaian laporan insiden oleh teknisi/staf *service desk*
8	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan
9	Penanganan insiden dan pemenuhan permintaan layanan *overdue*
10	Kesalahan penanganan insiden dan pemenuhan permintaan layanan

No	Risiko
11	Ketidakpuasan user dengan layanan
12	Ketidakjelasan status permintaan layanan dan insiden
13	Kesalahan pendefinisan tren pada laporan
14	Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan

Daftar kemungkinan risiko yang terjadi pada proses pengelolaan permintaan layanan dan insiden tersebut kemudian dianalisis berdasarkan *best practice* COBIT 5 *for Risk* APO12 dengan penentuan tipe, kategori, dan faktor risiko. Kemudian dilanjutkan dengan pemetaan risiko terhadap *control objective*, pembuatan skenario risiko, dan penilaian risiko.

5.5.1 Penentuan Tipe Risiko

Tahap pertama adalah menentukan tipe setiap risiko TI yang teridentifikasi. Tipe risiko dikategorisasikan dalam dua hal yaitu:

- '**P**' untuk tipe skenario risiko yang menunjukkan primer. Hal ini menunjukkan bahwa skenario risiko tersebut termasuk dalam tipe risiko yang memiliki nilai primer.
- '**S**' untuk tipe skenario risiko menunjukkan sekunder atau menunjukkan tipe yang lebih rendah.

Berikut penentuan tipe risiko TI pada *risk event* ditampilkan pada Tabel 5.8.

Tabel 5.8 Penentuan Tipe Risiko

No.	Risiko	Tipe Risiko		
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT operations and Service Delivery
1	Kesalahan pemahaman permintaan pengguna layanan	S	S	P
2	Keterlambatan respon *service desk*	S	S	P
3	Kesalahan pencatatan permintaan layanan dan insiden	S	S	P
4	Kegagalan akses sistem e-ticket	S	S	P
5	Log permintaan layanan dan insiden tidak lengkap	S	S	P
6	Penyalahgunaan hak akses permintaan layanan secara sengaja	S	S	P
7	Pengabaian laporan insiden oleh teknisi/staf service desk	S	S	P
8	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan	S	S	P
9	Penanganan insiden dan pemenuhan permintaan layanan overdue	S	S	P
10	Kesalahan penanganan insiden dan pemenuhan permintaan layanan	S	S	P
11	Ketidakpuasan user dengan layanan	S	S	P
12	Ketidakjelasan status permintaan layanan dan insiden	S	S	P
13	Kesalahan pendefinisan tren pada laporan	S	S	P

No.	Risiko	Tipe Risiko		
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT operations and Service Delivery
14	Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan	S	S	P

Berdasarkan Tabel 5.8 di atas, keseluruhan risiko termasuk dalam tipe *IT Operations and Service Delivery* karena skenario risiko pada *service desk* seluruhnya berupa aktivitas operasional dan pemberian layanan TI pada pengguna.

5.5.2 Penentuan Kategori Risiko

Selanjutnya adalah menentukan kategori terhadap kemungkinan risiko TI pada *risk event*. Berikut pemetaan kategori risiko ditampilkan pada Tabel 5.9.

Tabel 5.9 Penentuan Kategori Risiko

No	Kategori Risiko	ID Risiko	Risiko
1	*IT expertise and skill*	IT01	Penanganan insiden dan pemenuhan permintaan layanan overdue
2		IT02	Kesalahan penanganan insiden dan pemenuhan permintaan layanan
3		IT03	Kesalahan pemahaman permintaan pengguna layanan
4		IT04	Keterlambatan respon *service desk*

No	Kategori Risiko	ID Risiko	Risiko
5	*Staff operations (human error and malicious intent)*	SO01	Kesalahan pencatatan permintaan layanan dan insiden
6		SO02	Log permintaan layanan dan insiden tidak lengkap
7		SO03	Pengabaian laporan insiden oleh teknisi/staf *service desk*
8		SO04	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan
9		SO05	Ketidakpuasan user dengan layanan
10		SO06	Ketidakjelasan status permintaan layanan dan insiden
11		SO07	Kesalahan pendefinisan tren pada laporan
13	*Software*	SW01	Kegagalan akses sistem e-ticket
14		SW02	Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan
15	*Logical attacks*	LA01	Penyalahgunaan hak akses permintaan layanan secara sengaja

5.5.3 Penentuan Faktor Risiko

Setelah mengategorikan risiko berdasarkan ketentuan yang ada pada *best practice*, selanjutnya menentukan faktor yang mempengaruhi risiko terjadi pada proses pengelolaan permintaan layanan dan insiden, baik faktor internal maupun eksternal. Berikut penentuan faktor risiko ditampilkan pada Tabel 5.10.

Tabel 5.10 Penentuan Faktor Risiko

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
IT01	Penanganan insiden dan pemenuhan permintaan layanan overdue	***Complexity of IT*** Kompleksnya sistem TI yang dilaporkan. ***Strategic priorities*** Salah dalam melaksanakan strategi prioritas penanganan. ***Financial capacity*** Lamanya persetujuan pemenuhan permintaan oleh KaSubDit Layanan TSI dikarenakan di luar kapasitas finansial.	***Regulatory environment*** Peraturan organisasi yang membantasi untuk menangani insiden dan memenuhi permintaan layanan.
IT02	Kesalahan penanganan insiden dan pemenuhan permintaan layanan	***Operating model*** *Service desk* tidak mendokumentasi-kan (atau tidak lengkap) pendefinisian klasifikasi, prioritasi, serta prosedur permintaan & insiden sehingga salah dalam mendefinisikan di operasionalnya. ***Complexity of IT*** Kompleksnya sistem TI yang harus ditangani atau	***Technology status and evolution*** Perkembangan teknologi baru yang menyebabkan kompleksnya insiden terkait layanan TI.

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		di luar insiden yang umum ditangani oleh teknisi/*service desk*. ***Culture of enterprise*** Teknisi/*service desk* tidak terbiasa menangani pelaporan serupa. ***Strategic importance of IT in the enterprise*** Tidak terdapat strategi TI yang baik pada perusahaan terkait pengelolaan permintaan layanan dan insiden, seperti tidak terdapat pelatihan khusus penanganan insiden sehingga menyebabkan teknisi/*service desk* tidak menguasai perkembangan ilmu pengetahuan dalam menangani insiden.	
SO01	Kesalahan pencatatan permintaan layanan dan insiden	***Complexity of IT*** Sistem e-ticket kompleks dan banyak bug/error sehingga banyak kesalahan pencatatan.	***Technology status and evolution*** Evolusi teknologi yang mempengaruhi adaptasi sistem e-ticket

ID Risiko	Risiko	Faktor Risiko	
		Internal	Eksternal
SO02	Log permintaan layanan dan insiden tidak lengkap	***Operating model*** Kesalahan dalam operasional pengelolaan permintaan dan insiden.	***Technology status and evolution*** Perkembangan teknologi untuk *service desk* dalam mengelola pencatatan pelaporan.
SW01	Kegagalan akses sistem e-ticket	***Complexity of IT*** Sistem e-ticket kompleks dan banyak bug/error**.**	***Technology status and evolution*** Perkembangan teknologi menuntut sistem e-ticket untuk selalu diupdate. Threat landscape Ancaman serangan sistem dari pihak tidak berwenang.
LA01	Penyalahgu-naan hak akses permintaan layanan secara sengaja	***Complexity of IT*** Sistem e-ticket tidak menerapkan standar keamanan yang tinggi.	***Threat landscape*** Ancaman serangan sistem milik service desk dari pihak tidak berwenang.

Untuk hasil penentuan faktor risiko yang telah dilakukan secara lengkap telah terlampir pada **LAMPIRAN G**.

5.5.4 Pemetaan Risiko terhadap Proses Service Desk

Setiap kemungkinan risiko TI yang teridentifikasi merupakan risiko yang terdapat pada proses pengelolaan permintaan

layanan dan insiden oleh unit *service desk* DPTSI. Berikut pemetaan risiko terhadap proses *service desk* berdasarkan COBIT 5 DSS02 ditampilkan pada Tabel 5.11.

Tabel 5.11 Pemetaan Risiko terhadap Proses Service Desk

Kategori Risiko	ID Risiko	Risiko	Pemetaan Risiko Operasional
IT expertise and skill	IT01	Penanganan insiden dan pemenuhan permintaan layanan overdue	**DSS02.03** Memverifikasikan, menyetujui dan memenuhi permintaan layanan. **DSS02.05** Menyelesaikan dan Memulihkan Insiden.
	IT02	Kesalahan penanganan insiden dan pemenuhan permintaan layanan	**DSS02.01** Mendefinisikan skema klasifikasi insiden dan permintaan layanan. **DSS02.05** Menyelesaikan dan Memulihkan Insiden.
	IT03	Kesalahan pemahaman permintaan pengguna layanan	**DSS02.01** Mendefinisikan skema klasifikasi insiden dan permintaan layanan. **DSS02.03** Memverifikasikan, menyetujui dan memenuhi permintaan layanan. **DSS02.05** Menyelesaikan dan Memulihkan Insiden.

Kategori Risiko	ID Risiko	Risiko	Pemetaan Risiko Operasional
	IT04	Keterlambatan respon *service desk*	**DSS02.02** Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden. **DSS02.03** Memverifikasikan, menyetujui dan memenuhi permintaan layanan. **DSS02.05** Menyelesaikan dan Memulihkan Insiden.
Staff operations (human error and malicious intent)	SO01	Kesalahan pencatatan permintaan layanan dan insiden	**DSS02.02** Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden.
	SO02	Log permintaan layanan dan insiden tidak lengkap	**DSS02.02** Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden.
	SO03	Pengabaian laporan insiden oleh teknisi/staf *service desk*	**DSS02.03** Memverifikasikan, menyetujui dan memenuhi permintaan layanan. **DSS02.04** Menginvestigasikan, mendiagnosis dan mengalokasikan insiden.

Kategori Risiko	ID Risiko	Risiko	Pemetaan Risiko Operasional
	SO04	Kesalahan mengalokasi-kan penanganan insiden dan pemenuhan permintaan layanan	**DSS02.03** Memverifikasikan, menyetujui dan memenuhi permintaan layanan. **DSS02.04** Menginvestigasikan, mendiagnosis dan mengalokasikan insiden.
	SO05	Ketidakpuasan user dengan layanan	**DSS02.03** Memverifikasikan, menyetujui dan memenuhi permintaan layanan. **DSS02.05** Menyelesaikan dan Memulihkan Insiden. **DSS02.06** Menutup Permintaan Layanan dan Insiden.
	SO06	Ketidakjelasan status permintaan layanan dan insiden	**DSS02.07** Melacak Status dan Membuat Laporan
	SO07	Kesalahan pendefinisan tren pada laporan	**DSS02.07** Melacak Status dan Membuat Laporan.
Software	SW01	Kegagalan akses sistem e-ticket	**DSS02.02** Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden

Kategori Risiko	ID Risiko	Risiko	Pemetaan Risiko Operasional
	SW02	Laporan tidak terdistribusi-kan	**DSS02.07** Melacak Status dan Membuat Laporan.
Logical attacks	LA01	Penyalahgunaa n hak akses permintaan layanan secara sengaja	**DSS02.03** Memverifikasikan, menyetujui dan memenuhi permintaan layanan.

5.5.5 Pembuatan Skenario Risiko

Selanjutnya dilakukan pembuatan dan pembaharuan skenario risiko TI secara teratur berdasarkan dua jenis, yaitu skenario positif dan skenario negatif. Berikut skenario risiko TI ditampilkan pada Tabel 5.12.

Tabel 5.12 Pembuatan Skenario Risiko

ID Risiko	Risiko	Contoh Skenario	
		Skenario Negatif	**Skenario Positif**
IT01	Penanganan insiden dan pemenuhan permintaan layanan overdue	Penyelesaian penanganan laporan insiden dan permintaan layanan di luar batas waktu yang dijanjikan oleh *service desk* sehingga banyaknya komplain pengguna layanan.	Proses bisnis layanan berjalan dengan baik, penyelesaian penanganan laporan insiden dan permintaan layanan ssuai dengan durasi yang dijanjikan oleh *service desk*.
IT02	Kesalahan penanganan insiden dan pemenuhan permintaan layanan	Insiden tidak terselesaikan dan permintaan layanan tidak dipenuhi sesuai harapan pengguna.	Insiden terlapor ditangani dan keadaan normal dikembalikan seperti harapan pengguna. Permintaan layanan yang diajukan pengguna dapat dipenuhi sesuai harapan dan memuaskan pengguna.
IT03	Kesalahan pemahaman permintaan pengguna layanan	Permintaan layanan tidak terpenuhi sesuai harapan pengguna sehingga laporan permintaan layanan tidak dapat segera ditutup sehingga tidak memenuhi perjanjian tingkat layanan yang didokumentasikan dalam *Service Level Agreements* (SLA).	Laporan permintaan layanan dapat dipenuhi sesuai harapan pengguna sehingga tingkat layanan yang disepakati antara pengguna dan organisasi dapat terpenuhi.

ID Risiko	Risiko	Contoh Skenario	
		Skenario Negatif	**Skenario Positif**
IT04	Keterlambatan respon *service desk*	Banyaknya komplain pengguna layanan, pelaporan permintaan layanan dan insiden menumpuk pada sistem *service desk* sehingga proses bisnis tidak berjalan dengan baik.	Proses bisnis layanan berjalan dengan baik serta meningkatnya kepuasan pengguna.
SO01	Kesalahan pencatatan permintaan layanan dan insiden	Kesalahan dalam proses pengelolaan permintaan dan insiden selanjutnya sehingga insiden tidak terselesaikan dan permintaan layanan tidak dipenuhi sesuai harapan pengguna. Hal ini menimbulkan pelayanan *service desk* tidak prima.	Mempermudah dalam pengelolaan permintaan dan insiden hingga proses penutupan laporan. Insiden terselesaikan dan permintaan layanan dipenuhi sesuai harapan pengguna
SO02	Log permintaan layanan dan insiden tidak lengkap	Pemenuhan permintaan dan penanganan insiden tidak sesuai pelaporan yang diharapkan pengguna. Sehingga insiden tidak terselesaikan dan permintaan layanan tidak dipenuhi sesuai harapan pengguna	Log sesuai dengan pelaporan yang masuk ke sistem segera dapat dikelola. Insiden dapat dipulihkan dan permintaan layanan dipenuhi sesuai harapan pengguna.

ID Risiko	Risiko	Contoh Skenario	
		Skenario Negatif	**Skenario Positif**
SO03	Pengabaian laporan insiden oleh teknisi/staf *service desk*	*Service desk* mengabaikan laporan insiden dan permintaan layanan dari pengguna sehingga banyak laporan yang menumpuk sehingga tidak sesuai perjanjian tingkat layanan.	Pelaporan dapat segera ditangani / dipenuhi sehingga dapat memenuhi perjanjian tingkat layanan.
SO04	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan	Teknisi yang menangani pelaporan mengalami kesulitan dalam mengidentifikasi permintaan & insiden. Hal ini mengakibatkan insiden tidak terselesaikan dan permintaan layanan tidak dipenuhi sesuai harapan pengguna.	Laporan permintaan dan insiden dapat diidentifikasi dengan tepat oleh teknis sehingga insiden dapat diselesaikan dan permintaan layanan dipenuhi sesuai harapan pengguna..
SO05	Ketidakpuasan user dengan layanan	*Service desk* tidak melakukan verifikasi kepuasan pengguna terhadap laporan insiden dan permintaan layanan yang telah selesai ditanggani dan dipenuhi. Pengguna kecewa atas pelayanan *service desk*.	Laporan insiden dan permintaan layanan yang telah selesai ditanggani dan dipenuhi dapat dipastikan memenuhi kepuasan pengguna/pelapor layanan. Berkurangnya komplain pengguna dan meningkatkan kepercayaan pengguna terhadap layanan *service desk*.

ID Risiko	Risiko	Contoh Skenario	
		Skenario Negatif	**Skenario Positif**
SO06	Ketidakjelasan status permintaan layanan dan insiden	Pengguna tidak mengetahui apakah permintaan layanan dan insiden sedang direspon / selesai ditangani / telah ditutup sehingga pengguna/pelapor harus bertanya kembali ke *service desk*. Sedangkan *service desk* juga berisiko tidak mengetahui status permintaan layanan dan insiden yang sedang ditangani oleh teknisi (ketika telah alokasi / eskalasi dilakukan).	Baik pengguna/pelapor layanan, *service desk*, maupun teknisi mengetahui status permintaan layanan dan insiden dengan jelas sehingga laporan permintaan layanan dan insiden dapat segera dikelola dengan efektif.
SO07	Kesalahan pendefinisan tren pada laporan	Insiden terjadi berulang namun tidak diidentifikasi sebagai *problem*.	Tepat dalam mengidentifikasi insiden yang berubah status menjadi *problem* untuk segera diperbaiki hingga akar masalah.
SW01	Kegagalan akses sistem e-ticket	Pengguna tidak dapat mengakses sistem *e-ticket* untuk membuat pelaporan serta melacak status laporan. Menumpuknya pelaporan melalui sistem manual (*e-mail* dan telepon), serta *service desk* tidak	Pengguna dapat membuat pelaporan dan mengecek status, serta *service desk* dan teknisi dapat mengecek pelaporan untuk dikelola secara tanggap dan tepat.

ID Risiko	Risiko	Contoh Skenario	
		Skenario Negatif	**Skenario Positif**
		dapat melacak status pelaporan yang sedang ditangani.	
SW02	Laporan tidak terdistribusi-kan	Tidak adanya perubahan yang lebih baik terhadap evaluasi layanan pengelolaan permintaan layanan dan insiden.	Manajemen organisasi dapat mengevaluasi hasil pengelolaan permintaan layanan dan insiden berdasarkan laporan yang telah didistribusikan.
LA01	Penyalahgunaan hak akses permintaan layanan secara sengaja	Keamanan informasi pada sistem *service desk* atau sistem *e-ticket* tidak terlindungi. Kerugian organisasi terhadap pemenuhan permintaan di luar hak pengguna, baik finansial maupun aset kritis organisasi.	Keamanan informasi pada sistem *service desk* atau sistem *e-ticket* terlindungi. Organisasi tidak mengalami kerugian baik finansial dikarenakan pemenuhan permintaan layanan sesuai sebagaimana prosedurnya, serta aset kritis organisasi tidak terancam oleh pihak tidak berwenang.

5.5.6 Penilaian Risiko

Pada tahap penilaian risiko TI berdasarkan perkiraan frekuensi dan dampaknya besarnya keuntungan atau kerugian yang terkait dengan skenario risiko TI. Perhitungan rata-rata penilaian risiko untuk keseluruhan peringkat dampak, mengikuti aturan pembulatan desimal di mana apabila nilai desimal di bawah 0,5 maka bulatkan angka ke bawah satu digit, sebaliknya apabila nilai desimal di atas 0,5 maka bulatkan angka ke atas satu digit. Berikut hasil penilaian risiko TI yang telah dipetakan menjadi level penilaian risiko ditampilkan pada Tabel 5.13.

Tabel 5.13 Hasil Penilaian Risiko

ID Risiko	Risiko	Peringkat Frekuensi	Peringkat Dampak					Level Penilaian Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Keseluruhan Peringkat Dampak	
IT01	Penanganan insiden dan pemenuhan permintaan layanan overdue	4	1	1	3	1	1	Medium

ID Risiko	Risiko	Peringkat Frekuensi	Peringkat Dampak					Level Penilaian Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Keseluruhan Peringkat Dampak	
IT02	Kesalahan penanganan insiden dan pemenuhan permintaan layanan	2	1	1	4	1	2	Medium
IT03	Kesalahan pemahaman permintaan pengguna layanan	3	1	1	4	1	2	Medium
IT04	Keterlambatan respon *service desk*	4	1	1	4	1	2	High
SO01	Kesalahan pencatatan permintaan layanan dan insiden	3	1	1	4	1	2	Medium
SO02	Log permintaan layanan dan insiden tidak lengkap	3	1	1	4	1	2	Medium

ID Risiko	Risiko	Peringkat Frekuensi	Peringkat Dampak					Level Penilaian Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Keseluruhan Peringkat Dampak	
SO03	Pengabaian laporan insiden oleh teknisi/staf *service desk*	1	1	1	4	1	2	Low
SO04	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan	3	1	1	4	1	2	Medium
SO05	Ketidakpuasan user dengan layanan	4	1	1	3	1	1	Medium
SO06	Ketidakjelasan status permintaan layanan dan insiden	4	1	1	3	1	1	Medium
SO07	Kesalahan pendefinisan tren pada laporan	3	1	1	4	1	2	Medium

ID Risiko	Risiko	Peringkat Frekuensi	Peringkat Dampak					Level Penilaian Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Keseluruhan Peringkat Dampak	
SW01	Kegagalan akses sistem e-ticket	3	1	1	3	1	1	Medium
SW02	Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan	2	1	1	3	1	1	Low
LA01	Penyalahgunaan hak akses permintaan layanan secara sengaja	3	1	1	4	1	2	Medium

5.6 Pemetaan Risiko terhadap Control Objective

Hasil dari analisis termasuk penilaian risiko akan dipetakan dalam *control objective* yang dihasilkan dari pemetaan proses berdasarkan COBIT 5 DSS02 dengan *Service Desk Standard.* Pemetaan dilakukan dengan menghubungkan antara risiko dengan *control objective* guna memastikan apakah organisasi telah menerapkan kontrol yang tepat untuk menangani risiko. Tabel 5.14 berikut ini adalah hasil pemetaan risiko terhadap kontrol yang ada. Level risiko ini nantinya akan digunakan sebagai acuan pada perangkat audit yang telah disusun yaitu Laporan Temuan Audit dalam mengidentifikasi risiko terkait temuan audit yang nantinya akan digunakan sebagai dasar dalam melakukan rekomendasi perbaikan.

Tabel 5.14 Pemetaan Risiko terhadap Control Objective

ID Risiko	Risiko	Level Penilaian	Control Objective
IT01	Penanganan insiden dan pemenuhan permintaan layanan overdue	Medium	**CO.08** Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden.
IT02	Kesalahan penanganan insiden dan pemenuhan permintaan layanan	Medium	**CO.08** Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden. **CO.09** Memastikan Adanya Penggunaan Informasi Pengelolaan Insiden. **CO.10** Memastikan Adanya Penutupan Permintaan Layanan dan Insiden.

IT03	Kesalahan pemahaman permintaan pengguna layanan	Medium	**CO.01** Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian. **CO.06** Memastikan Adanya Verifikasi Hak Penggunaan Permintaan Layanan.
IT04	Keterlambatan respon *service desk*	High	**CO.01** Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian.
SO01	Kesalahan pencatatan permintaan layanan dan insiden	Medium	**CO.01** Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian. **CO.03** Memastikan Adanya Prosedur Pencatatan Permintaan Layanan dan Insiden.
SO02	Log permintaan layanan dan insiden tidak lengkap	Medium	**CO.02** Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden. **CO.03** Memastikan Adanya Prosedur Pencatatan

			Permintaan Layanan dan Insiden.
SO03	Pengabaian laporan insiden oleh teknisi/staf *service desk*	Low	**CO.08** Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden.
SO04	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan	Medium	**CO.09** Memastikan Adanya Alokasi ke Fungsi Spesialis.
SO05	Ketidakpuasan user dengan layanan	Medium	**CO.04** Memastikan Adanya Skema Prioritisasi Permintaan Layanan dan Insiden. **CO.05** Memastikan Adanya Klasifikasi Permintaan Layanan dan Insiden. **CO.10** Memastikan Adanya Penutupan Permintaan Layanan dan Insiden.
SO06	Ketidakjelasan status permintaan layanan dan insiden	Medium	**CO.10** Memastikan Adanya Penutupan Permintaan Layanan dan Insiden. **CO.11** Memastikan Adanya Laporan Pengelolaan Permintaan Layanan dan Insiden.

SO07	Kesalahan pendefinisan tren pada laporan	Medium	**CO.12** Memastikan Adanya Mekanisme Peningkatan Pengelolaan Permintaan Layanan dan Insiden
SW01	Kegagalan akses sistem e-ticket	Medium	**CO.02** Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden
SW02	Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan	Low	**CO.11** Memastikan Adanya Laporan Pengelolaan Permintaan Layanan dan Insiden.
LA01	Penyalahgunaan hak akses permintaan layanan secara sengaja	Medium	**CO.06** Memastikan Adanya Verifikasi Hak Penggunaan Permintaan Layanan. **CO.07** Memastikan Adanya Persetujuan Pemenuhan Permintaan Layanan.

Berdasarkan hasil pemetaan kemungkinan risiko proses pengelolaan permintaan layanan dan insiden dengan kendali/kontrol tujuan yang dilakukan guna memitigasi risiko yang ada, maka akan digunakan keseluruhan dua belas *control objective*. Setiap *control objective* yang terpetakan dengan risiko ini akan disusun menjadi dokumen perangkat audit.

5.7 Pembuatan Perangkat Audit

Pembuatan perangkat audit berdasarkan hasil pemetaan *control objective* dengan risiko proses pengelolaan permintaan layanan dan insiden yang telah dianalisis. Setiap perangkat audit yang

disusun terdiri dari dokumen perangkat audit dan dokumen panduan penggunaannya.

Perangkat audit memiliki dua belas (12) dokumen perangkat yang telah disusun berdasarkan *control objective* pada *Service Desk Standard*. Setiap *control objective* yang disusun menjadi dokumen perangkat audit ini memiliki ID dokumen dengan penamaan "P" yaitu Perangkat Audit, "02" yaitu berasal dari COBIT domain DSS02, kemudian diikuti dengan penomoran berupa angka urutan nomor ID *control objective*. Tabel 5.15 menampilkan daftar dokumen perangkat audit yang ada.

Tabel 5.15 Daftar Perangkat Audit

No.	ID Control Objective	ID Dokumen	Nama Dokumen
1	CO.01	PA02.01	Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian
2	CO.02	PA02.02	Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden
3	CO.03	PA02.03	Memastikan Adanya Prosedur Pencatatan Permintaan Layanan dan Insiden
4	CO.04	PA02.04	Memastikan Adanya Prioritisasi Permintaan Layanan dan Insiden
5	CO.05	PA02.05	Memastikan Adanya Klasifikasi Permintaan Layanan dan Insiden
6	CO.06	PA02.06	Memastikan Adanya Verifikasi Hak Penggunaan Permintaan Layanan
7	CO.07	PA02.07	Memastikan Adanya Persetujuan Pemenuhan Permintaan Layanan
8	CO.08	PA02.08	Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden

No.	ID Control Objective	ID Dokumen	Nama Dokumen
9	CO.09	PA02.09	Memastikan Adanya Penggunaan Informasi Pengelolaan Insiden
10	CO.10	PA02.10	Memastikan Adanya Penutupan Permintaan Layanan dan Insiden
11	CO.11	PA02.11	Memastikan Adanya Laporan Pengelolaan Permintaan Layanan dan Insiden
12	CO.12	PA02.12	Memastikan Adanya Peningkatan Pengelolaan Permintaan Layanan dan Insiden

Aktivitas pertama yang dilakukan dalam pembuatan dokumen perangkat audit ini adalah memastikan kesesuaian setiap *control objective* yang akan dibuat. Aktivitas kedua adalah menyusun prosedur audit untuk memenuhi setiap poin pemeriksaan berdasarkan acuan standar yang digunakan yaitu sub-konsep atau kontrol pada *Service Desk Standard*. Setiap penguraian prosedur audit ditentukan jenis pengujian (*testing*) yang akan dilakukan. Setelah dibuat prosedur audit beserta penentuan jenis *testing*, maka langkah selanjutnya adalah membuat beberapa poin pertanyaan atau *audit checklist* untuk memastikan prosedur audit dilakukan. *Audit checklist* yang dibuat untuk memenuhi kontrol pada poin pemeriksaan. Selain *audit checklist*, juga disertakan bukti apa yang harus ada ketika auditor menjawab iya, tidak atau parsial pada setiap *audit checklist* yang ada. Setiap *audit checklist* memiliki kolom Bukti dan Temuan. Pada kolom tersebut terdapat uraian bukti yang diekspektasikan ada dengan melihat kontrol dan kondisi nyata yang ada di organisasi, terlepas dari perbedaan penamaan yang digunakan oleh organisasi. Jika auditor menemukan ketidaksesuaian pada *audit checklist* terkait, maka temuan dituliskan pada kolom tersebut beserta bukti yang diperoleh. Langkah terakhir adalah membuat sebuah template laporan temuan audit untuk setiap perangkat.

Setelah seluruh dokumen perangkat audit telah disusun, selanjutnya dilakukan pembuatan Panduan Penggunaan Perangkat Audit yang terdiri dari tiga bagian, yaitu Pendahuluan, Panduan Umum, dan Panduan Khusus. Panduan penggunaan perangkat audit ini berupa dokumen yang terpisah dengan dokumen perangkat audit.

Halaman ini sengaja dikosongkan

BAB VI
HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan hasil yang didapatkan dari penulisan dan pembahasan secara keseluruhan yang didapatkan dari penelitian.

6.1 Hasil Perangkat Audit

Hasil pembuatan perangkat audit adalah dua belas (12) dokumen perangkat audit dan satu dokumen panduan penggunaan perangkat audit.

6.1.1 Dokumen Perangkat Audit

Setiap dokumen perangkat audit yang telah disusun memiliki dua komponen, yaitu Daftar Cek Audit (*Audit Checklist*) dan Laporan Temuan Audit.

a. Daftar Cek Audit

Di dalam daftar cek audit, terdapat poin pemeriksaan yang mengacu pada sub-konsep atau kontrol pada *Service Desk Standard* yang terpetakan dalam setiap dokumen perangkat audit. Pada setiap poin pemeriksaan akan diurakan menjadi beberapa langkah pemeriksaan atau prosedur yang mengarahkan pada pemenuhan kontrol pada poin pemeriksaan terkait. Setiap prosedur audit berisi pertanyaan-pertanyaan yang disebut *audit cheklist*. Penguraian prosedur audit untuk memastikan tercapainya poin pemeriksaan yang telah dirumuskan yang disesuaikan dengan Jenis Pengujian (*Testing*) yang akan dilakukan. *Audit checklist* ditentukan berdasarkan prosedur dengan melakukan pengisian pada bagian yang harus diisi dengan tanda centang (√).

Jenis pengujian terbagi menjadi *compliance* dan *substantive*. Jenis pengujian *compliance* memiliki pertanyaan pemeriksaan tentang ketersediaan dan kelengkapan pendokumentasian yang harus disiapkan oleh

organisasi, sedangkan jenis pengujian *substantive* memiliki pertanyaan pemeriksaan yang berisi lebih banyak pendetailan pada perangkat audit guna melakukan cek kesesuaian dan kebenaran setiap proses dan aktivitas yang dijalankan *service desk* dalam mengelola permintaan layanan dan insiden terhadap peraturan atau kebijakan yang ada.

Pada setiap pertanyaan *audit checklist* dilengkapi dengan kolom Bukti dan Temuan yang berisi bukti-bukti setiap poin pertanyaan *audit checklist* serta temuan ketidaksesuaian yang didapatkan oleh auditor selama proses pemeriksaan. Bukti yang didefinisikan pada perangkat audit adalah bukti yang diekspektasikan ada dengan melihat kontrol dan kondisi nyata yang ada di organisasi, terlepas dari bagaimana penamaannya. Sehingga tidak menutup kemungkinan ada bukti dengan nama lain namun memiliki konten yang sesuai dengan bukti yang diekspektasikan tersebut. Berikut pada Gambar 6.1 ditampilkan contoh dari Daftar Cek Audit pada perangkat audit dengan nomor ID Dokumen PA02.01.

	PERANGKAT AUDIT PENGELOLAAN PERMMINTAAN LAYANAN DAN INSIDEN PADA SERVICE DESK DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER KOTA SURABAYA						
	CO.01 Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian			PA02.01			
				AUDITOR			AUDITEE
TANGGAL :							
Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
1. Pemeriksaan adanya pendefinisian layanan yang disetujui oleh pelanggan bisnis dan dipublikasikan pada pengguna akhir	Auditor melakukan cek terkait adanya pendefinisian layanan	Compliance	Apakah organisasi memiliki pendefinisian layanan yang disediakan untuk pengguna?				(Dokumen katalog layanan, screenshot website)
	Auditor melakukan cek terkait persetujuan layanan oleh pelanggan bisnis	Substantive	Apakah layanan yang terdefinisi telah disetujui oleh pelanggan bisnis?				(Tanda tangan pada dokumen *Service Level Agreements* (SLAs))
	Auditor memeriksa apakah seluruh pengguna layanan mengetahui layanan yang ditawarkan DPTSI. a. Melakukan cek ketersediaan media publikasi b. Melakukan survei pada pengguna layanan	Substantive	Apakah terdapat media publikasi yang digunakan *service desk* pada pengguna layanan terkait layanan yang dimiliki organisasi ?				(Screenshot website, Foto publikasi layanan)
		Substantive	Apakah pengguna layanan mengetahui ketersediaan layanan yang dimiliki organisasi?				(Survei pengguna layanan)
	Auditor melakukan cek kesesuaian permintaan layanan dengan layanan yang terdefinisi	Substantive	Apakah seluruh permintaan layanan yang diajukan oleh pengguna telah sama seperti pendefinisian layanan?				(Log permintaan layanan)
2. Pemeriksaan adanya pendefinisian manajemen tingkat	Auditor melakukan cek terkait manajemen tingkat layanan sebagai proses	Compliance	Apakah terdapat pendefinisian perjanjian tingkat layanan organisasi?				(Dokumen *Service Level Agreements* (SLAs))

Gambar 6.1 Hasil Pembuatan Daftar Cek Audit

b. Laporan Temuan Audit

Laporan Temuan Audit merupakan sebuah formulir laporan pemeriksaan yang digunakan auditor dalam merangkum temuan dari proses pemeriksaan setiap kendali tujuan (*control objective*). Di dalam template laporan ini, auditor juga dapat menambahkan saran perbaikan terkait kendali/kontrol yang seharusnya dilakukan oleh *service desk* untuk memperbaiki hal-hal yang ternyata tidak sesuai dengan acuan standar yang digunakan, siapa yang bertanggung jawab, batas akhir penyelesaian pembahasan dan juga persetujuan dari pihak manajemen DPTSI.

Setiap elemen pada Laporan Temuan Audit ini didasari pada beberapa hal sesuai ISO 19011, di mana harus diperjelas elemen dalam pelaksanaan audit, seperti waktu serta objek proses audit. Maka pada Laporan Temuan Audit ini terdiri dari beberapa elemen yang harus diperhatikan dan tertuang dalam sebuah kolom, diantaranya:

- Tanggal Pemeriksaan – berisi waktu pelaksanaan audit.
- Auditor – berisi nama siapa yang bertugas melaksanakan audit pada *control objective* tersebut.
- Auditee – berisi nama siapa yang diperiksa oleh auditor.
- Kesimpulan – berisi kesimpulan temuan audit yang telah dilakukan selama proses pemeriksaan.
- Klasifikasi – berisi pemilihan klasifikasi mode level temuan yang menyatakan seberapa penting temuan yang telah didapatkan. Level klasifikasi yang lebih tinggi menunjukkan bahwa tindak lanjut perbaikan harus segera dilakukan oleh auditee atau organisasi terkait.
- Risiko Terkait – berisi risiko terkait temuan beserta levelnya berdasarkan analisis risiko yang telah dilakukan. Risiko terkait ini guna menunjukkan

seberapa penting *control objective* harus diterapkan untuk memitigasi atau menghindari kemungkinan risiko.

- Rekomendasi – berisi daftar rekomendasi atau usulan tindak lanjut berupa perbaikan yang disarankan oleh auditee kepada manajemen organisasi atau unit *service desk* sehingga *control objective* dapat dilaksanakan dengan baik.
- Penanggung Jawab Perbaikan – berisi nama siapa yang bertanggung jawab dalam tindak perbaikan yang diusulkan.
- Tanggal Penyelesaian Perbaikan – berisi waktu batas penyelesaian perbaikan atau tindak lanjut yang dilakukan oleh manajemen organisasi atau unit *service desk*.
- Pengesahan – berisi tanda tangan pengesahan oleh pihak manajemen organisasi yang terkait. Penandatanganan kolom pengesahan ini menunjukkan bahwa pihak organisasi menerima apa yang telah dituliskan auditor dan akan melakukan perbaikan sesuai dengan batas waktu yang telah ditentukan.

Dalam pembuatan template Laporan Temuan Audit ini, penulis mempertimbangkan pentingnya dilakukan perbaikan untuk setiap temuan yang dicatatkan. Laporan Temuan Audit ini nantinya akan diletakkan pada setiap perangkat audit dikarenakan adanya pertimbangan rincian dan tingkat kedetailan untuk setiap temuan *control objective*. Pada Gambar 6.2 dibawah ini merupakan contoh dari template Laporan Temuan Audit.

<table>
<tr><td colspan="3">LAPORAN TEMUAN AUDIT
No. Perangkat Audit : PA02.01
Control Objective : CO.01 Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian</td></tr>
<tr><td>Tanggal Pemeriksaan : (dd/mm/yy)</td><td>Auditor : (Tuliskan nama Auditor pemeriksa kontrol)</td><td>Auditee : (Tuliskan nama Auditee)</td></tr>
<tr><td colspan="2" rowspan="2">Kesimpulan Temuan :
(Tuliskan kesimpulan temuan auditor terhadap aktivitas yang diaudit di organisasi yang mengacu pada hirarki prosedur audit, tuliskan juga temuan compliance dan substantive masing-masing dengan penjelasannya)</td><td>Klasifikasi :
◯ Major non-conformity
◯ Minor non-comformity
◯ Observation
◯ Improvement Possibility</td></tr>
<tr><td>Risiko Terkait :
<table><tr><th>Risiko</th><th>Level</th></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td colspan="2">Rekomendasi :
(Tuliskan rekomendasi perbaikan sebagai usulan tindak lanjut dari auditor terhadap temuan yang sudah disampaikan)</td><td>Penanggung Jawab Perbaikan :
(Tuliskan nama penanggung jawab terhadap tindakan perbaikan)
Tanggal Penyelesaian Perbaikan :
(Tuliskan batas waktu untuk menyelesaikan tindak perbaikan)</td></tr>
<tr><td colspan="2">Pengesahan
Auditee :

(.....)</td><td>Auditor :

(.....)</td></tr>
</table>

Gambar 6.2 Hasil Pembuatan Template Laporan Temuan Audit

Untuk hasil pembuatan perangkat audit yang telah dilakukan secara lengkap disusun pada dokumen terpisah dengan buku tugas akhir.

6.1.2 Dokumen Panduan Penggunaan Perangkat Audit

Sebuah dokumen panduan perangkat audit yang telah disusun memiliki tiga bagian, berikut diantaranya:

1. Pendahuluan

Pada bagian pendahuluan menjelaskan mengenai latar belakang pembuatan panduan penggunaan perangkat audit. Selain itu dalam bagian ini juga terdapat beberapa sub-bagian diantaranya:

a. Tujuan - berisi uraian tujuan dari pembuatan dokumen panduan penggunaan perangkat audit.

b. Ruang Lingkup Dokumen – berisi penentuan ruang lingkup dokumen panduan penggunaan perangkat audit yang dibuat untuk digunakan auditor.

c. Definisi, Istilah, Singkatan – berisi penjabaran beberapa definisi, istilah, dan singkatan yang digunakan dalam perangkat audit pengelolaan permintaan layanan dan insiden.

d. Daftar Perangkat Audit – berisi daftar perangkat audit yang telah disusun, dengan menunjukkan ID Control Objective, ID Dokumen, dan Nama Dokumen.

e. Daftar Penilaian Risiko – berisi daftar risiko beserta hasil penilaian yang telah dilakukan oleh penulis beserta keterangan terkait bagaimana penulis mendapatkan hasil penilaian risiko tersebut.

f. **Ikhtisar Dokumen** – berisi ikhtisar dari dokumen panduan penggunaan perangkat audit.

Bagian pendahulan nantinya akan mempermudah dalam penggunaan dokumen panduan perangkat audit.

2. Panduan Umum

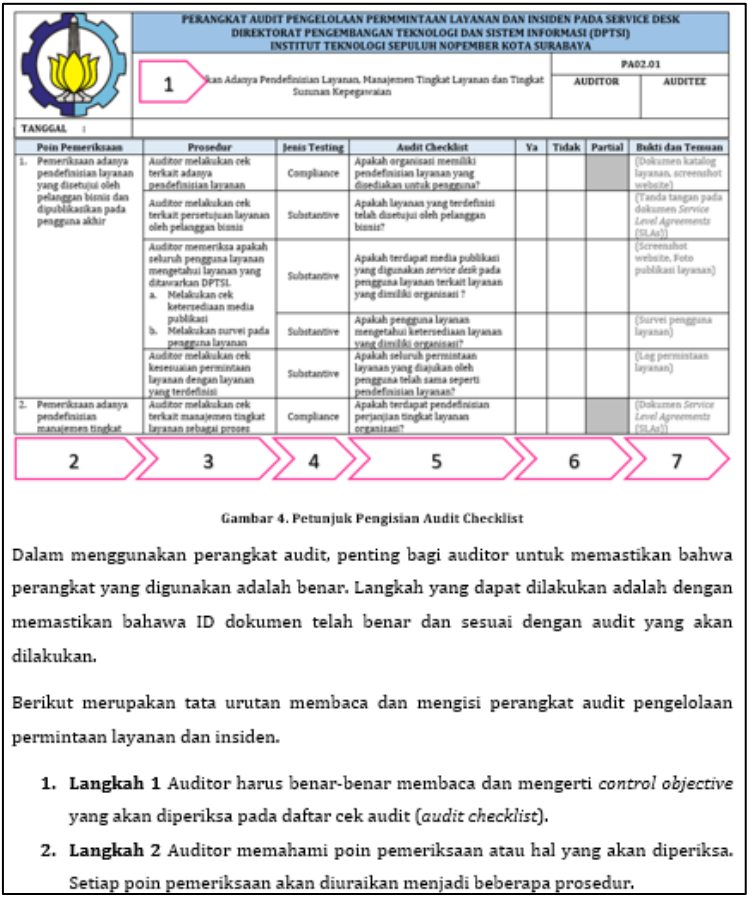
Pada bagian panduan umum menjelaskan beberapa petunjuk umum penggunaan dokumen perangkat audit. Panduan umum ini nantinya akan membantu auditor internal dalam melakukan pengisian dan penggunaan perangkat audit. Terdapat tiga sub-bagian pada panduan umum yang akan dibuat, yaitu terdiri dari:

a. Petunjuk Penggunaan Bagian Penilaian Risiko

Sub-bagian ini berisi hasil analisis risiko dan petunjuk penggunaan analisis risiko yang dapat digunakan auditor dalam pelaksanaan audit, khususnya melengkapi kolom "Risiko Terkait" pada Laporan Temuan Audit.

b. Petunjuk Pengisian Daftar Cek Audit

Dokumen perangkat audit tersusun dari dua komponen, yaitu Daftar Cek Audit (*audit checklist*) danLaporan Temuan Audit. Sub-bagian ini berisi petunjuk dalam menggunakan Daftar Cek Audit yang telah disusun. Di dalam panduan ini bagian utama yang dijelaskan adalah setiap kolom pada perangkat audit sesuai dengan penomoran untuk setiap *header* kolomnya, serta dilengkapi dengan penjelasan bagaimana cara membaca dan menggunakan daftar cek audit yang dapat terlihat pada Gambar 6.3 di bawah ini.



PERANGKAT AUDIT PENGELOLAAN PERMMINTAAN LAYANAN DAN INSIDEN PADA SERVICE DESK
DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)
INSTITUT TEKNOLOGI SEPULUH NOPEMBER KOTA SURABAYA

PA02.01

1 kan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Suzunan Kepegawaian

AUDITOR | AUDITEE

TANGGAL :

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
1. Pemeriksaan adanya pendefinisian layanan yang disetujui oleh pelanggan bisnis dan dipublikasikan pada pengguna akhir	Auditor melakukan cek terkait adanya pendefinisian layanan	Compliance	Apakah organisasi memiliki pendefinisian layanan yang disediakan untuk pengguna?				(Dokumen katalog layanan, screenshot website)
	Auditor melakukan cek terkait persetujuan layanan oleh pelanggan bisnis	Substantive	Apakah layanan yang terdefinisi telah disetujui oleh pelanggan bisnis?				(Tanda tangan pada dokumen *Service Level Agreements* (SLAs))
	Auditor memeriksa apakah seluruh pengguna layanan mengetahui layanan yang ditawarkan DPTSI. a. Melakukan cek ketersediaan media publikasi b. Melakukan survei pada pengguna layanan	Substantive	Apakah terdapat media publikasi yang digunakan *service desk* pada pengguna layanan terkait layanan yang dimiliki organisasi ?				(Screenshot website, Foto publikasi layanan)
		Substantive	Apakah pengguna layanan mengetahui ketersediaan layanan yang dimiliki organisasi?				(Survei pengguna layanan)
	Auditor melakukan cek kesesuaian permintaan layanan dengan layanan yang terdefinisi	Substantive	Apakah seluruh permintaan layanan yang diajukan oleh pengguna telah sama seperti pendefinisian layanan?				(Log permintaan layanan)
2. Pemeriksaan adanya pendefinisian manajemen tingkat	Auditor melakukan cek terkait manajemen tingkat layanan sebagai proses	Compliance	Apakah terdapat pendefinisian perjanjian tingkat layanan organisasi?				(Dokumen *Service Level Agreements* (SLAs))

2 3 4 5 6 7

Gambar 4. Petunjuk Pengisian Audit Checklist

Dalam menggunakan perangkat audit, penting bagi auditor untuk memastikan bahwa perangkat yang digunakan adalah benar. Langkah yang dapat dilakukan adalah dengan memastikan bahawa ID dokumen telah benar dan sesuai dengan audit yang akan dilakukan.

Berikut merupakan tata urutan membaca dan mengisi perangkat audit pengelolaan permintaan layanan dan insiden.

1. **Langkah 1** Auditor harus benar-benar membaca dan mengerti *control objective* yang akan diperiksa pada daftar cek audit (*audit checklist*).
2. **Langkah 2** Auditor memahami poin pemeriksaan atau hal yang akan diperiksa. Setiap poin pemeriksaan akan diuraikan menjadi beberapa prosedur.

Gambar 6.3 Petunjuk Pengisian Daftar Cek Audit

Dengan adanya panduan penggunaan daftar cek audit ini, auditor dapat memastikan bahwa perangkat yang digunakan adalah benar cara penggunaannya. Langkah awal panduan adalah memastikan auditor membaca dan memahami kontrol yang akan dilakukan pemeriksaan, baru kemudian dilanjutkan dengan langkah-langkah panduan berikutnya.

c. Petunjuk Pengisian Laporan Temuan Audit

Setelah melakukan proses audit, langkah yang harus dilakukan adalah dengan menuliskan langkah rekomendasi terhadap temuan-temuan yang dihasilkan. Terdapat beberapa bagian penting pada template laporan tersebut yang harus diperhatikan oleh auditor internal dalam menuliskan temuan dan langkah rekomendasi. Salah satu bagian dalam laporan temuan audit adalah klasifikasi temuan yang dapat membantu auditor dalam memberikan rekomendasi perbaikan. Penulis menentukan klasifikasi temuan audit berdasarkan ISO 9001:2008, berikut diantaranya [40]:

1. *Nonconformances*

   Ketidaksesuaian adalah berupa kegagalan total atau kegagalan parsial dari proses dalam sistem manajemen mutu. Sebuah ketidaksesuaian audit umumnya memerlukan analisis akar penyebab, eliminasi akar penyebab, dan/atau perubahan dalam bagaimana proses yang akan dilakukan. Ketidaksesuaian membutuhkan sebuah tindak perbaikan. Ketidaksesuaian terbagi menjadi dua klasifikasi, yaitu *major non-conformity* dan *minor non-conformity*.

   - *Major non-conformity*

     Sejumlah ketidaksesuaian dalam kontrol menyebabkan adanya kegagalan sistematis secara total atau kekurangan yang signifikan terhadap sistem mutu, baik sebagai insiden tunggal atau kombinasi dari sejumlah insiden serupa di bagian sistem mutu, atau kurangnya pelaksanaan bagian tertentu berdasarkan suatu standar yang berlaku.

   - *Minor non-conformity*

     Sebuah ketidaksesuaian dalam kontrol atau pelaksanaan prosedur yang cukup dapat menyebabkan kegagalan sistematis yang terbatas/parsial terhadap sistem mutu jika tidak diperbaiki. Jika suatu pola ketidaksesuaian minor

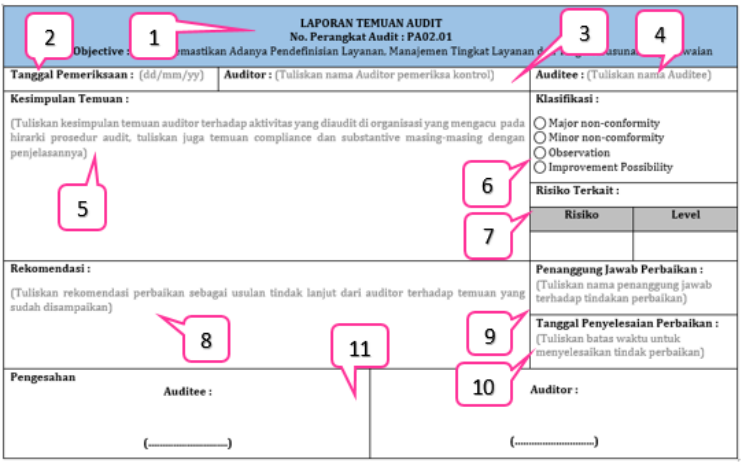
sering berulang secara berturut-turut pada selama penilaian audit, maka terdapat kegagalan sistematis atau kekurangan yang signifikan pada sistem sehingga klasifikasi menjadi *major non-conformity*.

2. *Observation*
   Proses, dokumen, atau aktivitas yang dilakukan telah sesuai dengan kontrol namun terdapat penyimpangan kecil yang tidak dapat diklasifikasikan pada ketidaksesuaian (conformance). Observasi memungkinkan ketidaksesuaian jika tidak diperbaiki. Hal ini umumnya disebabkan oleh pengawasan minor pada bagian auditee. Analisis akar penyebab jarang diperlukan untuk temuan dengan klasifikasi observasi, serta memungkinkan tidak dilakukan tindak perbaikan. Klasifikasi temuan observasi atau disebut temuan terisolasi harus dipresentasikan pada laporan temuan audit untuk mendapat tindakan pencegahan.

3. *Opportunities for Improvement* (*improvement possibility*)
   Merupakan temuan berdasarkan fakta dan data yang menunjukkan bahwa terdapat potensi peluang perbaikan. Auditee telah melakukan seluruh persyaratan pada kontrol. Tindakan tidak diperlukan untuk peluang perbaikan. Namun demikian, auditor harus memperoleh banyak data pendukung untuk menjadikan proses yang dilakukan auditee sempurna sesuai kontrol terkait.

Berdasarkan penjelasan klasifikasi pada ISO 19000:2008 di atas, penulis menggunakan empat klasifikasi temuan, yaitu *major non-conformity*, *minor non-conformity*, *observation*, dan *improvement possibility*.

Pada panduan umum ini, telah dijelaskan beberapa langkah pengisian template *audit report* atau laporan temuan audit seperti pada contoh Gambar 6.4 di bawah ini:



Gambar 6.4 Petunjuk Pengisian Laporan Temuan Audit

Di bawah Tabel 6.1 ini merupakan penjelasan dari setiap bagian pada Laporan Temuan Audit:

Tabel 6.1 Petunjuk Pengisian Laporan Temuan Audit

No.	Petunjuk Pengisian
1	Header penjelas laporan temuan audit yang berisi nomor dokumen perangkat audit beserta *control objective*.
2	Tanggal pemeriksaan kontrol yang berkaitan, diisi sesuai dengan kapan proses audit pada kontrol tersebut dilakukan
3	Nama auditor, diisi sesuai dengan siapa yang melakukan audit pada saat itu
4	Nama auditee, diisi sesuai dengan siapa saja yang diperiksa/diwawancara terkait kontrol
5	Kesimpulan Temuan, diisi sesuai dengan kesimpulan temuan apapun yang dihasilkan berdasarkan bukti yang ada
6	Klasifikasi, diisi dengan memberikan tanda silang (X) sesuai dengan temuan yang didapatkan, dengan ketentuan: • **Major non-conformity**: Jika organisasi benar-benar gagal untuk menerapkan kontrol yang ada

No.	Petunjuk Pengisian
	(ketidaksesuaian kontrol berdampak kegagalan total dari proses pada kontrol terkait). Organisasi memerlukan analisis akar penyebab, eliminasi akar penyebab, dan/atau perubahan dalam proses yang dilakukan. • **Minor non-conformity**: Jika organisasi gagal untuk menerapkan salah satu persyaratan dari poin pemeriksaan pada kontrol yang ada (ketidaksesuaian kontrol berdampak kegagalan minor/parsial dari proses pada kontrol terkait). Organisasi memerlukan analisis akar penyebab, eliminasi akar penyebab, dan/atau perubahan dalam proses yang dilakukan. • **Observation**: Jika organisasi telah menerapkan seluruh persyaratan dari poin pemeriksaan pada kontrol yang ada namun masih terdapat penyimpangan/kekurangan minor yang tidak dapat diklasifikasikan sebagai ketidaksesuaian kontrol. • **Improvement possibility**: Jika organisasi telah melakukan seluruh persyaratan dari poin pemeriksaan pada kontrol dengan baik, dan perlu dilakukan peningkatan lebih untuk menjadikannya sempurna.
7	Risiko terkait, disii dengan risiko beserta level penilaiannya dari Tabel 3. Daftar Penilaian Risiko yang berkaitan dengan kontrol tersebut.
8	Rekomendasi, diisi dengan usulan atau rekomendasi perbaikan dari Auditor yang harus dilakukan berdasarkan temuan yang dihasilkan
9	Penanggung Jawab Perbaikan, diisi sesuai dengan nama penanggung jawab yang bertugas dalam melakukan perbaikan
10	Tanggal Penyelesaian Perbaikan, diisi dengan tanggal perkiraan penyelesaian perbaikan yang akan dilakukan
11	Pengesahan, diisi dengan nama dan tanda tangan oleh masing-masing Auditor dan Auditee yang terlibat dalam proses pemeriksaan kontrol terkait. Pengesahan ini menandakan bahwa laporan temuan audit pada kontrol tersebut diterima oleh dua pihak (auditor dan auditee) dan auditee bersiap untuk melaksanakan perbaikan melalui daftar rekomendasi yang diusulkan oleh auditor.

3. Panduan Khusus

Bagian Panduan Khusus dibuat sebagai panduan bagi auditor internal dalam melakukan audit dengan beberapa kegiatan inisiasi yang dapat dilakukan. Dengan melihat pada perangkat yang telah dibuat dengan melakukan penyesuaian pada bagian panduan khusus ini, berikut beberapa penjelasan singkat mengenai bagian pada panduan khusus yang akan dibuat.

a. Petunjuk Peninjauan Dokumen Yang Dibutuhkan

Sebelum melakukan sebuah peninjauan pustaka dan dokumen, auditor internal harus mengetahui dimana tempat dan bagian yang bisa memberi semua yang dibutuhkan dalam proses pemeriksaan. Petunjuk peninjauan dokumen yang dibutuhkan ini merupakan suatu panduan yang didalamnya akan menjelaskan mengenai dimana auditor bisa mendapatkan dokumen dan pustaka, tujuan melakukan peninjauan terhadap dokumen tersebut, jenis dokumen yang dapat dikumpulkan, dan memilih jenis informasi yang dapat dihasilkan berdasarkan dokumen dan pustaka yang diperoleh.

b. Pengecualian

Merupakan bagian panduan khusus dimana menjelaskan beberapa pengecualian terkait kondisi yang terduga atau bahkan tidak terduga pada saat proses pelaksanaan audit pengelolaan permintaan dan insiden insiden berlangsung. Panduan ini melengkapi pengecualian dengan daftar-daftar pengecualian terhadap penggunaan perangkat audit seperti pencatatan narasumber, pencarian dokumen dan pustaka, hingga wawancara untuk setiap narasumber yang diperlukan.

Untuk hasil pembuatan panduan perangkat audit yang telah dilakukan secara lengkap disusun pada dokumen terpisah dengan buku tugas akhir.

6.2 Verifikasi Perangkat Audit

Pada tahap ini dilakukan verifikasi perangkat audit oleh Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi setelah perangkat audit telah disusun. Proses verifikasi ini dilakukan dengan melakukan penyesuaian antara *control objective* yang digunakan pada pembuatan perangkat dengan kesesuaiannya pada standar yang penulis gunakan yaitu COBIT 5 DSS02 dan *Service Desk Standard*. Tabel 6.2 berikut ini merupakan hasil verifikasi penyusunan dan pembuatan perangkat audit.

Tabel 6.2 Verifikasi Perangkat Audit

Poin Pemeriksaan	Kesesuaian Standar
CO.01 Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian	
Adanya pendefinisian tingkat susunan kepegawaian (staf) yang dikerahkan	*4.05 Stafing and scheduling*
Adanya pendefinisian layanan yang disetujui oleh pelanggan bisnis dan dipublikasikan pada pengguna akhir	*4.13 Service catalogue management*
Adanya pendefinisian manajemen tingkat layanan (*service level management*)	*5.03 Service level management*
CO.02 Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden	
Sistem manajemen layanan TI yang dapat menelusuri dan memfasilitasi penanganan seluruh permintaan layanan dan insiden dari setiap titik kontak	*4.06 IT service management system*
Adanya fungsionalitas sistem manajemen layanan TI	*4.07 IT service management system – product capability*
Ketersediaan *self-service*	*4.10 Self-service*
Proses terintegrasi untuk mengelola permintaan layanan dan insiden melalui sistem manajemen layanan TI dari seluruh saluran komunikasi	*5.05 Incident and service request management*
CO.03 Memastikan Adanya Prosedur Pencatatan Permintaan Layanan dan Insiden	
Prosedur pencatatan permintaan layanan dan insiden dari seluruh saluran komunikasi	*5.06 Incident and service request logging*
CO.04 Memastikan Adanya Prioritisasi Permintaan Layanan dan Insiden	

Poin Pemeriksaan	Kesesuaian Standar
Prosedur untuk memprioritaskan permintaan layanan dan insiden	*5.07 Prioritization*
CO.05 Memastikan Adanya Klasifikasi Permintaan Layanan dan Insiden	
Prosedur untuk mengklasifikasikan permintaan layanan dan insiden	*5.08 Categorization*
CO.06 Memastikan Adanya Verifikasi Hak Penggunaan Permintaan Layanan	
Mekanisme keamanan pada *service desk* untuk melindungi informasi	*4.15 Security*
CO.07 Memastikan Adanya Persetujuan Pemenuhan Permintaan Layanan	
Persetujuan finansial terhadap pemenuhan permintaan layanan	*4.14 Financial management*
CO.08 Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden	
Sistem untuk mendistribusikan permintaan layanan dan pelaporan insiden ke analis secara cepat	*4.03 Distribution of incoming interactions*
Sistem atau *tools* alarm / pemantau	*4.08 Remote access and control*
Proses diagnosis terotomasi	*5.01 Pro-active incident detection and remediation*
Ketersediaan manajemen pemasok / partner *service desk*	*4.16 Supplier and partner/3rd party management*
Prosedur untuk memastikan bahwa pengguna yang terdampak oleh insiden telah dikembalikan ke tingkat yang layanan yang disepakati (SLA) dan permintaan layanan telah dipenuhi dalam tingkat layanan yang disepakati	*5.10 Incident resolution and service request fulfillment*
CO.09 Memastikan Adanya Penggunaan Informasi Pengelolaan Insiden	
Sistem dan metode yang menangkap, merekam dan berbagi pengetahuan	*4.09 Knowledge management*
Terintegrasinya sistem pendukung layanan	*4.11 Integrated systems*
CO.10 Memastikan Adanya Penutupan Permintaan Layanan dan Insiden	
Proses untuk mengukur dan mengelola kepuasan pelanggan	*5.02 Managing customer satisfaction*
Perencanaan untuk mengelola komunikasi	*5.04 Communication*

Poin Pemeriksaan	Kesesuaian Standar
Prosedur untuk menentukan status permintaan layanan dan insiden	*5.09 Incident and service request status assignment and reporting*
Prosedur untuk menutup permintaan layanan dan insiden dari seluruh saluran komunikasi	*5.11 Incident and service request closure*
Adanya program pengukuran persepsi pelanggan (survei)	*7.01 Customer perception programme*
Adanya distribusi hasil survei kepada *service desk* dan pengguna	*7.02 Survey result management*
Adanya program peningkatan layanan oleh *service desk* melalui *feedback*	*7.03 Customer feedback management*
Adanya pengelolaan komplain	*7.04 Complaint management*
CO.11 Memastikan Adanya Laporan Pengelolaan Permintaan Layanan dan Insiden	
Laporan pengelolaan permintaan layanan dan insiden	*8.01 Reporting activities*
Adanya pengukuran terkait keberhasilan bisnis	*8.02 Business related metrics*
Adanya pemantauan, pengelolaan, dan pengukuran informasi jumlah permintaan layanan dan insiden yang dilaporkan	*8.03 Number of incidents and service requests*
Adanya pengumpulan dan analisis data terkait rata-rata waktu yang dibutuhkan untuk merespon permintaan layanan atau insiden	*8.04 Avarage time to respond*
Adanya pengumpulan dan analisis data terkait persentase panggilan telepon pengguna yang dihentikan sebelum menghubungi analis	*8.05 Abandon rate*
Adanya pengumpulan dan analisis data terkait rata-rata waktu untuk menangani insiden dan memenuhi permintaan layanan serta dibandingkan dengan tujuan yang didetailkan pada SLA	*8.06 Avarage time taken to resolve incidents or fulfil service requests*
Adanya pengumpulan dan analisis data terkait persentase dari insiden yang terselesaikan dan permintaan layanan yang terpenuhi yang memenuhi kepuasan pengguna	*8.07 First contact incident resolution and request fulfilment rate*

Poin Pemeriksaan	Kesesuaian Standar
Adanya pengumpulan dan analisis data terkait persentase dari insiden yang terselesaikan dan permintaan layanan yang terpenuhi yang memenuhi kepuasan pengguna tanpa eskalasi ke tim pendukung lain	*8.08 First level incident resolution and request fulfilment rate*
Adanya pengumpulan dan analisis data terkait persentase insiden dan permintaan layanan yang dibuka kembali	*8.09 Re-opened incident rate*
Adanya pengumpulan data backlog	*8.10 Backlog management*
Adanya pengumpulan data terkait persentase permintaan layanan dan insiden yang dieskalasi ke manajemen	*8.11 Percentage of hierarchic escalations (management notification)*
Adanya pengumpulan data terkait persentase permintaan layanan dan insiden yang dieskalasi ke teknisi	*8.12 Percentage of functional escalations (re-assignment)*
Adanya pengumpulan data terkait rata-rata waktu yang dibutuhkan untuk menyelesaikan insiden yang dianalisis dari prioritasnya	*8.13 Avarage resolution time by priority*
Adanya pengumpulan data terkait rata-rata waktu yang dibutuhkan untuk menyelesaikan insiden atau permintaan layanan berdasarkan kategori insiden atau tipe permintaan layanan.	*8.14 Average resolution time by incident category and service request type*
Adanya pengumpulan data terkait komitmen tingkat layanan dan membandingkannya dengan hasil kinerja aktual	*8.15 Comparison of overall service level goals to actual results*
Adanya pengumpulan data terkait frekuensi penggunaan alat *remote control* dan membandingkan hasilnya ke tujuan	*8.16 Remote control monitoring measured against goals*
Adanya pengumpulan data terkait persentase insiden dan permintaan layanan yang dilaporkan menggunakan saluran *self-logging* dan membandingkan hasil dengan tujuannya	*8.17 Self-logging monitoring measured against goals*
Adanya pengumpulan dan analisis data terkait jumlah penggunaan pengetahuan	*8.19 Knowledge usage*
Adanya pengumpulan dan analisis data terkait kualitas dan efektivitas pengetahuan serta membandingkan hasilnya dengan tujuan	*8.20 Knowledge quality and effectiveness*

Poin Pemeriksaan	Kesesuaian Standar
Adanya pengumpulan dan analisis data terkait persentase insiden yang disebabkan oleh perubahan dan membandingkan hasil dengan targetnya	*8.21 Monitoring incidents caused by changes measured against a target*
Adanya pengumpulan dan analisis data terkait total biaya dalam menjalankan operasinya dan dapat mengidentifikasi biaya pemberian layanan ke pelanggan	*8.22 Total cost of service*
Adanya pengumpulan dan analisis data terkait rata-rata biaya per insiden dan permintaan layanan dari operasi *service desk*	*8.23 Average cost per incident and service request (cost per contact)*
Adanya pengumpulan dan analisis data terkait biaya relatif dari operasi *service desk* melalui saluran komunikasi	*8.24 Average cost per incident and service request by channel (method received)*
CO.12 Memastikan Adanya Peningkatan Pengelolaan Permintaan Layanan dan Insiden	
Adanya proses manajemen masalah (*problem management*)	*5.12 Problem management*
Adanya proses manajemen perubahan TI (*IT change management*)	*5.13 IT change management*
Adanya proses untuk merencanakan dan mengawasi keberhasilan dari peluncuran *software* dan *hardware* yang baru	*5.14 Release and deployement management*
Adanya ketersediaan proses untuk memastikan keberhasilan pengenalan dari layanan TI yang baru atau yang diubah	*5.15 Service introduction*
Adanya proses manajemen konfigurasi	*5.16 Configuration and asset management*
Adanya rencana keberlanjutan layanan (*IT service continuity management*)	*5.17 IT service continuity management*
Prosedur pemantauan panggilan	*5.18 Telephone call monitoring*
Prosedur pemantauan permintaan layanan dan insiden	*5.19 Incident and service request monitoring*

Berdasarkan hasil verifikasi yang telah ditampilkan pada Tabel 6.2 di atas, dapat terlihat bahwa seluruh perangkat audit telah terpetakan dan terverifikasi dengan benar. Hasil verifikasi ini menandakan bahwa semua *control objective* yang digunakan

dalam pembuatan perangkat audit telah sesuai dengan standar yang digunakan sebagai acuan penyusunan perangkat. Selanjutnya perangkat audit yang telah terverifikasi disetujui oleh KaSubDit Layanan TSI yang menandakan bahwa perangkat auditsiap digunakan oleh organisasi.

6.3 Contoh Pengisian Perangkat Audit

Contoh pengisian perangkat audit dapat membantu auditor dalam menggunakan dan mengisi perangkat ketika proses pemeriksaan dilakukan. Berikut contoh pengisian daftar cek audit dan Laporan Temuan Audit untuk ID Dokumen PA02.01 yang ada pada perangkat audit dapat dilihat pada Tabel 6.3 Contoh Pengisian Perangkat Audit.

Tabel 6.3 Contoh Pengisian Perangkat Audit

	PERANGKAT AUDIT PENGELOLAAN PERMMINTAAN LAYANAN DAN INSIDEN PADA SERVICE DESK DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER KOTA SURABAYA		
	CO.01 Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian	**PA02.01**	
		AUDITOR *Andika*	**AUDITEE** *Putri*
TANGGAL :	*30/12/2016*		

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
1. Pemeriksaan adanya pendefinisian layanan yang disetujui oleh pelanggan bisnis dan dipublikasikan pada pengguna akhir	Auditor melakukan cek terkait adanya pendefinisian layanan	Compliance	Apakah organisasi memiliki pendefinisian layanan yang disediakan untuk pengguna?	√			*Tersedia pendefinisian layanan pada Dokumen katalog layanan dan screenshot website*
	Auditor melakukan cek terkait persetujuan layanan oleh pelanggan bisnis	Substantive	Apakah layanan yang terdefinisi telah disetujui oleh pelanggan bisnis?	√			*Tanda tangan pada dokumen Service Level Agreements (SLAs) (Pencapaian 100%)*

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
	Auditor memeriksa apakah seluruh pengguna layanan mengetahui layanan yang ditawarkan DPTSI. a. Melakukan cek ketersediaan media publikasi b. Melakukan survei pada pengguna layanan	Substantive	Apakah terdapat media publikasi yang digunakan *service desk* pada pengguna layanan terkait layanan yang dimiliki organisasi ?		√		*Tidak terdapat media publikasi. (Pendefinisian layanan tidak dipublikasi pada pengguna layanan)*
		Substantive	Apakah pengguna layanan mengetahui ketersediaan layanan yang dimiliki organisasi?			√	*Survei pengguna layanan (Pencapaian hanya 70% pengguna yang tahu)*
	Auditor melakukan cek kesesuaian permintaan layanan dengan layanan yang terdefinisi	Substantive	Apakah seluruh permintaan layanan yang diajukan oleh pengguna telah sama seperti pendefinisian layanan?	√			*Log permintaan layanan (Pencapaian 100%)*
2. Pemeriksaan adanya pendefinisian manajemen tingkat layanan	Auditor melakukan cek terkait manajemen tingkat layanan sebagai proses negosiasi untuk konten *Service*	Compliance	Apakah terdapat pendefinisian perjanjian tingkat layanan organisasi?	√			*Ada pada Dokumen Service Level Agreements (SLAs)*
		Substantive	Apakah pendefinisian tingkat kebutuhan			√	*Menyesuaikan antara Dokumen*

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
(*service level management*)	*Level Agreements* (SLAs), *Operational Level Agreements* (OLAs) dan *Underpinning Contracts* (UCs) guna menyeimbangkan kebutuhan bisnis dengan kapabilitas TI		layanan telah sesuai dengan tingkat layanan?				*Service Level Agreements (SLAs) dan Dokumen Service Level Requirements (SLRs) (Pencapaian 75%)*
		Compliance	Apakah terdapat pendefinisian perjanjian tingkat operasional organisasi?		√		*Tidak tersedia Dokumen OLAs (Tidak dilakukan pendefinisian perjanjian tingkat operasional dalam organisasi)*
		Substantive	Apakah pendefinisian perjajian tingkat operasional telah telah memenuhi perjanjian tingkat layanan?		√		*Tidak tersedia Dokumen OLAs. (Tidak dilakukan pendefinisian perjanjian tingkat operasional yang memenuhi*

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
							perjanjian tingkat layanan)
		Substantive	Apakah *service desk* dan pihak yang terkait telah menyetujui konten perjanjian tingkat operasional?		√		*Tidak tersedia Dokumen OLAs. (Tidak dilakukan pendefinisian perjanjian tingkat operasional yang disetujui)*
		Compliance	Apakah terdapat pendefinisian kontrak layanan antara organisasi dengan pemasok dukungan layanan eksternal?	√			*Ada pada Dokumen Underpinning Contracts (UCs)*
		Substantive	Apakah pendefinisian kontrak layanan dengan pemasok telah telah memenuhi perjanjian tingkat layanan?	√			*Menyesuaikan antara Dokumen Underpinning Contracts (UCs) dan kebutuhan bisnis sesuai Dokumen Service Level Agreements (SLAs)*

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
							(Pencapaian 100%)
		Substantive	Apakah *service desk* dan pihak yang terkait telah menyetujui konten kontrak layanan dengan pemasok eksternal?	√			*Tanda tangan pada dokumen Underpinning Contracts (UCs)*
3. Pemeriksaan adanya pendefinisian tingkat susunan kepegawaian (staf) yang dikerahkan untuk memenuhi layanan sesuai kontrak dan tingkat layanan yang ditetapkan	Auditor melakukan wawancara dengan *service desk* terkait adanya pendefinisian tingkat susunan kepegawaian yang diterapkan pada *service desk*	Substantive	Apakah seluruh layanan yg terdefinisi memiliki staf penyedia layanan?	√			*Ya, terdefinisi pada Dokumen katalog layanan serta Dokumen tugas pokok dan fungsi. (Pencapaian 100%)*
		Compliance	Apakah terdapat pendefinisian tingkat susunan kepegawaian (staf) pada *service desk* ?	√			*Ya, terdefinisi pada Dokumen tugas pokok dan fungsi*
		Substantive	Apakah pendefinisian tingkat susunan kepegawaian (staf)	√			*Ya, menyesuaikan antara Dokumen SLA serta*

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
			pada *service desk* telah memenuhi kontrak dan tingkat layanan yang ditetapkan?				*Dokumen tugas pokok dan fungsi, (Pencapaian 100%)*
	Auditor melakukan cek kesesuaian pendefinisian tingkat staf *service desk* untuk memenuhi kebutuhan tingkat layanan a. Menghitung jumlah tingkat layanan dibandingkan jumlah tingkat staf yang dikerahkan b. Menghitung jam kerja setiap staf untuk memenuhi	Substantive	Apakah pendefinisian jumlah tingkat staf didasarkan pada perhitungan tingkat layanan yang dibutuhkan?		√		*Tidak terdefinisi pada Dokumen tugas pokok dan fungsi yang sesuai dengan Dokumen SLA. (Pendefinisian jumlah tingkat staf tidak didasarkan pada perhitungan layanan yang dibutuhkan)*
		Substantive	Apakah penjadwalan jam kerja untuk setiap staf telah mencukupi kebutuhan tingkat layanan?		√		*Tidak sesuai antara jam kerja pada Dokumen tugas pokok dan fungsi dengan Dokumen SLA. (Penjadwalan jam kerja staf*

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
	kebutuhan tingkat layanan						*tidak memenuhi kebutuhan tingkat layanan)*
	Auditor melakukan survei pada staf *service desk* mengenai dokumentasi pendefinisian tingkat staf telah diketahui seluruhnya. a. Cek pembagian kerja b. Cek realisasi pembagian kerja	Substantive	Apakah seluruh staf *service desk* mengetahui ketersediaan dokumentasi pendefinisian tingkat staf pada *service desk*?			√	*Survei staf service desk* *(Pencapaian 80%)*
		Substantive	Apakah seluruh staf *service desk* telah mengelola permintaan layanan dan insiden sesuai pembagian tingkat staf yang ditetapkan?	√			*Sesuai hasil pengelolaan pada Dokumen Sasaran Kerja Pegawai (SKP) dengan pembagian tingkat staf pada Dokumen tugas pokok dan fungsi (Pencapaian 100%)*

<table>
<tr><td colspan="3">LAPORAN TEMUAN AUDIT
No. Perangkat Audit : PA02.01
Control Objective : CO.01 Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian</td></tr>
<tr><td>Tanggal Pemeriksaan : 30/12/2016</td><td>Auditor : Andika</td><td>Auditee : Putri</td></tr>
<tr><td colspan="2">Kesimpulan Temuan :
1. Pendefinisian layanan yang dimiliki organisasi tidak dipublikasikan pada pengguna layanan
2. Pada proses manajemen tingkat layanan tidak menegosiasi dan membuat perjanjian tingkat operasional
3. Pendefinisian tingkat staf tidak memenuhi layanan sesuai kontrak dan tingkat layanan yang ditetapkan</td><td>Klasifikasi :
◯ Major non-conformity
⊗ Minor non-comformity
◯ Observation
◯ Improvement Possibility
Risiko Terkait :
<table><tr><th>Risiko</th><th>Level</th></tr><tr><td>Keterlambatan respon service desk</td><td>medium</td></tr></table></td></tr>
<tr><td colspan="2">Rekomendasi :
1. Perlu adanya sosialisasi dan publikasi lebih lanjut terkait layanan yang disediakan oleh organisasi pada pengguna
2. Perlu untuk membuat perjanjian tingkat operasional yang terdokumentasi dalam dokumen OLAs
3. Perlu untuk memperhitungkan kebutuhan tingkat layanan dan penjadwalan jam kerja untuk memenuhi layanan yang telah disepakati</td><td>Penanggung Jawab Perbaikan:
Rama Aji
Tanggal Penyelesaian Perbaikan :
25/01/2017</td></tr>
</table>

BAB VII
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan kesimpulan yang dihasilkan dari pengerjaan tugas akhir, beserta saran yang dapat bermanfaat untuk perbaikan di penulisan selanjutnya.

7.1 Kesimpulan

Berdasarkan proses dan tahapan yang telah dilakukan dalam penulisan tugas akhir ini, maka dapat diambil kesimpulan yang menjawab rumusan masalah yang telah ditentukan, yaitu sebagai berikut:

1. Berdasarkan hasil analisis empat belas risiko yang telah dilakukan, didapatkan bahwa risiko yang paling banyak terjadi pada proses operasional yang dilakukan *service desk* adalah risiko kesalahan pemahaman permintaan pengguna layanan, keterlambatan respon *service desk*, dan ketidakpuasan *user* (pengguna) dengan layanan.
2. Risiko terkait proses pengelolaan permintaan layanan dan insiden pada *service desk* dengan level tertinggi adalah keterlambatan respon *service desk* dikarenakan frekuensi terjadinya risiko tersebut termasuk tinggi yaitu berkisar 10-100 kali per-tahun dengan dampak penurunan kepuasan pengguna terhadap layanan *service desk* organisasi yang ditimbulkan oleh risiko tersebut termasuk signifikan.
3. Dari dua belas *control objective* yang telah ditentukan, didapatkan bahwa *control objective* yang dapat memitigasi risiko dengan level penilaian tertinggi adalah memastikan adanya pendefinisian layanan, manajemen tingkat layanan dan tingkat susunan kepegawaian. Sedangkan *control objective* yang paling banyak dapat memitigasi risiko adalah memastikan adanya pendefinisian layanan, manajemen tingkat layanan dan tingkat susunan kepegawaian, memastikan adanya mekanisme pemenuhan permintaan layanan

dan penanganan insiden, serta memastikan adanya penutupan permintaan layanan dan insiden di mana masing-masing dapat memitigasi tiga risiko. Oleh karena itu, ketiga *control objective* tersebut dapat diprioritaskan dalam pelaksanaan audit.

4. Keseluruhan perangkat audit yang telah dibuat berdasarkan dua belas *control objective* memiliki rincian 58 poin pemeriksaan, 236 prosedur, serta 415 pertanyaan *checklist audit* dengan jenis *testing* 230 *substantive* dan 185 *compliance*. Semakin banyak poin pemeriksaan, maka semakin banyak prosedur serta pengujian *substantive* dan *compliance* pada perangkat.

7.2 Saran

Saran yang dapat diberikan oleh penulis yang diharapkan dapat dikembangkan di masa mendatang diantaranya adalah:

1. Analisis risiko yang dilakukan penulis pada penilaian dampak penurunan kepuasan pengguna terhadap layanan *service desk* memiliki keterbatasan, yaitu menggunakan metode survei dengan ruang lingkup populasi hanya dari mahasiswa ITS dengan tingkat kepercayaan 85%. Untuk memperoleh hasil penilaian yang lebih akurat, dapat digunakan nilai indeks penurunan kepuasan pengguna berdasarkan survei yang dilakukan *service desk* untuk seluruh pengguna layanan di lingkungan ITS dengan tingkat kepercayaan di atas 90%.
2. Penulis membutuhkan waktu yang cukup lama dan kurang efisien dalam melakukan pemetaan *control objective* sehingga untuk memudahkan penelitian selanjutnya dapat dibuat sebuah alur tata cara pemetaan antara aktivitas pada COBIT 5 DSS02 dan *Service Desk Standard* untuk menghasilkan *control objective*.

DAFTAR PUSTAKA

[1] DPTSI, "Direktorat Pengembangan Teknologi dan Sistem Informasi," 2013. [Online]. Available: http://dptsi.its.ac.id/?page_id=150.

[2] ISACA, COBIT 5 : Enabling Process, Amerika: ISACA, 2012.

[3] J. V. Bon, A. d. Jong, A. Kolthof, M. Pieper, R. Tjassing, A. v. d. Veen and T. Verheijen, Foundations of IT Service Management Based on ITIL V3. 3th ed, Van Haren Publishing, Zaltbommel, 2007.

[4] A. A. TYBCom, "Accountancy Auditing," [Online]. Available: http://archive.mu.ac.in/myweb_test/study%20TYBCom%20Accountancy%20Auditing-II.pdf.

[5] D. R. Sulistyaningrum, Pembuatan Perangkat Audit Berbasis Risiko untuk Manajemen Insiden pada Service Desk Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya, Surabaya: ITS, 2015.

[6] S. Christian, Pembuatan Panduan Audit Keamanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 pada Direktorat Sistem Informasi Universitas Airlangga, Surabaya: ITS, 2015.

[7] W. F. M. Jr., "An Approach to Learning Risk-Based Auditing," *Elsevier Ltd.,* pp. 276-287, 2014.

[8] O. Illoh, S. Aghili and S. Butakov, "Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates," *Conference Paper,* 2015.

[9] D. R. Indah, Harlili and M. A. Firdaus, "Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk," *Proceeding of The 1st International Conference on Computer Science and Engineering,* pp. 113-118, 2014.

[10] D. M. Guy, C. W. Alderman and A. J. Winters, Auditing, Jilid I, Jakarta: Erlangga, 2002.

[11] A. A. Arens, R. J. Elder and M. S. Beasley, Auditing and Assurance Services: An Integrated Approach. 4th ed., Upper Saddle River, New Jersey: Pearson Prentice Hall, 2012.

[12] J. A. Hall, “Chapter 17 - Auditing & Assurance,” in *Accounting Information System 4th ed*, 2004, pp. 17-1 - 17-8.

[13] R. Sarno, Audit Sistem Informasi & Teknologi Informasi, Surabaya: ITS Press, 2009.

[14] L. B. Sawyer, Internal Auditing, New York, 2005.

[15] M. Gregg, “Chapter 1: The Audit Process,” in *Exam Prep CISA: Certified Information Systems Auditor*, United States of America, Que Publishing, 2007, pp. 26-41.

[16] A. Halim, Auditing: Dasar-Dasar Audit Laporan Keuangan, UPP STIM YKPN, 2015.

[17] Sumijan, “Audit Sistem Informasi,” Padang.

[18] ISO, IS/ISO 19011 (2011): Guidelines for Auditing Management, NEW DELHI, 2012.

[19] R. Tampubolon, Audit Room: Risk and Systems-Based Internal Auditing, Audit Intern Berbasis Risiko, Jakarta, 2005.

[20] D. Christina, “Pemahaman Dasar Praktik Internal Audit berbasis Risiko (Risk-based Audit),” 22 October 2010. [Online]. Available: https://dianechristina.wordpress.com/2010/10/22/pemahaman-dasar-praktik-internal-audit-berbasis-risiko-risk-based-audit/. [Accessed 11 September 2016].

[21] O. University, Oxford English Dictionary, Oxford: Oxford University Press, 1997.

[22] P. M. Institute, A Guide to the Project Management Body of Knowledge (4th Edition), Project Management Institute, 2009.

[23] H. Metinaro, “Analisis Risiko Menggunakan Metode Cause-Effect,” *Journal of Business and Entrepreneurship*, vol. 2, p. 3, 2014.

[24] ISO/IEC, Information technology -- Security techniques-Information security risk management, ISO/IEC FIDIS 27005:2008, 2008.

[25] Gary Stoneburner, Alice Goguen, Alexis Feringa, Risk Management Guide for Information Technology Systems, National Institute of Standard Technology, 2002.

[26] D. Hubbard, The Failure of Risk Management: Why It's Broken and How to Fix It, New York: John Wiley & Sons, 2009, p. 46.

[27] A. Amri, “Kerangka Kerja Manajemen Risiko,” Institut Teknologi Bandung, 15 November 2015. [Online]. Available: http://blogs.itb.ac.id/. [Accessed 26 April 2016].

[28] C. J. Alberts and A. J. Dorofee, OCTAVE Method Implementation Guide Version 2.0, Carnegie Mellon University, 2001.

[29] C. Kusuma, “Perbandingan COSO-ERM Integrated Framework dengan ISO31000:2009 Risk Management - Principles and Guidelines,” CRMS Indonesia, 11 April 2014. [Online]. Available: http://crmsindonesia.org/knowledge/crms-articles/perbandingan-coso-erm-integrated-framework-dengan-iso31000-2009-risk-managem. [Accessed 10 October 2016].

[30] ISACA, Cobit 5 for risk, Amerika: ISACA, 2013.

[31] itSMF, “An Introductory Overview of ITIL® 2011 Aligned to the 2011 editions,” in *An Introductory Overview of ITIL® 2011*, London, TSO (The Stationery Office, 2012, p. 42.

[32] The ITIL Advisory Group, ITIL V3 Service Operation.

[33] T. D. Susanto, Manajemen Layanan Teknologi Informasi, Surabaya: Asosiasi Sistem Informasi Indonesia (AISINDO), 2016.

[34] SDI, The Service Desk Standard, Service Desk Institute.

[35] M. Syahmi, Analisis Struktur Service Desk di Perguruan Tinggi (Studi Kasus: Institut Teknologi Sepuluh Nopember Surabaya), Surabaya: ITS, 2015.

[36] W. Salisbury, W. Chin, A. Gopal and P. Newsted, “"Research report: Better theory through measurement developing a scale to capture consensus on appropiation,” *Information System Research*, vol. 13, pp. 91-203, 2002.

[37] A. G. Woodside, Case Study Research: Theory, Methods, Practice, Bingley: Emerald Group Publishing Limited, 2010.

[38] C. B. Meyer, “A Case Study Methodology,” p. 330, 17 May 2011.

[39] R. K. Yin, Case Study Research Design and Method, Sage Publication, 1994.

[40] A. W. Phillips, ISO 9001:2008 Internal Audits Made Easy, United States of America: ASQ Quality Press, 2009.

Halaman ini sengaja dikosongkan

BIODATA PENULIS

Penulis bernama lengkap Sarah Putri Ramadhani merupakan anak ketiga dari tiga bersaudara yang dilahirkan di Kota Surabaya pada tanggal 17 Februari 1995. Penulis menempuh 12 tahun masa pendidikan formal di Kota Surabaya. Riwayat pendidikan penulis dimulai pada tahun 2001 di SD Muhammadiyah 4 Surabaya, SMPN 1 Surabaya pada 2007, dan SMAN 2 Surabaya pada 2010. Pada tahun 2013, penulis meneruskan Pendidikan Tinggi Negeri di Jurusan Sistem Informasi FTIf, Institut Teknologi Sepuluh Nopember dan terdaftar dengan NRP 5213100185.

Selama menjadi mahasiswa, penulis aktif sebagai anggota aktif di Himpunan Mahasiswa Sistem Informasi. Selain itu, penulis juga aktif berorganisasi di BEM Fakultas FTIf sebagai staf Departemen *External Affairs* kepengurusan 2014/2015 dan berbagai kepanitiaan. Ketertarikan penulis pada bidang audit menjadikan penulis untuk memilih laboratorium Manajemen Sistem Informasi (MSI) sebagai topik dan tempat dalam menyelesaikan Tugas Akhir. Penulis pernah menjalani Kerja Praktik selama dua bulan di Sekretariat Jenderal Dewan Energi Nasional, Jakarta Selatan. Penulis dapat dihubungi melalui e-mail sarahputrirmdhni@gmail.com.

Halaman ini sengaja dikosongkan

LAMPIRAN A
SERVICE DESK STANDARD

Tabel A.1 Service Desk Standard

Concept 4 – Partnerships & Resources Akses untuk kebutuhan sumber daya dan *tools* untuk mencapai tujuan
4.03 Distribution of incoming interactions Untuk memastikan bahwa insiden dan permintaan layanan disampaikan kepada analis secara cepat dan terdapat sistem untuk mendistribusikan interaksi melalui telepon, atau metode komunikasi lainnya. ***4.04 Diagnosis and testing environment*** Operasi pendukung TI memiliki *hardware*, *software*, dan teknologi lainnya dalam memfasilitasi insiden untuk analis dalam memberikan penyelesaian masalah yang efisien. ***4.05 Stafing and scheduling*** Jenis dan tingkat sumber daya staf *service desk* dikerahkan untuk memenuhi layanan sesuai kontrak dan tingkat layanan yang dibutuhkan. ***4.06 IT service management system*** Ada sistem manajemen layanan TI yang diimplementasikan yang menelusuri dan memfasilitasi penanganan seluruh insiden pengguna dan/atau permintaan layanan dari setiap titik kontak. ***4.07 IT service management system – product capability*** Fungsi sistem manajemen layanan TI menyediakan fasilitas interaksi pencatatan dan pelacakan yang komprehensif dan efektif bersama dengan pelaporan manajemen insiden dan kemampuan proses manajemen layanan TI lainnya. ***4.08 Remote access and control***

Service desk memiliki sistem dan *tools* untuk meningkatkan kemampuan dan secara efektif memantau dan mengontrol sumber daya, secara cepat mendiagnosis isu, untuk menangani insiden dan memberikan layanan dari dan ke lokasi terpantau.

4.09 Knowledge management

Ada sistem dan metode yang menangkap, merekam dan berbagi pengetahuan untuk menjawab pertanyaan umum, mencari kesalahan yang diketahui untuk meningkatkan pelayanan kepada pengguna akhir.

4.10 Self-service

Terdapat fasilitas *self-service* yang menyediakan komunikasi ke organisasi. *Self-service* memberikan akses ke pengguna untuk informasi yang dibutuhkan terkait pertanyaan, penanganan insiden, mencatat insiden atau permintaan layanan tanpa bantuan *service desk*.

4.11 Integrated systems

Sistem pendukung terintegrasi untuk menyediakan keuntungan seperti efisiensi, akurasi dan kapabilitas, dengan demikian meningkatkan kegunaan dari informasi pendukung.

4.13 Service catalogue management

Service desk memberikan layanan yang didefinisikan dalam katalog layanan yang disetujui oleh pelanggan bisnis.

4.14 Financial management

Manajemen *service desk* mendemonstrasikan pemahaman realistis dari hubungan antara kebutuhan *service desk*, penganggaran dana, tingkat staf, teknologi dan fasilitas serta memahami hasil kinerja *service desk* dan organisasi TI.

4.15 Security

Ada pengukuran keamanan untuk melindungi *service desk* dan informasi guna menjaga integritas sistem, menjaga kerahasiaan informasi pengguna dan untuk *service desk* memenuhi misinya.

4.16 Supplier and partner/3rd party management

Ada manajemen pemasok *service desk* untuk mendukung mekanisme pengiriman pemasok.

Concept 5 – Processes & Procedures

Bagaimana operasi pendukung TI mengidentifikasi, mengulas, mendokumentasikan, dan merevisi proses dan prosedurnya dengan tujuan untuk mengoptimalkan tingkat dukungan.

5.01 Pro-active incident detection and remediation

Terdapat proses diagnosis terotomasi untuk mendeteksi insiden, menyediakan notifikasi kepada *service desk*, dan memberi tindakan yang tepat.

5.02 Managing customer satisfaction

Ada proses untuk mengukur dan mengelola kepuasan pelanggan yang bertujuan untuk membangun loyalitas dan dukungan.

5.03 Service level management

Ada proses manajemen tingkat layanan untuk secara teratur menegosiasikan konten *Service Level Agreement* (SLA) dengan pelanggan (pembuat keputusan), konten *Operational Level Agreements* (OLAs) dengan kelompok dukungan internal, dan konten *Underpinning Contracts* (UCs) dengan pemasok dukungan eksternal yang bertujuan untuk menyeimbangkan kebutuhan bisnis dan kemampuan TI.

5.04 Communication

Ada perencanaan untuk mengelola komunikasi antara *service desk*, pengguna akhir, serta bermacam partner dan pemasok dukungan dengan proses yang tepat untuk mendukungnya.

5.05 Incident and service request management

Proses terintegrasi untuk mengelola insiden dan permintaan layanan untuk seluruh saluran.

5.06 Incident and service request logging

Terdapat prosedur untuk mencatat insiden dan permintaan layanan dari seluruh saluran komunikasi.

5.07 Prioritization

Terdapat prosedur untuk memprioritaskan insiden dan permintaan layanan untuk memastikan alokasi, utilisasi, dan dukungan sumber daya yang tepat.

5.08 Categorization

Terdapat prosedur untuk mengategorisasikan insiden dan permintaan layanan untuk memastikan visibilitas siklus hidup yang efektif dan memberikan output pelaporan yang bernilai.

5.09 Incident and service request status assignment and reporting

Terdapat prosedur untuk menentukan status insiden dan permintaan layanan dan untuk mengomunikasikan kembali statusnya kepada pengguna.

5.10 Incident resolution and service request fulfillment

Terdapat prosedur untuk memastikan bahwa pengguna yang terdampak oleh insiden telah dikembalikan ke tingkat layanan yang disepakati (SLA), dan permintaan layanan telah dipenuhi dalam tingkat layanan yang disepakati.

5.11 Incident and service request closure

Terdapat prosedur untuk menutup insiden dan permintaan layanan dari seluruh saluran komunikasi, serta diikuti secara rutin untuk memastikan layanan yang konsisten.

5.12 Problem management

Ada proses manajemen masalah untuk mengeliminasi insiden berulang yang bertujuan untuk memastikan efektivitas dan efisiensi operasi dukungan TI.

5.13 IT change management

Ada proses manajemen perubahan untuk memastikan bahwa perubahan lingkungan TI termasuk layanan, dokumentasi atau kemampuan staff, secara sukses diimplementasikan.

5.15 Service introduction

Ada proses, atau sekumpulan proses untuk memastikan keberhasilan pengenalan dari layanan TI yang baru atau yang diubah ke dalam lingkungan produksi, dan diasosiasikan kepada *service desk* untuk dukungan layanan.

5.16 Configuration and asset management
Ada proses manajemen konfigurasi yang memastikan akurasi dari data manajemen aset dan konfigurasi yang termasuk identifikasi, notifikasi, dan remediasi dari data yang tidak akurat.
5.17 IT service continuity management
Ada perencanaan keberlanjutan layanan yang secara teratur dipelihara untuk mengelola gangguan layanan pada *service desk* baik keadaan yang direncanakan maupun yang tidak terduga.
5.18 Telephone call monitoring
Ada prosedur pemantauan panggilan yang memungkinkan manajemen *service desk* untuk memastikan bahwa kualitas interaksi antara *service desk* dan pengguna akhir dipertahankan.
5.19 Incident and service request monitoring
Terdapat prosedur pemantauan insiden dan permintaan layanan untuk memastikan bahwa proses manajemen insiden dan pemenuhan permintaan ditaati, kualitas informasi yang dicatat dipertahankan, dan tingkat pengetahuan dari analis telah sesuai.

Concept 7 – Managing Customer Satisfaction
Informasi kepuasan pengguna yang dicatat dan digunakan untuk mencapai tujuan organisasi dan ekspektasi pelanggan.

7.01 Customer perception programme
Service desk memantau dan mengukur persepsi pelanggan untuk mempertahankan dan meningkatkan kualitas layanan.
7.02 Survey result management
Hasil dari survei secara terbuka disebarluaskan untuk mendorong tindakan perbaikan.
7.03 Customer feedback management
Masukan pelanggan digunakan *service desk* dalam program peningkatan layanan terus-menerus.
7.04 Complaint management
Komplain dikelola secara konsisten dan kepercayaan pengguna akhir akan dipulihkan.

Concept 8 – Performance Results Hasil kinerja operasi pendukung TI diukur melalu kinerja yang telah direncanakan.
8.01 Reporting activities Informasi akurat secara konsisten diproduksi dan disebarkan kepada pemangku kepentingan terkait yang bertujuan untuk mendukung tujuan dukungan bisnis. ***8.02 Business related metrics*** Keberhasilan bisnis secara jelas dimasukkan ke dalam pemantauan dan laporan metrik *service desk.* ***8.03 Number of incidents and service requests*** Jumlah insiden dan permintaan layanan yang dilaporkan kepada *service desk* dipantau, dikelola, dan diukur secara rutin dan konsisten. ***8.04 Avarage time to respond*** *Service desk* secara rutin dan konsisten mengumpulkan dan menganalisis rata-rata waktu yang dibutuhkan untuk merespon insiden atau permintaan layanan. ***8.05 Abandon rate*** *Service desk* secara rutin dan konsisten mengumpulkan dan menganalisis data tentang persentase panggilan telepon pengguna yang dihentikan sebelum menghubungi analis dukungan. ***8.06 Avarage time taken to resolve incidents or fulfil service requests*** *Service desk* secara rutin dan konsisten mengumpulkan data trata-rata waktu untuk menangani insiden dan memenuhi permintaan layanan dan dibandingkan dengan tujuan yang didetailkan pada SLA. ***8.07 First contact incident resolution and request fulfilment rate*** *Service desk* secara rutin dan konsisten mengumpulkan dan menganalisis data persentase dari insiden yang terselesaikan dan permintaan layanan yang terpenuhi yang memenuhi kepuasan pengguna. ***8.08 First level incident resolution and request fulfilment rate***

Service desk secara rutin dan konsisten mengumpulkan dan menganalisis persentase dari insiden yang terselesaikan dan permintaan layanan yang terpenuhi yang memenuhi kepuasan pengguna oleh *Service desk* tanpa eskalasi ke tim pendukung lainnya.

8.09 Re-opened incident rate

Service desk secara rutin dan konsisten mengumpulkan data persentase insiden dan permintaan layanan yang ditutup, kemudian dibuka kembali untuk tambahan tindak lebih lanjut.

8.10 Backlog management

Service desk secara rutin dan konsisten mengumpulkan data tentang total jumlah insiden dan permintaan layanan terbuka dibandingkan dengan usianya di seluruh tim pendukung dan menggunakannya untuk efek penyelesaian masalah yang cepat.

8.11 Percentage of hierarchic escalations (management notification)

Service desk secara rutin dan konsisten mengumpulkan data tentang persentase insiden atau permintaan layanan yang dieskalasi ke manajemen untuk menghindari penyimpangan SLA.

8.12 Percentage of functional escalations (re-assignment)

Service desk secara rutin dan konsisten mengumpulkan data tentang persentase insiden, dan layanan atau perubahan permintaan yang ditransfer ke tim teknikal dengan tingkat keahlian yang lebih tinggi untuk menghindari penyimpangan SLA dan untuk memantau kecepatan transfer antara tim pendukung.

8.13 Avarage resolution time by priority

Service desk secara rutin dan konsisten mengumpulkan data tentang rata-rata waktu yang dibutuhkan untuk menyelesaikan insiden yang dianalisis dari prioritasnya.

8.14 Average resolution time by incident category and service request type

Service desk secara rutin dan konsisten mengumpulkan data tentang rata-rata waktu yang dibutuhkan untuk menyelesaikan insiden atau permintaan layanan berdasarkan kategori insiden atau tipe permintaan layanan.

8.15 Comparison of overall service level goals to actual results
Service desk secara rutin dan konsisten mengumpulkan data tentang komitmen tingkat layanan dan membandingkannya dengan hasil kinerja aktual.
8.16 Remote control monitoring measured against goals
Service desk secara rutin dan konsisten mengumpulkan data tentang frekuensi penggunaan alat *remote control* dan membandingkan hasilnya ke tujuan.
8.17 Self-logging monitoring measured against goals
Service desk secara rutin dan konsisten mengumpulkan data tentang persentase insiden dan permintaan layanan yang dilaporkan menggunakan saluran *self-logging* dan membandingkan hasil dengan tujuannya.
8.19 Knowledge usage
Service desk secara mengumpulkan dan menganalisis data tentang berapa kali jumlah pengetahuan digunakan.
8.20 Knowledge quality and effectiveness
Service desk secara rutin mengumpulkan dan menganalisis data tentang kualitas dan efektivitas pengetahuan serta membandingkan hasilnya dengan tujuan.
8.21 Monitoring incidents caused by changes measured against a target
Service desk secara rutin dan konsisten mengumpulkan data tentang persentase insiden yang disebabkan oleh perubahan dan membandingkan hasil dengan targetnya.
8.22 Total cost of service
Service desk secara rutin dan konsisten mengumpulkan data tentang total biaya dalam menjalankan operasinya dan dapat mengidentifikasi biaya pemberian layanan ke pelanggan.
8.23 Average cost per incident and service request (cost per contact)
Service desk secara rutin dan konsisten mengumpulkan data tentang rata-rata biaya per insiden dan permintaan layanan dari operasi *service desk.*

8.24 Average cost per incident and service request by channel (method received)

Service desk secara rutin dan konsisten mengumpulkan data tentang biaya relatif dari operasi *service desk* melalui saluran seperti telepon, email, live chat, SMS, self-service, media sosial, walk-in.

8.26 Staf turnover

Service desk memelihara kesinambungan staf yang memadai untuk memastikan bahwa tingkat layanan secara konsisten terpenuhi.

Halaman ini sengaja dikosongkan

LAMPIRAN B
PROTOCOL INTERVIEW

INTERVIEW 1

Tujuan Interview

Mengetahui kondisi implementasi layanan TI *service desk* pada SubDirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS.

Goals

- Permasalahan (insiden) layanan TI
- Permintaan layanan TI oleh pengguna
- Struktur organisasi
- Tupoksi
- Layanan yang ditangani oleh *service desk* DPTSI
- Kondisi kekinian proses pada *service desk*

Tabel B.1 Interview 1

No.	Pertanyaan
1	Bagaimanakah gambaran umum dan struktur organisasi DPTSI ?
2	Apa tugas pokok dan fungsi SubDirektorat Layanan Teknologi dan Sistem Informasi (termasuk di dalamnya adalah *service desk*) ?
3	Apa saja bentuk layanan yang ditangani oleh *service desk* ? (Hardware/Software/jarigan/ketiganya ?) dan meliputi Hardware/Software/Jaringan apa saja?
4	Apa saja insiden yang sering terjadi dan permintaan layanan yang diajukan oleh pengguna pada layanan DPTSI ? dan bagaimana penanganannya ?
5	Siapa yang biasanya bertugas menangani permintaan layanan dan insiden tersebut ?
6	Apakah ada prosedur khusus (SOP) pengelolaan permintaan layanan dan insiden ? Jika ada, apa saja SOP nya ?
7	Hal-hal apa saja yang dirasa masih kurang dalam pengelolaan permintaan layanan dan insiden ini ?
8	Apakah ada langkah lebih lanjut mengenai pengelolaan permintaan layanan dan insiden seperti maintenance untuk langkah perbaikan dan pencegahan ?

INTERVIEW 2

Tujuan Interview

Mengetahui kondisi kekinian *service desk* dalam implementasi pengelolaan permintaan layanan dan insiden.

Goals

- Alur Pengelolaan Permintaan Layanan dan Insiden
- Teknologi informasi (sistem aplikasi) yang digunakan

Tabel B.2 Interview 2

No.	Pertanyaan
1	Seperti apa bentuk *service desk* yang ada pada DPTSI ITS?
2	Sistem aplikasi apa saja yang digunakan oleh *service desk* DPTSI ?
3	Siapa saja yang menjadi admin/bertanggung jawab/pengelola sistem aplikasi *service desk* ? (daftar perbagian staf memegang tanggung jawab pada bagian apa saja ?)
4	Apakah teknologi informasi sudah sangat membantu kinerja layanan ?
5	Siapa yang mengelola *service desk* ? Siapa saja yang menggunakannya ? Siapa yang bertanggung jawab ?
6	Aktivitas apa saja yang ada pada *service desk* ?
7	Bagaimana proses atau alur yang ada pada *service desk* ? (pendefinisian → penutupan)
8	Apakah *service desk* pernah dilakukan evaluasi sebelumnya ?
9	Apakah ada standarisasi khusus dalam melakukan pengelolaan permintaan layanan dan insiden?
10	Apakah dilakukan klasifikasi (berdasarkan tipe dan kategori) serta memprioritasikan permintaan layanan dan insiden ?
11	Apakah dampak yang dialami ketika permintaan layanan tidak dipenuhi dan insiden tidak diatasi / lama diatasi ?

No.	Pertanyaan
12	Apakah yang dilakukan oleh *service desk* ketika permintaan layanan dan insiden tidak segera ditangani oleh pihak yang bertanggung jawab (setelah eskalasi) ?
13	Berdasarkan log insiden: • Berapa lama waktu penanganannya • Apakah semua insiden dicatat • Apa saja insiden yang terjadi
14	Apa saja masalah yang terjadi pada *service desk* ?
15	Bagaimana cara melakukan pelaporan ? bagaimana bentuknya ?

INTERVIEW 3

Tujuan Interview

Mengetahui permasalahan atau risiko pada proses pengelolaan permintaan layanan dan insiden pada *service desk* DPTSI.

Goals

- Risiko TI pada proses pengelolaan permintaan layanan dan insiden
- Kondisi sistem aplikasi yang digunakan

Tabel B.3 Interview 3

No.	Pertanyaan
1	Adakah permasalahan/ancaman/gangguan yang pernah terjadi terkait sistem aplikasi *service desk* ini ?
2	Adakah permasalahan / ancaman yang pernah terjadi / kemungkinan risiko terkait proses pengelolaan permintaan layanan dan insiden pada *service desk*?
3	Apakah organisasi sudah pernah melakukan identifikasi risiko terhadap proses maupun sistem aplikasi *service desk* tersebut?
4	Tanyakan mengenai kemungkinan risiko yang terjadi pada web application service desk berdasarkan yg telah dibuat kemungkinannya, kemudian tanyakan mengenai: • Disebabkan oleh faktor internal atau eksternal • Seberapa sering terjadinya

	• Apakah dampak yang mungkin timbul apabila pemasalahan tersebut benar-benar terjadi, dilihat dari empat aspek: - Produktivitas → rugi pendapatan selama satu tahun (%) - Biaya tanggapan → beban terkait dengan mengelola kejadian yang merugikan (Rp) - Keunggulan kompetitif → penurunan kepuasan pengguna (indeks) - Hukum → kepatuhan terhadap peraturan-denda (Rp)

Berikut kemungkinan risiko berdasarkan sumber literatur yang dijadikan acuan dalam proses *interview* 3 dan untuk menjawab pertanyaan poin ke-empat ditunjukkan pada Tabel C.4.

Tabel B.4 Interview 3 Risiko

No	Risiko
1	Kesalahan pemahaman permintaan pengguna layanan
2	Keterlambatan respon *service desk*
3	Kesalahan pencatatan permintaan layanan dan insiden
4	Sistem aplikasi tidak dapat diakses
5	Log permintaan layanan dan insiden tidak lengkap
6	Penyalahgunaan hak akses permintaan layanan secara sengaja
7	Pengabaian laporan insiden oleh teknisi/staf *service desk*
8	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan
9	Penanganan insiden dan pemenuhan permintaan layanan *overdue*
10	Kesalahan penanganan insiden dan pemenuhan permintaan layanan
11	Ketidakpuasan user dengan layanan
12	Ketidakjelasan status permintaan layanan dan insiden
13	Kesalahan pendefinisan tren pada laporan
14	Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan

OBSERVASI

Tujuan Observasi

Mengetahui alur dan proses pengelolaan permintaan layanan dan insiden secara detail.

Goals

Checklist kelengkapan proses pengelolaan permintaan layanan dan insiden sesuai COBIT 5 *for Risk* untuk menggali lebih dalam risiko terkait proses.

Tabel B.5 Checklist Observasi

Proses	Checklist (√)	Keterangan
Mendefinisikan skema klasifikasi insiden dan permintaan layanan		
Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden		
Memverifikasikan, menyetujui dan memenuhi permintaan layanan		
Menginvestigasikan, mendiagnosis dan mengalokasikan insiden		
Menyelesaikan dan Memulihkan Insiden		
Menutup Permintaan Layanan dan Insiden		
Melacak Status dan Membuat Laporan		

Halaman ini sengaja dikosongkan

LAMPIRAN C
KUESIONER SURVEI

KUESIONER PENURUNAN KEPUASAN PENGGUNA
TERHADAP LAYANAN SERVICE DESK DPTSI

Tujuan: Kuesioner berikut dilakukan untuk tujuan penelitian Tugas Akhir Jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember (ITS) dalam melihat tingkat penurunan kepuasan pengguna terhadap layanan *service desk* pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI). Kuesioner ini tidak akan disalah gunakan oleh surveyor dan akan digunakan sebaik-baiknya untuk keperluan penelitian Tugas Akhir.

Nama :
NRP :
Angkatan : ☐ 2016 ☐ 2014
(pilih salah satu) ☐ 2015 ☐ 2013++

Berilah tanda centang ☑ pada salah satu jawaban Anda.

Petunjuk :

Dari pernyataan berikut ini, pilihlah skala antara 1-5 yang membuat Anda sebagai pengguna layanan mengalami penurunan kepuasan :

1 = Penurunan Sangat Sedikit
2 = Penurunan Sedikit
3 = Netral
4 = Penurunan Banyak
5 = Penurunan Sangat Banyak

Tabel C.1 Kuesioner

No.	Pernyataan	1	2	3	4	5
1	Ketika *service desk* tidak memenuhi permintaan dan menangani keluhan sesuai harapan saya, maka kepuasan saya mengalami :					
2	Ketika *service desk* terlambat dalam merespon laporan keluhan dan permintaan saya, maka kepuasan saya mengalami :					
3	Ketika *service desk* mengabaikan laporan keluhan dan permintaan saya, maka kepuasan saya mengalami :					
4	Ketika *service desk* selesai menangani laporan keluhan dan permintaan saya di luar batas waktu yang dijanjikan, maka kepuasan saya mengalami :					
5	Ketika *service desk* tidak melakukan verifikasi kepuasan saya untuk memastikan bahwa laporan keluhan dan permintaan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami :					

6	Ketika *service desk* tidak memberi keluhan dan permintaan informasi status laporan saya (sedang direspon / selesai ditangani / telah ditutup), maka kepuasan saya mengalami :					
7	Ketika *service desk* tidak menangani masalah yang berulang kali saya keluhkan hingga akar permasalahan, maka kepuasan saya mengalami :					
8	Ketika *service desk* tidak mengalami peningkatan dalam melayani permintaan dan keluhan saya, maka kepuasan saya mengalami :					
9	Ketika sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak dapat saya akses, maka kepuasan saya mengalami:					
10	Ketika keamanan informasi pada sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak terlindungi, maka kepuasan saya mengalami :					

Halaman ini sengaja dikosongkan

LAMPIRAN D
HASIL INTERVIEW

HASIL INTERVIEW 1

Tanggal	:	24 November 2016
Waktu	:	09.00-11.00
Lokasi	:	DPTSI ITS
Narasumber	:	Bapak Jainul Arifin, Ibu Widiyaningsih, dan Ibu Mudjiatin
Jabatan	:	Staf *service desk*

Tabel D.1 Hasil Interview 1

No.	Uraian Pertanyaan dan Jawaban
1	Bagaimanakah gambaran umum dan struktur organisasi DPTSI ?
	Jawaban: Service desk tidak ada struktur organisasi. TUPOKSI ada di OTK. Ada 3 orang (jobdesk ada di SKP dan SIM kepegawaian, nanti bisa lihat dokumen SKP nya)

No.	Uraian Pertanyaan dan Jawaban
2	Apa tugas pokok dan fungsi SubDirektorat Layanan Teknologi dan Sistem Informasi (termasuk di dalamnya adalah *service desk*) ?
	Jawaban: TUPOKSI Subdirektorat Layanan TSI terdapat di Peraturan Rektor, sedangkan service desk terdapat di dokumen SKP masing-masing staf
3	Apa saja bentuk layanan yang ditangani oleh *service desk* ? (Hardware/Software/jarigan/ketiganya ?) dan meliputi Hardware/Software/Jaringan apa saja?
	Jawaban: Tidak ada bentuk pelaporan lewat telepon, hanya lewat sistem (email). Layanan LPTSI ada email, domain, sistem informasi, pengembangan & maintenance SI, jaringan --> termasuk hardware, software, jaringan, dan layanan.
4	Apa saja insiden yang sering terjadi dan permintaan layanan yang diajukan oleh pengguna pada layanan DPTSI? dan bagaimana penanganannya ?
	Jawaban: Paling sering jaringan, seperti jaringan atau koneksi putus. Untuk setiap jurusan jika tidak ada teknisi maka pihak service desk akan eskalasi langsung ke teknisi jaringan milik DPTSI (software untuk deteksi seluruh insiden ada pantau.its)
5	Siapa yang biasanya bertugas menangani permintaan layanan dan insiden tersebut ?

No.	Uraian Pertanyaan dan Jawaban
	Jawaban: Service desk dan unit lain di subdirektorat DPTSI
6	Apakah ada prosedur khusus (SOP) pengelolaan permintaan layanan dan insiden ? Jika ada, apa saja SOP nya ?
	Jawaban: Ada SOP yang terstandar (ISO th 2008) dalam menangani permintaan layanan dan insiden. SOP ini ada di seluruh layanan.
7	Hal-hal apa saja yang dirasa masih kurang dalam pengelolaan permintaan layanan dan insiden ini?
	Jawaban: Service desk tidak mengetahui status pelaporan setelah ditangani (apabila pelaporan manual melalui email, tidak melalui sistem e-ticket). Maka setelah ini akan diarahkan ke e-ticket supaya dapat melacak.
8	Apakah ada langkah lebih lanjut mengenai pengelolaan permintaan layanan dan insiden seperti maintenance untuk langkah perbaikan dan pencegahan ?
	Jawaban: Terdapat langkah maintenance yang menginisiasi service desk (dikomunikasikan dengan kepala subdirektorat) maupun dari unit-unit yang menangani permintaan layanan dan insiden

HASIL INTERVIEW 2

Tanggal	:	24 November 2016
Waktu	:	09.00-11.00
Lokasi	:	DPTSI ITS
Narasumber	:	Bapak Jainul Arifin, Ibu Widiyaningsih, dan Ibu Mudjiatin
Jabatan	:	Staf *service desk*

Tabel D.2 Hasil Interview 2

No.	Uraian Pertanyaan dan Jawaban
1	Seperti apa bentuk *service desk* yang ada pada DPTSI ITS?
	Jawaban: Sistem e-ticket (web application service desk dalam proses uji coba di ITS) bentuknya website. Sistem alur pertama user klik e-ticket, isi form (isi alamat email) lalu nanti komunikasi lewat email, seluruh komplain dr unit2 masuk ke DPTSI lalu didisposisi (eskalasi) ke unit yg dapat menangani insiden tersebut. Saat penanganan-menutup status itu diserahkan ke unit yg menangani (service desk sudah terputus komunikasi dengan user), namun service desk dapat melacak statusnya.
2	Sistem aplikasi apa saja yang digunakan oleh *service desk* DPTSI ?
	Jawaban: Ada pantau.its (untuk mendeteksi insiden jaringan yang dikelola oleh service desk dan subdirektorat jaringan) dan e-ticket (untuk pelaporan insiden yang dikelola oleh service desk). E-ticket sudah dirilis, namun masih

No.	Uraian Pertanyaan dan Jawaban
	banyak kekurangan. tahun masih salah dan tidak mengakomodasi manajemen. Pengguna hanya dapat mengisi form pelaporan, tidak ada self-service.
3	Siapa saja yang menjadi admin/bertanggung jawab/pengelola sistem aplikasi *service desk* ? (daftar perbagian staf memegang tanggung jawab pada bagian apa saja ?)
	Jawaban: Admin service desk ada satu ada pak Jainal yang mengelola sistem e-ticket.
4	Apakah teknologi informasi sudah sangat membantu kinerja layanan ?
	Jawaban: Masih dalam tahap uji coba. Namun sistem e-ticket ini dapat sangat membantu, karena service desk dapat melacak status penanganan serta mengukur kinerja unit yang menangani insiden/permintaan layanan (apakah cepat atau lambat)
5	Siapa yang mengelola *service desk* ? Siapa saja yang menggunakannya ? Siapa yang bertanggung jawab ?
	Jawan: • Yang mengelola : Koordinator Direktorat Layanan TSI • Yang menggunakan : Seluruh civitas ITS yang menggunakan, termasuk mahasiswa, dosen, lembaga, dll. • Yang bertanggung jawab : Service desk mengelola permintaan layanan dan insiden, serta menangani terkait layanan. Sedangkan yang menangani terkait hadware dan software adalah subdirektorat pengembangan, lalu yang menangani terkait jaringan adalah subdirektorat infrastruktur dan keamanan SI.
6	Aktivitas apa saja yang ada pada *service desk* ?
	Jawaban:

No.	Uraian Pertanyaan dan Jawaban
	Mengelola permintaan layanan dan insiden. Tidak ada biaya terkait permintaan layanan.
7	Bagaimana proses atau alur yang ada pada *service desk* ? (pendefinisian → penutupan)
	Jawaban: Sudah ada pengkategorian. Tidak ada pencatatan jika melalui email (hanya mendapat laporan email, lalu komunikasi dari pencatatan hingga selesai dilakukan di email). Ada verifikasi ke kepala subdirektorat terkait permintaan layanan (jika di luar kuasa service desk untuk memenuhi) dapat berupa lisan (hubungi langsung) atau surat pengajuan permintaan layanan (dibuat oleh user) dan diserahkan ke kepala untuk persetujuan, selain itu ada verifikasi mengenai penyelesaian insiden ke kasubdit (sekiranya service desk bingung siapa yang akan menangani, maka ditanyakan ke kasubdit untuk unit eskalasi yang tepat). Jika insiden/permintaan layanan dieskalasi, maka email akan diforward ke unit yang menangani hingga selesai (service desk tidak mengetahui status penyelesaian masalah). Penutupan dilakukan oleh unit yg menangani masalah. Laporan ada berupa SKP (berisi apa saja yg dilakukan service desk, insiden da permintaan layanan apa saja yg terjadi dalam suatu rentang waktu, serta melihat insiden berulang yang akan diarahkan menjadi problem)
8	Apakah *service desk* pernah dilakukan evaluasi sebelumnya?
	Jawaban: Pernah dilakukan evaluasi melalui pertemuan, baik komunikasi ketika meeting maupun melalui WA dengan kepala subdirektorat.
9	Apakah ada standarisasi khusus dalam melakukan pengelolaan permintaan layanan dan insiden?
	Jawaban: Belum ada, namun hanya ada standar dalam menangani insiden (berdasarkan ISO).
10	Apakah dilakukan klasifikasi (berdasarkan tipe dan kategori) serta memprioritasikan permintaan layanan dan insiden ?

No.	Uraian Pertanyaan dan Jawaban
	Jawaban: Ada klasifikasi (jaringan/software/layanan/hardware), lalu diprioritaskan berdasarkan urgensitas (kepentingan dan lebih dahulu melaporkan).
11	Apakah dampak yang dialami ketika permintaan layanan tidak dipenuhi dan insiden tidak diatasi / lama diatasi?
	Jawaban: Unit jaringan kekurangan sumber daya untuk menangani insiden sehingga lama ditangani. Sering ada komplain terkait lamanya permintaan layanan dan insiden yang tidak terpenuhi secara cepat (namun service desk aktif mengomunikasikan status laporan ke user).
12	Apakah yang dilakukan oleh *service desk* ketika permintaan layanan dan insiden tidak segera ditangani oleh pihak yang bertanggung jawab (setelah eskalasi) ?
	Jawaban: Service desk selalu melakukan komunikasi (followup) dengan unit yang menangani permintaan layanan dan insiden. Biasanya followup dilakukan langsung satu hari setelah laporan dieskalasi ke unit tersebut.
13	Berdasarkan log insiden: • Berapa lama waktu penanganannya • Apakah semua insiden dicatat • Apa saja insiden yang terjadi
	Jawaban: • Penyelesaian insiden terkait aplikasi dan jaringan yang lama penanganannya (lebih dari 1 hari - lebih dari 1 bulan). Sedangkan untuk terkait email dan user-password penanganannya cepat (langsung ditangani). • Tidak ada pencatatan jika lewat email. Namun ada pencatatan otomatis melalui sistem e-ticket. • Jaringan, software, layanan, dan hardware.

No.	Uraian Pertanyaan dan Jawaban
14	Apa saja masalah yang terjadi pada *service desk* ?
	Jawaban: Service desk tidak dapat memantau status pelaporan ketika sedang ditangani hingga ditutup oleh unit yang telah didistribusikan/dieskalasi. Hal ini dikarenakan fitur feedback dan pemantauan status pada e-ticket belum sempurna / masih banyak kekurangannya.
15	Bagaimana cara melakukan pelaporan ? bagaimana bentuknya ?
	Jawaban: User melapor melalui e-mail dan e-ticket. Jika melalui telepon akan diarahkan untuk mengirimkan laporan e-mail sehingga dapat dijadikan bukti pencatatan laporan dan memudahkan eskalasi/forward ke unit yang menangani. Jika melalui e-ticket maka mengisi melalui form pelaporan.

HASIL INTERVIEW 3

Tanggal	:	24 November 2016
Waktu	:	09.00-11.00
Lokasi	:	DPTSI ITS
Narasumber	:	Bapak Jainul Arifin, Ibu Widiyaningsih, dan Ibu Mudjiatin
Jabatan	:	Staf *service desk*

Tabel D.3 Hasil Interview 3

No.	Uraian Pertanyaan dan Jawaban
1	Adakah permasalahan/ancaman/gangguan yang pernah terjadi terkait sistem aplikasi *service desk* ini ?
	Jawaban: Waktu pelaporan masih sering salah (tanggal atau waktu berubah tidak sesuai waktunya), bug aplikasi, serta di awal pengembangan sistem e-ticket terdapat unit yang menangani insiden dan memenuhi permintaan sering lupa username&password e-ticket.
2	Adakah permasalahan / ancaman yang pernah terjadi / kemungkinan risiko terkait proses pengelolaan permintaan layanan dan insiden pada *service desk*?
	Jawaban: Masalah salah mengalokasikan/mendistribusikan penanganan insiden & pemenuhan permintaan layanan (salah kirim email ke unit yang seharusnya tidak menangani laporan tersebut).
3	Apakah organisasi sudah pernah melakukan identifikasi risiko terhadap proses maupun sistem aplikasi *service desk* tersebut?

	Jawaban: Belum pernah.
4	Tanyakan mengenai kemungkinan risiko yang terjadi pada web application service desk berdasarkan yg telah dibuat kemungkinannya, kemudian tanyakan mengenai: • Disebabkan oleh faktor internal atau eksternal • Seberapa sering terjadinya • Apakah dampak yang mungkin timbul apabila pemasalahan tersebut benar-benar terjadi, dilihat dari empat aspek: - Produktivitas → rugi pendapatan selama satu tahun (%) - Biaya tanggapan → beban terkait dengan mengelola kejadian yang merugikan (Rp) - Keunggulan kompetitif → penurunan kepuasan pengguna (indeks) - Hukum → kepatuhan terhadap peraturan-denda (Rp)
	Jawaban pada Tabel D.4 Hasil Interview 3 Daftar Kemungkinan Risiko

Tabel D.4 Hasil Interview 3 Risiko

No.	Risiko	Pernah Terjadi	Keterangan
1	Kesalahan pemahaman permintaan pengguna layanan	√	Kesalahan dalam memahami permintaan yang diajukan oleh pengguna layanan sehingga pemenuhan permintaan tidak sesuai harapan pengguna.
2	Keterlambatan respon *service desk*	√	Pelaporan permintaan layanan dan insiden yang diajukan oleh pengguna tidak segera direspon oleh service desk sehingga menyebabkan tidak optimalnya pengelolaan permintaan layanan dan insiden.
3	Kesalahan pencatatan permintaan layanan dan insiden	√	Pencatatan waktu pelaporan masih sering salah pada sistem e-ticket (tanggal atau waktu berubah tidak sesuai kondisi pelaporan) , serta kesalahan lain terkait pencatatan pelaporan melalui e-mail dan e-ticket
4	Kegagalan akses sistem e-ticket	√	Bug sistem e-ticket sehingga menyebabkan baik pengguna maupun teknisi/admin service desk tidak dapat mengakses dan menggunakannya.

No.	Risiko	Pernah Terjadi	Keterangan
5	Log permintaan layanan dan insiden tidak lengkap	√	Apabila log pencatatan permintaan layanan dan insiden pada e-mail maupun sistem e-ticket ada yang terhapus sebelum ditangani, atau pengguna tidak lengkap dalam mengisi formulir pelaporan pada sistem e-ticket.
6	Penyalahgunaan hak akses permintaan layanan secara sengaja	√	Penyalahgunaan hak akses pengguna dengan meminta layanan di luar hak nya, maupun menyampaikan keluhan atas layanan TI yang tidak sesuai dengan hak akses yang didefinisikan dalam manajemen user. Risiko ini dapat ditangani dengan surat yang diajukan oleh pengguna terkait pelaporan.
7	Pengabaian laporan insiden oleh teknisi/staf service desk	√	Teknisi (unit pada DPTSI yang bertanggung jawab menangani insiden atau memenuhi permintaan layanan) atau staf service desk tidak menanggapi laporan yang diajukan oleh pengguna, baik melalui e-mail maupun sistem e-ticket.
8	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan	√	Service desk melakukan kesalahan dalam mendistribusikan / mengalokasikan / mengeskalasi insiden dan pemenuhan permintaan layanan kepada teknisi atau unit yang bertanggung jawab dalam menanganinya sehingga pelaporan tidak ditangani secara cepat dan tepat.

No.	Risiko	Pernah Terjadi	Keterangan
9	Penanganan insiden dan pemenuhan permintaan layanan overdue	√	Waktu penanganan insiden dan pemenuhan permintaan layanan overdue atau di luar dari SLA (Service Level Agreement) yang dijanjikan kepada pengguna.
10	Kesalahan penanganan insiden dan pemenuhan permintaan layanan		Kejadian berupa kesalahan dalam penanganan insiden yang disebabkan oleh: 1. Teknisi atau staf *service desk* tidak menguasai keluhan yang dilaporkan pengguna. Risiko ini belum pernah terjadi dikarenakan insiden selalu dapat tertangani. 2. Service desk salah dalam mendefinisikan kategori / klasifikasi permintaan layanan dan insiden untuk membantu dalam proses pendistribusian penanganan, juga disebabkan oleh salah dalam mendefinisikan prosedur pengelolaan permintaan layanan dan insiden.
11	Ketidakpuasan user dengan layanan	√	Ketidakpuasan pengguna terhadap layanan TI pada service desk dengan adanya komplain disebabkan oleh lamanya penanganan insiden maupun pemenuhan permintaan, juga tidak terdapat verifikasi kepuasan pengguna terhadap layanan.

No.	Risiko	Pernah Terjadi	Keterangan
12	Ketidakjelasan status permintaan layanan dan insiden		Tidak terdapat distribusi status permintaan layanan dan insiden antara service desk,teknisi, dan pengguna layanan. Status ini menunjukkan apakah permintaan layanan dan insiden sedang direspon, telah selesai ditangani, atau telah ditutup oleh service desk maupun teknisi.
13	Kesalahan pendefinisan tren pada laporan		Kesalahan dalam mendefinisikan tren berupa pelaporan permintaan layanan dan insiden yang ada pada laporan sehingga menyebabkan sering terulangnya insiden serupa, atau lamanya proses penanganan insiden dan permintaan layanan.
14	Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan	√	Laporan pengelolaan permintaan layanan dan insiden yang dibuat tidak terdistribusi karena tidak terdapat pertemuan khusus yang membahas mengenai progres pengelolaan permintaan layanan dan insiden pada service desk, melainkan hanya melalui percakapan online (Whatsap). Serta kemungkinan risiko dokumen SKP (berisi hasil pekerjaan setiap staf service desk) tidak dapat di-upload ke sistem untuk dicek oleh KaSubDit)

HASIL OBSERVASI

Tanggal	:	24 November 2016
Waktu	:	09.00-11.00
Lokasi	:	DPTSI ITS
Narasumber	:	Bapak Jainul Arifin, Ibu Widiyaningsih, dan Ibu Mudjiatin
Jabatan	:	Staf *service desk*

Tabel D.5 Hasil Observasi

Proses	Checklist	Keterangan
Mendefinisikan skema klasifikasi insiden dan permintaan layanan	√	Dilakukan untuk mengetahui kategori / klasifikasi permintaan layanan dan insiden untuk membantu dalam proses pendistribusian penanganan. Selain itu juga dilakukan pendefinisian prioritas pengelolaan. Tidak terdapat pendefinisian prosedur pengelolaan permintaan layanan dan insiden, melainkan hanya prosedur penanganan/pemenuhannya saja. Terdapat proses pelaporan permintaan layanan dan insiden dari user (pengguna) ke service desk melalui e-mail atau sistem e-ticket.

Proses	Checklist	Keterangan
Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden	√	Pelaporan yang masuk melalui sistem e-ticket atau e-mail (apabila melalui telepon akan diarahkan untuk mengisi formulir di e-ticket atau mengirimkan e-mail), tidak ada pencatatan berupa rekap pelaporan jika melalui e-mail, sedangkan log pelaporan melalui sistem e-ticket otomatis terekap. Klasifikasi berdasarkan jenis permintaan layanan dan insiden, yaitu apakah terkait jaringan, hardware, software, atau layanan. Klasifikasi ini untuk memudahkan dalam mendistribusikan penanganan laporan. Sedangkan prioritasi berdasarkan urgensi permintaan layanan dan insiden (apabila hanya sekedar bertanya, maka dikesampingkan), serta berdasarkan urutan laporan yang terlebih dahulu masuk.
Memverifikasikan, menyetujui dan memenuhi permintaan layanan	√	Hanya untuk beberapa permintaan layanan saja yang diverifikasi, yaitu apabila service desk tidak tau pelaporan permintaan layanan dan insiden harus didistribusikan kemana, terkait hak user yang harus disetujui oleh kasubdit, atau terkait biaya. Kemudian permintaan layanan dipenuhi oleh service desk, kecuali untuk permintaan yang tidak dapat dipenuhi, maka dialokasikan/dieskalasi/didistribusikan ke unit yang dapat memenuhinya. Service desk mengalokasikan permintaan ke unit lain melalui forward e-mail (jika pelaporan melalui e-mail), sedangkan jika melalui sistem e-ticket maka unit tersebut dapat langsung melihat form pelaporannya melalui sistem.
Menginvestigasikan, mendiagnosis dan	√	Terdapat proses mencari penyebab insiden tersebut, sebelum akhirnya ditangani oleh *service desk* atau didistribusikan ke unit yang dapat menanganinya.

Proses	Checklist	Keterangan
mengalokasikan insiden		
Menyelesaikan dan Memulihkan Insiden	√	Insiden ditangani oleh service desk apabila bersifat umum atau dapat langsung ditangani. Apabila tidak dapat ditangani oleh *service desk*, maka ditangani oleh unit yang telah didistribusikan. Apabila insiden ditangani oleh unit di luar service desk, maka komunikasi antara user dengan service desk akan dialihkan kepada unit yang menangani. Komunikasi dengan user ketika proses penanganan insiden adalah melalui e-mail (baik apabila user melaporkan melalui e-ticket, service desk maupun unit yang menangani akan menghubungi user melalui e-mail).
Menutup Permintaan Layanan dan Insiden	√	Service desk maupun unit lain yang menangani permintaan layanan dan insiden akan mengomunikasikan hasil penanganan kepada user, untuk mengetahui apakah user sudah puas dan pelaporan dapat ditutup.
Melacak Status dan Membuat Laporan	√	Service desk melacak kembali status pelaporan melalui sistem e-ticket, apakah pelaporan kembali dibuka oleh user atau sudah benar-benar ditutup. Namun apabila melalui e-mail dan yang menangani adalah unit lain, maka service desk mengomunikasikan status tersebut langsung kepada unit yang menangani baik melalui e-mail maupun telepon. Laporan service desk terhadap hasil pengelolaan permintaan layanan dan insiden dilakukan dengan pembuatan dokumen SKP (terkait apa saja yang telah dilakukan oleh setiap staf service desk) dan baik pertemuan maupun komunikasi via Whatsapp dengan kepala sub direktorat layanan.

Halaman ini sengaja dikosongkan

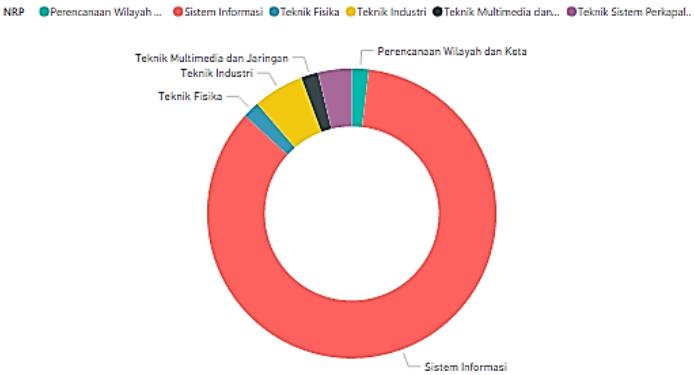
LAMPIRAN E
HASIL SURVEI

Tanggal Pengisian Kuesioner : 28 Desember – 31 Desember 2016
Jumlah Responden : 53 responden

A. Demografi Data

Informasi terkait responden mengenai demografi identitas responden meliputi: NRP (Jurusan) dan Jenis Angkatan

1. NRP (Jurusan)
   Responden yang dituju merupakan pengguna layanan unit *service desk* DPTSI, dimana sebagian besar yang menggunakan layanan ialah mahasiswa. Berikut merupakan jurusan dari responden (mahasiswa Institut Teknologi Sepuluh Nopember).



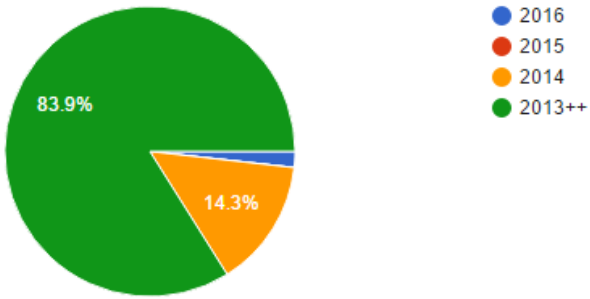
Gambar E.1 Demografi Data Jurusan

Berdasarkan grafik diatas, dapat diketahui bahwa:
- 84.91% responden berasal dari Jurusan Sistem Informasi
- 5.66 % responden berasal dari Jurusan Teknik Industri

- 1.89% responden berasal dari Jurusan Perencanaan Wilayah dan Kota
- 1.89% responden berasal dari Jurusan Teknik Fisika
- 1.89% responden berasal dari Jurusan Teknik Multimedia dan Jaringan
- 3.77% responden berasal dari Jurusan Teknik Sistem Perkapalan.

Maka dapat disimpulkan bahwa mayoritas responden berasal dari Jurusan Sistem Informasi.

2. Jenis Angkatan



Gambar E.2 Demografi Data Angkatan

Berdasarkan grafik diatas, dapat diketahui bahwa:

- 83.9% responden merupakan mahasiswa angkatan 2013++
- 14.3% responden merupakan mahasiswa angkatan 2014
- 1.8% respoonden merupakan mahasiswa angkatan 2016.

Maka dapat disimpulkan bahwa mayoritas responden merupakan mahasiswa angkatan 2013++.

B. Analisis Deskriptif Data Kuesioner

Penelitian ini memanfaatkan skala *Likert* lima poin dengan nilai 1-5, memiliki penilaian yang dimana nilai terendah menunjukan penurunan kepuasan yang rendah menuju nilai tertinggi menunjukan penurunan kepuasan yang tinggi. Nilai-nilai tersebut menunjukan persepsi responden terhadap pernyataan yang diberikan. Berikut pada Tabel E.1 merupakan rentang skala likert yang digunakan untuk melihat hasil respon kuesioner.

Tabel E.1 Rentang Skala Likert

Nilai Skala Likert	Keterangan Skala Likert	Rentang Skala Likert
1	Penurunan Sangat Sedikit	1,00 – 1,50
2	Penurunan Sedikit	1,51 – 2,50
3	Netral	2,51 – 3,50
4	Penurunan Banyak	3,51 – 4,50
5	Penurunan Sangat Banyak	4,51 – 5,00

Berikut pada Tabel E.2 merupakan rekap hasil kuesioner yang diambil dari total 53 responden.

Tabel E.2 Rekap Hasil Survei

ID	Pertanyaan	Jumlah Jawaban Responden					Total	Mean	Keterangan
		1	2	3	4	5			
K01	Ketika *service desk* tidak memenuhi permintaan dan menangani keluhan sesuai harapan saya, maka kepuasan saya mengalami :	0	7	5	33	8	53	3.79	Penurunan Banyak
K02	Ketika *service desk* terlambat dalam merespon laporan keluhan dan permintaan saya, maka kepuasan saya mengalami :	0	12	7	25	9	53	3.58	Penurunan Banyak
K03	Ketika *service desk* mengabaikan laporan keluhan dan permintaan saya, maka kepuasan saya mengalami :	1	2	3	24	23	53	4.24	Penurunan Banyak
K04	Ketika *service desk* selesai menangani laporan keluhan dan permintaan saya di luar batas waktu yang dijanjikan, maka kepuasan saya mengalami :	3	15	10	22	3	53	3.13	Netral
K05	Ketika *service desk* tidak melakukan verifikasi kepuasan saya untuk memastikan bahwa laporan keluhan dan permintaan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami :	7	12	15	17	2	53	2.87	Netral
K06	Ketika *service desk* tidak memberi keluhan dan permintaan informasi status laporan saya (sedang	0	15	9	24	5	53	3.36	Netral

ID	Pertanyaan	Jumlah Jawaban Responden					Total	Mean	Keterangan
		1	2	3	4	5			
	direspon / selesai ditangani / telah ditutup), maka kepuasan saya mengalami :								
K07	Ketika *service desk* tidak menangani masalah yang berulang kali saya keluhkan hingga akar permasalahan, maka kepuasan saya mengalami :	0	5	14	21	13	53	3.79	Penurunan Banyak
K08	Ketika *service desk* tidak mengalami peningkatan dalam melayani permintaan dan keluhan saya, maka kepuasan saya mengalami :	2	10	14	20	7	53	3.37	Netral
K09	Ketika sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak dapat saya akses, maka kepuasan saya mengalami:	1	14	14	20	4	53	3.23	Netral
K10	Ketika keamanan informasi pada sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak terlindungi, maka kepuasan saya mengalami :	1	5	9	23	15	53	3.87	Penurunan Banyak

Halaman ini sengaja dikosongkan

LAMPIRAN F
CONTROL OBJECTIVE

Tabel F.1 Pemetaan Control Objective

Proses COBIT 5	Service Desk Standard	Control Objective
DSS02.01 Mendefinisikan skema klasifikasi insiden dan permintaan layanan	*4.05 Stafing and scheduling* *4.13 Service catalogue management* *5.03 Service level management*	Memastikan Adanya Pendefinisian Layanan, Manajemen Tingkat Layanan dan Tingkat Susunan Kepegawaian
DSS02.02 Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden	*4.06 IT service management system* *4.07 IT service management system – product capability* *4.10 Self-service* *5.05 Incident and service request management*	Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden
	5.06 Incident and service request logging	Memastikan Adanya Prosedur Pencatatan Permintaan Layanan dan Insiden
	5.07 Prioritization	Memastikan Adanya Skema Prioritisasi Permintaan Layanan dan Insiden

	5.08 Categorization	Memastikan Adanya Klasifikasi Permintaan Layanan dan Insiden
DSS02.03 Memverifikasikan, menyetujui dan memenuhi permintaan layanan	*4.15 Security*	Memastikan Adanya Verifikasi Hak Penggunaan Permintaan Layanan
	4.14 Financial management	Memastikan Adanya Persetujuan Pemenuhan Permintaan Layanan
	4.16 Supplier and partner/3rd party management *5.10 Incident resolution and service request fulfillment*	Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden
DSS02.04 Menginvestigasikan, mendiagnosis dan mengalokasikan insiden	*4.03 Distribution of incoming interactions* *4.08 Remote access and control* *5.01 Pro-active incident detection and remediation*	Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden
	4.09 Knowledge management *4.11 Integrated systems*	Memastikan Adanya Penggunaan Informasi Pengelolaan Insiden
DSS02.05 Menyelesaikan dan Memulihkan Insiden	*5.10 Incident resolution and service request fulfillment*	Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden

DSS02.06 Menutup Permintaan Layanan dan Insiden	*5.02 Managing customer satisfaction* *5.04 Communication* *5.09 Incident and service request status assignment and reporting* *5.11 Incident and service request closure* *7.01 Customer perception programme* *7.02 Survey result management* *7.03 Customer feedback management* *7.04 Complaint management*	Memastikan Adanya Penutupan Permintaan Layanan dan Insiden
DSS02.07 Melacak Status dan Membuat Laporan	*8.01 Reporting activities* *8.02 Business related metrics* *8.03 Number of incidents and service requests* *8.04 Avarage time to respond* *8.05 Abandon rate* *8.06 Avarage time taken to resolve incidents or fulfil service requests* *8.07 First contact incident resolution and request fulfilment rate* *8.08 First level incident resolution and request fulfilment rate* *8.09 Re-opened incident rate* *8.10 Backlog management*	Memastikan Adanya Laporan Pengelolaan Permintaan Layanan dan Insiden

	8.11 Percentage of hierarchic escalations (management notification) *8.12 Percentage of functional escalations (re-assignment)* *8.13 Avarage resolution time by priority* *8.14 Average resolution time by incident category and service request type* *8.15 Comparison of overall service level goals to actual results* *8.16 Remote control monitoring measured against goals* *8.17 Self-logging monitoring measured against goals* *8.19 Knowledge usage* *8.20 Knowledge quality and effectiveness* *8.21 Monitoring incidents caused by changes measured against a target* *8.22 Total cost of service* *8.23 Average cost per incident and service request (cost per contact)* *8.24 Average cost per incident and service request by channel (method received)*	

	5.12 Problem management *5.13 IT change management* *5.14 Release and deployement management* *5.15 Service introduction* *5.16 Configuration and asset management* *5.17 IT service continuity management* *5.18 Telephone call monitoring* *5.19 Incident and service request monitoring*	Memastikan Adanya Peningkatan Pengelolaan Permintaan Layanan dan Insiden

Halaman ini sengaja dikosongkan

LAMPIRAN G
FAKTOR RISIKO

Tabel G.1 Faktor Risiko

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
IT01	Penanganan insiden dan pemenuhan permintaan layanan overdue	***Complexity of IT*** Kompleksnya sistem TI yang dilaporkan. ***Strategic priorities*** Salah dalam melaksanakan strategi prioritas penanganan. ***Financial capacity*** Lamanya persetujuan pemenuhan permintaan oleh KaSubDit Layanan TSI dikarenakan di luar kapasitas finansial.	***Regulatory environment*** Peraturan organisasi yang membantasi untuk menangani insiden dan memenuhi permintaan layanan.
IT02	Kesalahan penanganan insiden dan pemenuhan permintaan layanan	***Operating model*** *Service desk* tidak mendokumentasikan (atau tidak lengkap) pendefinisian klasifikasi, prioritasi, serta prosedur permintaan & insiden sehingga salah dalam mendefinisikan di operasionalnya. ***Complexity of IT***	***Technology status and evolution*** Perkembangan teknologi baru yang menyebabkan kompleksnya insiden terkait layanan TI.

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		Kompleksnya sistem TI yang harus ditangani atau di luar insiden yang umum ditangani oleh teknisi/*service desk*. ***Culture of enterprise*** Teknisi/*service desk* tidak terbiasa menangani pelaporan serupa. ***Strategic importance of IT in the enterprise*** Tidak terdapat strategi TI yang baik pada perusahaan terkait pengelolaan permintaan layanan dan insiden, seperti tidak terdapat pelatihan khusus penanganan insiden sehingga menyebabkan teknisi/*service desk* tidak menguasai perkembangan ilmu pengetahuan dalam menangani insiden.	
IT03	Kesalahan pemahaman permintaan pengguna layanan	***Complexity of IT*** Kompleksnya sistem TI yang harus dipenuhi. ***Culture of enterprise***	***Technology status and evolution*** Perkembangan teknologi baru yang menyebabkan kompleksnya permintaan terkait layanan TI.

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		Teknisi/*service desk* tidak melakukan konfirmasi ulang kepada pelapor terhadap harapan terkait permintaan layanan yang diajukan. Hal ini mengakibatkan kesalahan pemahaman yang dialami dalam mengidentifikasi permintaan tidak segera terverfikasi hingga selesai pemenuhan yang ternyata tidak sesuai dengan harapan pelapor.	
IT04	Keterlambatan respon *service desk*	***Startegic priorities*** *Service desk* tidak memiliki prioritas strategis dalam menanggapi permintaan layanan dan insiden, seperti pelaporan mana yang harus ditanggapi terlebih dahulu berdasarkan urgensi dan dampaknya. Hal ini mengakibatkan kurang responsifnya *service desk* dalam menangani permintaan layanan dan insiden. ***Culture of the enterprise*** Tidak terciptanya budaya organisasi yang merepresentasikan etos kerja tinggi	***Competitive environment*** Tingginya standar layanan TI di organisasi lain yang mempengaruhi standar tingkat respon yang dikatakan responsif pada *service desk*.

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		termasuk dalam hal pelayanan TI pada unit *service desk* yang mengakibatkan rendahnya tingkat respon dalam pelayanan. Selain itu, tidak terdapat prosedur dan SLA yang terdokumentasi sebagai panduan proses terstandar yang mendorong *service desk* untuk memenuhi tingkat layanan yang disetujui dan dijanjikan kepada pengguna layanan.	
SO01	Kesalahan pencatatan permintaan layanan dan insiden	***Complexity of IT*** Sistem *e-ticket* kompleks dan banyak *bug/error* sehingga banyak kesalahan pencatatan.	***Technology status and evolution*** Evolusi teknologi yang mempengaruhi adaptasi sistem *e-ticket*
SO02	Log permintaan layanan dan insiden tidak lengkap	***Operating model*** Kesalahan dalam operasional pengelolaan permintaan dan insiden.	***Technology status and evolution*** Perkembangan teknologi untuk *service desk* dalam mengelola pencatatan pelaporan.
SO03	Pengabaian laporan insiden oleh	***Culture of the enterprise*** Teknisi/staf *service desk* kurang responsif.	***Regulatory environment***

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
	teknisi/staf *service desk*		Tidak terdapat peraturan atau kebijakan yang jelas terkait pengelolaan.
SO04	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan	***Operating model*** *Service desk* tidak mengalokasikan pelaporan sesuai dengan pendefinisian yang dilakukan.	***Regulatory environment*** Pengaruh perubahan peraturan terkait tugas pokok dan fungsi tiap SubDirektorat.
SO05	Ketidakpuasan user dengan layanan	***Operating model*** *Service desk* & teknisi tidak melaksanakan operasional layanan sesuai standar, khususnya dalam menangani laporan insiden dan memenuhi permintaan layanan, serta tidak melakukan verifikasi kepuasan pengguna terhadap hasil penanganan laporan.	***Competitive environment*** Tingginya standar layanan TI di organisasi lain yang mempengaruhi standar kepuasan *user*.
SO06	Ketidakjelasan status permintaan layanan dan insiden	***Operating model*** Model pengoperasian *service desk* tidak tersentralisasi, di mana apabila pelaporan telah dieskalasi ke bagian teknisi atau pemasok pemenuhan permintaan dan	***Technology status and evolution*** *Service desk* tidak memiliki teknologi/sistem informasi yang dapat mengakomodasi dalam distribusi atau pengembalian status pelaporan

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		penanganan inisden, maka pengguna/pelapor layanan langsung berhubungan dengan pihak bersangkutan sedangkan *service desk* tidak memiliki akses komunikasi langsung kepada pengguna. Terkait perubahan status pemenuhan permintaan dan penanganan insiden yang dilakukan tidak didistribusikan kembali kepada *service desk* atau pengguna sehingga menimbulkan ketidakjelasan status.	permintaan layanan dan insiden sehingga dapat diakses oleh seluruh pengguna TI baik oleh *service desk*, pelapor dan teknisi.
SO07	Kesalahan pendefinisan tren pada laporan	***Culture of the enterprise*** Tidak terdapat rapat pertemuan yang membahas laporan pengelolaan permintaan layanan & insiden.	***Technology status and evolution*** Tuntutan perkembangan TI dalam mengevaluasi tren permintaan dan insiden.
SW01	Kegagalan akses sistem e-ticket	***Complexity of IT*** Sistem *e-ticket* kompleks dan banyak *bug/error*.	***Technology status and evolution*** Perkembangan teknologi menuntut sistem *e-ticket* untuk selalu diupdate**.** ***Threat landscape***

ID Risiko	Risiko	Faktor Risiko	
		Internal	**Eksternal**
			Ancaman serangan sistem dari pihak tidak berwenang.
SW02	Laporan tidak terdistribusi-kan	***Complexity of IT*** Sistem tidak dapat mendistribusikan laporan secara otomatis & merata. ***Culture of enterprise*** Tidak terdapat rapat pertemuan yang membahas laporan pengelolaan permintaan layanan & insiden.	***Regulatory environment*** Tidak ada kebijakan dan prosedur terkait laporan pengelolaan permintaan layanan dan insiden.
LA01	Penyalahgunaan hak akses permintaan layanan secara sengaja	***Complexity of IT*** Sistem *e-ticket* tidak menerapkan standar keamanan yang tinggi.	***Threat landscape*** Ancaman serangan sistem milik *service desk* dari pihak tidak berwenang.