TUGAS AKHIR – KS141501

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA *HELPDESK* SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

INFORMATION TECHNOLOGY PROCESS RISK ASSESSMENT BASED ON COBIT 5 FRAMEWORK AT HELPDESK SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

Chitra Utami Putri
NRP 5213 100 193

Dosen Pembimbing
Hanim Maria Astuti, S.Kom., M.Sc
Feby Artwodini, S.Kom., M.T

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

TUGAS AKHIR – KS 141501

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA *HELPDESK* SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

Chitra Utami Putri
NRP 5213 100 193

Dosen Pembimbing 1:
Hanim Maria Astuti, S.Kom., M.Sc

Dosen Pembimbing 2:
Feby Artwodini, S.Kom., M.T

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

FINAL PROJECT – KS 141501

INFORMATION TECHNOLOGY PROCESS RISK ASSESSMENT BASED ON COBIT 5 FRAMEWORK AT HELPDESK SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

Chitra Utami Putri
NRP 5213 100 193

Supervisor 1 :
Hanim Maria Astuti, S.Kom., M.Sc

Supervisor 2 :
Feby Artwodini, S.Kom., M.T

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Institute of Technology Sepuluh Nopember
Surabaya 2017

LEMBAR PENGESAHAN

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA *HELPDESK* SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

TUGAS AKHIR

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

Oleh:

Chitra Utami Putri
5213 100 193

Surabaya, Januari 2017

KETUA
JURUSAN SISTEM INFORMASI

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

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA *HELPDESK* SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

TUGAS AKHIR

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

Oleh :
Chitra Utami Putri
5213 100 193

Disetujui Tim Penguji : Tanggal Ujian : 12 Januari 2017
Periode Wisuda: Maret 2017

Hanim Maria Astuti, S.Kom., M.Sc. **(Pembimbing 1)**

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

Ir. Achmad Holil Noor Ali, M.Kom. **(Penguji 1)**

Eko Wahyu Tyas, S.Kom., MBA **(Penguji 2)**

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA *HELPDESK* SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

Nama Mahasiswa : CHITRA UTAMI PUTRI
NRP : 5213 100 193
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing 1: Hanim Maria Astuti, S.Kom., M.Sc
Dosen Pembimbing 2: Feby Artwodini, S.Kom., M.T

ABSTRAK

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) merupakan salah satu lembaga yang bertanggungjawab untuk menyelenggarakan pelayanan Teknologi dan Sistem Informasi (TSI) di Institut Teknologi Sepuluh Nopember (ITS) Surabaya. Salah satu pelayanan TSI yang disediakan ialah pengelolaan insiden dan pemenuhan permintaan layanan, dimana unit fungsional yang melaksanakan proses tersebut ialah unit Helpdesk pada Subdirektorat Layanan Teknologi dan Sistem Informasi. Manajemen insiden dan pemenuhan permintaan layanan merupakan serangkaian proses teknologi informasi yang memegang peranan cukup penting namun rentan mengalami kesalahan yang dapat menimbulkan risiko. Oleh karena itu, perlu dilakukan identifikasi dan penilaian risiko proses teknologi informasi untuk menghindari terhambatnya proses bisnis dan meminimalisir kerugian.

Untuk melakukan identifikasi proses TI, kerangka kerja yang relevan ialah COBIT 5 Enabling process, serta untuk melakukan manajemen risiko dibantu dengan standar COBIT 5

for risks. Risiko diidentifikasi dari proses bisnis helpdesk dan kondisi kekinian yang terjadi di organisasi. Penggalian data didapatkan dari hasil wawancara dan observasi, untuk kemudian dicocokkan dengan kondisi ideal sesuai proses COBIT 5 DSS02 Manage Service Requests and Incidents, lalu dilakukan identifikasi, penilaian dan manajemen risiko berdasarkan proses COBIT 5 APO12 Manage Risks.
Produk akhir yang dihasilkan dari tugas akhir ini ialah hasil penilaian dan langkah mitigasi risiko proses manajemen insiden dan permintaan layanan berdasarkan kerangka kerja COBIT 5 yang dapat digunakan sebagai acuan untuk mengelola risiko agar dapat mengantisipasi kerugian.

Kata Kunci: manajemen insiden, pemenuhan permintaan layanan, manajemen risiko, identifikasi risiko, penilaian risiko, mitigasi risiko, risiko proses TI, COBIT 5, COBIT 5 for Risk.

INFORMATION TECHNOLOGY PROCESS RISK ASSESSMENT BASED ON COBIT 5 FRAMEWORK AT HELPDESK SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

Name	**: CHITRA UTAMI PUTRI**
NRP	**: 5213 100 193**
Department	**: Information Systems FTIF-ITS**
Supervisor 1	**: Hanim Maria Astuti, S.Kom., M.Sc**
Supervisor 2	**: Feby Artwodini, S.Kom., M.T**

ABSTRACT

Direktorat Pengembangan Teknologi Sistem Informasi (DPTSI) is a part of Institut Teknologi Sepuluh Nopember Surabaya that are responsible for the service of Information Technology Systems. One of IT services provided is incident management and requests fulfillment, which managed by helpdesk unit at Subdirektorat Layanan Teknologi dan Sistem Informasi. Incident management and requests fulfillment are a set of processes that holds an important role yet prone to errors that could pose some risks. Hence, identification and assessment of IT risks are really necessarry to avoid obstacle in business processes and minimize losses.

In order to identify IT process, the relevant framework is COBIT 5 Enabling process, and using COBIT 5 for risks for conduct risk management. Risks are identified from helpdesk's business processes and existing condition that occur in the organization. Data are obtained from interviews and observations, then to be cohered with corresponding ideal conditions based on COBIT 5 process DSS02 Manage Service Requests and Incidents. Then risk can be identified, assessed and managed based on APO12 Manage Risks COBIT 5 process.

Hence the output is to gain an IT risk management document that contains list of IT risk assessment and risk

control justification which can be a reference for helpdesk Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS in managing IT risk.
The final product of this study are the risk assessment result and also its mitigations of incident management and requests fulfillment processes based on the COBIT 5 framework that can be used as a reference for managing risks in order to anticipate losses.

Keywords: incident management, requests fulfillment, risk management, risk identifiaction, risk assessment, risk mitigation, IT process-related risk, COBIT 5, COBIT 5 for Risk.

"Halaman ini sengaja dikosongkan"

KATA PENGANTAR

Syukur Alhamdulillah dipanjatkan oleh peneliti atas segala petunjuk, pertolongan, kasih sayang, dan kekuatan yang diberikan oleh Allah SWT. Hanya karena ridho-Nya, peneliti dapat menyelesaikan laporan Tugas Akhir, dengan judul **PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA *HELPDESK* SUBDIREKTORAT LAYANAN TEKNOLOGI DAN SISTEM INFORMASI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

Pada kesempatan ini, penulis ingin menyampaikan banyak terima kasih kepada semua pihak yang telah memberikan dukungan, bimbingan, arahan, bantuan, dan semangat dalam menyelesaikan tugas akhir ini, yaitu kepada:

- Orang tua dan keluarga penulis yang senantiasa mendoakan dan mendukung, khususnya Mama dan Papa yang selalu mendorong penulis untuk segera menyelesaikan tugas akhir ini.
- Ibu Hanim Maria Astuti, S.Kom., M.Sc dan Ibu Feby Artwodini S.Kom., M.T, selaku dosen pembimbing yang yang telah meluangkan waktu untuk membimbing dan mendukung dalam penyelesaian tugas akhir ini.
- Ibu Mudjiyatin, Bapak Jainul Arifin, Ibu Wiwin Rochmawati dan Ibu Widyaningsih. yang telah menjadi narasumber untuk kebutuhan penelitian mahasiswa.
- Bapak Radityo Prasetianto Wibowo, S.Kom., M.Kom., selaku dosen wali yang senantiasa memberikan pengarahan selama penulis menempuh masa perkuliahan dan pengerjaan tugas akhir ini.

- Caesar Fajriansah, sebagai sosok yang selalu setia menemani, membantu dan menyemangati dari awal masuk perkuliahan hingga pengerjaan tugas akhir ini selesai.
- Teman – teman seperjuangan Lab MSI dan Grup Penelitian DPTSI (Sarah, Mahesti, Selina, Sherly, Firzah, Yura dan Mega) serta teman-teman Beltranis yang bersama-sama berusaha dan saling membantu serta menyemangati untuk menyelesaikan penelitian ini.
- Teman-teman All We Can Eat (Jockey, Oriehanna, Garini, Hisyam, Pandu, Denny, Pakaya) dan HOD Kost (Nadya, Rara, Pijar, Abel, Nevy) yang telah memberikan semangat dalam menyelesaikan penelitian ini.
- Pak Hermono, selaku admin laboratoriun MSI yang membantu penulis dalam hal administrasi penyelesaian tugas akhir.
- Serta pihak lain yang telah mendukung dan membantu dalam kelancaran penyelesaian tugas akhir ini.

Penyusunan laporan ini masih jauh dari sempurna, untuk itu peneliti menerima kritik dan saran yang membangun untuk perbaikan di masa mendatang. Penelitian ini diharapkan dapat menjadi salah satu acuan bagi penelitian – penelitian yang serupa dan bermanfaat bagi pembaca.

Surabaya, Januari 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

"Halaman ini sengaja dikosongkan"

DAFTAR BAGAN

BAB I
PENDAHULUAN

Pada bab pendahuluan akan diuraikan proses identifikasi masalah penelitian yang meliputi latar belakang masalah, perumusan masalah, batasan masalah, tujuan tugas akhir, manfaat kegiatan tugas akhir dan relevansi terhadap pengerjaan tugas akhir. Berdasarkan uraian pada bab ini, harapannya gambaran umum permasalahan dan pemecahan masalah pada tugas akhir dapat dipahami.

1.1 Latar Belakang

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya adalah salah satu organisasi yang berada di Institut Teknologi Sepuluh Nopember Surabaya terkait penanganan masalah komputer, jaringan dan teknologi informasi [1], sehingga DPTSI ITS telah menggunakan teknologi informasi (TI) untuk menunjang proses bisnisnya. Dalam kasus ini, kebelangsungan proses bisnis Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS memegang peranan yang penting bagi keberlangsungan proses bisnis, terutama pada bagian *helpdesk* dalam mengelola insiden (*incident management*) dan pemenuhan permintaan layanan (*requests fulfillment).*

Helpdesk merupakan titik utama bagi pengguna ketika terjadi suatu gangguan layanan, permintaan layanan, atau permintaan perubahan lainnya. *Helpdesk* menyediakan komunikasi satu titik antara pengguna dan organisasi [2]. Dalam kesehariannya, *helpdesk* di Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI memanfaatkan peran TI untuk membantu menyelesaikan permintaan. Namun dibalik penggunaan TI yang memberikan kemudahan pada berbagai aspek kegiatan bisnis, tidak jarang menghasilkan kesalahan dan risiko yang dapat menghambat dan memberikan kerugian pada proses bisnis organisasi [3].

Risiko adalah variasi dalam hal-hal yang mungkin terjadi secara alami atau kemungkinan terjadinya peristiwa diluar yang diharapkan yang dapat menjadi ancaman terhadap properti dan

dapat menimbulkan kerugian finansial akibat bahaya yang terjadi. Manajemen risiko merupakan pendekatan yang dilakukan terhadap risiko yaitu dengan memahami, mengidentifikasi dan mengevaluasi suatu kemungkinan risiko [4]. Identifikasi dan pengelolaan risiko sangat penting dilakukan agar pihak internal maupun eksternal organisasi dapat mengantisipasi terjadinya bahaya maupun kerusakan yang dapat merugikan bisnis, baik dari segi finansial maupun operasional [5].

Risiko proses TI adalah risiko yang muncul dari serangkaian aktivitas TI yang tersistematis dan memiliki tujuan. Risiko TI merupakan hal yang detail namun juga rentan dari kesalahan dan ancaman, selain itu risiko proses TI juga belum banyak di teliti, karena penelitian risiko biasanya berfokus pada aset TI [6]. Selain didentifikasi, penilaian risiko TI juga diperlukan dalam meningkatkan perlindungan teknologi informasi dan aspek-aspek didalamnya, untuk dapat diketahui risiko mana yang berdampak paling signifikan [3].

DPTSI ITS merupakan organisasi yang berkembang dan memiliki aktivitas yang beragam, sehingga ancaman, kerentanan dan risiko dari proses teknologi informasi di Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS semakin kompleks [3]. Selain itu belum pernah dilakukan identifikasi dan penilaian risiko tersendiri terkait pengelolaan layanan dan insiden di DPTSI ITS. Oleh karena itu, *helpdesk* membutuhkan suatu kontrol melalui identifikasi dan penilaian risiko dari proses-proses TI yang terjadi di Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS.

Untuk melakukan identifikasi dan penilaian risiko diperlukan kerangka kerja dan standar untuk membantu dalam melakukan penelitian [7]. Kerangka kerja dan standar yang relevan yang terkait dengan penelitian ini yaitu COBIT 5 *Enabling Processes* terkait identifikasi manajemen insiden dan pemenuhan permintaan layanan, dan COBIT 5 *for Risk* terkait manajemen risiko. Proses TI yang sudah teridentifikasi dari kondisi kekinian nantinya akan dipetakan dengan proses TI ideal pada COBIT 5 *Enabling Process.*

Domain yang digunakan pada kerangka kerja COBIT 5 adalah *Deliver Service and Support* (DSS) yaitu pada proses DSS02 *Manage Service Request and Incidents* dan *domain Align, Plan and Organise* (APO) yaitu proses APO12 *Manage Risk*. Domain DSS dipilih karena dianggap sesuai dengan kondisi teknologi informasi yang ada pada organisasi yang bertanggung jawab dalam kebutuhan untuk mengirimkan layanan, melayani, dan mendukung layanan teknologi informasi. Domain lain yaitu APO (*Align, Plan, and Organize*) akan dirasa sesuai diterapkan pada metodologi manajemen risiko teknologi informasi karena proses didalamnya sangat kompleks [8].

Dengan demikian, salah satu bentuk dukungan dalam menjaga optimalisasi proses TI pada *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI adalah dengan melakukan manajemen risiko untuk memastikan risiko yang muncul dapat ditangani agar tidak mengganggu proses bisnis yang sedang berjalan [9].

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan di atas, berikut adalah rumusan masalah yang dijadikan acuan dalam pembuatan tugas akhir ini :

1. Apa saja risiko yang terdapat pada unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS Surabaya?
2. Bagaimana hasil penilaian risiko yang terdapat pada unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS Surabaya berdasarkan pendekatan COBIT *for risk*?
3. Bagaimana hasil pemetaan risiko proses TI pada unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS Surabaya dengan proses TI COBIT 5 *Enabling Processes* sebagai langkah mitigasi risiko?

1.3 Batasan Masalah

Dalam pengerjaan tugas akhir ini, ada beberapa batasan masalah yang harus diperhatikan, yaitu sebagai berikut:

1. Studi kasus yang digunakan hanya pada bagian *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi Teknologi dan Sistem Informasi (TSI) Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya dan hanya berdasarkan proses manajemen insiden dan pemenuhan permintaan layanan.
2. Kerangka kerja dan metode yang digunakan pada penelitian ini berdasarkan standar dan metodologi pada COBIT 5 *for Risk* untuk pengelolaan risiko serta menggunakan kerangka kerja COBIT 5 *Enabling Processes* untuk mengidentifikasi proses TI terkait manajemen insiden dan permintaan layanan.
3. Tindakan manajemen risiko yang dilakukan dalam penelitian ini hanya sampai pada penilaian dan memberikan langkah mitigasi risiko sesuai proses TI pada kerangka kerja COBIT 5.
4. Aktivitas pada proses APO12 *Manage Risk* pada COBIT 5 yang digunakan hanya sampai aktivitas APO12.02 yaitu menganalisis risiko.

1.4 Tujuan Tugas Akhir

Berdasarkan perumusan masalah yang disebutkan sebelumnya, tujuan yang akan dicapai melalui tugas akhir ini adalah:

1. Mengetahui apa saja risiko yang terdapat pada unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS Surabaya.
2. Mengetahui hasil penilaian risiko terhadap proses TI yang terdapat pada unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS Surabaya berdasarkan pendekatan COBIT *for risk.*
3. Mengetahui hasil pemetaan risiko dengan proses TI pada COBIT 5 *Enabling Processes* sebagai langkah mitigasi untuk

unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS Surabaya.

1.5 Manfaat Tugas Akhir

Melalui tugas akhir ini diharapkan dapat memberi manfaat yaitu:

1. Bagi dunia akademis, tugas akhir ini diharapkan dapat memberikan kontribusi mengenai implementasi manajemen risiko proses teknologi informasi di unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi di DPTSI ITS Surabaya berdasarkan pendekatan COBIT 5 *for Risk*, sehingga dapat dijadikan sebagai acuan untuk penelitian selanjutnya.
2. Bagi DPTSI, penilaian risiko yang dihasilkan dan langkah mitigasi yang diusulkan diharapkan dapat digunakan sebagai panduan atau acuan untuk mengelola risiko serta pedoman untuk mengantisipasi kerugian pada unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi yang sesuai dengan *best practice*.

1.6 Relevansi

Relevansi tugas akhir ini terhadap laboratorium Perencanaan dan Topik yang diangkat pada penelitian ini yaitu mengenai pembuatan dokumen manajemen risiko yang mengacu pada kerangka kerja COBIT 5. Dalam lingkup penelitian laboratorium manajemen sistem informasi, penelitian ini masuk dalam topik manajemen risiko dan menghasilkan luaran berupa pembuatan dokumen manajemen risiko. Penelitian ini juga mempunyai relevansi erat dengan mata kuliah wajib Manajemen Risiko Teknologi Informasi (MRTI), Manajemen Layanan Teknologi Informasi (MLTI) dan Tata Kelola Teknologi Informasi (TKTI). Sehingga dapat dikatakan bahwa penelitian ini telah mempunyai relevansi sesuai dengan *roadmap* laboratorium Manajemen Sistem Informasi pada Jurusan Sistem Informasi.

1.7 Target Luaran

Target luaran dari pengerjaan tugas akhir ini adalah sebagai berikut:

1. Hasil penilaian risiko beserta langkah mitigasi berdasarkan proses TI terkait pengelolaan permintaan layanan dan insiden pada *helpdesk* DPTSI ITS.
2. Dokumentasi pengerjaan Tugas Akhir berupa buku Tugas Akhir dan Paper atau Jurnal Ilmiah

1.8 Sistematika Penulisan

Sistematika penulisan tugas akhir ini dibagi menjadi tujuh bab, yakni:

BAB I PENDAHULUAN

Bab ini berisi pendahuluan yang menjelaskan latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat, relevansi dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Definisi dan penjelasan pustaka yang dijadikan referensi beserta penelitian sebelumnya yang terkait dalam pembuatan tugas akhir ini akan dijelaskan pada bab dua. Teori yang dipaparkan di antaranya mengenai Risiko Proses TI, Manajemen Risiko TI, Manajemen Insiden, *Service Fullfillment*, COBIT 5 *Enabling Processes*, COBIT 5 *for Risk*, domain APO12 dan DSS02 COBIT 5, serta konsep-konsep lain yang berkaitan dengan pembuatan tugas akhir.

BAB III METODOLOGI

Bab ini menggambarkan uraian dan urutan pekerjaan yang akan dilakukan dalam penyusunan tugas akhir ini.

BAB IV PERANCANGAN

Bab ini menjelaskan perancangan perangkat yang dilakukan oleh penulis untuk mengumpulkan data kondisi kekinian.

BAB V IMPLEMENTASI

Bab ini menjelaskan hasil yang didapatkan dari proses pengumpulan data, yakni meliputi kondisi kekinian, kondisi yang

diharapkan dari pihak organisasi, dan apa saja hambatan yang dihadapi ketika mengumpulkan data.

BAB VI HASIL DAN PEMBAHASAN

Bab ini berisi tentang bagaimana kesenjangan yang terjadi antara kondisi kekinian dan kondisi ideal, kemudian menjelaskan bagaimana proses pembuatan dokumen SOP, serta proses verifikasi dan validasi SOP dilakukan untuk dapat melihat apakah SOP yang telah dibuat dapat diterapkan atau tidak.

BAB VII PENUTUP

Bab ini berisi tentang simpulan dari keseluruhan tugas akhir dan saran maupun rekomendasi terhadap penelitian tugas akhir ini untuk perbaikan ataupun penelitian lanjutan yang memiliki kesamaan dengan topik yang diangkat.

“Halaman ini sengaja dikosongkan”

BAB II
TINJAUAN PUSTAKA

Bab ini akan menjelaskan mengenai penelitian sebelumnya dan dasar teori yang dijadikan acuan atau landasan dalam pengerjaan tugas akhir ini. Landasan teori akan memberikan gambaran secara umum dari landasan penjabaran tugas akhir ini.

2.1 Penelitian Sebelumnya

Pada pengerjaan tugas akhir ini terdapat beberapa penelitian terkait yang dapat dijadikan sebagai bahan referensi studi literatur untuk menyelesaikan tugas akhir ini. Berikut merupakan beberapa penelitian yang studi kasusnya berkaitan dengan penelitian tugas akhir yang disajikan pada Tabel 2.1.

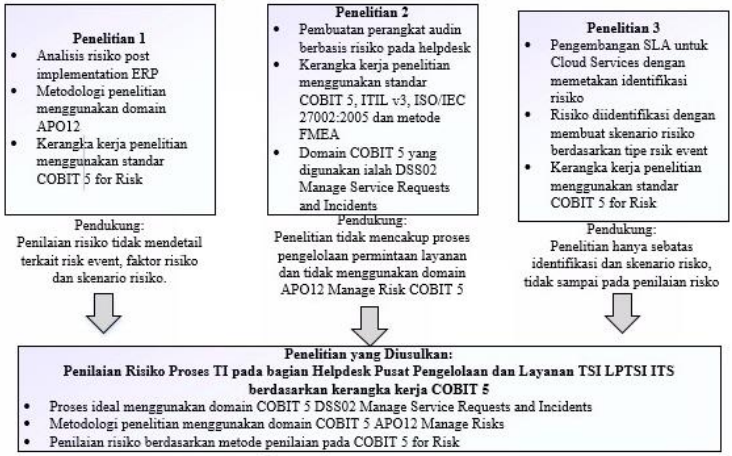
Tabel 2.1 Penelitian Sebelumnya

Penelitian Ke-1	
Judul Penelitian	***Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk*** [10]
Nama Peniliti, Tahun	Dwi Rosa Indah; Harlilil Afriyan Firdaus, 2014
Deskripsi Umum Penelitian	Penelitian ini menghasilkan sebuah dokumen penilaian risiko berdasarkan standar COBIT 5 *for Risk* untuk risiko dibidang proyek ERP. Penelitian risiko dilakukan pada saat pasca implementasi ERP dalam rangka mencapai kesuksesan implementasi ERP berdasarkan *Critical Sucess Factors* [10].
Hubungan dengan Tugas Akhir	Penilaian risiko dilakukan menggunakan standar COBIT 5 for Risk dengan mengacu pada domain APO12 *Manage Risk*.
Kelebihan Penelitian	Penelitian ini menggunakan dua standar, yaitu *CSF of Post Implementation ERP* dan COBIT 5 *for Risk*.
Kekurangan Penelitian	Penelitian ini tidak mendetail terkait analisis risiko, penelitian ini tidak menjabarkan detail tipe risiko, skenario risiko, dan faktor risiko.
Penelitian Ke-2	
Judul Penelitian	**Pembuatan Perangkat Audit Berbasis Risiko untuk Manajemen Insiden pada**

	Helpdesk Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya [11]
Nama Peniliti, Tahun	Dyah Retnani Sulistyaningrum, 2015
Deskripsi Umum Penelitian	Penelitian ini membuat perangkat audit berbasis risiko untuk *helpdesk* PT PDAM Surabaya yang mengacu pada kerangka kerja COBIT 5, ITIL v3 dan ISO/IEC 27002:2005 serta metode FMEA untuk penilaian risiko. Proses yang ditekankan ialah manajemen insiden yang mengacu pada domain DSS02 - *Manage Service Request and Incidents* di COBIT 5 [11].
Hubungan dengan Tugas Akhir	Analisis penilaian risiko berdasarkan domain DSS02 - *Manage Service Request and Incidents* di COBIT 5.
Kelebihan Penelitian	Penelitian ini menghasilkan perangkat audit berbasis risiko.
Kekurangan Penelitian	Penelitian ini hanya memfokuskan pada manajemen insiden, sedangkan proses *helpdesk* juga mencakup proses pengelolaan permintaan layanan. Selain itu proses penilaian risiko pada penelitian ini tidak menggunakan domain *APO12 Manage Risk* COBIT 5.
Penelitian Ke-3	
Judul Penelitian	***Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates***
Nama Peniliti, Tahun	Onyeka Illoh, Shaun Aghili, dan Sergey Butakov, 2015
Deskripsi Umum Penelitian	Penelitian ini membuat *template Service Level Agreement* (SLA) untuk *cloud services* melalui pemetaan skenario risiko dan tipe risiko berdasarkan standar COBIT 5 *for Risk* domain APO12 *Manage Risk* dengan komponen SLA [12].
Hubungan dengan Tugas Akhir	Penggunaan standar COBIT 5 *for Risk* domain APO12 *Manage Risk* dalam menganalisis risiko.
Kelebihan Penelitian	Penelitian ini melakukan pemetaaan SLA dengan identifikasi skenario risiko.

Kekurangan Penelitian	Penelitian ini hanya sebatas mengidentifikasi jenis-jenis dan skenario risiko, tidak sampai melakukan penilaian risiko.

Berdasarkan keterkaitan dengan penelitian-penelitian sebelumnya yang dijabarkan diatas, sehingga kontribusi penelitian pada tugas akhir ini ialah memberikan penilaian risiko proses TI berdasarkan kerangka kerja COBIT 5 untuk bagian *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS yang sebelumnya belum memiliki pedoman tersendiri. Harapannya hasil penilaian risiko tersebut dapat membantu pihak Subdirektorat Pengelolaan Layanan DPTSI ITS dalam melakukan antisipasi dan pengelolaan risiko terkait proses TI seperti manajemen insiden dan permintaan layanan. Berikut merupakan analisis gap dari ketiga penelitian terdahulu tersebut yang ditunjukkan pada Bagan 2.1.



Bagan 2.1 Analisis Gap Penelitian Sebelumnya

2.2 Dasar Teori

Bagian ini akan membahas teori dan bahan penelitian lain yang menjadi dasar informasi untuk mengerjakan tugas akhir ini.

2.2.1 Risiko

Risiko adalah akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan [13]. Menurut beberapa pengertian para ahli, risiko antara lain merupakan:

1. Risiko adalah suatu variasi dari hasil-hasil yang dapat terjadi selama periode tertentu [14].
2. Suatu kemungkinan dalam investasi dimana suatu pihak akan menerima imbal hasil (*return*) atau keuntungan yang berbeda dari imbas hasil yang diharapkan [15].
3. Risiko merupakan penyebaran/penyimpangan hasil aktual yang berbeda dari hasil yang diharapkan [16].
4. Ketidakpastian tentang peristiwa masa depan atas hasil yang diinginkan atau tidak diinginkan [17].
5. Risiko adalah ketidakpastian (*uncertainty*) yang mungkin melahirkan peristiwa kerugian (*loss*) [18].
6. Wujud dari risiko dapat bermacam-macam, antara lain [19]:
    - Berupa kerugian atas harta/kekayaan atau penghasilan, misalnya diakibatkan oleh kebakaran, pencurian, pengangguran, dan sebagainya.
    - Berupa penderitaan seseorang, misalnya sakit/cacat karena kecelakaan.
    - Berupa tanggung jawab hukum, misalnya risiko dari perbuatan atau peristiwa yang merugikan orang lain.
    - Berupa kerugian karena perubahan keadaan pasar, misalnya terjadinya perubahan harga, perubahan selera konsumen dan sebagainya.

Dari definisi-definisi tersebut dapat disimpulkan bahwa risiko merupakan sebuah kemungkinan terjadinya suatu prisitwa yang sangat erat kaitannya dengan ketidakpastian serta ancaman atau bahaya yang bersifat merugikan. Namun risiko bersifat memiliki probabilitas dan dampak yang nantinya akan menimbulkan pengetahuan baru, sedangkan ketidakpastian hanya memberikan dampak. Risiko perlu diidentifikasi dan di mitigasi agar dapat diketahui kemungkinan munculnya risiko untuk diantisipasi dalam upaya mencegah kerugian.

Pandangan tradisional menggambarkan risiko sebagai potensi kejadian yang akan mengancam pencapaian tujuan organisasi atau proyek. Namun, menurut stigma yang saat ini berkembang, risiko tidak hanya diartikan sebagai hal yang negatif, tapi juga positif. Risiko positif (upside risk) disebut juga sebagai peluang (opportunity). Peluang merupakan hal-hal yang dapat mendukung atau mengakselerasi pencapaian tujuan organisasi atau proyek [20].

2.2.2 Risiko Teknologi Informasi

Risiko teknologi informasi sangat erat kaitannya dengan keamanan informasi, dimana informasi merupakan aset yang sangat penting bagi sebuah organisasi dan jika terganggu dapat menimbulkan dampak yang signifikan terhadap proses bisnis organisasi. Risiko tersebut dapat berupa ancaman teknologi informasi dan kerentanan teknologi informasi dari sebuah organisasi. Berikut merupakan pengkategorian risiko menurut komponen sistem informasi yaitu perangkat keras (*hardware*), perangkat lunak (*software*), telekomunikasi atau jaringan (*network*), basis data (*database*), prosedur, dan orang-orang yang terlibat di dalamnya (*people*) yang disajikan dalam Tabel 2.2 [21].

Tabel 2.2 Pengkategorisasian Risiko Berdasarkan Komponen Sistem Informasi [21]

Komponen Sistem Informasi	Ancaman
People	*Human error*, sabotase, *hacking*, *cracking*, penyalahgunaan *password*
Procedure	Kesalahan konfigurasi, kesalahan penggunaan aplikasi
Hardware	Pencurian *hardware*, kerusakan *hardware*
Software	*Virus*, *malware*, bug, *worm*, *trojan*
Data	Kehilangan data, penyalahgunaan data, pencurian data
Network	Penyalahgunaan akses *firewall*, *connection lost*

2.2.3 Proses Teknologi Informasi

Proses Teknologi Informasi (TI) merupakan sebuah runtutan peristiwa sistematis dan terstruktur yang terjadi dalam proses bisnis yang menggunakan teknologi dan sistem informasi pada pelaksanaannya dalam mencapai tujuannya. TI yang tidak dikelola secara sistematis akan mengganggu proses bisnis dan melemahkan kegiatan bisnis, karena tujuan diterapkannya TI adalah untuk mendukung organisasi dalam mencapai tujuan usahanya. Manajemen TI memiliki proses sendiri – dan banyak dari proses-proses tersebut umum di organisasi dari semua ukuran dan di berbagai sektor. Proses-proses yang dikerahkan untuk mengelola organisasi TI itu sendiri membutuhkan baik untuk menjadi efektif maupun untuk memastikan bahwa organisasi TI memberikan dukungan terhadap kebutuhan bisnis [22]. Proses teknologi informasi merupakan salah satu *enablers* yang diaplikasikan dalam melakukan manajemen risiko [23].

2.2.4 Risiko Proses Teknologi Informasi

Proses utama menurut COBIT 5 terdapat pada domain *Deliver Support Systems* (DSS), *Build Acquire Implement* (BAI), *Evaluate, Direct and Monitor* (EDM) serta *Align, Plan and Organise* (APO) [24]. Risiko proses teknologi informasi merupakan gangguan dan ancaman bahaya yang muncul dari serangkaian proses TI yang dimiliki oleh sebuah organisasi. Risiko-risiko teknologi infromasi yang diambil nantinya akan mengacu dari proses manajemen insiden dan pemenuhan permintaan layanan di Subdirektorat layanan DPTSI yang disesuaikan dengan standar.

2.2.5 Manajemen Risiko

Beberapa definisi manajemen risiko menurut para ahli antara lain sebagai berikut:

1. Manajemen risiko didefinisikan sebagai proses identifikasi, pengukuran, dan kontrol keuangan dari sebuah risiko yang mengancam aset dan penghasilan dari sebuah perusahaan atau proyek yang dapat menimbulkan kerusakan atau kerugian pada perusahaan tersebut [25].

2. Manajemen risiko merupakan proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternatif penanganan resiko, dan memonitor dan mengendalikan penanganan risiko [26].
3. Manajemen risiko merupakan proses membangun dan memelihara keamanan sistem informasi di dalam organisasi. Jantung dari manajemen risiko adalah penilaian risiko, dimana risiko dari sistem diidentifikasi dan dievaluasi untuk menyesuaikan kontrol kemanan [27].
4. Manajemen risiko didefinisikan sebagai suatu pendekatan yang komprehensif untuk menangani semua kejadian yang menimbulkan kerugian [28].

Berdasarkan beberapa pengertian para ahli diatas, maka dapat disimpulkan bahwa manajemen risiko merupakan sebuah proses pengelolaan dan kontrol di dalam sebuah organisasi untuk melindungi aset dari ancaman dan kerugian.

2.2.6 Manajemen Risiko Teknologi Informasi

Manajemen risiko memegang peranan penting sebagai tindakan perlindungan dan pengambilan langkah mitigasi bagi aset informasi dan seluruh hal yang berkaitan dengan teknologi informasi yang dapat menghambat proses bisnis. Manajemen risiko teknologi informasi merupakan kemampuan organisasi dalam mengurangi risiko-risiko TI yang mungkin akan menghambat pencapaian tujuan organisasi terkait dengan pemanfaatan TI itu sendiri [29].

Pengertian lain tentang manajemen risiko teknologi informasi menurut *National Institute of Standards and Technology*, manajemen risiko meliputi tiga proses, yaitu *risk assessment, risk mitigation,* dan *evaluation assessment* [6].

1. ***Risk assessment***, proses ini merupakan tahap dimana risiko diidentifikasi dan mencari dampak risiko untuk mencari kontrol mitigasi yang sesuai.
2. ***Risk mitigation***, merupakan proses memprioritaskan tingkat keparahan risiko, mengevaluasi penyebab dan dampak risiko dan mengimplementasikan kontrol yang tepat dalam

mengurangi risiko yang sudah di identifikasi di proses *risk assesment*.

3. ***Evaluation and assessment***, di tahap ini kunci dari proses-proses manajemen risiko dilakukan, dimana risiko yang sudah di evaluasi ditindaklanjuti dengan diberikan panduan *best practice* agar program manajemen risiko yang dilakukan berhasil.

Menurut kerangka kerja COBIT 5 Enabling Processes [24], terdapat empat pilihan strategi penanganan risiko yang dapat dipilih oleh suatu organisasi yaitu sebagai berikut [5]:

1. Menerima risiko (*Acceptance*), apabila risiko yang dihadapi sudah diketahui dan tidak dapat dicegah, sehingga suatu organisasi perlu menerima risiko tersebut, dimana perusahaan memutuskan untuk menerima kerugian, manfaat, atau keuntungan yang mungkin muncul dari risiko yang terjadi. Organisasi menggunakan risiko ini bisa terjadi karena dua hal, yaitu ketika risiko kecil sekali dampaknya atau besar sekali dampaknya. Untuk risiko yang kecil dampaknya, organisasi biasanya akan menggunakan sumber dayanya yang terbatas untuk menyelesaikan risiko lain yang lebih besar dampaknya. Sedangkan risiko yang berdampak besar sekali misalnya terjadinya bencana alam. Hal ini dilakukan karena jika terjadi bencana alam, kerusakan dan kerugian perusahaan sudah tidak dapat dihindarkan, namun organisasi tetap memiliki strategi-strategi tertentu untuk menjaga agar proses bisnis tetap bisa berjalan.
2. Membuat mitigasi risiko (*Mitigation*), apabila risiko yang dihadapi diberi perlakukan khusus dengan menerapkan kontrol yang sesuai atau organisasi dapat memberikan biaya khusus yang efektif (*effective cost*). Organisasi berusaha untuk mengurangi dampak yang mungkin ditimbulkan dan frekuensi kemungkinan terjadinya risiko. Biasanya organisasi menerapkan teknik ini sehingga risiko yang tadinya memiliki dampak yang sangat besar dapat dikurangi dampaknya pada level dimana dapat diterima oleh perusahaan tersebut.

3. Menghindari risiko (*Avoidance*), apabila risiko yang dihadapi terlalu besar sehingga proses dan aktivitas yang berhubungan dengan risiko tersebut perlu diberhentikan apabila dampaknya dinilai tidak lagi relevan dengan organisasi tersebut. Sehingga organisasi lebih memilih untuk tidak melakukan aktivitas tersebut karena dapat menimbulkan risiko yang memiliki dampak yang signifikan.
4. Melakukan transfer risiko (*Transference*), apabila risiko yang dihadapi terlalu sulit untuk ditangani sendiri, sehingga risiko tersebut perlu dialihkan ke pihak ke-tiga. Pengalihan biasanya dapat dilakukan dengan cara kontraktual pada klausa kontraknya dan jaminan atau bank garansi serta dengan asuransi atau organisasi lain yang lebih kompeten dalam penanganan risiko tersebut.

2.2.7 *Helpdesk* DPTSI

Helpdesk atau *Service Desk* merupakan salah satu fungsi umum di lingkup *service* operation secara umum yang dibutuhkan dalam pengelolaaan layanan TI. *Helpdesk* merupakan titik utama bagi pengguna ketika terjadi suatu gangguan layanan, *service request*, atau permintaan perubahan lainnya. *Helpdesk/ Service Desk* menyediakan komunikasi satu titik antara pengguna dan organisasi [2].

Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI memiliki tugas untuk menyediakan layanan TI kepada pengguna. Sebagai salah satu bentuk penyediaan layanan TI, subdirektorat layanan DPTSI memiliki suatu unit fungsional *helpdesk* yang menangani berbagai macam keluhan dan permintaan layanan TI di lingkungan ITS. Permasalahan layanan TI yang ditangani oleh *helpdesk* sebagian besar terkait dengan insiden dan permintaan layanan TI seperti menyelesaikan kesalahan teknis, menjawab pertanyaan, memenuhi permintaan layanan, dan permintaan akses layanan [30].

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 *helpdesk* subdirektorat layanan DPTSI ITS dengan berbagai cara diantaranya melalui telepon, *fax*, *e-mail* atau langsung mengunjungi kantor DPTSI ITS. *Helpdesk* subdirektorat layanan DPTSI ITS mencatat permasalahan layanan TI yang dilaporkan pengguna kemudian mendistribusikannya ke setiap divisi yang sesuai untuk menyelesaikan permasalahan layanan TI [30].

2.2.8 Manajemen Insiden dan Permintaan Layanan TI

Pada dasarnya proses yang dilakukan oleh *helpdesk* antara lain adalah mengelola insiden dan memenuhi permintaan layanan.

2.2.8.1 Manajemen Insiden

Insiden adalah sesuatu yang terjadi diluar rencana berupa gangguan yang mengakibatkan pengurangan kualitas terhadap layanan TI. Tujuan utama dari proses manajemen insiden adalah untuk mengembalikan layanan secepat mungkin dapat agar beroperasi normal seperti biasa dan meminimalisasi dampak yang merugikan operasional bisnis, sehingga memastikan dan mempertahankan ketersediaan layanan dengan kualitas terbaik [31]. Manajemen insiden meliputi setiap peristiwa yang mengganggu atau dapat mengganggu layanan. Hal ini termasuk peristiwa yang disampaikan langsung oleh pengguna, baik melalui *helpdesk*/*service desk* atau melalui antarmuka dari alat bantu manajemen insiden [32]. Sebuah model insiden harus mencakup [33]:

3. Langkah-langkah yang harus diambil untuk menangani insiden
4. Pembagian peran dan tanggung jawab
5. Skala waktu dan ambang batas untuk menyelesaikan tindakan
6. Prosedur eskalasi dan peran eskalasi
7. Bukti aktivitas-aktivitas yang dibutuhkan.

2.2.8.2 Permintaan Layanan TI (*Service Request*)

Proses permintaan layanan mengacu pada tuntutan oleh pengguna. Permintaan tersebut dapat mengenai perubahan kecil, mengubah *password*, meng-*install* aplikasi perangkat

lunak tambahan, meminta informasi, dan sebagainya. Jika insiden adalah peristiwa yang tidak direncanakan, permintaan layanan merupakan peristiwa yang direncanakan. Sebuah organisasi biasanya telah membentuk tim khusus untuk memenuhi permintaan tersebut. Untuk permintaan yang sering berulang, ditetapkan sebuah model yang terancang untuk memenuhi permintaan tersebut [33]. Permintaan layanan pada manajemen layanan TI yang umumnya dilakukan oleh *helpdesk* terdiri dari dua proses, yaitu pemenuhan permintaan (*request fulfillment*) dan manajemen akses (*access management*).

a. Pemenuhan Permintaan Layanan (*Service Request*)

Request fulfillment adalah sebuah proses yang bertanggung jawab untuk mengelola siklus hidup semua permintaan layanan TI [31]. Tujuan dari proses ini antara lain adalah menerima layanan standar bagi pengguna dalam menyampaikan permintaan, menyediakan informasi kepada pengguna dan pelanggan mengenai ketersediaan layanan dan prosedur, menyediakan komponen layanan standar yang diminta, membantu dengan informasi umum, keluhan, atau komentar [31].

b. Manajemen Akses (*Access Management*)

Manajemen akses berkaitan dengan pemberian hak akses ke pihak yang berwenang untuk mencegah penggunaan akses terhadap pihak yang tidak berwenang [34]. Aktivitas proses manajemen akses dimulai dengan permintaan akses oleh pengguna yang dapat disampaikan dalam bentuk sebuah permintaan permintaan layanan melalui sistem pemenuhan permintaan pada *helpdesk* atau *helpdesk* [31]. Tujuan dari manajemen akses adalah menyediakan hak bagi pengguna untuk dapat menggunakan satu atau sejumlah layanan TI [31].

Proses manajemen insiden dan pemenuhan permintaan layanan sering kali tidak berjalan dengan lancar, banyak terdapat kesalahan dan risiko-risiko yang kerap muncul, mulai dari proses pencatatan insiden atau layanan sampai ke proses penutupannya. Untuk itu, perlu dilakukan identifikasi dan

penilaian risiko-risiko tersebut agar bisa diantisipasi untuk menghindari kerugian terhadap dampak bisnis.

2.2.9 Kerangka Kerja Manajemen Insiden

a. ITIL V3

Information Technology Infrastructure Library (ITIL) adalah sebuah kerangka kerja yang terdiri dari kumpulan *best practices* pengelolaan layanan. Ada 5 proses siklus hidup layanan dalam ITIL, yaitu [35] :

1. *Service Strategy*, pada tahap ini dilakukan pengembangan strategi untuk mengubah manajemen service TI menjadi sebuah aset strategis dari organisasi.
2. *Service Design*, pada tahap ini dilakukan pembangunan panduan manajemen layanan TI berdasarkan strategi yang sudah dikembangkan sebelumnya pada tahap *Service Strategy*. Selain itu panduan dibangun berdasarkan kebijakan yang berlaku dalam organisasi dan untuk pemenuhan kepuasan pelanggan.
3. *Service Transition*, pada tahap ini dilakukan proses transisi dari tata kelola yang lama kepada tata kelola yang baru yang sudah dikembangkan dalam tahap *Service Design*.
4. *Service Operation*, pada bagian ini berisi langkah-langkah best practice untuk melakukan manajemen layanan TI.
5. *Continual Service Improvement*, pada bagian ini dilakukan pengelolaan masukan dari pelanggan yang kemudian dikolaborasikan kedalam empat tahap diatas. Hal ini bertujuan untuk meningkatkan hasil keluaran dari kegiatan *Service Strategy*, *Service Design*, *Service Transition*, dan *Service Operation*.

Menurut ITIL, pengertian insiden adalah sebuah interupsi atau pengurangan kualitas dari layanan TI. Selain itu sebuah kesalahan konfigurasi pada sistem dapat dikatakan

sebagai insiden walaupun belum menimbulkan masalah yang berarti pada sistem tersebut [35]. Manajemen insiden pada kerangka kerja ITIL v3 berada pada siklus *Service Operation*. Berikut adalah aktivitas-aktifitas dalam manajemen insiden berdasarkan kerangka kerja ITIL V3 [2]:

1. Identifikasi insiden (*incident identification*)
2. Pencatatan insiden (*incident logging*)
3. Pengkategorisasian insiden (*incident categorization*)
4. Prioritas insiden *(incident priorization*)
5. Diagnosa awal insiden (*initial diagnosis*)
6. Eskalasi insiden (*incident escalation*)
7. Investigasi dan diagnosis indsiden (*investigation and diagnosis*)
8. Resolusi insiden (*resolution and recovery*)
9. Penutupan insiden (*incident closure*)

b. COBIT 5

Manajemen insiden pada COBIT 5 dibahas pada domain *Deliver, Service, and Support* (DSS) yang ke dua yaitu *Manage Service Request and Incident*. Dalam domain DSS02 tersebut didefinisikan beberapa proses atau *key management practices* yang terdiri dari berbagai macam aktivitas didalamnya. DSS02 sendiri menyediakan standarisasi respon yang tefektif dan efisien untuk pengelolaan permintaan dari pengguna dan memberikan resolusi untuk semu jenis insiden. [11] DSS02 menyediakan upaya mengembalikan layanan pada kondisi normal, mencatat dan memenuhi kebutuhan user, dan melakukan investigasi, diagnosa, eskalasi, dan penanganan insiden [24].

Kerangka kerja ini dipilih karena COBIT 5 merupakan sebuah best practice yang dibuat untuk melakukan manajemen dan tata kelola perusahaan TI yang memiliki bahasa high *level objective* yang dapat mendefinisikan proses-proses TI yang tidak terdapat pada ITIL [24]. Selain

itu, ITIL lebih detail dalam menjabarkan proses terkait manajemen layanan, sedangkan COBIT 5 merangkum proses-proses besar yang ada. Karena fokus penelitian ini tidak pada manajemen layanan, COBIT 5 dirasa cukup sesuai karena domain DSS02 *Manage Service Requests and Incidents* yang dipaakai saling berhubungan nantinya dengan proses pengelolaan risiko yang juga memakai domain COBIT 5 APO12 *Manage Risks*.

2.2.10 Kerangka Kerja Manajemen Risiko

Keberhasilan manajemen risiko tergantung pada efektivitas kerangka manajemen yang menyediakan landasan yang akan ditanamkan pada sebuah organisasi. Kerangka kerja membantu dalam mengelola 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 [7].

Untuk dapat melakukan manajemen 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.

2.2.10.1 Kerangka Kerja Manajemen Risiko Umum

Berikut merupakan kerangka kerja manajemen risko yang umum yang digunakan dalam berbagai bidang:

a. ISO/IEC 31000

The International Organization for Standardization (ISO) 31000:2009 merupakan sebuah standar internasional tentang manajemen risiko yang disusun dengan tujuan memberikan prinsip dan panduan generik untuk penerapan manajemen risiko. ISO 31000: 2009 menyediakan prinsip, kerangka kerja, dan proses manajemen risiko yang dapat

digunakan sebagai arsitektur manajemen risiko dalam usaha menjamin penerapan manajemen risiko yang efektif [36]. Proses-proses manajemen risiko menurut ISO/IEC 31000 [37] adalah:

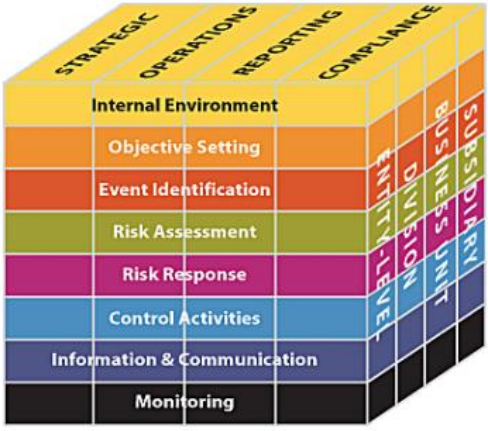
1. *Establishing the Context*
   Dalam proses ini ditetapkan beberapa konteks untuk melakukan *risk assesment*, antara lain konteks internal organisasi, konteks eksternal yang mempengaruhi organisasi tersebut, konteks manajemen risiko yang memfokuskan pada penangan risiko yang diidentifikasi, dan kriteria risiko sebagai parameter yang disepakati oleh suatu organisasi.
2. *Risk Identification*
   Merupakan sebuah proses detail dimana mengidentifikasi risiko-risiko yang terdapat di sekitar lingkungan suatu organisasi, mulai dari kategori risiko, penyebab risiko, tingkat keparahan risiko probabilitas terjadinya risiko hingga dampak yang disebabkan oleh risiko-risiko tersebut.
3. *Risk Analysis*
   Merupakan sebuah proses menganalisis lebih lanjut penyebab, dampak dan konsekuensi yang ditimbulkan oleh risiko yang telah diidentifikasi.
4. *Risk Evaluation*
   Merupakan proses membandingkan hasil analisis risiko dengan kriteria risiko untuk menentukan bagaimana penanganan risiko yang akan diterapkan [36].
5. *Risk Treatment*
   Proses ini merupakan strategi untuk melakukan mitigasi risiko yang terbagi menjadi beberapa pilihan, yaitu:
   - Menghindari risiko (*risk avoidance*)
   - Mitigasi risiko (*risk reduction*)
   - Transfer risiko kepada pihak ketiga (*risk sharing*)
   - Menerima risiko (*risk acceptance*).

ISO/IEC 31000 menimplementasikan prinsip "*Plan*, *Do*, *Check*, *Act*", yaitu dengan melakukan:

(1) Perencanaan kerangka kerja manajemen risiko;
(2) Penerapan manajemen risiko;
(3) Monitoring dan *review* terhadap kerangka kerja manajemen risiko;
(4) Perbaikan kerangka kerja manajemen risiko secara berkelanjutan.

b. ERM COSO

Pada tahun 2004, COSO (*Committee of Sponsoring Organization of the Treadway Commission)* menerbitkan *Enterprise Risk Management Integrated Framework* yang menggambarkan komponen-komponen penting, prinsip dan konsep dari manajemen risiko perusahaan untuk seluruh organisasi, tanpa memandang ukurannya [38]. COSO ERM Framework terdiri dari delapan komponen yang harus ada dan berjalan agar dapat dikatakan sebagai ERM efektif yang dapat dilihat pada Gambar 2.1 berikut.



Gambar 2.1 Kerangka Kerja ERM COSO [38]

2.2.10.2 Kerangka Kerja Manajemen Risiko Teknologi Informasi

Berikut merupakan kerangka kerja manajemen risiko yang berkaitan dengan risiko teknologi informasi.

b. ISO/IEC 27001&2

ISO 27001 adalah suatu standar tersertifikasi untuk *Information Security Management System* (ISMS) atau Sistem Manajemen Kemanan Informasi (SMKI). ISO 27001 menyediakan kerangka kerja yang memungkinkan suatu organisasi memastikan bahwa pengukuran keamanan informasi berjalan dengan efektif dan merekomendasikan suatu rangkaian pengendalian keamanan spesifik [39]. Standard ini mencakup seluruh elemen dalam sebuah organisasi untuk mengawasi dan mengendalikan integritas keamanan informasi, meminimalkan risiko dan memastikan kesesuaian terhadap standar dan hukum. ISO 27001 mengadopsi prinsip PDCA (*Plan-Do-Check-Act*) sebagai basis dalam pelaksanaan ISMS. Pemaparan ISO/IEC 27001 [39] mencakup bagian:

- *Context of the organization*
- *Leadership*
- *Planning*
- *Support*
- *Operation*
- *Performance evaluation*
- *Improvement*
- *Annex: A Reference control objectives and control*

Sedangkan ISO/IEC 27002 melengkapi konteks dari ISO/IEC 27001. Standar ini sebagai dasar dan *best practice* dalam mengembangkan standar kemanan organisasi dan praktik dari manajemen keamanan yang efektif. Tujuan dari ISO 27002 ini yaitu untuk mengidentifikasi penilaian risiko dan menunjukkan kontrol keamanan informasi yang sesuai. ISO 27002 menetapkan 35 objektif *control* dan lebih dari

114 *control* untuk melindungi kerahasiaan, integritas dan ketersediaan informasi. *Control objective* yang diberikan berada pada tingkat yang cukup tinggi dan pada dasarnya meliputi spesifikasi persyaratan fungsional umum untuk arsitektur manajemen keamanan informasi organisasi [40].

c. OCTAVE

OCTAVE (*The Operationally Critical Threat, Asset, and Vulnerability Evaluation*) digunakan seabgai metode yang digunakan untuk mengidentifikasi dan mengevaluasi information security risk. OCTAVE berfokus pada aset dari teknologi informasi yang dimiliki organisasi dalam melakukan manajemen risiko [41]. Pendekatan OCTAVE menggunakan tiga tahapan, yaitu membangun proses profil ancaman berdasarkan aset yang ada (*Build Asset-Based Threat Profiles*), melakukan identifikasi kerentanan dari infrasruktur (*Develop Security Strategy and Plans*), dan mengembangkan rencana dan strategi keamanan (*Develop Security Strategy and Plans*).

d. COBIT 5 *for Risk*

COBIT 5 *for Risk* adalah panduan komprehensif yang dibuat secara khusus untuk mengelola risiko TI di dalam organisasi. Kerangka kerja ini dipilih karena risiko yang diidentifikasi berdasarkan proses TI yang terjadi. COBIT 5 *for Risk* berisi panduan detail untuk organisasi dalam mengantisipasi dampak kerugian bisnis dengan mempertimbangkan banyak faktor dan aspek-aspek.

2.2.11 COBIT 5 *Enabling Processes*

COBIT merupakan kerangka kerja terkait tata kelola dan manajemen teknologi informasi. COBIT dikembangkan oleh *Information Technology Governance Institute* (ITGI) yang merupakan bagian dari *Information Systems Audit and Control Association* (ISACA). COBIT merupakan sekumpulan

dokumentasi dan panduan untuk membantu auditor, manajer, dan pengguna untuk menjembatani pemisah (*gap*) antara risiko bisnis, kebutuhan proses, dan permasalahan-permasalahan teknis agar bisa memenuhi kebutuhan *stakeholder* akan teknologi dan informasi [42].
COBIT mengalami beberapa evolusi yang cukup panjang demi menjadi kerangka kerja yang semakin baik agar bisa [43] digunakan dalam menerapkan *Governance of Enterprise IT*. Sampai saat ini, rilisan terbaru dari COBIT adalah COBIT 5. Implementasi teknologi informasi dalam sebuah organisasi membutuhkan kerangka kerja yang sesuai, COBIT dapat membantu memenuhi kebutuhan bisnis, mengorganisasi aktivitas teknologi informasi ke dalam proses model yang dapat diterima secara umum, mengidentifikasi sumber teknologi informasi utama, mendefinisikan sasaran proses TI manajemen yang harus dipertimbangkan.

2.2.12 COBIT 5 *for Risk*

Perspektif manajemen risiko mengacu pada bagaimana cara pengelolaan dan penanganan risiko. COBIT 5 *for Risk* memiliki perspektif manajemen risiko yang terkait cara melakukan proses identifikasi, analisis, dan cara untuk merespon risiko. Perspektif ini membutuhkan *core risk processes* untuk diimplementasikan, yaitu APO12 (*Manage Risk*). Berikut gambaran singkat dari kedua *control objectives* tersebut yang disajikan pada Tabel 2.3.

Tabel 2.3 Perspektif Manajemen Risiko berdasarkan COBIT 5 for Risk [23]

Core Risk Processes	**Justifikasi**
EDM03 ***Ensure Risk Optimisation***	Proses ini meliputi pemahaman, artikulasi, dan komunikasi dari risiko perusahaan dan toleransinya serta pemastian kembali identifikasi dan manajemen risiko untuk nilai perusahaan yang berkaitan dengan penggunaan TI beserta dampaknya. Tujuan dari proses ini adalah:

Core Risk Processes	**Justifikasi**
	• Mendefinisikan dan mengkomunikasikan *thresholds* risiko dan memastikan bahwa risiko yang terkait TI telah diketahui; • Mengelola risiko terkait TI yang kritis dengan efektif dan efisien; • Memastikan risiko terkait TI perusahaan tidak melebihi batasan.
APO12 ***Manage Risk***	Proses ini meliputi identifikasi lanjutan, penilaian dan pengurangan risiko terkait TI dalam tingkat toleransi yang diatur oleh manajemen eksekutif perusahaan. Manajemen risiko terkait TI perusahan harus diintegrasikan dengan seluruh ERM. Biaya dan manfaat terkait pengelolaan risiko harus diseimbangkan dengan cara: • Mengumpulkan data terkait analisis risiko; • Memelihara profil risiko perusahaan dan melakukan artikulasi risiko; • Mendefinisikan tindakan portfolio manajemen risiko dan melakukan respon terhadap risiko.

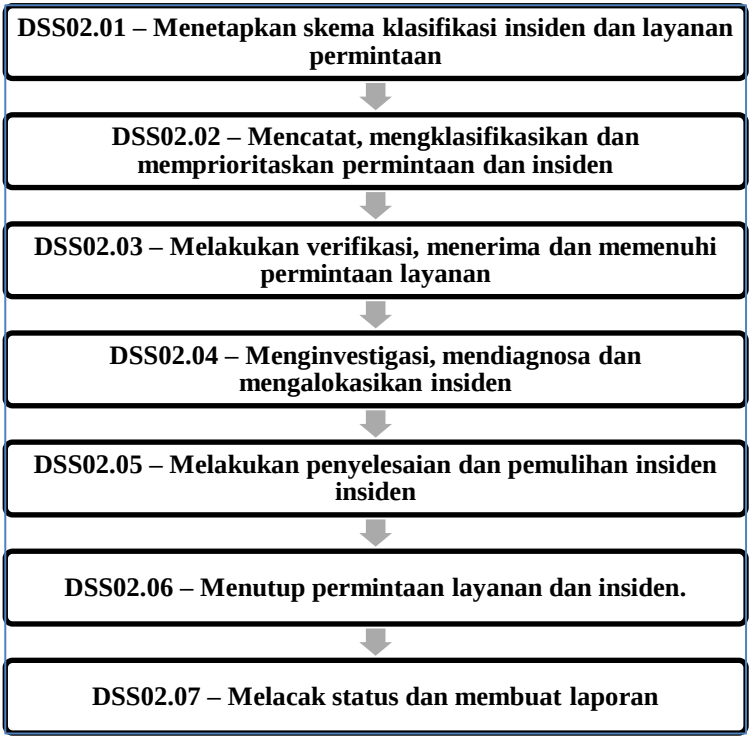
2.2.13 Domain Kerangka Kerja COBIT 5

Kerangka kerja COBIT 5 terdiri dari 5 domain yang dibagi kedalam 37 proses. Masing-masing domain berorientasi pada proses TI, kelima domain tersebut yaitu *Deliver Service and Support* (DSS), *Align Plan and Organise* (APO), *Evaluate Direct and Monitor* (EDM), *Build Acquire and Implement* (BAI) dan *Monitor Evaluate and Assess* (MEA). Proses TI dalam COBIT 5 dibagi kedalam dua area utama yaitu *management* dan *governance*. Area utama tersebut ditentukan berdasarkan aktivitas proses yang ada didalamnya atau dalam COBIT 5 disebut *Key Management Practice*. Domain yang termasuk dalam area *management* adalah *Evaluate Direct and Monitor* (EDM), sedangkan pada area *governance* domain yang termasuk didalamnya adalah *Deliver Service and Support*

(DSS), *Align Plan and Organise* (APO), *Evaluate Direct and Monitor* (EDM) serta *Build Acquire and Implement* (BAI).
Pada penelitian ini, dua proses TI utama yang menjadi acuan pada penelitian ini ialah pada domain DSS yaitu proses DSS02 – *Manage Service Requests and Incidents* terkait identifikasi dan manajemen insiden dan permintaan layanan serta *domain* APO yaitu pada proses APO12 – *Manage Risks* yang digunakan sebagai metodologi penelitian dalam mengidentifikasi dan menilai risiko berdasarkan aktivitas yang ada dalam proses DSS02.

2.2.14 DSS02 – Manage Service Requests and Incidents

Manajemen Insiden dan permintaan layanan terdiri serangkaian proses runtut yang harus diikuti agar insiden dan permintaan dapat diselesaikan dengan baik, proses dan aktivitas tersebut menurut kerangka kerja COBIT 5 Enabling Processeses yaitu DSS02 *Manage Service Request and Incidents* yang terbagi menjadi 7 sub proses disajikan dalam Bagan 2.1 [24].



Bagan 2.1 Proses DSS02 - *Manage Service Request and Incidents*

2.2.14.1 DSS02.01 – Menetapkan Skema Klasifikasi Insiden

Proses ini mendefinisikan klasifikasi skema dan model dari insiden dan permintaan layanan. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Menetapkan dan mendefinisikan klasifikasi permintaan layanan dan skema prioritisasi beserta kriteria untuk pendaftaran masalah, untuk memastikan pendekatan yang konsisten dalam menangani, menginformasikan pengguna dan melakukan analisis tren.
2. Mendefinisikan bentuk insiden untuk mengetahui kesalahan untuk membuat resolusi yang efisien dan efektif.
3. Mendefinisikan model permintaan layanan berdasarkan tipe permintaan layanan untuk memungkinkan dilakukan

secara mandiri dan layanan yang efisien untuk permintaan yang standar.
4. Mendefinisikan peraturan dan prosedur eskalasi insiden, terutama untuk insiden utama dan insiden keamanan.
5. Mendefinisikan pengetahuan permintaan layanan dan kegunaannya.

2.2.14.2 DSS02.02 – Mencatat, Mengklasifikasikan dan Memprioritaskan permintaan dan insiden

Proses ini meliputi identifikasi, perekaman atau pencatatan, pengklasifikasian permintaan layanan dan insiden dan menetapkan prioritas sesuai dengan tingkat kritis bisnis dan *service agreements*. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Menetapkan dan mendefinisikan klasifikasi permintaan layanan dan skema prioritisasi beserta kriteria untuk pendaftaran masalah, melakukan pencatatan semua permintaan dan insiden serta semua informasi yang terkait, sehingga bisa di tangani secara efektif dan laporan tersebut bisa dipelihara.
2. Untuk memungkinkan analisis tren, diperlukan klasifikasi permintaan layanan dengan melakukan identifikasi tipe dan kategori dari permintaan tersebut.
3. Melakukan prioritisasi permintaan layanan berdasarkan definisi layanan dari SLA terhadap proses bisnis perusahaan dan tingkat urgensi.

2.2.14.3 DSS02.03 – Melakukan Verifikasi, Menerima dan Memenuhi Permintaan Layanan

Dalam proses ini, organisasi harus memilih prosedur permintaan yang sesuai dan memverifikasikannya dengan permintaan layanan yang sudah disesuaikan dengan kriteria permintaan. Proses ini memerlukan persetujuan finansial jika dibutuhkan dan memenuhi permintaan sesuai dengan prosedur. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Melakukan verifikasi terhadap hak untuk menggunakan permintaan layanan, jika dimungkinkan, alur proses yang telah didefinisikan dan perubahan standar.

2. Memperoleh persetujuan finansial dan fungsonal atau tanda tangan, jika dibutuhkan, atau persetujuan otomatis untuk persetujuan dalam perubahan yang standar.
3. Melakukan pemenuhan 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.

2.2.14.4 DSS02.04 – Menginvestigasi, Mendiagnosa dan Mengalokasikan Insiden

Proses ini meliputi identifikasi dan perekaman atau pencatatan gejala-gejala insiden, menentukan penyebab-penyebab yang memungkinkan dan mengalokasikan solusi. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Mengidentifikasikan dan mendeksripsikan gejala yang relevan untuk mendirikan penyebab yang paling tepat dari insiden tersebut.
2. Jika insiden tersebut tidak tersedia, buat sebuah log baru.
3. Menetapkan insiden ke fungsi spesialis.

2.2.14.5 DSS02.05 – Melakukan Penyelesaian dan Pemulihan Insiden

Proses ini meliputi pendokumentasian, pengaplikasian dan melakukan uji coba solusi-solusi yang sudah diidentifikasi atau *workarounds* dan melakukan aksi pemulihan untuk mengembalikan *IT-related service*. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Memilih dan menggunakan resolusi insiden yang tepat (*temporary workaround* dan/atau solusi tetap).
2. Merekam *workaround* mana yang digunakan untuk melakukan resolusi insiden.
3. Melakukan aksi pemulihan (jika dibutuhkan).
4. Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat dipakai sebagai sumber pengetahuan mendatang.

2.2.14.6 DSS02.06 – Menutup Permintaan Layanan dan Insiden

Proses ini meliputi verifikasi terhadap kepuasan pengguna terhadap solusi insiden dan/atau pemenuhan permintaan, dan melakukan penutupan. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Melakukan verifikasi dengan pengguna yang berpengaruh (apabila setuju) bahwa layanan permintaan mereka telah dipenuhi dan diselesaikan dengan baik.
2. Menutup layanan permintaan dan insiden

2.2.14.7 DSS02.07 – Melacak Status dan Membuat Laporan

Proses ini meliputi pelacakan sekala berkala, analisis dan melaporkan insiden serta pemenuhan tren permintaan untuk menyediakan untuk peningkatan layanan di masa mendatang. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Mengawasi dan melacak eskalasi insiden dan resolusi dan penanganan permintaan untuk melakukan progress penyelesaian.
2. Mengidentifikasi informasi stakeholder dan kebutuhan mereka untuk pemenuhan data dan laporan. Idenfitikasi laporan secara berkala.
3. Menganalisis insiden dan layanan permintaan dengan mengkategorisasikan tren.
4. Membuat dan mendistribusikan laporan berkala atau menyediakan *controlled access* ke *online data*.

2.2.15 APO12 - *Manage Risk*

APO12 *Manage Risk* membantu pengelolaan risiko dan pembuatan mitigasi risiko proses TI karena proses didalamnya sangat kompleks Proses ini meliputi indetifikasi secara keberlanjutan, penilaian dan pengurangan risiko terkait TI dalam tingkatan toleransi yang telah ditetapkan manajemen eksekutif organisasi [24]. Berikut enam sub proses yang ada pada APO12 *Manage Risk Optimization* yang digambarkan pada Bagan 2.2.

Bagan 2.2 Proses APO12 - Manage Risk

2.2.15.1 APO12.01 - Mengumpulkan Data

Proses ini meliputi identifikasi dan pengumpulan data-data relevan untuk secara efektif mendapatkan identifikasi risiko terkait TI, proses analisis dan pembuatan laporan. Aktivitas-aktivitas dalam proses ini [24]:

1. Membangun dan mempertahankan metode untuk pengumpulan, klasifikasi dan analisis data terkait risiko TI, mengakomodasi beberapa jenis kejadian, beberapa kategori risiko TI dan beberapa faktor risiko.
2. Menyimpan data yang relevan pada lingkungan operasional internal dan eksternal perusahaan yang dapat melakukan peran penting dalam pengelolaan risiko TI.

3. 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 agreemen*t) untuk pengungkapan peristiwa yang umum.
4. Menyimpan data pada *risk event* yang disebabkan atau dapat menyebabkan dampak terhadap manfaat TI/ nilai pemberdayaan, program dan proyek TI, dan/atau operasi TI dan layanan TI. Mengambil data yang relevan dari isu-isu terkait, insiden, masalah dan investigasi.
5. Untuk kelas dari *event* sejenis, organisir data yang sudah dikumpulkan dan beri *highlight* terhadap *contributing factors*. Tentukan *contributing factors* secara umum melalui *multiple events*.
6. Tentukan kondisi spesifik yang tersedia atau tidak ada saat terjadi risiko, serta kondisi dari pengaruh frekuensi kejadian dan *loss magnitude*.
7. Lakukan *periodic event* dan analisis faktor risiko untuk mengidentifikasi isu-isu risiko yang muncul, serta pahami hubungan antara faktor risiko internal dan eksternal.

2.2.15.2 APO12.02 - Menganalisis Risiko

Proses ini meliputi pengembangan informasi yang berguna untuk mendukung pengambilan keputusan risiko ke dalam faktor risiko bisnis yang relevan. ktivitas-aktivitas dalam proses ini adalah [24]:

1. Menentukan luas dan kedalaman yang sesuai dari upaya analisis risiko, mempertimbangkan semua faktor risiko dan aset bisnis yang kritis, mengatur analisis ruang lingkup risiko setelah melakukan analisis *cost-benefit*.
2. Membangun dan secara teratur memperbarui skenario risiko TI, termasuk skenario *cascading* dan/atau jenis ancaman yang muncul secara kebetulan, serta mengembangkan ekspektasi untuk kegiatan kontrol

tertentu, kemampuan untuk mendeteksi, dan tindakan respon lainnya.

3. Memperkirakan frekuensi dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko TI. Memperhitungkan semua faktor risiko yang berlaku, mengevaluasi kontrol operasional yang sudah diketahui dan mengestimasi tingkat risiko residual.
4. Membandingkan risiko residual toleransi risiko yang dapat diterima dan mengidentifikasi *exposure* yang mungkin memerlukan respon risiko.
5. Menganalisis cost-benefit dari respon risiko yang potensial seperti *avoid, reduce/Mitigate (Treat), transfer/share*, dan *accept*/*take* serta *exploite/seize*. Tentukan respon risiko mana yang sesuai.
6. Menspesifikasikan *high-level requirements* untuk program atau proyek yang akan diimplementasikan terhadap respon risiko yang dipilih. Identifikasikan kebutuhan dan ekspektasi tehadap *key controls* yang sesuai untuk tindakan mitigasi risiko.
7. Memvalidasi analisis risiko sebelum mengambil keputusan, mengkonfirmasi bahwa analisis sejalan dengan kebutuhan perusahaan, serta memverifikasi estimasi telah diperiksa dan dikalibrasi.

2.2.15.3 APO12.03 - Memelihara Profill Risiko

Proses ini meliputi pemeliharaan sebuah penyimpanan risiko yang diketahui dan atribut-atributnya, seperti ekspektasi frekuensi, dampak yang potensial dan respon dari sumber daya terkait, serta kapabilitas dan kontrol-kontrol yang sedang diterapkan. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Proses bisnis *inventory*, termasuk personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual yang kritis, vendor, pemasok dan agen *outsourcing*, dan mendokumentasikan ketergantungan pada proses manajemen layanan TI dan sumber daya infrastruktur TI.
2. Menentukan dan menyepakati mana layanan TI dan sumber daya infrastruktur TI yang sangat penting untuk

mempertahankan proses bisnis operasional. Menganalisa dependensi dan mengidentifikasi kelemahan.
3. Melakukan agregasi skenario risiko saat berdasarkan kategori, lini bisnis dan area fungsional.
4. Secara teratur, mengumpulkan semua informasi profil risiko dan mengkonsolidasikan ke profil risiko agregat.
5. Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan untuk identifikasi cepat, serta memantau tren risiko dan risiko saat ini.
6. Mengumpulkan informasi tentang peristiwa risiko TI yang telah terwujud untuk dimasukkan ke dalam profil risiko TI dari perusahaan.
7. Mengumpulkan informasi dari status rencana tindakan risiko untuk dimasukkan ke dalam profil risiko TI dari perusahaan.

2.2.15.4 APO12.04 - Mengartikulasi Risiko

Proses ini menyediakan informasi dari kondisi terkini terkait TI dan peluang pada waktu yang tepat sesuai kebutuhan *stakeholder* untuk membuat respon yang tepat. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Melaporkan hasil analisis risiko kepada semua stakeholder yang terkena dampak dalam dalam format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, termasuk probabilitas dan rentang kerugian atau keuntungan bersama dengan tingkat kepercayaan yang memungkinkan manajemen untuk menyeimbangkan risk-return.
2. Menyediakan pembuatan keputusan dengan pemahaman tentang skenario *worst-case* dan *most-probable*, dikarenakan *diligence exposures*, dan reputasi yang signifikan, hukum atau pertimbangan peraturan yang berlaku.
3. Melaporkan profil risiko saat ini untuk semua *stakeholder*, termasuk efektivitas dari proses manajemen risiko, mengontrol efektivitas, kesenjangan,

ketidakkonsistensian, redudansi, status perbaikan, dan dampaknya terhadap profil risiko.

4. Mengkaji ulang hasil penilaian obyektif pihak ketiga, audit internal, dan ulasan jaminan kualitas dan peta mereka dengan profil risiko. Hasil kaji ulang kesenjangan diidentifikasi dan *exposure* untuk menentukan kebutuhan untuk analisis risiko tambahan.
5. Secara periodik, untuk area dengan risiko relatif dan kapasitas risiko paritas, identifikasi peluang terkait TI yang akan memungkinkan penerimaan risiko yang lebih besar dan meningkatkan *growth and return*.

2.2.15.5 APO12.05 - Menentukan Portofolio Aksi Manajemen Risiko

Proses ini meliputi pengelolaan peluang dalam mengurangi terjadinya risiko ke tingkat yang dapat diterima sebagai portofolio. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Memelihara penyimpanan kontrol-kontrol pada tempatnya untuk mengelola risiko dan risiko yang memungkinkan yang harus diambil sesuai dengan *risk appetite* dan toleransinya.
2. Menentukan apakah setiap entitas organisasi memantau risiko dan menerima pertanggungjawaban untuk beroperasi dalam tingkat toleransi individu dan portofolio.
3. Menentukan satu set proposal proyek yang seimbang dimana dirancang untuk mengurangi risiko dan/atau proyek-proyek yang memungkinkan peluang usaha strategis, mengingat *cost/benefit*, dampak pada profil risiko saat ini dan peraturan yang berlaku.

2.2.15.6 APO12.06 - Melakukan Respon terhadap Risiko

Proses ini meliputi respon secara berkala dengan pengukuran yang efektif terhadap batas kerugian dari peristiwa yang melibatkan TI. Aktivitas-aktivitas dalam proses ini adalah [24]:

1. Siapkan, pelihara dan rencanakan tes yang mendokumentasikan langkah-langkah spesifik yang harus diambil saat terjadi risiko dapat menyebabkan dampak

operasional yang signifikan atau terjadi insiden dengan dampak bisnis yang serius, termasuk jalur eskalasi di seluruh perusahaan.

2. Kategorisasikan insiden, kemudian bandingkan eksposur yang sebenarnya terhadap batas toleransi risiko. Komunikasikan dampak bisnis kepada para pembuat keputusan sebagai bagian dari pembuatan laporan, kemudian perbarui profil risiko.
3. Menerapkan rencana respon yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.
4. Periksa kejadian di masa lalu yang merugikan dan membuat hilangnya peluang, kemudian tentukan penyebabnya. Komunikasikan penyebab tersebut, kebutuhan respon risiko tambahannya, serta proses perbaikan risiko terhadap pengambilan keputusan untuk memastikan penyebab. Respon kebutuhan dan proses perbaikan sudah termasuk dalam proses tata kelola risiko.

2.2.16 Metode Penilaian Risiko Berdasarkan COBIT5 *for Risk*

Untuk melakukan penilaian risiko berdasarkan kerangka kerja COBIT 5 *for risk*, perlu dilakukan identifikasi terkait informasi risiko yang harus ditentukan seperti tipe risiko, kategori risiko, faktor risiko, skenario risiko, kontrol risiko, proses COBIT 5 yang terkait, serta frekuensi dan dampak (*magnitude*) dari masing-masing risiko.

2.2.16.1 Tipe Risiko

Risiko yang sudah diidentifikasi dapat dikategorisasikan berdasarkan tipe dari risiko tersebut.

Tipe risiko dibagi menjadi tiga kategori, yaitu sebagai berikut [23]:

a. *IT benefit / value enablement risk*, dimana risiko yang diidentifikasi masuk ke dalam kategori manfaat atau nilai risiko TI, yaitu apabila risiko terkait dengan (kehilangan) kesempatan untuk meanfaatkan TI dalam meningkatkan efisiensi atau efektivitas proses bisnis atau sebagai *enabler*

untuk inisiatif bisnis baru. Contohnya adalah teknologi yang digunakan dalam inisiatif bisnis baru dan teknologi yang digunakan untuk mengefisiensikan proses operasional.

b. *IT programme and project delivery risk*, dimana risiko yang diidentifikasi masuk ke dalam kategori program dan proyek risiko TI, yaitu apabila risiko terkait dengan kontribusi TI untuk membuatkan atau meningkatkan solusi bisnis, biasanya dalam bentuk proyek dan program. Contohnya adalah kualitas proyek, relevansi proyek dan kelebihan waktu proyek dari yang ditentukan.
c. *IT operations and service delivery risk*, dimana risiko yang diidentifikasi masuk ke dalam kategori operasional dan layanan risiko TI, yaitu apabila risiko terkait dengan stabilitas operasional, ketersediaan, perlindungan dan pemulihan layanan TI, dimana risiko dapat membawa kerugian atau pengurangan nilai perusahaan. Contohnya adalah gangguan pada layanan TI, masalah keamanan dan isu-isu terkait.

Kemudian untuk memudahkan pembagian tingkat kiritikalisasi risiko, tipe risiko dikategorisasikan dalam dua hal yaitu [23]:

a. Primer atau biasa dilambangkan dengan huruf ‘P’ untuk tipe skenario risiko yang menunjukkan primer atau menunjukkan tingkat yang lebih tinggi.
b. Sekunder atau biasa dilambangkan dengan huruf ‘S’ untuk tipe skenario risiko menunjukkan sekunder atau menunjukkan tipe yang lebih rendah.

2.2.16.2 Kategori Risiko

Mengacu kepada standar COBIT 5 *for Risks*, terdapat dua puluh kategori risiko TI untuk setiap risiko yang diidentifikasi, berikut merupakan pembagian dua puluh kategori risiko tersebut yang disajikan pada Tabel 2.4 [23].

Tabel 2.4 Pembagian Kategori Risiko [23]

No.	Kategori	Pengertian
1.	*Portfolio establishment and maintenance*	Pengadaan dan pemeliharaan portofolio
2.	*Programme/ projects life cycle management*	Manajemen siklus hidup program atau proyek

No.	Kategori	Pengertian
	(programme/ project initiation, economics, delivery, quality and termination)	(inisiasi program/proyek, biaya, *delivery*, kualitas dan penutupan proyek)
3.	*IT investment decision making*	Investasi pengambilan keputusan TI
4.	*IT expertise and skills*	Ketrampilan dan kemampuan TI
5.	*Staff operations (human error and malicious intent)*	Staff operasional (kesalahan dan niat buruk manusia)
6.	*Information (data breach: damage, leakage and access)*	Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses)
7.	*Architectural (vision and design)*	Arsitektur (visi dan desain)
8.	*Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)*	Infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan)
9.	*Software*	Perangkat lunak
10.	*Business ownership of IT*	Kepemilikan bisnis TI
11.	*Supplier selection/performanse, contractual compliance, termination of service and transfer*	Pemilihan kinerja pemasok, penyesuaian kontrak, pemberhentian layanan dan pengalihan
12.	*Regulatory compliance*	Pemenuhan regulasi
13.	*Geopolitical*	Geopolitik
14.	*Insfrastructure theft or destruction*	Pencurian infrastruktur atau pengrusakan
15.	*MalwaSre*	Virus
16.	*Logical attacks*	Penyerangan logikal
17.	*Industrial action*	Aksi industri
18.	*Environmental*	Lingkungan sekitar
19.	*Acts of Nature*	Bencana alam

No.	Kategori	Pengertian
20.	*Innovation*	Inovasi

2.2.16.3 Faktor Risiko

Faktor risiko adalah kondisi yang mempengaruhi frekuensi dan/atau dampak bisnis dari skenario risiko. Faktor risiko dapat dapat diklasifikasikan ke dalam dua kategori utama, yaitu [23]:

- **Faktor Kontekstual**, dimana faktor ini dapat dibagi menjadi dua kategori yaitu faktor internal dan faktor eskternal, perbedannya ialah pada tingkat kontrol perusahaan dalam menangani risiko tersebut. Berikut merupakan penjelasan ke-dua faktor tersebut.
  a. ***Internal Contextual Factors***, dimana faktor ini diberlakukan untuk risiko yang berada dibawah kendali perusahaan, meskipun organisasi tidak selalu mudah untuk berubah. Untuk faktor internal, meliputi beberapa pilihan aspek berikut yang disajikan dalam Tabel 2.5 berikut.

Tabel 2.5 Aspek Internal Contextual Factors [23]

Aspek *Internal Contextual Factors*	Deskripsi
Enterprise goals and objectives (Tujuan perusahaan)	Apakah kebutuhan stakeholders dan bagaimana hal ini dapat dipengaruhi oleh risiko?
Strategic importance of IT in the enterprise (Kepentingan Strategis TI dalam Perusahaan)	Apakah TI adalah sebuah pembeda strategis, *enabler* fungsional, atau mendukung fungsi?
Complexity of IT (Kompleksitas TI)	Apakah TI memiliki kompleksitas yang tinggi (contoh: arsitektur kompleks, *merger* baru) ataukah TI yang sederhana, terstandarisasi dan efisien?
Complexity of the enterprise (Kompleksitas Perusahaan)	(termasuk dalam penyebaran geografis dan meliputi nilai rantai. Contohnya dalam

Aspek *Internal Contextual Factors*	**Deskripsi**
	lingkungan manufaktur) apakah sebuah perusahaan manfaktur dan distribusi bagian, dan/atau juga melakukan aktivitas peraktitan?
Degree of change (Tingkat Perubahan)	Tingkat perubahan yang dialami perusahaan.
Change management capability (Kapabilitas Manajemen Perubahan)	Tingkat sejauh mana perusahaan mampu menangani perubahan organisasi.
The risk management philosopy (Filosofi Manajemen Risiko)	Filosofi risiko apakah yang diterapkan perusahaan (contoh pengambilan risiko atau penolakan risiko) dan apa hubungannya dengan nilai perusahaan?
Operating model (Model Pengoperasian)	Tingkat sejauh mana perusahaan beroperasi secara independen atau terhubung dengan klien/ pemasok, serta tingkat sentralisasi / desentralisasi.
Startegic priorities (Prioritas Strategis)	Prioritas strategis dari perusahaan?
Culture of the enterprise (Budaya Perusahaan)	Apakah budaya eksisting perusahaan membutuhkan perubahan untuk dapat secara efektif mencakup manajemen risiko?
Financial capacity (Kemampuan Finansial)	Kapasitas perusahaan untuk menyediakan dukungan finansial untuk menambah dan memelihara lingkungan TI dan mengoptimalkan risiko.

b. ***External contextual factors***, dimana faktor ini diberlakukan untuk risiko yang berada diluar kendai perusahaan. Untuk faktor eksternal, meliputi beberapa pilihan aspek berikut yang disajikan dalam Tabel 2.6.

Tabel 2.6 Aspek External Contextual Factors [23]

Aspek *External Contextual Factors*	**Deskripsi**
Market/economic factors (Faktor ekonomi)	Sektor industri di mana perusahaan beroperasi. Contoh: mengoperasi dalam sektor finansial membutuhkan kebutuhan TI dan kapabiitas TI yang berbeda daripada mengoperasikan dalam lingkungan manufaktur. Faktor ekonomi dapat termasuk, contohnya: nasionalisasi, merger dan akuisisi, dan konsolidasi.
Rate of change in the market in which the enterprise operates (Laju perubahan dalam pasar di mana perusahaan beroperasi)	Apakah model bisnis berubah secara fundamental? Apakah produk atau layanan terdapat pada akhir momen siklus hidup yang penting?
Competitive environment (Lingkungan Kompetitif)	Lokasi dimana perusahaan beroperasi.
Geopolitical situation (Situasi Geopolitik)	Apakah lokasi geografis digunakan untuk bencana alam yang sering terjadi? Apakah politik lokal dan konteks ekonomi secara keseluruhan menggambarkan risiko tambahan?
Regulatory environment (Lingkungan Peraturan)	Apakah perusahaan ditujukan untuk peraturan baru atau lebih ketat terkait TI atau peraturan dampak

Aspek *External Contextual Factors*	Deskripsi
	TI? Apakah ada persyaratan kepatuhan lain di luar peraturan, misalnya, spesifik industri, secara kontrak?
Technology status and evolution (Status Teknologi dan Evolusi)	Apakah perusahaan menggunakan keadaan seni teknologi dan, yang lebih penting, seberapa cepat teknologi yang relevan berkembang?
Threat landscape (Ancaman)	Bagaimana ancaman relevan berkembang dalam hal frekuensi terjadi dan tingkat kemampuan?

2.2.16.4 Skenario Risiko

Skenario risiko TI adalah deskripsi dari suatu peristiwa yang berhubungan dengan TI yang dapat menyebabkan dampak bisnis, ketika risiko terjadi dan perkiraan apabila risiko terjadi [23]. Pembuatan skenario risiko berdasarkan dua jenis, yaitu skenario positif dan skenario negatif.

2.2.16.5 Pemetaan risiko dengan Proses COBIT 5

Risiko yang sudah diidentifikasi dan diberikan kontrol risiko dapat dipetakan dengan proses yang ada pada COBIT 5 *Enabling Process* sesuai keterkaitan tipe, faktor dan skenario risiko tersebut.

2.2.16.6 Penilaian Risiko Berdasarkan Frekuensi dan Dampak (*Magnitude*) Risiko

Berdasarkan acuan standar COBIT 5 *for Risk*, penilaian risiko dibagi berdasarkan dua aspek, yaitu aspek frekuensi dan *magnitude* (dampak). Untuk aspek frekuensi, peringkat dan parameternya dapat disesuaikan dengan konteks organisasi. Berikut merupakan contoh pembuatan parameter dan peringkat frekuensi risiko yang disajikan pada Tabel 2.7 [23].

Tabel 2.7 Contoh Parameter dan Peringkat Frekuensi Risiko[23]

Peringkat Frekuensi	Frekuensi Risiko
0	$N \leq 0{,}01$
1	$0{,}01 < N \leq 0{,}1$
2	$0{,}1 < N \leq 1$
3	$1 < N \leq 10$
4	$10 < N \leq 100$
5	$100 < N$

Magnitude risiko dibagi berdasarkan empat jenis, yaitu:

1. Produktivitas (*Productivity*), aspek ini dikur dari sisi *Revenue Loss Over One Year*, dimana dapat dilihat dari dampak kerugian finansial yang dialami organisasi selama kurun waktu periode tertentu. Bentuk kerugian yang dialami ITS dapat dilihat dari beberapa aspek, antara lain:
   - Lambatnya kinerja staff organisasi yang mengelola permintaan layanan dan insiden sehingga proses bisnis terhambat.
   - Kerugian finansial yang dimiliki organisasi.
   - Kerusakan terhadap aset milik organisasi sehingga tidak layak/tidak dapat digunakan.

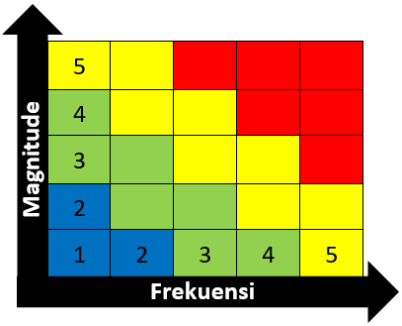
Setiap aspek kerugian dihitung berupa kerugian persentase (%) yang dialami ITS selama kurun waktu satu tahun

2. Biaya Tanggapan (*Cost of Response*), aspek ini diukur dari sisi *Expenses Associated With Managing the Loss Event*. Biaya tanggapan (*cost of response*) merupakan biaya yang harus dikeluarkan oleh organisasi dalam menangani yang merugikan dari setiap risiko yang terjadi
3. Keunggulan Kompetitif (*Competitive Advantage*), aspek ini diukur dari sisi *Drop-in Customer Satisfaction Ratings*, yaitu diukur dari penurunan kepuasan pengguna layanan akibat terjadinya skenario risiko. Indeks kepuasan pengguna nantinya didapatkan dari hasil survei dengan mengambil beberapa *sampling*.
4. Hukum (*Legal*), aspek ini merupakan dampak berupa biaya denda yang harus ditanggung oleh organisasi akibat terjadinya risiko yang berdampak pada hukum. Nilai

pengukurannya berupa biaya denda yang harus ditanggung oleh organisasi.

2.2.16.7 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 2.2 [23].



Gambar 2.2 Peta Frekuensi dan *Magnitude* Risiko [23]

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 2.8 [23].

Tabel 2.8 Level Prioritas Risiko [23]

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

2.2.17 Respon Mitigasi Risiko

Manajemen risiko adalah proses proaktif dimana dilakukan pengelolaan dan antisipasi risiko sebelum mereka terjadi. Risiko terbagi menjadi positif dan negatif. Risiko ngeatif dapat membahayakan tujuan proyek dan risiko positif dapat memberikan dampak positif terhadap proyek. Jika untuk

merespon resiko negatif menggunakan strategi *avoid*, *transfer*, *Mitigate (Treat)* dan *accept*, maka respon untuk risiko positif dibedakan menjadi *exploit*, *share*, *ehance* and *ignore*. Berikut merupakan strategi respon risiko yang disajikan pada Tabel 2.10 [44].

Tabel 2.9 Mitigasi Risiko Positif dan Negatif [44]

Response Risiko Negatif	Strategi Umum	Respons Risiko Positif
Avoid	*Eliminate uncertainty*	*Exploit*
Transfer	*Allocate ownership*	*Share*
Mitigate (Treat)	*Modify exposure*	*Enhance*
Accept	*Include in baseline*	*Ignore*

Menurut COBIT 5, terdapat terdapat empat pilihan strategi penanganan risiko negatif yang dapat dipilih oleh suatu organisasi yaitu, [23]:

1. *Acceptance*, yaitu apabila risiko yang dihadapi sudah diketahui dan tidak dapat dicegah, sehingga suatu organisasi perlu menerima risiko tersebut, dimana perusahaan memutuskan untuk menerima kerugian, manfaat, atau keuntungan yang mungkin muncul dari risiko yang terjadi.
2. *Sharing/Transfer*, apabila risiko yang dihadapi terlalu sulit untuk ditangani sendiri, sehingga risiko tersebut perlu dialihkan ke pihak ke-tiga.
3. *Avoidance*, apabila risiko yang dihadapi terlalu besar sehingga proses dan aktivitas yang berhubungan dengan risiko tersebut perlu diberhentikan apabila dampaknya dinilai tidak lagi relevan dengan organisasi tersebut.
4. *Mitigation*, apabila risiko yang dihadapi diberi perlakukan khusus dengan menerapkan kontrol yang sesuai atau organisasi dapat memberikan biaya khusus yang efektif (*effective cost*) bila diperlukan.

Berikut merupakan penjelasan respon untuk melakukan mitigasi positif [44]:

1. *Exploit* adalah usaha yang dilakukan untuk mengeliminasi ketidakpastian dengan cara memastikan peluang terjadi.

Tujuan dari strategi ini adalah meningkatkan kemungkinan keterjadian peluang hingga 100%. Eksploitasi merupakan strategi paling agresif dibandingkan yang lainnya. Strategi ini biasanya dipilih untuk kesempatan terbaik dengan probabilitas dan dampak tinggi yang tidak dapat dilewatkan oleh proyek atau organisasi.

2. *Enhance* adalah strategi respons peluang dengan cara meningkatkan kemungkinan terjadinya peluang tersebut. Dalam hal ini, meskipun beberapa tindakan diambil untuk meningkatkan keterjadian peluang, tidak ada jaminan bahwa peluang tersebut akan terjadi.
3. *Share* adalah strategi respons peluang dengan melibatkan pihak ketiga yang dianggap mampu untuk menangani, memaksimalkan kemungkinan keterjadian, serta meningkatkan potensi manfaat ketika peluang terjadi. Sama halnya ketika risiko/ancaman terjadi, pihak ketiga yang dibagi wajib turut bertanggung jawab atas pengelolaannya.
4. *Ignore* adalah strategi terakhir dalam merespons peluang dengan mengabaikannya. Hal ini sama artinya dengan strategi penerimaan risiko.

“Halaman ini sengaja dikosongkan”

BAB III
METODOLOGI PENELITIAN

Pada bagian ini akan dijelaskan mengenai metodologi dalam melakukan pengerjaan Tugas Akhir, sehingga langkah-langkah pengerjaan menjadi lebih sistematis dan terorganisir. Berikut ini merupakan tahapan metodologi pengerjaan tugas akhir berdasarkan kerangka kerja COBIT 5 *for Risk* pada proses APO12 – *Manage Risk* yang digambarkan pada Bagan 3.1.

I.		**TAHAP INISIASI KEBUTUHAN**		
INPUT		**PROSES**		**OUTPUT**
Literatur COBIT 5 *Enabling Processes* dan COBIT 5 *for Risk*		Mempelajari bahan literatur		Konsep manajemen risiko berdasarkan COBIT 5
Konsep manajemen risiko berdasarkan COBIT 5 dan *Interview protocol*	→	Melakukan wawancara	→	Hasil wawancara
Dokumen tupoksi *helpdesk* Subdirektorat Layanan TSI DPTSI ITS dan hasil wawancara		Melakukan pemetaan proses TI *helpdesk* dengan proses TI di DSS02 COBIT 5		Hasil pemetaan proses TI *helpdesk* dengan proses TI di DSS02 COBIT 5
Hasil wawancara, hasil pemetaan proses TI *helpdesk* dengan proses TI di DSS02 COBIT 5		Menentukan kemungkinan risiko yang dapat terjadi		Hasil identifikasi risiko berdasarkan proses TI *helpdesk*

II. TAHAP PENGUMPULAN DATA (*COLLECT DATA*)		
INPUT	**PROSES**	**OUTPUT**
Hasil identifikasi risiko berdasarkan proses TI *helpdesk*	Menganalisis tipe risiko	Hasil identifikasi risiko beserta tipenya
Hasil identifikasi risiko beserta tipenya	Menganalisis kategori risiko	Hasil identifikasi kategori untuk setiap risiko
	Menganalisis penyebab (faktor risiko)	Daftar faktor penyebab risiko dan *risk event*
III. TAHAP MENGANALISIS RISIKO (*ANALYZE RISK*)		
INPUT	**PROSES**	**OUTPUT**
Hasil identifikasi risiko (*risk event*)	Membuat skenario (dampak) risiko proses TI	Daftar skenario (dampak) risiko proses TI
Daftar skenario (dampak) risiko proses TI	Membuat kuesioner dampak (*magnitude*) risiko	Hasil kuesioner dampak (*magnitude*) risiko
Hasil kuesioner dampak (*magnitude*) risiko dan hasil identifikasi kategori risiko	Menilai risiko TI berdasarkan frekuensi dan dampak (*magnitude*) risiko	Hasil penilaian risiko TI berdasarkan frekuensi dan dampak (*magnitude*) risiko
Hasil penilaian risiko TI berdasarkan frekuensi dan dampak (*magnitude*) risiko	Menentukan respon yang tepat untuk setiap risiko proses TI	Hasil identifikasi respon risiko
Hasil penilaian risiko TI berdasarkan	Melakukan pemetaan risiko	Hasil risiko berdasarkan proses TI

frekuensi dan dampak (*magnitude*) risiko dan hasil identifikasi respon setiap risiko		berdasarkan proses TI COBIT 5 yang sesuai		COBIT 5 yang sesuai
Hasil risiko berdasarkan proses TI COBIT 5 yang sesuai		Menentukan analisis langkah mitigasi berdasarkan aktivitas proses TI COBIT 5		Daftar langkah mitigasi risiko

Bagan 3.1 Metodologi Penelitian

3.1 Tahap Inisasi Kebutuhan

Pada tahapan inisiasi kebutuhan dilakukan wawancara untuk mengidentifikasi permasalahan dan kondisi kekinian subdirektorat layanan DPTSI ITS mempelajari bahan literatur, dan melakukan pemetaan proses *helpdesk* dengan proses pada COBIT 5. Serta melaukan analisis kemungkinan risiko yang muncul dari pemetaan proses *helpdesk* dengan proses TI COBIT 5. Berikut beberapa proses yang ada dalam tahap inisasi kebutuhan.

3.1.1 Mempelajari Bahan Literatur

Hal pertama yang perlu dilakukan adalan memahami literatur terkait. Studi literatur dilakukan dengan mengumpulkan berbagai informasi dan referensi mengenai topik penelitian. Hal ini dilakukan untuk menunjang pengetahuan guna melakukan pengelolaan risiko di subdirektorat layanan DPTSI ITS. Literatur yang digunakan yaitu buku akademik, *paper*, *thesis*, dan jurnal terkait pengelolaan risiko, serta buku panduan kerangka kerja terstandar COBIT 5 *Enabling Process* dan COBIT 5 *for Risk*. Hasil dari proses ini adalah konsep manajemen risiko berdasarkan kerangka kerja COBIT 5 *Enabling Process* dan COBIT 5 *for Risk*. Selain itu juga

dilakukan pengumpulan data terkait risiko-risiko proses TI yang kemungkinan terjadi beserta insiden terkait TI yang telah terjadi di organisasi di DPTSI melalui buku Tugas Akhir para alumni Jurusan Sistem Informasi.

3.1.1.1 Menentukan Metodologi Manajemen Risiko

Dengan pemahaman oleh teori-teori tersebut, akan ditetapkan metodologi pengujian yang sesuai dengan konteks permasalahan di *helpdesk* subdirektorat layanan DPTSI ITS. Pada tahap ini dilakukan pembuatan metodologi pengelolaan risiko berdasarkan proses APO12 – *Manage Risk* yang mengacu pada standar COBIT 5 *for Risk.* Namun karena penelitian ini hanya sampai pada penilaian risiko, sehingga proses pada APO12 *Manage Risk* berhenti sampai APO12.02 yaitu menganalisis risiko.

3.1.2 Melakukan Wawancara

Pada tahap ini peneliti membuat daftar pertanyaan-pertanyaan berdasarkan pemahaman literatur pada tahap sebelumnya yang bertujuan untuk mempermudah peneliti dalam melakukan wawancara kepada narasumber. Setelah membuat *interview protocol* dan mempelajari bahan literatur yang berkaitan dengan teori-teori manajemen risiko dengan berbagai pendekatannya, hal yang perlu dilakukan adalah mengidentifikasi permasalahan, kondisi kekinian dan tujuan penelitian pada subdirektorat layanan DPTSI ITS terkait penanganan risiko. Untuk mendukung analisis tersebut, perlu dilakukan proses penggalian informasi kepada narasumber yang memiliki pengetahuan tentang teknologi informasi yang ada pada pusat pengelolaan layanan DPTSI. Wawancara dilakukan berdasarkan pertanyaan-pertanyaan yang terdapat pada *Interview Protocol*.

3.1.3 Melakukan Pemetaan Proses pada *Helpdesk* dengan COBIT 5

Pada tahap ini dilakukan pemetaan proses pengelolaan permintaan layanan dan isinden pada *helpdesk* Subdirektorat

Layanan Teknologi dan Sistem Informasi DPTSI dengan pendekatan *best practice* COBIT 5 DSS02 *Manage Service Requests and Incidents* untuk mengetahui apakah proses yang dilakukan oleh *helpdesk* sudah sesuai dengan proses ideal pada standar.

3.1.4 Menentukan kemungkinan risiko yang dapat terjadi

Setelah mengetahui pemetaan proses TI *helpdesk* dengan proses TI pada domain DSS02 *Manage Service Requests and Incidents* COBIT 5, selanjutnya dapat diidentifikasi risiko-risiko yang dapat terjadi sesuai per aktivitas dari hasil pemetaan proses TI *helpdesk* terkait pengelolaan permintaan layanan dan insiden.

Keluaran yang dihasilkan pada tahap inisiasi kebutuhan adalah pemahaman konsep manajemen risiko dari standar COBIT 5 *Enabling Processes* dan COBIT 5 *for Risk*, penetapan metodologi pengerjaan penelitian yakni berdasarkan proses APO12 – *Manage Risk* yang mengacu pada standar COBIT 5 *for Risk*, *interview protocol* dan hasil wawancara terkait definisi permasalahan disertai dengan kondisi kekinian dari Subdirektorat layanan DPTSI ITS, dan juga hasil pemetaan proses TI *helpdesk* Subdirektorat layanan DPTSI ITS dengan proses TI DSS02 COBIT 5, serta analisis kemungkinan risiko yang dapat terjadi dari proses TI *helpdesk*.

3.2 Tahap Pengumpulan Data

Tahapan ini dilakukan untuk mempermudah penelitian dalam mengumpulkan data dan informasi terkait proses TI dan risikonya di *helpdesk* Subdirektorat layanan DPTSI ITS. Berikut beberapa proses yang ada dalam tahap pengumpulan data.

3.2.1 Menganalisis Tipe Risiko

Setelah mendapatkan sejumlah data dan informasi kondisi kekinian dari hasil wawancara pihak *helpdesk* subdirektorat layanan DPTSI ITS, maka data yang berperan signifikan dalam proses manajemen risiko TI perlu dikembangkan untuk

kemudian diolah dalam pembuatan tabel pemetaan risiko dengan tipe yang sesuai. Tipe risiko dapat dikategorikan menjadi tiga bagian, yaitu risiko yang masuk ke manfaat atau nilai risiko TI, program dan proyek risiko TI, atau operasional dan layanan risiko TI .

3.2.2 Manganalisis Kategori Untuk Setiap Risiko

Setelah membuat daftar risiko berdasarkan tipenya, setiap risiko yang ada dapat dikategorisasikan, tujuannya agar memudahkan dalam mengidentifikasi risiko. Kategori risiko yang digunakan mengacu ke-dua puluh kategori yang terdapat pada standar COBIT 5 *for risk*.

3.2.3 Menganalisis Faktor Penyebab Risiko

Setelah risiko dikategorisasikan, langkah terakhir ialah menentukan faktor-faktor penyebab dari masing-masing risiko yang sudah diidentifikasi, baik dari faktor internal organisasi maupun faktor eksternal. Jenis faktor internal dan eksternal yang digunakan mengacu pada daftar faktor risiko kontekstual pada standar COBIT 5 *for risk*.

Keluaran yang dihasilkan pada tahap ini adalah hasil identifikasi risiko berupa tabel analisis tipe risiko, hasil tabel identifikasi kategori untuk setiap risiko, serta tabel faktor penyebab masing-masing risiko proses TI pada *helpdesk* Subdirektorat Layanan TSI DPTSI. Ketiga tabel tersebut kemudian digabung menjadi sebuah *risk event*.

3.3 Tahap Menganalisis Risiko

Pada tahapan ini dilakukan pengelolaan lebih lanjut terhadap daftar risiko yang telah diidentifikasi tipe, kategori, penyebab, yang telah dipetakan terhadap proses *helpdesk* Subdirektorat layanan TSI DPTSI untuk dibuatkan daftar skenario (dampak) risiko. Pada tahap ini juga dilakukan analisis penilaian risiko berdasarkan frekuensi keuntungan maupun kerugian yang disebabkan oleh risiko. Kemudian masing-masing risiko ditentukan respon penanganannya berdasarkan empat pilihan

manajemen risiko yaitu *avoid*, *Mitigate (Treat)*, *transfer* atau *accept*. Setelah itu dilakukan pemetaan risiko terhadap proses COBIT 5 yang sesuai untuk ditentukan langkah mitigasinya. Berikut merupakan proses-proses yang ada dalam tahap menganalisis risiko.

3.3.1 Membuat Skenario Risiko Proses TI

Skenario risiko TI dibuat menjadi dua jenis, yaitu skenario positif dan skenario negatif. Pembuatan skenario dilakukan untuk setiap risiko, skenario risiko merupakan dampak bila terjadi risiko tersebut yang dibedakan menjadi dampak baik (skenario positif) dan buruk (skenario negatif).

3.3.2 Membuat kuesioner dampak (*magnitude*) risiko

Aspek penilaian risiko terbagi menjadi empat, salah satunya ialah *competitive advantage* yang dilihat dari penurunan kepuasan pelanggan. Untuk mengukurnya, diperlukan survei untuk mengetahui indeks penurunan kepuasan pelanggan apabila dampak (skenario) risiko terjadi. Untuk itu, sebelum melakukan penilaian risiko, dibuatkan kuesioner yang ditujukan untuk mengukur indeks penurunan kepuasan pelanggan tersebut yang pertanyaannya dibuat berdasarkan skenario (dampak risiko).

3.3.2.1 Melakukan Pemetaan Risiko dengan Pertanyaan Kuesioner

Untuk memudahkan perhitungan hasil kuesioner, dilakukan pemetaan risiko dengan pertanyaan kuesioner yang sudah dibuat sebelum nantinya melakukan penilaian risiko. Pemetaan risiko dengan pertanyaan kuesioner dikategorikan berdasarkan persamaan dampak (skenario) risiko.

3.3.3 Menilai Risiko TI berdasarkan Frekuensi dan Dampak (*Magnitude*) Risiko

Penilaian risiko dibuat berdasarkan perkiraan frekuensi dan besarnya keuntungan atau kerugian (*magnitude* risiko), terkait dengan skenario risiko yang telah dibuat sebelumnya. Perkiraan

frekuensi dibagi berdasarkan jumlah terjadinya risiko sesuai periode waktu tertentu.
Magnitude risiko menurut COBIT 5 dibedakan menjadi empat bagian, yaitu :

- Produktivitas, yaitu seberapa besar kerugian yang dialami organisasi karena risiko.
- Biaya tanggapan, yaitu biaya yang dikeluarkan untuk menangani risiko
- Keunggulan kompetitif, yaitu penururan kepuasan pelanggan terhadap layanan sistem, dimana pada tahap ini dibuat kuesioner berdasarkan dampak risiko untuk mengukur penurunan kepuasan pelanggan.
- Hukum, yaitu seberapa besar denda yang harus dibayar organisasi dari risiko yang melanggar hukum dan regulasi.

Perhitungan besarnya keuntungan atau kerugian didasarkan pada tipe *magnitude* risiko, untuk nantinya dihitung dan masing-masing risiko dikategorisasikan berdasarkan levelnya, yaitu *low risk, medium risk, high risk* dan *very high risk*.

3.3.4 Menentukan Respon Risiko

Setelah mengetahui level risiko, maka dapat dibuat justifikasi penanganan untuk setiap risiko TI. Justifikasi manajamen risiko dapat dibedakan menjadi empat macam, yaitu *avoid* atau dihindari, *accept* atau diterima, *transfer* atau di transfer ke pihak ke-tiga maupun *Mitigate (Treat)* yaitu dibuatkan langkah mitigasinya.

3.3.5 Melakukan Pemetaan Risiko Proses TI terhadap Proses TI yang Sesuai sebagai Langkah Mitigasi

Pemetaan risiko dilakukan dengan cara menentukan risiko berdasarkan klasifikasi yang sesuai dengan proses atau *key management practice* COBIT 5 setelah itu diidentifikasi aktivitas dari serangkaian proses TI yang dapat dilakukan organisasi untuk langkah mitigasi risiko.

Keluaran dari tahap menganalisis risiko adalah tabel skenario untuk setiap risiko proses TI, kuesioner untuk penilaian risiko beserta hasil rekapannya, hasil pemetaan risiko dengan pertanyan kuesioner, tabel penilaian risiko TI berdasarkan frekuensi, tabel besarnya *magnitude* risiko, tabel respon risiko (*avoid, Mitigate (Treat), transfer, accept*) untuk setiap risiko proses TI, serta hasil pemetaan risiko dengan proses COBIT 5 yang sesuai untuk mitigasi risiko.

"Halaman ini sengaja dikosongkan"

BAB IV
PERANCANGAN

Pada bagian ini akan dijelaskan mengenai perancangan pengerjaan tugas akhir. Perancangan yang dibuat meliputi perancangan studi kasus dan perancangan terkait hal-hal yang akan dilakukan untuk mengerjakan tugas akhir.

4.1 Perancangan Studi Kasus

Studi kasus memungkinkan peneliti dalam menelti data pada konteks tertentu. Studi kasus didefinisikan sebagai penyelidikan empiris yang mengidentifikasi fenomena kontemporer dalam konteks kehidupan nyata dengan menggunakan cara – cara tersistematis dalam pengumpulan data, seperti observasi dan wawancara [45]. Terdapat tiga jenis studi kasus, yaitu [45]:

- Eksplorasi (penggalian), yaitu penggalian studi kasus dilakukan dengan menjelajahi fenomena apapun dalam data yang berfungsi sebagai tempat tujuan untuk peneliti.
- Deskriptif, yaitu dengan menggambarkan fenomena ilmiah yang terjadi di dalam data yang dimaksud. Tujuannya adalah menggambarkan data yang terjadi dalam bentuk narasi.
- *Explanatory* (penjelasan), yaitu menjelaskan fenomena dalam data secara jelas dan detail.

Penelitian tugas akhir ini menggunakan studi kasus jenis eksplorasi (penggalian) karena berdasarkan rumusan masalah pada penelitian ini, mengindikasikan penggalian data terkait risiko TI untuk selanjutnya diidentifikasi dan dilakukan penilaian sesuai dengan standar kerangka kerja COBIT 5. Eksplorasi dilakukan pada studi kasus untuk mendapatkan fenomena yang terjadi dan dijadikan dasar dalam melakukan identifikasi dan penilaian risiko TI.

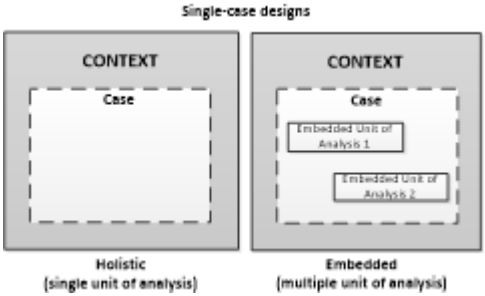
4.1.1 Tujuan Studi Kasus

Penelitian ini bertujuan untuk mengetahui penilaian risiko berdasarkan identifikasi risiko terkait proses TI pada *helpdesk*

terkait proses pengelolaan insiden dan pemenuhan permintaan layanan menggunakan kerangka kerja COBIT 5. Untuk mencapai tujuan penelitian tersebut, dilakukan metode penggalian data dengan wawancara, pengkajian dokumen dan observasi.

Penelitian ini tentunya membutuhkan studi kasus tersendiri yang nantinya dijadikan objek penelitian karena dinilai tidak relevan apabila tidak terdapat objek atau studi kasus dan proses penilaian risiko. Risiko nantinya diidentifikasi dari suatu unit kerja beserta proses-proses di dalamnya.

Studi kasus yang baik adalah yang berfokus pada satu kasus (*single case design*) atau berbagai kasus (*multiple case design*). Perancangan studi kasus yang digunakan pada tugas akhir ini adalah *single case design*, dimana terdapat dua tipe *single case design*, yaitu *single unit of analysis* dan *multiple units of analysis* [46]. Struktur *single case design* tersebut dapat dilihat pada Gambar 4.1.1.



Gambar 4.1 Tipe Studi Kasus *Single Case Design* [46]

Single unit of analysis dapat digunakan pada penelitian dengan kasus yang unik, kritis atau penyimpangan kasus. Sementara, *multiple units of analysis* dapat digunakan untuk melakukan replikasi temuan di seluruh studi kasus dengan cara membandingkan *sub-units* [46].

Tugas akhir ini menggunakan satu studi kasus dengan *single unit of analysis*, Karena satu studi kasus saja sudah sangat mewakili penelitian tugas akhir ini. *Unit of analysis* dalam tugas akhir ini adalah melakukan analisis terhadap risiko yang kerap

muncul pada *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS. Selama ini belum ada penelitian yang melakukan identifikasi dan penilaian risiko terhadap unit *helpdesk* subdirektorat layanan DPTSI, sehingga perlu dilakukan analisis untuk mengetahui bagaimana dampak dan frekuensi risiko tersebut agar bisa diantisipasi untuk menghindari kerugian

Dengan adanya studi kasus untuk penelitian tugas akhir ini, dibutuhkan proses penggalian kondisi kekinian terkait proses bisnis serta penggalian risiko TI yang kerap muncul dari unit *helpdesk*, dimana penggalian data tersebut nantinya dilakukan dengan metode wawancara, pengakjian dokumen dan observasi.

4.1.2 *Unit of Analysis*

Berdasarkan pada pemaparan pentingnya studi kasus terhadap sebuah penelitian sebagai objektif dalam mencapai tujuan penelitian, penelitian ini menggunakan studi kasus Direktorat Pengembangan Teknologi dan Sistem Informasi, khususnya pada bagian *helpdesk* pada Subdirektorat Layanan Teknologi dan Sistem Informasi. *Unit of analysis* yang digunakan oleh penelitian ini ialah analisis identifikasi dan penilaian risiko proses TI yang berfokus pada layanan TI *helpdesk* yang meliputi proses manajemen insiden dan pemenuhan permintaan layanan TI di DPTSI ITS.

4.2 Persiapan Pengumpulan Data

Persiapan pengumpulan data yang akan dilakukan meliputi metode yang akan digunakan, narasumber dan objek yang dibutuhkan, serta uraian rancangan pertanyaan yang digunakan untuk mengumpulkan data.

Penggalian informasi pada bagian *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS akan dilakukan pengkajian dokumen, melakukan wawancara oleh narasumber terkait, serta membuat kuesioner untuk menentukan metode penilaian risiko.

Pengkajian dokumen dilakukan pada dokumen yang berisi informasi terkait manajemen insiden yang dapat diperoleh dari staff dan unit *helpdesk* subdirektorat layanan DPTSI. Sedangkan untuk metode wawancara, pihak yang akan menjadi narasumber untuk wawancara adalah koordinator Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS serta unit *helpdesk* subdirektorat layanan DPTSI.

4.3 Perancangan Interview Protocol

Perancangan *interview protocol* merupakan perancangan daftar pertanyaan yang digunakan sebagai panduan penelitian agar ketika melakukan wawancara tidak bias dan terarah. *Interview protocol* ini nantinya akan digunakan untuk menggali kondisi kekinian terkait risiko-risiko yang kerap muncul pada bagian *helpdesk* terkait pengelolaan insiden dan permintaan layanan yang dilakukan oleh subdirektorat layanan DPTSI selama ini.

Perancangan awal pada *interview protocol* adalah perlu menambahkan informasi terkait pelaksanaan interview dan narasumber yang akan dituju, sebelum merancang daftar pertanyaan. Adapun tujuan dari penambahan informasi Pelaksanaan interview dan narasumber ini adalah untuk mendokumentasikan hasil interview dengan baik, karena dapat memberikan informasi kapan dan dimana pelaksanaan interview dan siapa yang dapat memberikan informasi – informasi terkait pengelolaan insiden dan layanan serta risikonya di subdirektorat layanan DPTSI. Konten dari informasi pelaksanaan interview dan narasumber dapat dilihat pada Tabel 4.1.

Tabel 4.1 Konten Informasi Pelaksanaan Interview

Informasi Pelaksanaan Interview	
Interviewer	:
Narasumber	:
Hari, Tanggal	:
Pukul	:
Lokasi	:
Informasi Narasumber	
Nama	:

Jabatan	:	
Instansi	:	
Lama bekerja	:	

Interview protocol yang dirancang mencakup beberapa pertanyaan dasar yang didasarkan pada proses DSS02 *Manage Service Requests and Incidents* terkait manajemen insiden dan permintaan layanan dan proses APO12 *Manage Risks* terkait manajemen risiko. Dimana untuk setiap *key management practices* tersebut memiliki tahapan aktivitas yang dapat dijadikan sebagai bahan pertanyaan. Selain itu, dalam perancangan *interview protocol* penulis perlu memetakan setiap pertanyaan sesuai dengan tujuan yang ingin dicapai dari wawancara. Tujuan dari pemetaan tersebut adalah untuk memudahkan saat bertanya karena maksud dan tujuan dari pertanyaan tersebut telah dimengerti. Hasil pemetaan dapat dilihat pada Tabel 4.2 dan Tabel 4.3.

Tabel 4.2 Pemetaan Tujuan Wawancara 1

Tujuan Wawancara	**Manajemen Praktik Kunci DSS02 *Manage Service Requests and Incidents***
Mengetahui pengelolaan insiden dan pemenuhan permintaan layanan pada *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI	- **DSS02.01 – Menetapkan skema klasifikasi insiden dan layanan permintaan**, DSS02.01 menjelaskan bahwa apabila terjadi sebuah insiden atau permintaan layanan, perlu dilakukan pembuatan skema klasifikasi, skema prioritasi serta kriteria permasalahan. Selain itu juga didefinisikan bentuk dan model insiden atau layanan serta peraturan dan prosedur eskalasinya apabila diperlukan. - **DSS02.02 – Mencatat, Mengklasifikasikan dan Memprioritaskan permintaan dan insiden**, DSS02.02 menjelaskan insiden atau layanan yang dilaporkan harus dicatat, di klasifikasikan berdasarkan tipe dan kategori dan prioritasinya sesuai dengan tingkat bisnis dan SLA. - **DSS02.03 – Melakukan Verifikasi, Menerima dan Memenuhi Permintaan Layanan**, DSS02.03 menjelaskan bahwa

Tujuan Wawancara	Manajemen Praktik Kunci DSS02 *Manage Service Requests and Incidents*
	organisasi harus memilih prosedur pengelolaan insiden atau layanan yang sesuai dan memverifikasikannya kemudian disesuaikan dengan kriteria permintaan. Proses ini memerlukan persetujuan finansial jika dibutuhkan dan memenuhi permintaan sesuai dengan prosedur. - **DSS02.04 – Menginvestigasi, Mendiagnosa dan Mengalokasikan Insiden,** DSS02.04 menjelaskan bahwa setiap insiden maupun layanan harus dilakukan identifikasi dan pencatatan gejala penyebab untuk memperisapkan pembuatan solusi. - **DSS02.05 – Melakukan Penyelesaian dan Pemulihan Insiden**, DSS02.05 menjelaskan bahwa perlu dilakukan pemilihan solusi yang tepat dan medokumentasikan aksi penyelesaian insiden atau layanan tersebut. - **DSS02.06 – Menutup Permintaan Layanan dan Insiden**, DSS02.06 menjelaskan bahwa perlu adanya verifikasi terhadap kepuasan *user* terhadap solusi insiden atau layanan dan melakukan penutupan. - **DSS02.07 – Melacak Status dan Membuat Laporan**, DSS02.07 menjelaskan bahwa perlu adanya pelacakan secara berkala dan pembuatan dokumentasi insiden maupun layanan yang telah terselesaikan.

Tabel 4.3 Pemetaan Tujuan Wawancara 2

Tujuan Wawancara	Manajemen Praktik Kunci APO12 *Manage Risks*
Mengetahui pengelolaan insiden dan pemenuhan permintaan layanan pada *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI	- **APO12.01 – Menetapkan skema klasifikasi insiden dan layanan permintaan**, APO12.01 menjelaskan bahwa proses pengidentifikasian risiko terkait TI membutuhkan metode, pencatatan serta pemahaman informasi terkait risiko seperti *risk event*, kategori risiko, faktor risiko. - **APO12.02 – Mencatat, Mengklasifikasikan dan Memprioritaskan permintaan dan insiden**, APO12.02 menjelaskan bahwa proses analisis risiko meliputi pengembangan informasi yang berguna untuk mendukung pengambilan keputusan risiko ke dalam faktor risiko bisnis yang relevan, seperti perhitungan frekuensi dan dampak kerugian atau keuntungan yang ditimbulkan dari risiko, membuat skenario risiko dan membuat mitigasi risiko.

Setelah merumuskan dan memetakan tujuan, maka selanjutnya adalah menyusun pertanyaan. Sebelum digunakan, *interview protocol* perlu ditelaah secara komprehensif. Tujuan dari penelaahan tersebut adalah untuk mereview kembali perancangan *interview protocol*. Jika ada kekurangan akan direvisi, namun bila semuanya sudah layak sesuai dengan keperluan di lapangan, maka selanjutnya akan dilakukan wawancara. Perancangan *interview protocol* dapat dilihat pada **LAMPIRAN A.**

4.4 Penggalian Data Kondisi Kekinian

Penggalian data kondisi kekinian yang dilakukan dalam pengerjaan tugas akhir ini adalah dengan menggunakan teknik wawancara. Wawancara dilakukan dengan menggunakan perangkat *interview protocol* yang terlampir pada **LAMPIRAN A.**

4.4.1 Wawancara

Wawancara dilakukan untuk mengumpulkan informasi langsung dari narasumber. Teknik wawancara yang dipilih adalah teknik wawancara semi terstruktur. Hal ini dikarenakan penulis menggunakan instrument atau perangkat namun ketika wawancara sedang berlangsung, penulis tidak harus berfokus pada perangkat tersebut.

Wawancara yang akan dilakukan ditujukan kepada narasumber yang memahami proses bisnis *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI. Narasumber tersebut adalah Ibu Hanim Maria Asturi S.Kom., M.Sc, selaku koordinator Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI dan unit *helpdesk* yang melayani insiden dan permitanaan layanan. Berikut adalah beberapa poin tujuan utama yang akan diajukan dalam wawancara:

1. Proses penanganan insiden dan pemenuhan permintaan layanan,
2. Risiko yang kerap muncul dari insiden dan permintaan layanan.
3. Rencana atau strategi di masa depan untuk menangani dan mengantisipasi terjadinya risiko.

4.4.1.1 Penggalian Kondisi Kekinian

Tahap penggalian kondisi kekinian merupakan tahapan yang perlu dilakukan untuk menggali data dan informasi terkait kondisi kekinian *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI. Penggalian kondisi kekinian dilakukan dengan metode wawancara dan observasi. Penjelasan dari metode wawancara dapat dilihat pada Tabel 4.4, sementara untuk metode observasi dilakukan dengan melihat kondisi yang sedang berlangsung diruangan kerja *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi.

Tabel 4.4 Metode Penggalian Kondisi Kekinian

Wawancara
Menggali data dan informasi terkait: • Identifikasi insiden dan permintaan layanan, yang meliputi : - Aktivitas yang dilakukan pada saat mengelola insiden

Wawancara
- Aktivitas yang dilakukan pada saat memenuhi permintaan layanan. • Risiko yang kerap muncul terkait manajemen insiden dan permintaan layanan. • Kondisi yang diharapkan terkait pengelolaan insiden dan permintaan layanan. • Dokumentasi yang telah dilakukan selama proses manajemen insiden dan pemenuhan permintaan layanan. • Pihak yang terlibat dalam proses pengembangan SIM.

Wawancara ditujukan kepada *helpdesk* subdirektorat layanan TSI DPTSI dan dilakukan dengan menggunakan daftar pertanyaan (*interview protocol*). Pada Tabel 4.5 akan dipaparkan terkait tujuan, *input*, proses dan *output* dari tahap penggalian kondisi kekinian.

Tabel 4.5 Tahap Penggalian Kondisi Kekinian

Tujuan	*Input*	Proses	*Output*
Menggali data dan informasi terkait kondisi kekinian dari risiko pada pengelolaan insiden dan pemenuhan permintaan layanan	Kondisi ideal berdasarkan standar acuan, *Interview Protocol*.	1. Menyiapkan *interview protocol* yang telah dirancang dalam tahap persiapan. 2. Melakukan wawancara. 3. Melakukan observasi diruang kerja *helpdesk* Subdirektorat layanan TSI DPTSI.	Kondisi kekinian dan kondisi yang diharapkan oleh *helpdesk* subdirektorat layanan DPTSI terkait risiko pada pengelolaan insiden dan pemenuhan permintaan layanan

Pada Tabel, dapat diketahui tujuan yang ingin dicapai dari adanya tahapan penggalian kondisi kekinian, apa saja masukan yang dibutuhkan untuk melakukan penggalian kondisi kekinian dan bagaimana proses dari penggalian kondisi kekinian

tersebut, serta keluaran apa yang dihasilkan dari tahapan penggalian kondisi kekinian ini.

4.4.2 Observasi

Metode ini dilakukan dengan cara melakukan pengamatan secara langsung pada bagian *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI. Metode ini bertujuan untuk mendapatkan informasi mengenai kondisi nyata yang terjadi dalam kegiatan pengelolaan insiden dan pemenuhan permintaan layanan. Selain itu, dengan adanya metode ini penulis dapat mempelajari kondisi yang sesungguhnya terhadap kinerja *helpdesk* dalam melayani dan mengelola insiden mulai dari mengidentifikasi insiden, mencatat dan membuat *log* insiden, eskalasi, sampai menutup insiden.

4.4.3 Pengkajian Dokumen

Pengkajian dokumen dilakukan dengan cara menganalisis dokumen tugas pokok fungsi *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi, dokumen *log* insiden yang berasal dari Sistem Informasi *helpdesk*, dan dokumen terkait risiko *helpdesk* dan dokumen pendukung lain untuk melengkapi bukti dalam menganalisis dan menilai risiko berdasarkan pendekatan COBIT 5.

Berikut merupakan pemetaan perancangan penggalian data kondisi kekinian untuk penelitian ini yang ditunjukkan pada Tabel 4.6.

Tabel 4.6 Pemetaan Penggalian Data Kondisi Kekinian

Tujuan	*Goals*	Sumber
Metode Wawancara		
Mendapatkan informasi terkait kondisi kekinian dari proses bisnis *helpdesk* dalam menangani insiden maupun layanan di Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI.	• Proses bisnis *helpdesk* • Struktur organisasi *helpdesk* • Layanan yang ditangani *helpdesk* • Tugas pokok fungsi *helpdesk* • Standar acuan *helpdesk* • Pengelolaan manajemen insiden dan pemenuhan permintaan layanan TI. • Sistem Informasi *helpdesk*	COBIT 5 – DSS02 *Manage Service Requests and Incidents*
Untuk mendapatkan detail informasi terkait kesalahan dan risiko yang kerap muncul dari proses pengelolaan insiden dan pemenuhan permintaan layanan oleh *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI..	• Kesalahan yang kerap terjadi pada *helpdesk* saat mengelola insiden dan memenuhi permintaan layanan. • Risiko TI yang muncul dari proses pengelolaan insiden dan pemeuhan permintaan layanan	• COBIT 5 – APO12 *Manage Risks* • Penelitian Dyah Retnani Sulistya-ningrum [11]
Mendapatkan detail informasi terkait rencana lanjutan dalam menangani dan	• Kondisi kekinian organisasi terhadap risiko yang terjadi	COBIT 5 – APO12 *Manage Risks*

Tujuan	*Goals*	Sumber
mengantisipasi terjadinya risiko.	• Rencana atau strategi dalam menangani risiko.	
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* • Log pencatatan hingga penanganan permintaan layanan dan insiden	• COBIT 5 – DSS02 *Manage Service Requests and Incidents* • Penelitian Dyah Retnani Sulistya-ningrum [11]
Metode Analisis Dokumen		
Mengetahui kondisi kekinian *helpdesk* yang terdokumentasi	• Dokumen tupoksi *helpdesk* DPTSI • Dokumen log permintaan layanan dan insiden • Dokumen penelitian terkait risiko TI pada manajemen layanan TI	COBIT 5 – DSS02 *Manage Service Requests and Incidents* Dyah Retnani Sulistya-ningrum

4.4.4 Survei

Survei melalui kuesioner dilakukan untuk menghitung salah satu dampak (*magnitude*) risiko yaitu *competitive advantage* yang dapat dilihat dari segi penurunan kepuasan pelanggan. Penurunan kepuasan pelanggan dapat diukur melalui indeks yang dilakukan dengan pengisian kuesioner dengan mengambil sampel mahasiswa yang merupakan pengguna layanan unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem

Informasi. Jumlah pengguna layanan TI di lingkungan ITS sangat besar sehingga ruang lingkup populasi akan di spesifikkan untuk pengguna layanan TI dari seluruh mahasiswa Insitut Teknologi Sepuluh Nopember yaitu sekitar 15000 orang. Selanjutnya jumlah populasi ini akan dihitung menggunakan metode Slovin, yaitu metode yang digunakan untuk mencari jumlah sampel responden minimal. Rumus Slovin adalah [47]:

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

Keterangan:

n = Ukuran sampel
N = Jumlah Populasi
e = Presentase toleransi kesalahan karena kesalahan pengambilan sampel

Sehingga diperoleh:

$$n = \frac{15.000}{1+15000(0.15)^2}$$

$$n = \frac{15.000}{1+338.5}$$

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

Berdasarkan perhitungan tersebut, dengan nilai *e* = 0.15 didapatkan sebanyak 44 orang yang akan menjadi sampel dari populasi sebanyak 15.000 orang. Pada tahap ini akan digunakan metode *simple random sampling*, dimana akan dihasilkan data dari kuesioner yang didapatkan dari 44 responden tersebut.

4.4.5 Metode Pengolahan Data

Pengolahan hasil wawancara akan dilakukan dengan mendokumentasikan hasil wawancara yang tersimpan pada *recoreder* dengan menggunakan *Microsoft Word*. Jawaban dari narasumber dimasukkan kedalam tabel hasil wawancara dengan

cara mengedit dan menyusun kalimat dengan benar, sehingga dapat menjadi sebuah narasi deskriptif yang mudah dipahami. Kemudian, untuk melakukan penilaian risiko, dilakukan prioritasi terhadap risiko berdasarkan aspek frekuensi dan dampak (*magnitude*) risiko. *Tools* yang akan digunakan ialah *Microsoft Excel* untuk memudahkan penulisan tabel dan menghitung rata-rata nilai risiko.

4.5 Pendekatan Analisis

Setelah data terkumpul, selanjutnya dilakukan pendekatan analisis. Analisis ini dilakukan untuk mengetahui hubungan antara data yang didapat dengan pendekatan yang dilakukan untuk pengerjaan penelitian. Beberapa analisis yang akan dilakukan adalah:

1. Analisis dengan pendekatan konseptual, yaitu dilakukan analisis tugas pokok dan fungsi (tupoksi) *hepdesk* subdir layanan TSI DPTSI serta kondisi kekinian pengelolaan permintaan layanan dan insiden pada *helpdesk*. 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. Setiap alur dan proses ini nantinya akan disesuaikan dengan COBIT 5 DSS02.
2. 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.
3. Analisis penilaian risiko berdasarkan aspek frekuensi dan dampak terhadap risiko pada *risk event* berdasarkan *best practice* COBIT 5 *for Risk* APO12.
4. Analisis mitigasi risiko berdasarkan pemetaan proses TI yang sesuai standar COBIT 5.

4.6 Perancangan Penilaian Risiko

Penilaian risiko yang akan dibuat mengacu pada *template* yang disediakan dalam standar COBIT 5 *for Risk* pada proses

APO12. Aspek yang harus dibuat dalam penilaian risiko TI adalah tipe risiko, kategori risiko, faktor risiko, skenario risiko, respon risiko, pemetaan risiko terhadap proses di COBIT 5 dan justifikasi penilaian risiko.

4.6.1 Perancangan Pemetaan Analisis Risiko terhadap Proses di COBIT 5

Pemetaan kemungkinan risiko yang teridentifikasi terhadap proses *helpdesk* terkait pengelolaan permintaan layanan dan insiden berdasarkan COBIT 5 domain DSS02 dipetakan kepada proses di COBIT 5 yang sesuai. Berikut perancangan *template* pemetaan risiko terhadap proses ditunjukkan pada Tabel 4.7.

Tabel 4.7 Perancangan Pemetaan Risiko terhadap Proses DSS02 COBIT5

No.	Pemetaan Risiko Operasional (Aktivitas DSS02)	Risiko	Keterangan
1.	(ex. DSS01.01 Perform operational procedures)	Risiko 1	Keterangan Risiko 1
2.	(ex. DSS01.01 Perform operational procedures)	Risiko 2	Keterangan Risiko 2

4.6.2 Perancangan Tipe Risiko

Berikut perancangan tipe risiko berdasarkan tipe risiko yang disajikan pada Tabel 4.8.

Tabel 4.8 Perancangan Tipe Risiko

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

4.6.3 Perancangan Kategori Risiko

Berikut *template* untuk pemetaan risiko dengan kategori risiko yang sesuai disajikan dalam Tabel 4.9.

Tabel 4.9 Perancangan Kategori Risiko

No	Risk Category TI	ID Risiko	Risiko
1	*(ex. Portofolio establishment anda maintenance*)	(ex. PEM001)	Risiko 1
2	*(ex. IT investment decision making*)	(ex. IDM001)	Risiko 2

4.6.4 Perancangan Pemetaan Faktor Risiko

Berikut perancangan *template* pemetaan faktor risiko kontekstual yang disajikan pada Tabel 4.10.

Tabel 4.10 Perancangan Faktor Kontekstual Risiko

No.	Risiko	Faktor Risiko Kontekstual	
		Internal	External
1.	Risiko 1	(ex. ***Culture of the enterprise*** *penjelasan aspek faktor*)	(ex. ***Regulatory environment*** *penjelasan aspek faktor*)
2.	Risiko 2	(ex. ***Financial capacity*** *penjelasan aspek faktor*)	(ex. ***Competitive environment*** *penjelasan aspek faktor*)

4.6.5 Perancangan Skenario Risiko

Berikut perancangan *template* skenario (dampak) risiko ditunjukkan pada Tabel 4.11.

Tabel 4.11 Perancangan Skenario Risiko

No.	Risiko	Skenario Risiko	
		Skenario Negatif	Skenario Positif
1.	Risiko 1	Pemaparan skenario negatif	Pemaparan skenario positif

4.6.6 Perancangan Justifikasi Penilaian Risiko

Penilaian risiko diidentifikasi berdasarkan aspek frekuensi dan dampak (*magnitude*) risiko.

4.6.6.1 Frekuensi

Frekuensi risiko menunjukkan banyaknya risiko yang terjadi dalam satu periode tertentu, biasanya satu periode dihitung selama satu tahun. Berikut merupakan perancangan justifikasi ukuran parameter yang digunakan dalam menentukan tingkat terjadinya risiko yang disajikan dalam Tabel 4.12.

Tabel 4.12 Perancangan Justifikasi Frekuensi Risiko

Peringkat Frekuensi	Frekuensi Risiko	Keterangan
1	$0{,}01 < N \leq 0{,}1$	***Very Low*** - Kemungkinan risiko terjadi sangat rendah. - Ada kemungkinan risiko terjadi dalam keadaan yang sangat khusus (kemungkinan kecil). - Frekuensi kegagalan terjadi lebih dari 0,01 kali dan kurang dari sama dengan 0,1 kali dalam satu tahun.
2	$0{,}1 < N \leq 1$	***Low*** - Kemungkinan risiko terjadi rendah. - Risiko 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 risiko terjadi cukup tinggi. - Risiko 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 risiko terjadi tinggi.

Peringkat Frekuensi	Frekuensi Risiko	Keterangan
		- Ada kemungkinan risiko 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*** - Risiko sangat tidak mungkin untuk dihindari. - Risiko 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.

4.6.6.2 Dampak (*Magnitude*)

Dampak (*magnitude*) risiko merupakan pengukuran tingkat keparahan potensi kerugian atau keuntungan/kesempatan dari terjadinya risiko terhadap bisnis, yang diukur dari aspek produktivitas (*productivity*), biaya tanggapan (*cost of response*), keunggulan kompetitif (*competitive advantage*), dan hukum (*legal*) di mana setiap dampak memiliki pengukuran parameter. Berikut adalah tabel perancangan justifikasi dampak (*magnitude*) risiko yang disajikan pada Tabel 4.13.

Tabel 4.13 Perancangan Justifikasi Dampak (*Magnitude*) Risiko

Peringkat Dampak	Dampak			
	Produktivitas	**Biaya Tanggapan**	**Keunggulan Kompetitif**	**Hukum**
	Kerugian Pendapatan Selama Satu Tahun	Beban terkait dengan Mengelola Kejadian yang Merugikan	Penurunan Kepuasan Pengguna	Kepatu-han terhadap Peraturan – Denda
1	0,1%<I≤1%	Rp100K<I≤Rp1juta	0,5 < 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≤Rp500juta	2 < I ≤ 2,5	<Rp500 juta
5	10%<I	Rp500 juta<I	2,5 < I	>Rp500 juta

Keterangan: I (*Impact*) adalah dampak risiko.

Ke-empat dampak tersebut kemudian dirata-rata sehingga memiliki satu penilaian peringkat dampak. Berikut pemaparan secara detail untuk justifikasi pengukuran parameter dampak risiko untuk setiap aspek.

c. Produktivitas (*Productivity)*

Produktivitas dilihat dari dampak kerugian finansial yang dialami ITS selama kurun waktu satu tahun. Bentuk kerugian yang dialami ITS dapat dilihat dari beberapa aspek, antara lain:

- Lambatnya kinerja staff DPTSI yang mengelola permintaan layanan dan insiden sehingga proses bisnis ITS terhambat.
- Kerugian finansial yang dimiliki 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 yang disajikan pada Tabel 4.14.

Tabel 4.14 Perancangan Justifikasi Dampak Risiko (Aspek Produktivitas)

Peringkat Dampak	**Produktivitas**	
	Rugi Pendapatan Selama Satu Tahun	Keterangan
1	0,1%<I≤1%	***Very Low*** - Kegagalan menimbulkan kerugian yang sangat rendah - Kerugian yang dialami melalui beberapa aspek sebesar lebih dari 0,1% dan kurang dari sama dengan 1% dalam satu tahun
2	1%<I≤3%	***Low*** - Kegagalan menimbulkan kerugian yang rendah - 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%

d. Biaya Tanggapan (*Cost of Response*)

Biaya tanggapan (*cost of response*) merupakan biaya yang harus dikeluarkan oleh organisasi (ITS) dalam menangani yang merugikan dari setiap risiko yang terjadi. Berikut merupakan perancangan justifikasi dari aspek biaya tanggapan yang ditunjukkan pada Tabel 4.15.

Tabel 4.15 Perancangan Justifikasi Dampak Risiko (Aspek Biaya Tanggapan)

Peringkat Dampak	**Biaya Tanggapan**	
	Beban terkait dengan Mengelola Kejadian yang Merugikan	Keterangan
1	Rp100K<I≤Rp1juta	***Very Low*** Untuk menangani skenario risiko, organisasi mengeluarkan biaya yang sangat rendah, yaitu lebih dari seratus ribu rupiah dan 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***

Peringkat Dampak	Biaya Tanggapan	
	Beban terkait dengan Mengelola Kejadian yang Merugikan	Keterangan
		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.

e. Keunggulan Kompetitif (*Competitive Advantage*)
Keunggulan kompetitif diukur dari penurunan kepuasan pengguna layanan akibat terjadinya skenario risiko. Indeks kepuasan pengguna nantinya didapatkan dari hasil survei yang dilakukan oleh DPTSI kepada pengguna layanan. Berikut merupakan perancangan justifikasi dampak risiko aspek keunggulan kompetitif yang ditunjukkan pada Tabel 4.16.

Tabel 4.16 Perancangan Justifikasi Dampak Risiko (Aspek Keunggulan Kompetitif)

Peringkat Dampak	Keunggulan Kompetitif		
	Penurunan Kepuasan Pengguna	**Rentan Skala Likert Kuesioner**	**Keterangan**
1	I ≤ 1	1,00 – 1,50	***Very Low*** Kegagalan menyebabkan penurunan kepuasan

Peringkat Dampak	Keunggulan Kompetitif		
	Penurunan Kepuasan Pengguna	Rentan Skala Likert Kuesioner	Keterangan
			pelanggan yang sangat tidak signifikan (sangat rendah) terhadap layanan sistem
2	$1 < I \leq 1,5$	1,51 – 2,50	***Low*** Kegagalan menyebabkan penurunan kepuasan pelanggan yang tidak signifikan (rendah) terhadap layanan sistem
3	$1,5 < I \leq 2$	2,51 – 3,50	***Moderate*** Kegagalan menyebabkan penurunan kepuasan pelanggan cukup tidak signifikan (netral) terhadap layanan sistem
4	$2 < I \leq 2,5$	3,51 – 4,50	***High*** Kegagalan menyebabkan penurunan kepuasan pelanggan yang signifikan (tinggi) terhadap layanan sistem
5	$2,5 < I$	4,51 – 5,00	***Very High*** Kegagalan menyebabkan penurunan kepuasan pelanggan yang sangat signifikan (tinggi) terhadap layanan sistem

4.6.6.1 Perancangan Kuesioner Risiko

Berikut merupakan template perancangan kuesioner dimana pertanyaannya didasarkan pada dampak (skenario) risiko yang diajukan untuk pengguna layanan sistem DPTSI yang disajikan pada Tabel 4.17. Untuk kuesioner lengkap terdapat pada **LAMPIRAN D**.

Tabel 4.17 Perancangan Kuesioner Risiko

ID Per-nyataan	Pernyataan	1	2	3	4	5
K01	Pertanyaan Kuesioner 1					
K02	Pertanyaan Kuesioner 2					

4.6.6.2 Perancangan Pemetaan Kuesioner dengan Risiko

Berikut merupakan *template* pemetaan pertanyaan kuesioner dengan risiko untuk memudahkan melihat hasil kuesioner dimana pemetaan dilakukan berdasarkan persamaan dampak (skenario) risiko yang disajikan pada Tabel 4.18.

Tabel 4.18 Perancangan Kuesioner Risiko

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
K01	Pertanyaan Kuesioner 1 :	Risiko 1	Pemaparan skenario positif	Pemaparan skenario negatif
		Risiko 2	Pemaparan skenario positif	Pemaparan skenario negatif

f. Hukum (*Legal*)

Aspek Hukum merupakan dampak berupa biaya denda yang harus ditanggung oleh organisasi (ITS) akibat terjadinya risiko yang berdampak pada hukum. Nilai pengukurannya berupa biaya denda (rupiah)

yang harus ditanggung oleh organisasi. Berikut merupakan perancangan justifikasi penilaian dampak risiko berdasarkan aspek hukum yang ditunjukkan pada Tabel 4.19.

Tabel 4.19 Perancangan Justifikasi Dampak Risiko (Aspek 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.

Dan berikut merupakan *template* untuk penilaaian dampak (*magnitude*) risiko yang meliputi ke-empat aspek dampak risiko yang disajikan pada Tabel 4.20.

Tabel 4.20 Perancangan Template Penilaian Risiko

ID Risiko	Risiko	Peringkat Frekuensi	Peringkat Dampak					Level Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Rata-Rata Peringkat Dampak	
(ex. PEM001)	Risiko 1	(ex. 2)	(ex. 1)	(ex. 2)	(ex. 1)	(ex. 3)	(ex.2)	(ex. Medium)

4.6.7 Perancangan Respon Risiko

Berikut merupakan tabel perancangan untuk *template* respon risiko berdasarkan pilihan respon risiko menurut COBIT 5, yaitu *risk acceptance* (diterima), *mitigation* (mitigasi), *avoidance* (dihindari), *share/transfer* (dialihkan) yang disajikan pada Tabel 4.21.

Tabel 4.21 Perancangan Respon Risiko

Kategori Risiko	ID Risiko	Risiko	Respon Risiko
(ex. Portofolio establishment and a maintenance)	(ex. PEM001)	Risiko 1	(ex. Mitigate (Treat))
(ex. IT investment decision making)	(ex. IDM001)	Risiko 2	(ex. Avoid)

4.6.8 Perancangan Pemetaan Proses TI Mitigasi Risiko

Berikut merupakan *template* perancangan pemetaan risiko dengan proses TI COBIT 5 yang sesuai sebagai langkah mitigasi risiko yang disajikan pada Tabel 4.22.

Tabel 4.22 Perancangan Pemetaan Proses TI Mitigasi Risiko

Kategori Risiko TI	ID	Risiko	Pemetaan Dengan Proses COBIT 5	Langkah Mitigasi	Pe-nanggung Jawab
(ex. *IT experti se and skill)*	(ex. IES 001)	Risiko 1	(ex. APO07 *Manage Human Resource*)	(ex. **APO07.03** ***Maintain the skills and competencie s of personnel*** - dan keamanan)	*(ex: Manager*)

"Halaman ini sengaja dikosongkan"

BAB V
IMPLEMENTASI

Pada bab ini menjelaskan hasil dari proses penentuan studi kasus dan perancangan perangkat penggalian data yang didapatkan melalui wawancara dan observasi

5.1 Hasil Wawancara

Berdasarkan perancangan perangkat penggalian data, telah diketahui bahwa narasumber yang dituju adalah unit *helpdesk* Subdir Layanan TSI, yaitu Ibu Mudjiyatin, Bapak Jainul Arifin, Ibu Wiwin Rochmawati dan Ibu Widyaningsih serta Koordinator Subdir Layanan TSI DPTSI yaitu Ibu Hanim Maria Astuti. Wawancara telah dilakukan pada Digital Innovation Lounge DPTSI ITS pada tanggal 24 November 2016 dan 5 Desember 2016 yang secara detail dapat dilihat pada **LAMPIRAN B**. Dari hasil wawancara dan observasi tersebut didapatkan beberapa fakta atau temuan yang menggambarkan kondisi kekinian proses pengelolaan insiden dan pemenuhan permintaan layanan serta risiko yang kerap muncul beserta pengelolaannya yang secara singkat diuraikan dalam poin berikut.

- Pelanggan DPTSI adalah unit didalam ITS.
- Subdirektorat layanan TSI terdiri dari 1 kepada subdirektorat, 1 kepala divisi dan 4 *helpdesk.*
- *Helpdesk* sudah memanfaatkan peran TI dalam proses penanganan insiden dan pemenuhan permintaan layanannya yaitu melalui sistem *e-ticket* ITS.
- Alur proses pelaporan permitaan yaitu pengguna melaporkan permintaan atau keluhannya kepada *helpdesk* baik melalui telepon, *e-mail*, maupun sistem *e-ticket*, kemudian *helpdesk* memproses permintaannya, kemudian melakukan eskalasi kepada *helpdesk* yang ahli dibidangnya, kemudian pengguna langsung berhubungan dengan *helpdesk* yang menangani bidang tersebut, lalu diberikan pengguna diberikan solusi, pengguna memberikan umpan balik, kemudian permintaan ditutup.

- Proses pengelolaan insiden dan layanan belum mengacu pada standar tertentu.
- Ada beberapa tahap penting yang dilewatkan *helpdesk* dalam menjalankan proses pengelolaan insiden dan pemenuhan permintaan layanan, seperti tidak mencatat keluhan yang masuk, tidak mendokumentasikan alurnya serta tidak membuat laporan pada setiap permintaan yang masuk.
- Sebelumnya belum pernah dilakukan terkait penelitian manajemen risiko pada *helpdesk* subdir layanan DPTSI.
- Proses pengelolaan risiko pada *helpdesk* juga belum mengacu pada standar tertentu.

5.2 Gambaran Umum Direktorat Pengembangan Teknologi dan Sistem Informasi

Direktorat Pengembangan Teknologi dan Sistem Informasi bertugas untuk menyediakan dan mengelola layanan teknologi informasi di lingkungan ITS. Terkait peran, DPTSI berperan untuk mendukung aktivitas akademik, penelitian dan pengabdian masyarakat, serta manajerial di lingkungan ITS dalam rangka membantu ITS mencapai visi misinya. Direktorat Pengembangan Teknologi dan Sistem Informasi dipimpin oleh seorang Direktur, yang dalam menjalankan tugasnya bertanggung jawab kepada Wakil Rektor III [48].

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.

Struktur Organisasi DPTSI

DPTSI dipimpin oleh seorang direktur bernama Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom yang dibawahnya memiliki tiga Kepala Subdirektorat yang terdiri atas [48]:

a. Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi;
b. Subdirektorat Pengembangan Sistem Informasi yang dibantu oleh Seksi Pengembangan Aplikasi pada Perangkat Bergerak; dan
c. Subdirektorat Layanan Teknologi dan Sistem Informasi yang dibantu oleh Seksi Layanan Data dan Informasi.

Direktorat Pengembangan Teknologi dan Sistem Informasi dipimpin oleh seorang Direktur, yang dalam menjalankan tugasnya bertanggung jawab kepada Wakil Rektor III. Berikut merupakan gambaran struktur organisasi DPTSI ITS yang disajikan pada Bagan

Bagan 5.1 Struktur Organisasi DPTSI

Tugas Pokok dan Fungsi DPTSI

Direktorat Pengembangan Teknologi dan Sistem Informasi mempunyai tugas melaksanakan penyiapan perumusan kebijakan pengembangan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi,

pemeliharaan, dan pelaporan di bidang teknologi dan sistem informasi. Dalam melaksanakan tugasnya, Direktorat Pengembangan Teknologi dan Sistem Informasi menyelenggarakan fungsi [48]:

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

5.3 Gambaran Umum Sub Direktorat Layanan Teknologi dan Sistem Informasi DPTSI

Sub Direktorat Layanan Teknologi dan Sistem Informasi DPTSI ITS adalah satu dari tiga sub direktorat yang mendukung fungsi Direktorat Pengembangan Teknologi dan Sistem Informasi dalam menyediakan dan mengelola layanan teknologi dan sistem informasi.

Menurut Peraturan Rektor Nomor 10 tahun 2016 tentang OTK ITS [48], Subdirektorat Layanan Teknologi dan Sistem Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, operasional layanan, pengawasan dan pemantauan, evaluasi, dan pelaporan untuk layanan teknologi dan sistem informasi. Dalam melaksanakan tugas, Subdirektorat Layanan Teknologi dan Sistem Informasi menyelenggarakan fungsi [48]:

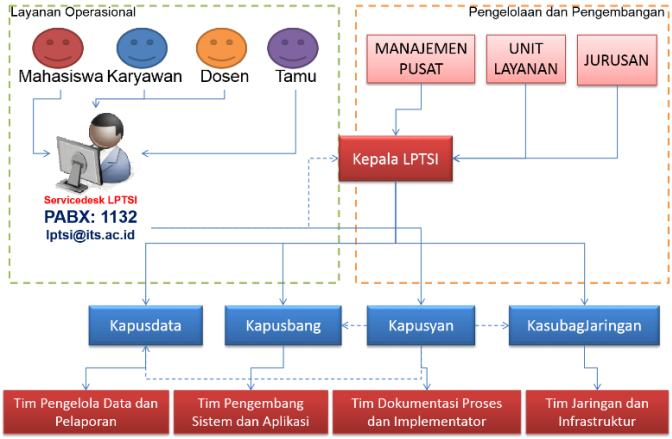
a. penyiapan bahan perumusan kebijakan dan standar mutu layanan teknologi dan
b. sistem informasi;
c. pelaksanaan operasional layanan teknologi dan sistem informasi;
d. pelaksanaan pengawasan dan pemantauan layanan teknologi dan sistem informasi;
e. pelaksanaan evaluasi dan pelaporan layanan teknologi dan sistem informasi.

Subdirektorat Layanan Teknologi dan Sistem Informasi dipimpin oleh seorang Kepala Subdirektorat yang dalam

melaksanakan tugasnya bertanggung jawab kepada Direktur Pengembangan Teknologi dan Sistem Informasi. Kepala Sub Direktorat Layanan Teknologi dan Sistem Informasi memiliki bawahan yaitu Kepala Divisi Layanan Teknologi dan Sistem Informasi, yang dalam sehari-harinya membantu pelaksanaan tupoksi Sub direkotorat Layanan dan melaksanakan tugas khusus dari pimpinan.

5.3.1 Gambaran Umum *Helpdesk* Sub Direktorat Layanan Teknologi dan Sistem Informasi DPTSI

Helpdesk merupakan unit fungsional yang dimiliki DPTSI, tepatnya dari Sub Direktorat Layanan Teknologi dan Sistem Informasi di DPTSI ITS. *Helpdesk* menangani berbagai macam keluhan dan permasalahan layanan TI yang terjadi di lingkungan ITS. Permasalahan layanan yang dikelola oleh *helpdesk* terkait dengan insiden layanan TI, permintaan layanan TI, serta pengelolaan akses pengguna terhadap layanan TI, dimana yang termasuk pengguna layanan TI di lingkungan ITS adalah mahasiswa, karyawan, dosen dan tenaga kependidika serta tamu. Pengguna layanan ini dapat menyampaikan permasalahan dan keluhan yang dialami ketika menggunakan layanan TI kepada *helpdesk*. Penyampaian permasalahan dan keluhan dapat dilakukan kepada *helpdesk* DPTSI melalui email dptsi@its.ac.id, www.umpanbalik.its.ac.id, atau datang secara langsung ke DPTSI untuk menyampaikan permasalahan [1]. Berikut *service desk flow* yang digunakan oleh DPTSI saat ini yang ditunjukkan pada gambar 2.12 sebagai berikut:

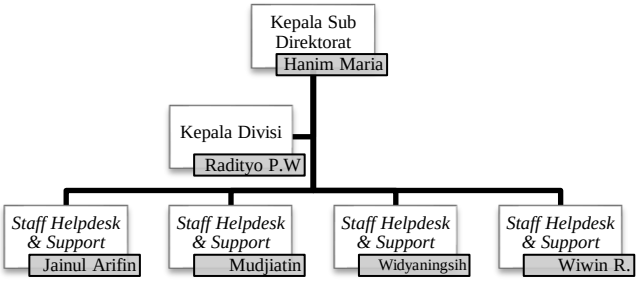


Gambar 5.1 Alur Layanan (*Helpdesk Flow*) DPTSI [1]

Helpdesk dipimpin oleh Kepala Subdirektorat, yaitu Ibu Hanim Maria Astuti dan dan Kepala Divisi, yaitu Bapak Radityo Prasetianto Wibowo. *Helpdesk* Subdir Layanan TSI DPTSI terdiri dari empat orang yang masing-masing memiliki bidang keahlian khusus, yaitu:

1. Ibu Mudjiyatin sebagai *helpdesk* terkait pengelolaan e-mail dan komplain pengguna serta sebagai administrator umum
2. Ibu Wiwin Rochmawati sebagai *helpdesk* terkait website, *domain* dan *hosting*
3. Bapak Jainul Arifin sebagai *helpdesk* terkait pengelolaan e-mail dan komplain pengguna serta sebagai administrator umum
4. Ibu Widyaningsih sebagai *helpdesk* terkait manajemen user, SIM dan Office365.

Berikut merupakan struktur organisasi dari unit *helpdesk* di Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS yang disajikan pada Bagan 5.1.



Bagan 5.2 Struktur Organisasi Helpdesk DPTSI

Sehari-harinya *helpdesk* sudah memanfaatkan peran TI dengan menggunakan *e-mail* dan sistem *e-ticket* berbasis *website* sebagai sarana untuk user menyampaikan keluhan maupun permintaannya. Berikut merupakan tugas pokok fungsi unit *helpdesk* DPTSI yang disajikan pada Tabel 5.1 [49].

Tabel 5.1 Tugas Pokok Fungsi Unit Helpdesk DPTSI [49]

No.	Tugas Pokok dan Fungsi
Mengelola keluhan dari pengguna layanan LPTSI	
1	Mempersiapkan *helpdesk* dan perlengkapannya
2	Menerima keluhan, melakukan pencatatan dan kategorisasi keluhan layanan
3	Melakukan troubleshoot atas keluhan yang diterima oleh subdit LTSI a. *Troubleshoo*t terkait email b. *Troubleshoot* terkait penggunaan *software* berlisensi c. *Troubleshoot* terkait penggunaan *software* dan os
4	Melakukan eskalasi keluhan ke subdit Pengembangan Sistem Informasi (PSI) atau IKTI (Infrastruktur dan Keamanan Teknologi Informasi) apabila penanganan di luar kapasitas helpdesk

No.	Tugas Pokok dan Fungsi
5	Memantau penanganan keluhan
6	Menginformasikan status keluhan kepada pengguna yang mengalami insiden/masalah
7	Meng-*update* 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

5.4 Gambaran Umum Proses Manajemen Insiden dan Pemenuhan Permintaan Layanan Sub Direktorat Layanan TSI

Salah satu tugas pokok dari unit *helpdesk.* Sub Direktorat Layanan Teknologi dan Sistem Informasi DPTSI adalah melakukan pengelolaan insiden dan memenuhi permintaan layanan dengan baik. Karena pengelolaan insiden dan permintaan layanan merupakan hal yang akan berhubungan langsung dengan pengguna layanan, maka *helpdesk* harus selalu sigap dalam memenuhi permintaan maupun keluhan yang masuk dari pengguna layanan. Pengelolaan insiden dan layanan yang baik harus sesuai prosedur mulai dari pelaporan, pencatatan, eskalasi sampai pendokumentasian laporan.

Berdasarkan wawancara yang dilakukan kepada unit *helpdesk* subdir layanan DPTSI, skenario pelaporan insiden maupun permintaan layanan, adalah pengguna membuat pengaduan kepada salah satu *helpdesk*, dan dapat diselesaikan langsung oleh *helpdesk*, apabila *helpdesk* yang menerima tersebut tidak dapat menyelesaikan permintaan pengguna, makan akan diteruskan ke *helpdesk* yang lebih ahli di bidangnya sesuai dengan permasalahan/permintaan pengguna, kemudian pengguna akan berhubungan langsung dengan *helpdesk* yang akan menyelesaikan permintaannya dan sudah tidak berurusan dengan *helpdesk* yang pertama.

Proses pelaporan insiden pada subdir layanan DPTSI dapat dilakukan menggunakan tiga saluran, yaitu melalui telepon, *e-mail*, maupun sistem *e-ticket*. Untuk ketiga saluran tersebut terdapat 2 adminstrator umum namun juga merupakan salah satu *helpdesk* subdir layanan DPTSI. Ketika user melaporkan keluhan maupun permintaannya, *helpdesk* menerima insiden maupun permintaan yang masuk, jika administrator tersebut tidak dapat menangani insiden maupun permintaan yang diinginkan pengguna, maka admin akan mengalihkan permintaan tersebut kepada *helpdesk* lainnya yang lebih ahli di bidangnya. Ketika insiden maupun permintaan telah berhasil ditangani dan diselesaikan, selanjutnya pengguna akan diminta umpan balik mengenai layanan tersebut, kemudian status insiden maupun permintaan ditutup dengan meminta persetujuan pengguna terlebih dahulu, namun jika pengguna tidak merespon melebihi batas waktu yang ditentukan, maka insiden akan ditutup secara otomatis oleh adminstrator.

Pada studi kasus yang digunakan oleh penulis, pengelolaan insiden maupun permintaan yang dilakukan oleh *helpdesk* subdir layanan DPTSI masih sangat jauh dari proses ideal berdasarkan kerangka kerja COBIT 5. Pengelolaan insiden dan permintaan layanan yang dilakukan pada studi kasus beberapa diantaranya terdapat beberapa aktivitas pada domain DSS02 COBIT 5 yang tidak dilakukan, seperti tidak selalu dicatatnya permintaan yang masuk, tidak melakukan

analisis tren, tidak dibuatnya dokumentasi laporan per insiden maupun permintaan yang masuk. Hal ini disebabkan tidak ada pendekatan yang konsisten seperti tidak adanya *log* tempat pencatatan insiden, tidak diharuskannya pembuatan laporan untuk masing-masing insiden maupun tidak ada standar acuan yang diterapkan oleh unit *helpdesk* subdir layanan DPTSI. Hal ini tentunya mengurangi performa kualitas pengelolaan insiden dan permintaan layanan oleh subdir layanan TSI. Untuk lebih jelasnya, pemetaan hasil observasi kondisi proses TI pada *helpdesk* dengan kondisi ideal pada COBIT 5 dapat dilihat pada **LAMPIRAN C.**

5.5 Proses Manajemen Insiden Berdasarkan Standard

Proses pengelolaan insiden merupakan sebuah aktivitas yang harus diberikan perhatian cukup tinggi oleh perusahaan. mengingat insiden merupakan suatu perisitwa yang tidak direncanakan bahkan mungkin tidak terduga yang terjadi pada layanan TI sehingga dapat menurunkan kualitas layanan TI. Dengan adanya manajemen insiden, diharapkan proses bisnis dapat segera diperbaiki agar kembali pulih sehingga bisa berjalan normal sehingga bisa meminimalisir dampak. Berdasarkan standar yang digunakan pada penelitian ini, yaitu *domain* DSS02 *Manage Incidents and Request*s COBIT 5, berikut merupakan proses pengelolaan insiden dan layanan ideal sesuai standar yang disajikan pada Tabel 5.2.

Tabel 5.2 Proses Manajemen Insiden Berdasarkan Standard

Proses DSS02 COBIT 5
DSS02.01 Mendefinisikan insiden dan skema klasifikasi permintaan layanan
DSS02.02 Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden
DSS02.03 Memverifikasikan, menyetujui dan memenuhi permintaan layanan
DSS02.04 Menginvestigasikan, mendiagnosis dan mengalokasikan insiden
DSS02.05 Menyelesaikan dan melakukan pemulihan insiden
DSS02.06 Menutup permintaan layanan dan insiden

Proses DSS02 COBIT 5
DSS02.07 Melacak status dan membuat laporan

5.6 Risiko Proses Pengelolaan Insiden dan Pemenuhan Permintaan Layanan pada *Helpdesk*

Sebelum melakukan analisis risiko TI yang terjadi pada *helpdesk* Subdirektorat Layanan TSI DPTSI, dilakukan penggalian informasi terkait kemungkinan risiko yang akan terjadi pada setiap proses pada alur pengelolaan insiden dan permintaan layanan TI. Berikut merupakan daftar risiko yang diperoleh melalui analisis penelitian sebelumnya [11] dan kondisi kekinian dari penggalian data di *helpdesk* Subdirektorat Layanan DPTSI yang disajikan pada Tabel 5.3.

Tabel 5.3 Analisis Risiko pada *Helpdesk*

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
DSS02.01 – Menetapkan skema klasifikasi insiden dan layanan permintaan				
1.	Menetapkan dan mendefinisikan klasifikasi permintaan layanan dan skema prioritisasi beserta kriteria untuk pendaftaran masalah, untuk memastikan pendekatan yang konsisten dalam menangani, menginformasikan	Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan permintaan layanan	*Helpdesk* melakukan kesalahan dalam pembuatan sistem kategorisasi atau prioritasi insiden dan permintaan layanan. Kesalahan bisa berupa sistem kategorisasi atau prioritasi yang tidak relevan dengan	*Helpdesk* tidak memiliki pengetahuan yang memadai terkait pembuatan sistem prioritasi dan kategorisasi layanan TI yang baik dan benar

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
	pengguna dan melakukan analisis tren.		layanan TI, sistem kategorisasi atau prioritasi tidak lengkap.	
2.	Mendefinisikan bentuk insiden untuk mengetahui kesalahan untuk membuat resolusi yang efisien dan efektif.	Kesalahan *entry* data dari pengguna (pelapor)	Pengguna (pelapor) salah memberikan informasi terkait insiden atau permintaan layanan TI yang mereka ajukan, seperti memasukkan NRP yang salah, tanggal yang salah, kode jurusan yang salah, nama yang salah.	Pengguna tidak teliti atau *human error* pada saat mengisikan detail informasi yang diminta
3.		Kegagalan akses sistem *e-ticket*	Sistem *e-ticket* tidak dapat digunakan oleh pengguna untuk melaporkan insiden	Adanya *error* atau *bug* pada sistem

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
			dan meminta layanan TI yang disebabkan oleh *error* atau *bug*	
4.	Mendefinisikan model permintaan layanan berdasarkan tipe permintaan layanan untuk memungkinkan dilakukan secara mandiri dan layanan yang efisien untuk permintaan yang standar.	Kesalahan memahami permintaan pengguna	*Helpdesk* melakukan kesalahan dalam memahami detail dan informasi dari permintaan atau insiden yang diajukan oleh pengguna	*Helpdesk* lalai atau tidak teliti (*human error*) pada saat membaca detail dan informasi permintaan layanan TI atau insiden yang masuk seperti nama insiden atau permintaan layanan, penyebab awal kejadian, kategori dan priroritas insiden atau layanan.
5.	Mendefinisikan pengetahuan permintaan layanan dan kegunaannya.			

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
6.	Mendefinisikan peraturan dan prosedur eskalasi insiden, terutama untuk insiden utama dan insiden keamanan.	*Helpdesk* lupa atau tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	*Helpdesk* lupa atau sengaja tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	*Helpdesk* tidak responsif dalam memberikan informasi kepada unit pengelola insiden dan permintaan layanan
DSS02.02 – Mencatat, mengklasifikasikan dan Memprioritaskan Permintaan dan Insiden				
7.	Menetapkan dan mendefinisikan klasifikasi permintaan layanan dan skema prioritisasi beserta kriteria untuk pendaftaran masalah, melakukan pencatatan semua permintaan dan insiden serta semua informasi yang terkait, sehingga bisa di tangani secara efektif	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk sehingga tidak terdapat log insiden atau permintaan layanan TI	Proses pengelolaan insiden dan permintaan layanan TI dan layanan tidak diawasi dan tidak mengacu pada standar tertentu

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
	dan laporan tersebut bisa dipelihara.			
8.	Untuk memungkinkan analisis tren, diperlukan klasifikasi permintaan layanan dengan melakukan identifikasi tipe dan kategori dari permintaan tersebut.	Kesalahan pengalokasian kategorisasi atau prioritas insiden dan permintaan layanan	*Helpdesk* melakukan kesalahan dalam mengalokasikan insiden dan permintaan layanan kategori atau prioritas yang tepat dan relevan seperti *helpdesk* mengalokasikan insiden dan permintaan layanan ke kategori yang tidak relevan, serta mendahulukan insiden atau permintaan layanan yang tingkat	*Helpdesk* tidak memahami sistem kategorisari atau sistem prioritas insiden yang tersedia.

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
			urgensitasnya lebih rendah dan dampaknya kecil.	
9.	Melakukan prioritisasi permintaan layanan berdasarkan definisi layanan dari SLA terhadap proses bisnis perusahaan dan tingkat urgensi.	Keterlambatan respon *helpdesk*	*Helpdesk* tidak segera menangani permintaan dan insiden yang masuk, sehingga pengelolaan layanan menjadi terhambat	*Helpdesk* tidak responsif dalam menangani insiden dan permintaan TI yang masuk
DSS02.03 – Melakukan Verifikasi, Menerima dan Memenuhi Permintaan Layanan				
10.	Melakukan verifikasi terhadap hak untuk menggunakan permintaan layanan, jika dimungkinkan, alur proses yang telah didefinisikan dan perubahan standar.	Penyalahgunaan hak akses permintaan layanan TI	Terdapat penyalahgunaan hak akses untuk permintaan layanan TI yang tidak sesuai dengan hal-hal yang didefinisikan dalam manajemen *user*.	Pengguna tidak memiliki dasar pengetahuan manajemen akses dan terdapatnya celah yang bisa diretas

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
11.	Memperoleh persetujuan finansial dan fungsional atau tanda tangan, jika dibutuhkan, atau persetujuan otomatis untuk persetujuan dalam perubahan yang standar.	*Helpdesk* tidak mengajukan persetujuan finansial dan fungsional yang dibutuhkan	Helpdesk lupa atau tidak mengajukan persetujuan finansial atau fungsional yang dibutuhkan untuk menangani insiden atau permintaan layanan TI	Proses pengelolaan insiden dan permintaan layanan TI dan layanan tidak diawasi dan tidak mengacu pada standar tertentu
12.	Melakukan pemenuhan 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.	Prosedur pengelolaan insiden tidak tersedia secara tertulis	Tidak tersedianya prosedur tertulis yang ditetapkan untuk pengelolaan insiden dan permintaan layanan yang dimiliki organisasi	
DSS02.04 – Menginvestigasi, Mendiagnosa dan Mengalokasikan Insiden				

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
13.	Mengidentifikasikan dan mendeksripsikan gejala yang relevan untuk mendirikan penyebab yang paling tepat dari insiden tersebut.	Kesalahan mendiagnosa gejala insiden	*Helpdesk* melakukan kesalahan dalam mendiagnosa insiden dikarenakan data dan informasi yang ada tidak lengkap	Kesalahan pendefinisian bentuk dan model insiden, data dan informasi terkait insiden tidak lengkap.
14.	Jika insiden tersebut tidak tersedia, buat sebuah log baru.	Kesalahan pencatatan (*logging)* insiden atau permintaan layanan	*Helpdesk* melakukan kesalahan pencatatan informasi insiden dan permintaan layanan, seperti kesalahan menulis nama pengguna, NRP, tanggal, kategori dan informasi lain sehingga data yang ada tidak sesuai	Terdapat kesalahan pencatatan kategori, tingkat prioritas, identitas pelapor, tanggal kejadian, status insiden atau permintaan layanan TI

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
15.		*Log* insiden atau permintaan layanan TI tidak lengkap	*Helpdesk* tidak mencatat informasi insiden dan permintaan layanan dengan detail, seperti tidak menulis nama pengguna, tanggal, kategori dan informasi lain sehingga data tidak lengkap. Log insiden atau permintaan layanan TI yang dibuat tidak disimpan pada direktori khusus, sehingga tidak helpdesk tidak memiliki log histori insiden dan	*Helpdesk* tidak mencatat detail informasi lengkap terkait layanan TI dan insiden yang masuk seperti identitas pelapor, nama insiden, tanggal kejadian, penyebab, status, prioritas, kategori, serta *log* insiden dan permintaan layanan TI tidak di evaluasi secara berkala oleh pihak manajemen

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
			permintaan layanan TI	
16.	Menetapkan insiden ke fungsi spesialis.	Kesalahan melakukan distribusi (eskalasi) insiden atau permintaan layanan TI	*Helpdesk* melakukan kesalahan dalam melakukan pengalihan/distribusi (eskalasi) insiden atau permintaan layanan dimana pihak yang di eskalasi tidak sesuai dengan bidang dan keahliannya.	*Helpdesk* lalai atau tidak teliti (*human error*) pada saat mendistribusikan insiden atau permintaan layanan TI ke pihak yang benar
17.		Pihak yang di eskalasi melakukan kesalahan penanganan insiden atau permintaan layanan TI	Pihak yang di eskalasi tidak menguasi penanganan insiden dan pemenuhan permintaan layanan TI yang diberikan karena	Data dan informasi yang tersedia tidak lengkap, adanya data yang tidak relevan, kurangnya pengetahuan

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
			kemampuannya tidak memadai	mengenai insiden atau permintaan layanan TI terkait
18.		Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan TI yang masuk	Pihak yang di eskalasi tidak menanggapi/ mengabaikan penanganan insiden dan pemenuhan permintaan layanan TI yang diberikan	Pihak yang di eskalasi kurang responsif dan tanggap dalam melaksanakan pekerjaannya
DSS02.05 – Melakukan Penyelesaian dan Pemulihan Insiden				
19.	Memilih dan menggunakan resolusi insiden yang tepat (*temporary workaround* dan/atau solusi tetap).	Sistem yang mendukung penanganan layanan TI tidak berfungsi	Sistem yang mendukung penanganan layanan TI seperti sistem informasi, *software* dan *hardware* tidak dapat digunakan atau tidak tersedia	Terdapat kegagalan seperti *malware*, *virus*, *bug* sistem atau kerusakan teknis pada sistem yang membantu

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
				penanganan insiden
20.	Mencatat *workaround* mana yang digunakan untuk melakukan resolusi insiden.	Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI	*Helpdesk* melakukan kesalahan dalam memilih solusi penanganan insiden dan layanan TI sehingga layanan tidak terselesaikan	*Helpdesk* tidak teliti dalam memilih solusi penanganan insiden yang sesuai dengan penyebab dan dampaknya
21.	Melakukan aksi pemulihan (jika dibutuhkan).	Kesalahan dalam melakukan eksekusi penanganan insiden atau pemenuhan layanan TI	Unit *helpdesk* melakukan kesalahan dalam menangani insiden atau permintaan layanan TI	*Helpdesk* melakukan kesalahan dalam pendefinisian bentuk dan model insiden, kesalahan, memasukkan kategorisasi insiden atau

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
				prioritasi insiden, kesalahan memilih solusi insiden.
		Penanganan insiden atau permintaan layanan TI melebihi batas waktu yang disepakati	Waktu penanganan insiden melebihi batas waktu yang ditentukan atau disepakati bersama atau diluar dari SLA (*Service Level Agreement*) yang dijanjikan kepada pengguna.	Terdapat hal yang menghambat proses penangan layanan seperti data yang tidak lengkap, *helpdesk slowrespon*, pihak yang dieskalasi tidak dapat dihubungi
22.	Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat dipakai sebagai sumber pengetahuan mendatang.	Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap	*Helpdesk* tidak membuat dokumentasi laporan penyelesaian insiden dan permintaan layanan TI untuk	Laporan insiden tidak berisikan detail informasi lengkap seperti berisikan nama insiden atau

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
			dijadikan catatan historis *helpdesk* yang berisikan nama insiden atau permintaan layanan, kategori, prioritas, tanggal kejadian, identitas pelapor, penyebab, pihak yang menangani, solusi permasalahan.	permintaan layanan, kategori, prioritas, tanggal kejadian, identitas pelapor, penyebab, pihak yang menangani, solusi permasalahan.
DSS02.06 – Menutup Permintaan Layanan dan Insiden				
23.	Melakukan verifikasi dengan pengguna yang berpengaruh (apabila setuju) bahwa layanan permintaan mereka telah dipenuhi dan diselesaikan dengan baik.	Ketidakpuasan pengguna terhadap layanan yang diberikan	Pengguna atau pelaporan insiden dan permintaan layanan TI tidak puas dengan pelayanan yang diberikan oleh *helpdesk* dalam	Kinerja unit helpdesk tidak sesuai dengan keinginan pengguna (pelapor)

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
			memenuhi permintaannya	
24.		Pengguna enggan memberikan *feedback* layanan TI	Pengguna tidak mau memberikan *feedback* terhadap penyelesaian insiden atau pemenuhan permintaan layanan TI yang diajukan	Kinerja unit helpdesk tidak sesuai dengan keinginan pengguna (pelapor) dan pengguna tidak puas terhadap pelayanan yang diberikan
25.	Menutup layanan permintaan dan insiden.	Pengguna tidak menyetujui status penutupan insiden	Pengguna tidak menyetujui status penutupan insiden yang diajukan oleh *helpdesk* karena masih belum puas terhadap pelayanan yang didapatkan	Kinerja unit helpdesk tidak sesuai dengan keinginan pengguna (pelapor)

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
26.		Pengguna tidak diinformasikan mengenai penutupan insiden	Pengguna tidak diberikan infromasi mengenai status penutupan insiden atau permintaan layanan TI yang diajukannya	*Helpdesk* tidak responsif serta tidak adanya sistem yang notifikasi penutupan insiden dan permintaan layanan TI.
27.		Pengguna tidak merespon penutupan insiden atau permintaan layanan TI	Penguna tidak merespon status penutupan insiden yang disediakan lewat sistem *e-ticket* maupun tidak membalas *e-mail* unit *helpdesk*	Pengguna tidak tanggap terhadap layanan TI yang diajukan atau pengguna belum puas terhadap pelayanan yang diberikan
DSS02.07 – Melacak Status dan Membuat Laporan				
28.	Mengawasi dan melacak eskalasi insiden dan resolusi dan penanganan	Ketidakjelasan status insiden atau permintaan layanan	*Helpdesk* tidak menginformasikan kepada pengguna	Tidak adanya sistem untuk mengecek status

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
	permintaan untuk melakukan progress penyelesaian. Mengidentifikasi informasi stakeholder dan kebutuhan mereka untuk pemenuhan data dan laporan. Idenfitikasi laporan secara berkala.		mengenai status insiden atau permintaan layanan TI yang dilaporkannya sehingga pengguna tidak mengetahui status penanganan laporannya.	insiden atau permintaan layanan TI yang dilaporkan pengguna, serta *helpdesk* tidak responsif dalam menginformasikan status insiden atau permintaan layanan TI kepada pengguna.
29.	Menganalisis insiden dan layanan permintaan dengan mengkategorisasikan tren.	Kesalahan pendefinisian tren dalam laporan	Kesalahan dalam mendefinisikan tren berupa pelaporan permintaan layanan dan insiden yang ada pada laporan sehingga menyebabkan sering	Helpdesk tidak memiliki pengetahuan yang memadai terkait proses pengelolaan insiden dan

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
			terulangnya insiden serupa, atau lamanya proses penanganan insiden dan permintaan layanan.	permintaan layanan TI
30.	Membuat dan mendistribusikan laporan berkala atau menyediakan *controlled access* ke *online data*.	Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan	Laporan yang dibuat tidak terdistribusi karena tidak terdapat pertemuan khusus yang membahas mengenai progres pengelolaan permintaan layanan dan insiden pada helpdesk, melainkan hanya melalui percakapan online (Whattsap). Serta kemungkinan risiko dokumen SKP (berisi	Pihak manajemen tidak mengawasi proses manajemen insiden dan permintaan layanan TI

No	Aktivitas DSS02 – Manage Service Requests and Incidents	Risiko	Keterangan	Penyebab
			hasil pekerjaan setiap staf helpdesk) tidak dapat di-upload ke sistem untuk dicek oleh KaSubDit)	
31.		Bocornya laporan kepada pihak lain	Laporan insiden bocor atau terdistribusikan kepada pihak yang tidak berwenang.	Terdapat celah keamanan yang dapat dimasuki pihak lain

Daftar kemungkinan risiko yang terjadi pada proses pengelolaan insiden dan permintaan layanan tersebut kemudian dianalisis lagi menggunakan pendekatan *domain* APO12-*Manage Risk* COBIT 5 untuk menentukan tipe, kategori, faktor (penyebab), dan skenario (dampak) risiko untuk dilakukan penilaian risiko.

5.5 Gambaran Umum Proses Manajemen Risiko Sub Direktorat Layanan TSI

Risiko merupakan sebuah peristiwa yang tidak dapat dihindari, sehingga perlu dilakukan pengelolaan khusus untuk mengatur risiko tersebut. Berdasarkan hasil wawancara, Sub Direktorat Layanan TSI belum pernah dilakukan penelitian terkait risiko sehingga belum pernah melakukan proses manajemen atau pengelolaan risiko dan tentunya belum ada penerapan standar khusus terkait manajemen risiko. Jika ada kesalahan atau risiko yang muncul, Subdir Layanan DPTSI hanya menerima atau melakukan antisipasi risiko jika risiko tersebut merugikan organisasi.

Karena organisasi ini tidak beriorientasi kepada keuntungan, maka risiko yang paling dihindari ialah risiko yang menurunkan kepuasan pelanggan dan risiko yang memakan banyak waktu.

Namun proses manajemen risiko yang dilakukan pada studi kasus ini masih sangat jauh dari proses ideal pada standar COBIT 5 *for risk*, bahkan hampir tidak ada aktivitas menurut COBIT 5 yang sudah diterapkan oleh Subdir layanan DPTSI, antisipasi yang sudah dilakukan untuk menghindari risiko pun juga tidak ada yang ditetapkan secara tertulis.

5.6 Proses Manajemen Risiko Berdasarakan Standard

Sama halnya dengan proses manajemen insiden, proses pengelolaan risiko juga merupakan suatu hal yang harus diberikan perhatian yang cukup tinggi oleh organisasi, mengingat risiko merupakan sebuah ketidakpastian yang dapat terjadi kapanpun yang dapat mengakibatkan terhambatnya proses bisnis organisasi. Dengan adanya manajemen risiko, diharapkan risiko dapat terkelola dengan baik dan dapat diantisipasi untuk menghindari kerugian. Berikut merupakan proses manajemen risiko berdasarkan standar yang digunakan pada penelitian ini, yaitu *domain* APO12 *Manage Risks* COBIT 5 yang disajikan pada Tabel 5.4.

Tabel 5.4 Proses Manajemen Risiko Berdasarakan Standard

COBIT 5
APO12.01 Mengumpulkan Data
APO12.02 Menganalisis Risiko
APO12.03 Memelihara Profil Risiko
APO12.04 Mengartikulasi Risiko
APO12.05 Menentukan Portofolio Aksi Manajemen Risiko
APO12.06 Melakukan Respon terhadap Risiko

Namun dikarenakan penelitian ini hanya sampai penilaian risiko, maka aktivitas yang digunakan berhenti sampai APO12.02.

5.7 Hambatan

Dalam melakukan proses pengambilan data, penulis terbantu dengan tanggapan pihak LPTSI yang memiliki respon cepat dan bersedia ditemui di LPTSI. Namun ada beberapa hambatan yang perlu dilalui oleh penulis, diantaranya adalah:

1. Terbatasnya pengetahuan narasumber (*helpdesk*) membuat peneliti mengalami kesulitan dalam proses menggali informasi yang dibutuhkan. Oleh karena itu, penulis perlu menyesuaikan pemahaman narasumber terkait pemilihan tata cara penyampaian pertanyaan yang mudah dipahami.
2. Terbatasnya waktu wawancara manejemen terkait pengelolaan risiko karena wawancara dilaksanakan bersamaan dengan topik yang berbeda sehingga informasi yang dibutuhkan tidak tercakup semua.
3. Dari sisi penggalian risiko, penulis mengalami kesulitan dalam mendefinisikan risiko kepada narasumber (*helpdesk*). Hal ini disebabkan karena

pemahaman narasumber terkait risiko dan manajemen risikonya masih sangat terbatas.

4. Dari sisi penerapan proses standar, penulis mengalami kesulitan karena sebelumnya belum penah dilakukan penerapan proses pengelolaan insiden dan penanganan risiko menurut standar tertentu. Terlebih untuk proses manajemen risiko, karena belum pernah dilakukan penelitian terkait manajemen risiko pada *helpdesk* Subdir Layanan DPTSI, sehingga pihak *helpdesk* pun masih sangat awam dengan istilah risiko.

"*Halaman ini sengaja dikosongkan*"

BAB VI
HASIL DAN PEMBAHASAN

6.1 Analisis Tipe Risiko

Pross pertama yang dilakukan ialah membuat daftar risiko yang didokumentasikan dalam serta menentukan tipe risiko berdasarkan *type of risks*, dimana tipe risiko dibagi menjadi tiga, yaitu:

- *IT benefit / value enablement risk*, diisi dengan 'P' (Primer) apabila risiko terkait TI sebagai *enabler* untuk meningkatkan solusi binis, sedangkan jika tidak terkait maka diisi dengan 'S'.
- *IT programme and project delivery risk*, diisi dengan 'P' (Primer) apabila risiko terkait dengan program dan proyek TI, sedangkan jika tidak terkait maka diisi dengan 'S'.
- *IT operations and service delivery risk*, diisi dengan 'P' (Primer) apabila risiko terkait dengan ketersediaan layanan, stabilitas operasional dan gangguan layanan, sedangkan jika tidak terkait maka diisi dengan 'S'.

Kemudian pada setiap risiko yang sudah diidentifikasi dilakukan kategorisasi untuk setiap tipe risiko berdasarkan kepentingkan tipe skenario risiko tersebut, yaitu tipe 'P' untuk tipe primer atau lebih tinggi, serta tipe 'S' untuk tipe sekunder atau lebih rendah. Berikut merupakan analisis tipe risiko analisis risiko pada proses DSS02 *Manage Service Requests and Incidents* Subdir Layanan DPTSI yang ditunjukkan pada Tabel 6.1.

Tabel 6.1 Analisis Tipe Risiko

No	Risiko	Tipe Risiko		
		IT Benefit/ Value Enablement Risk	***IT Programme and Project Delivery Risk***	***IT Operations and Service Delivery Risk***
1.	Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan permintaan layanan	S	S	P
2.	Kesalahan *entry* data dari pengguna (pelapor)	S	S	P
3.	Kegagalan akses sistem *e-ticket*	S	S	P
4.	Kesalahan memahami permintaan pengguna	S	S	P
5.	*Helpdesk* lupa atau tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	S	S	P
6.	*Helpdesk* tidak	S	S	P

No	Risiko	Tipe Risiko		
		IT Benefit/ Value Enablement Risk	***IT Programme and Project Delivery Risk***	***IT Operations and Service Delivery Risk***
	mencatat insiden atau permintaan layanan TI yang masuk			
7.	Kesalahan pengalokasian kategorisasi atau prioritas insiden dan permintaan layanan	S	S	P
8.	Keterlambatan respon *helpdesk*	S	S	P
9.	Penyalahgunaan hak akses permintaan layanan TI	S	S	P
10.	*Helpdesk* tidak mengajukan persetujuan finansial dan fungsional yang dibutuhkan	S	S	P
11.	Prosedur pengelolaan insiden tidak tersedia secara tertulis	S	S	P

No	Risiko	Tipe Risiko		
		IT Benefit/ Value Enablement Risk	***IT Programme and Project Delivery Risk***	***IT Operations and Service Delivery Risk***
12.	Kesalahan mendiagnosa gejala insiden	S	S	P
13.	Kesalahan pencatatan (*logging)* insiden atau permintaan layanan	S	S	P
14.	*Log* insiden atau permintaan layanan TI tidak lengkap	S	S	P
15.	Kesalahan melakukan distribusi (eskalasi) insiden atau permintaan layanan TI	S	S	P
16.	Pihak yang di eskalasi melakukan kesalahan penanganan insiden atau permintaan layanan TI	S	S	P
17.	Pihak yang dieskalasi mengabaikan insiden atau	S	S	P

No	Risiko	Tipe Risiko		
		IT Benefit/ Value Enablement Risk	***IT Programme and Project Delivery Risk***	***IT Operations and Service Delivery Risk***
	permintaan layanan TI yang masuk			
18.	Sistem yang mendukung penanganan layanan TI tidak berfungsi	S	S	P
19.	Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI	S	S	P
20.	Kesalahan dalam melakukan eksekusi penanganan insiden atau pemenuhan layanan TI	S	S	P
21.	Penanganan insiden atau permintaan layanan TI melebihi batas waktu yang disepakati	S	S	P

No	Risiko	Tipe Risiko		
		IT Benefit/ Value Enablement Risk	***IT Programme and Project Delivery Risk***	***IT Operations and Service Delivery Risk***
22.	Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap	S	S	P
23.	Ketidakpuasan pengguna terhadap layanan yang diberikan	S	S	P
24.	Pengguna enggan memberikan *feedback* layanan TI	S	S	P
25.	Pengguna tidak menyetujui status penutupan insiden	S	S	P
26.	Pengguna tidak diinformasikan mengenai penutupan insiden	S	S	P
27.	Pengguna tidak merespon penutupan insiden atau	S	S	P

No	Risiko	Tipe Risiko		
		IT Benefit/ Value Enablement Risk	***IT Programme and Project Delivery Risk***	***IT Operations and Service Delivery Risk***
	permintaan layanan TI			
28.	Ketidakjelasan status insiden atau permintaan layanan	S	S	P
29.	Kesalahan pendefinisian tren dalam laporan	S	S	P
30.	Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan	S	S	P
31.	Bocornya laporan kepada pihak lain	S	S	P

Berdasarkan hasil tabel tipe risiko diatas, dapat diketahui bahwa semua risiko bertipe *IT Operations and Service Delivery Risk*, dikarenakan proses bisnis *helpdesk* terkait dengan stabilitias operasional dan ketersediaan layanan, sehingga semua risiko bersifat primer (P) pada tipe *IT Operations and Service Delivery Risk*. *Helpdesk* tidak memiliki proyek atau program TI tertentu dan tidak menghasilkan *IT* sebagai *enabler* bisnis, sehingga kedua tipe tersebut diisikan dengan ‘S’ (sekunder).

6.2 Analisis Kategori Risiko

Setelah risiko diidentifikasi berdasarkan tipe risiko, langkah selanjutnya ialah melakukan pemetaan kategori risiko berdasarkan kategori yang telah ditentukan pada standar COBIT 5 *for risks*. Berikut merupakan Tabel detail dua puluh kategorisasi risiko menurut COBIT 5 *for risk* yang disajikan pada Tabel 6.2.

Tabel 6.2 Justifikasi Kategori Risiko

No.	Kategori	Pengertian	Justifikasi
1.	*Portfolio establishment and maintenance*	Pengadaan dan pemeliharaan portofolio	Risiko yang termasuk perencanaan, *blueprint*, *maintenance*
2.	*Programme/ projects life cycle management (programme/ project initiation, economics, delivery, quality and termination)*	Manajemen siklus hidup program atau proyek (inisiasi program/proyek, biaya, *delivery*, kualitas dan penutupan proyek)	Risiko yang termasuk dalam manajemen siklus hidup program atau proyek (inisiasi program/proyek, biaya, *delivery*, kualitas dan penutupan proyek)
3.	*IT investment decision making*	Investasi pengambilan keputusan TI	Risiko yang berhubungan dengan pengambilan keputusan investasi TI
4.	*IT expertise and skills*	Ketrampilan dan kemampuan TI	Risiko yang berhubungan dengan ketrampilan dan kemampuan TI SDM

No.	Kategori	Pengertian	Justifikasi
5.	*Staff operations (human error and malicious intent)*	Staff operasional (kesalahan dan niat buruk manusia)	Risiko yang berhubungan dengan kesalahan staff operasional seperti yang tidak disengaja (*human error*) atau kesalahan yang disengaja
6.	*Information (data breach: damage, leakage and access)*	Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses)	Risiko yang berhubungan dengan data dan informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses)
7.	*Architectural (vision and design)*	Arsitektur (visi dan desain)	Risiko yang berhubungan dengan tujuan (visi) dan desain
8.	*Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)*	Infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan)	Risiko yang berhubungan dengan infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan)
9.	*Software*	Perangkat lunak	Risiko yang berhubungan

No.	Kategori	Pengertian	Justifikasi
			dengan perangkat lunak
10.	*Business ownership of IT*	Kepemilikan bisnis TI	Risiko yang berhubungan dengan bisnis TI
11.	*Supplier selection/performance, contractual compliance, termination of service and transfer*	Pemilihan kinerja pemasok, penyesuaian kontrak, pemberhentian layanan dan pengalihan	Risiko yang berhubungan dengan pemilihan kinerja pemasok, penyesuaian kontrak, pemberhentian layanan dan pengalihan
12.	*Regulatory compliance*	Pemenuhan regulasi	Risiko yang berhubungan dengan regulasi organisasi
13.	*Geopolitical*	Geopolitik	Risiko yang berhubungan dengan geopolitik dan hukum
14.	*Insfrastructure theft or destruction*	Pencurian infrastruktur atau pengrusakan	Risiko yang berhubungan dengan pencurian infrastruktur atau pengrusakan
15.	*Malware*	Virus	Risiko yang berhubungan dengan virus, *worm, malware*

No.	Kategori	Pengertian	Justifikasi
16.	*Logical attacks*	Penyerangan logikal	Risiko yang berhubungan dengan penyerangan *logical attacks* seperti peretasan *web application*
17.	*Industrial action*	Aksi industri	Risiko yang berhubungan dengan aksi industri
18.	*Environmental*	Lingkungan sekitar	Risiko yang berhubungan dengan lingkungan sekitar
19.	*Acts of Nature*	Bencana alam	Risiko terkait bencana alam
20.	*Innovation*	Inovasi	Risiko terkait inovasi

Setelah diketahui kriteria kategori risiko agar dapat dipetakan, berikut merupakan pemetaan risiko proses TI DSS02 *Manage Service Requests and Incidents* pda Subdir Layanan DPTSI berdasarkan kategori yang ada pada COBIT 5 yang disajikan pada Tabel 6.3.

Tabel 6.3 Analisis Kategori Risiko

No	Kategori Risiko TI	ID Risiko	Risiko
1.	*IT expertise and skill*	IES001	Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan permintaan layanan
2.		IES002	Kesalahan memahami permintaan pengguna

No	Kategori Risiko TI	ID Risiko	Risiko
3.		IES003	Kesalahan pengalokasian kategorisasi atau prioritas insiden dan permintaan layanan
4.		IES004	Keterlambatan respon *helpdesk*
5.		IES005	Pihak yang di eskalasi melakukan kesalahan penanganan insiden atau permintaan layanan TI
6.		IES006	Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI
7.		IES007	Kesalahan dalam melakukan eksekusi penanganan insiden atau pemenuhan layanan TI
8.		IES008	Kesalahan pendefinisian tren dalam laporan
9.		IES009	Kesalahan mendiagnosa gejala insiden
10.	*Staff operation (human error and malicious intent)*	SOH001	Kesalahan *entry* data dari pengguna (pelapor)
11.		SOH002	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk
12.		SOH003	*Helpdesk* lupa atau tidak menginformasikan

No	Kategori Risiko TI	ID Risiko	Risiko
			prosedur eskalasi insiden kepada teknis
13.		SOH004	*Helpdesk* tidak mengajukan persetujuan finansial dan fungsional yang dibutuhkan
14.		SOH005	Kesalahan pencatatan (*logging)* insiden atau permintaan layanan
15.		SOH006	*Log* insiden atau permintaan layanan TI tidak lengkap
16.		SOH007	Kesalahan melakukan distribusi (eskalasi) insiden atau permintaan layanan TI
17.		SOH008	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan TI yang masuk
18.		SOH009	Penanganan insiden atau permintaan layanan TI melebihi batas waktu yang disepakati
19.		SOH010	Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap
20.		SOH011	Ketidakpuasan pengguna terhadap layanan yang diberikan
21.		SOH012	Pengguna enggan memberikan *feedback* layanan TI

No	Kategori Risiko TI	ID Risiko	Risiko
22.		SOH013	Pengguna tidak menyetujui status penutupan insiden
23.		SOH014	Pengguna tidak diinformasikan mengenai penutupan insiden
24.		SOH015	Pengguna tidak merespon penutupan insiden atau permintaan layanan TI
25.		SOH016	Ketidakjelasan status insiden atau permintaan layanan
26.		SOH017	Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan
27.	*Information (data,breanch: damage,leakage and access)*	IDB001	Penyalahgunaan hak akses permintaan layanan TI
28.		IDB002	Bocornya laporan pada pihak lain
29.	*Software*	SOF001	Kegagalan akses sistem *e-ticket*
30.	*Regulatory Compliance*	REC001	Prosedur pengelolaan insiden tidak tersedia secara tertulis
31.	*Malware*	MWR001	Sistem yang mendukung penanganan layanan TI tidak berfungsi

Setelah dilakukan pemetaan risiko dengan kategori yang sesuai, dapat diketahui bahwa:

1. Risiko yang teridentifikasi paling banyak terpetakan pada kategori *staff operations (human error and malicious*

intent) yaitu sebanyak 17 (tujuh belas) risiko, dimana risiko terkait kesalahan staff yang disengaja maupun tidak disengaja.

2. Pada kategori *IT expertise and skills* teridentifikasi sebanyak 9 (sembilan) risiko, diana risiko disebabkan oleh kurang memadainya pengetahuan dan keterampilan TI staff.
3. Pada kategori *information (data,breanch: damage,leakage and access)* teridentifikasi sebanyak 2 (dua) risiko, dimana risiko terkait dengan pencurian informasi dan penyalahgunaan akses.
4. Pada kategori *software* teridentifikasi sebanyak 1 (satu) risiko, dimana risiko merupakan risiko yang terkait dengan kegagalan dari perangkat lunak.
5. Pada kategori *regulatory compliance* teridentifikasi sebanyak 1 (satu) risiko, dimana risiko merupakan hal dari ketidaksesuaian organisasi dengan peraturan atau prosedur umum yang ada.
6. Dan pada kategori *malware* teridentifikasi sebanyak 1 (satu) risiko, dimana risiko disebabkan oleh *worm* dan virus komputer lain.

6.3 Analisis Faktor Risiko

Setelah mengategorikan risiko berdasarkan ketentuan yang ada pada *best practice*, selanjutnya menentukan faktor (penyebab) yang mempengaruhi risiko terjadi pada proses pengelolaan permintaan layanan dan insiden, baik faktor (penyebab) internal maupun eksternal. Berikut merupakan justifikasi faktor risiko COBIT 5 yang disajikan pada Tabel 6.4 untuk faktor internal dan Tabel 6.5 untuk faktor eksternal.

Tabel 6.4 Justifikasi Faktor Internal Risiko

Aspek *Internal Contextual Factors*	**Justifikasi**
Enterprise goals and objectives (Tujuan perusahaan)	Risiko disebabkan dari kebutuhan *stakeholders* yang mempengaruhi tujuan perusahaan.
Strategic importance of IT in the enterprise (Kepentingan Strategis TI dalam Perusahaan)	Risiko disebabkan karena perusahaan tidak memiliki strategi yang baik dalam memanfaatkan TI sebagai sebuah pembeda strategis, *enabler* fungsional, atau mendukung fungsi.
Complexity of IT (Kompleksitas TI)	Risiko disebabkan karena TI memiliki kompleksitas yang tinggi (contoh: arsitektur kompleks, *merger* baru) atau TI yang sederhana, terstandarisasi dan efisien.
Complexity of the enterprise (Kompleksitas Perusahaan)	Risiko disebabkan karena perusahaan memiliki kompleksitas yang tinggi.
Degree of change (Tingkat Perubahan)	Risiko disebabkan karena tingkat perubahan yang dialami perusahaan.
Change management capability (Kapabilitas Manajemen Perubahan)	Risiko disebabkan karena perusahaan sedang menangani perubahan organisasi.
The risk management philosopy (Filosofi Manajemen Risiko)	Risiko disebabkan karena filosofi penanganan risiko yang diterapkan perusahaan.
Operating model (Model Pengoperasian)	Risiko disebabkan karena model pengoperasian bisnis perusahaan.
Strategic priorities (Prioritas Strategis)	Risiko disebabkan karena organisasi tidak memiliki prioritas strategi yang tepat dalam menjalankan proses bisnis.

Aspek *Internal Contextual Factors*	Justifikasi
Culture of the enterprise (Budaya Perusahaan)	Risiko disebabkan karena tidak adanya kebijakan atau prosedur khusus perusahaan terutama dalam hal manajemen risiko.
Financial capacity (Kemampuan Finansial)	Risiko disebabkan karena perusahaan tidak mampu menyediakan kebutuhan finansial.

Tabel 6.5 Justifikasi Faktor Eksternal Risiko

Aspek *External Contextual Factors*	Justifikasi
Market/economic factors (Faktor ekonomi)	Risiko disebabkan karena faktor ekonomi atau pasar.
Rate of change in the market in which the enterprise operates (Laju perubahan dalam pasar di mana perusahaan beroperasi)	Risiko disebabkan karena perubahan model bisnis secara fundamental.
Competitive environment (Lingkungan Kompetitif)	Risiko disebabkan karena lokasi dan lingkungan dimana perusahaan beroperasi.
Geopolitical situation (Situasi Geopolitik)	Risiko disebabkan karena lokasi geografis perusahaan terkait kondisi alam, politik lokal dan konteks ekonomi.
Regulatory environment (Lingkungan Peraturan)	Risiko disebabkan karena perusahaan tidak memiliki peraturan atau kebijakan terkait TI dan dampaknya.
Technology status and evolution (Status Teknologi dan Evolusi)	Risiko disebabkan karena perkembangan teknologi dan seni (IPTEKS).
Threat landscape (Ancaman)	Risiko disebabkan karena ancaman dari kondisi alam.

Dan berikut penentuan faktor risiko sesuai dengan daftar faktor risiko yang ada pada COBIT 5 disajikan pada Tabel 6.6.

Tabel 6.6 Analisis Faktor Risiko

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
1.	Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan permintaan layanan	***Culture of enterprise*** **-** Tidak terdapat kebijakan dan prosedur khusus untuk pembuatan sistem kategorisasi dan prioritasi insiden dan layanan TI. ***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/*helpdesk* tidak menguasai perkembangan ilmu pengetahuan dalam menangani insiden.	***Regulatory environment-*** Tidak terdapat peraturan atau kebijakan yang jelas terkait pengelolaan insiden dan permintaan layanan.
2.	Kesalahan *entry* data dari pengguna (pelapor)	***Complexity of IT*** **-** Kompleksnya sistem TI yang harus dipenuhi pengguna. ***Operating Model*** **-** Pengguna tidak	***Technology status and evolution-*** Perkembangan teknologi baru yang menyebabkan

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		terbiasa menggunakan model operasi yang digunakan dalam melaporkan keluhan.	kompleksnya permintaan terkait layanan TI.
3.	Kegagalan akses sistem *e-ticket*	***Complexity of IT*** - Sistem *e-ticket* kompleks dan memiliki banyak *bug* dan *error*. ***The risk management philosopy***- Organisasi tidak menyiapkan strategi untuk mencegah kerusakan sistem dari *bug* dan *error*.	***Technology status and evolution***- Perkembangan teknologi menuntut sistem e-ticket untuk selalu di *maintenance* berkala. ***Threat landscape***- Ancaman serangan sistem dari pihak yang tidak berwenang.
4.	Kesalahan memahami permintaan pengguna	***Complexity of IT***- Kompleksnya sistem TI yang harus dipenuhi. ***Culture of enterprise***- *Helpdesk* tidak melakukan konfirmasi ulang kepada pelapor terhadap harapan terkait permintaan layanan yang diajukan. Hal ini mengakibatkan kesalahan pemahaman yang dialami dalam	***Technology status and evolution***- Perkembangan teknologi baru yang menyebabkan kompleksnya permintaan terkait layanan TI.

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		mengidentifikasi permintaan tidak segera terverfikasi hingga selesai pemenuhan yang ternyata tidak sesuai dengan harapan pelapor.	
5.	*Helpdesk* lupa atau tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	***Culture of enterprise***- Tidak terdapat kebijakan dan prosedur tertulis khusus untuk melakukan eskalasi insiden yang disosialisasikan kepada semua unit pengelola insiden dan permintaan layanan.	***Regulatory environment***- Tidak terdapat peraturan atau kebijakan yang jelas terkait pengelolaan insiden dan permintaan layanan.
6.	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk	***Culture of enterprise*** - Tidak terciptanya kebijakan atau prosedur yang mengharuskan *helpdesk* untuk mencatat dengan lengkap semua laporan pengguna yang masuk.	***Competitive environment***- Tingginya standar layanan TI di organisasi lain yang mempengaruhi standar *log* insiden dan permintaan layanan TI.
7.	Kesalahan pengalokasian kategorisasi atau prioritas insiden dan permintaan layanan	***Culture of enterprise*** - Tidak terciptanya sistem kategorisasi dan sistem prioritas untuk permintaan	***Competitive environment***- Tingginya standar layanan TI di organisasi lain yang

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		layanan dan insiden yang sesuai dengan standar. ***Strategic importance of IT in the enterprise*** - Tidak terdapat strategi TI yang baik pada perusahaan terkait pengelolaan permintaan layanan dan insiden, seperti tidak terdapat sistem kategorisasi yang mudah dipahami, tepat, dan mengacu pada standar serta tidak disosialisasikannya sistem prioritas berdasarkan tingkat kritis dan dampak dari insiden dan permintaan layanan.	mempengaruhi standar pengalokasian dan prioritas insiden oleh *helpdesk*.
8.	Keterlambatan respon *helpdesk*	***Startegic priorities-*** *Helpdesk*tidak memiliki prioritas strategis dalam menanggapi permintaan layanan dan insiden, seperti pelaporan mana yang harus ditanggapi terlebih dahulu berdasarkan tingkat urgensitas dan dampaknya. ***Culture of the***	***Competitive environment-*** Tingginya standar layanan TI di organisasi lain yang mempengaruhi standar tingkat respon yang dikatakan responsif pada *helpdesk.*

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		enterprise- Tidak terciptanya budaya organisasi yang merepresentasikan etos kerja tinggi termasuk dalam hal pelayanan TI pada unit *helpdesk* yang mengakibatkan rendahnya tingkat respon dalam pelayanan. Selain itu, tidak terdapat prosedur dan SLA yang terdokumentasi sebagai panduan proses terstandar yang mendorong *helpdesk*untuk memenuhi tingkat layanan yang disetujui dan dijanjikan kepada pengguna layanan.	
9.	Penyalahgunaan hak akses permintaan layanan TI	***Complexity of IT-*** Sistem *e-ticket* tidak menerapkan standar keamanan yang tinggi. ***The risk management philosopy-*** Organisasi tidak menyiapkan strategi untuk	***Threat landscape-*** Ancaman serangan sistem dari pihak yang tidak berwenang.

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		penyalahgunaan hak akses agar.	
10.	*Helpdesk* tidak mengajukan persetujuan finansial dan fungsional yang dibutuhkan	***Culture of enterprise*** - Tidak terdapat kebijakan dan prosedur tertulis untuk mengajukan persetujuan finansial dan fungsional yangmengacu pada standar. ***Strategic importance of IT in the enterprise*** - Tidak terdapat strategi TI yang baik pada perusahaan terkait pengelolaan permintaan layanan dan insiden, seperti tidak adanya keterlibatan pihak manajemen dalam mengawasi pengelolaan insiden dan permintaan layanan.	***Regulatory environment***- Tidak terdapat peraturan atau kebijakan yang jelas terkait pengelolaan insiden dan permintaan layanan.
11.	Prosedur pengelolaan insiden tidak tersedia secara tertulis	***Culture of enterprise*** - Tidak terciptanya kebijakan atau peraturan yang mengharuskan *helpdesk* untuk membuat prosedur pengelolaan insiden dan permintaan	***Regulatory environment***- Tidak terdapat peraturan atau kebijakan yang jelas terkait pengelolaan insiden dan permintaan layanan.

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		layanan TI. ***Strategic importance of IT in the enterprise -*** Tidak terdapat strategi TI yang baik pada perusahaan terkait pembuatan prosedur tertulis yang ditetapkan untuk pengelolaan insiden dan permintaan layanan TI.	
12.	Kesalahan mendiagnosa gejala insiden	***Complexity of IT-*** *Helpdesk* tidak memahami permintaan layanan TI atau insiden yang kompleks.	***Technology status and evolution-*** Perkembangan teknologi layanan TI sehingga menimbulkan permasalahan TI baru.
13.	Kesalahan pencatatan (*logging)* insiden atau permintaan layanan	***Operating model-*** Kesalahan dalam pencatatan operasional pengelolaan permintaan dan insiden.	***Technology status and evolution-*** Perkembangan teknologi untuk *helpdesk*dalam mengelola pencatatan pelaporan.
14.	*Log* insiden atau permintaan layanan TI tidak lengkap	***Culture of the enterprise-*** Tidak terciptanya budaya organisasi yang merepresentasikan etos kerja tinggi termasuk dalam hal	***Regulatory environment-*** Tidak terdapat peraturan atau kebijakan yang jelas terkait pengelolaan insiden dan

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		pelayanan TI pada unit *helpdesk* yang mengakibatkan rendahnya tingkat respon dalam pelayanan. Selain itu, tidak terdapat prosedur dan SLA yang terdokumentasi sebagai panduan proses terstandar yang mendorong *helpdesk*untuk memenuhi tingkat layanan yang disetujui dan dijanjikan kepada pengguna layanan.	permintaan layanan terutama untuk kelengkapan *log* insiden.
15.	Kesalahan melakukan distribusi (eskalasi) insiden atau permintaan layanan TI	***Operating model-*** *Helpdesk*tidak mengalokasikan insiden dan permintaan layanan TI sesuai dengan pendefinisian yang dilakukan.	***Regulatory environment-*** Pengaruh perubahan peraturan terkait tugas pokok dan fungsi tiap SubDirektorat.
16.	Pihak yang di eskalasi melakukan kesalahan penanganan insiden atau permintaan layanan TI	***Operating model-*** *Helpdesk* tidak mendokumentasikan pendefinisian klasifikasi, prioritasi, serta prosedur permintaan & insiden sehingga salah dalam mendefinisikan di operasionalnya.	***Technology status and evolution-*** Perkembangan teknologi baru yang menyebabkan kompleksnya insiden terkait layanan TI.

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		Complexity of IT- Kompleksnya sistem TI yang harus ditangani atau di luar insiden yang umum ditangani oleh teknisi/*helpdes*k. ***Culture of enterprise***- Teknisi/*helpdesk* 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/*helpdesk* tidak menguasai perkembangan ilmu pengetahuan dalam menangani insiden.	
17.	Pihak yang dieskalasi mengabaikan insiden atau permintaan	***Complexity of IT***- Kompleksnya sistem TI yang harus ditangani atau di luar insiden yang	***Regulatory environment***- Tidak terdapat peraturan atau kebijakan yang

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
	layanan TI yang masuk	umum ditangani oleh teknisi/*helpdesk*. ***Culture of enterprise-*** Teknisi/*helpdesk* 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 kebijakan batas waktu untuk menangani laporan yang masuk serta sanksi khusus apabila mengabaikan pekerjaan.	jelas terkait pengelolaan insiden dan permintaan layanan terutama untuk kelengkapan *log* insiden.
18.	Sistem yang mendukung penanganan layanan TI tidak berfungsi	***Complexity of IT-*** Sistem *hardware* dan *software* yang digunakan memiliki celah kelemahan serta tidak berkualitas. ***The risk management philosopy-*** Organisasi tidak	***Technology status and evolution-*** Perkembangan teknologi menuntut sistem terkomputerisasi untuk selalu di *maintenance* berkala. ***Threat landscape-*** Ancaman

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		menyiapkan strategi untuk mencegah kerusakan sistem dan infrastruktur.	serangan sistem dari pihak tidak berwenang.
19.	Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI	***Complexity of IT-Helpdesk*** tidak memahami pendefinisian permintaan layanan TI atau insiden yang kompleks.	***Technology status and evolution-*** Perkembangan teknologi layanan TI sehingga menimbulkan permasalahan TI baru.
20.	Kesalahan dalam melakukan eksekusi penanganan insiden atau pemenuhan layanan TI	***Operating model-Helpdesk*** tidak mendokumentasikan pendefinisian klasifikasi, prioritasi, serta prosedur permintaan dan insiden sehingga salah dalam mendefinisikan di operasionalnya. ***Complexity of IT-*** Kompleksnya sistem TI yang harus ditangani atau di luar insiden yang umum ditangani oleh teknisi/*helpdes*k. ***Culture of enterprise-*** Teknisi/*helpdesk* tidak terbiasa menangani pelaporan serupa. ***Strategic***	***Technology status and evolution-*** Perkembangan teknologi baru yang menyebabkan kompleksnya insiden terkait layanan TI.

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		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/*helpdesk* tidak menguasai perkembangan ilmu pengetahuan dalam menangani insiden.	
21.	Penanganan insiden atau permintaan layanan TI melebihi batas waktu yang disepakati	***Complexity of IT-*** Kompleksnya sistem TI yang dilaporkan serta data yang tidak lengkap. ***Strategic priorities-*** Terdapat kesalahan dalam melaksanakan strategi prioritas penanganan. ***Financial capacity-*** Lamanya persetujuan pemenuhan permintaan oleh KaSubDit Layanan TSI dikarenakan di luar kapasitas finansial organisasi.	***Regulatory environment-*** Tidak adanya kebijakan organisasi yang mengawasi proses pengelolaan insiden dan memenuhi permintaan layanan.

No	Risiko	Faktor Risiko	
		Internal	Eksternal
22.	Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap	***Culture of the enterprise-*** Tidak terciptanya budaya organisasi yang merepresentasikan etos kerja tinggi termasuk dalam hal kelengkapan pendokumentasian layanan TI dan insiden yang masuk serta tidak adanya rapat rutin atau evaluasi yang membahas kelengkapan laporan insiden.	***Regulatory environment-*** Tidak terdapat peraturan atau kebijakan yang jelas terkait pengelolaan insiden dan permintaan layanan terutama untuk kelengkapan dokumentasi insiden dan permintaan layanan TI.
23.	Ketidakpuasan pengguna terhadap layanan yang diberikan	***Operating model-*** *Helpdesk* tidak melaksanakan operasional layanan sesuai standar. ***Culture of enterprise-*** Tidak terciptanya budaya organisasi yang berorientasi kepada kepuasan pengguna dengan memberikan pelayanan yang prima.	***Competitive environment-*** Tingginya standar layanan TI di organisasi lain yang mempengaruhi standar kepuasan pengguna.
24.	Pengguna enggan memberikan *feedback* layanan TI	***Culture of the enterprise-*** Tidak terciptanya budaya organisasi yang berorientasi	***Competitive environment-*** Tingginya standar layanan TI di organisasi lain

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		kepada kepuasan pengguna dengan memperhatikan kritik dan saran pengguna.	yang mempengaruhi standar kepuasan pengguna.
25.	Pengguna tidak menyetujui status penutupan insiden	***Operating model***- *Helpdesk* tidak melaksanakan operasional layanan sesuai standar serta harapan pengguna. ***Culture of enterprise***- Tidak terciptanya budaya organisasi yang berorientasi kepada kepuasan pengguna dengan memberikan pelayanan yang prima.	***Competitive environment***- Tingginya standar layanan TI di organisasi lain yang mempengaruhi standar kepuasan pengguna.
26.	Pengguna tidak diinformasikan mengenai penutupan insiden	***Culture of enterprise***- Tidak terciptanya budaya organisasi yang berorientasi kepada kepuasan pengguna dengan selalu menjaga komunikasi dengan pengguna dengan memberikan informasi terkini terkait pelaporan pengguna. ***Strategic importance of IT in the enterprise***-	***Regulatory environment***- Tidak terdapat peraturan atau kebijakan yang jelas terkait pengelolaan insiden dan permintaan layanan terutama untuk menginfromasikan status permintaan layanan atau insiden yang dilaporkan pengguna.

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		Tidak terdapat strategi TI yang baik pada perusahaan terkait pengelolaan permintaan layanan dan insiden, seperti tidak terdapat kebijakan untuk selalu menginformasikan status pelaporan yang diajukan pengguna.	
27.	Pengguna tidak merespon penutupan insiden atau permintaan layanan TI	***Operating model-*** *Helpdesk* tidak melaksanakan operasional layanan sesuai standar serta keinginan pengguna. ***Culture of enterprise-*** Tidak terciptanya budaya organisasi yang berorientasi kepada kepuasan pengguna dengan memberikan pelayanan yang prima.	***Competitive environment-*** Tingginya standar layanan TI di organisasi lain yang mempengaruhi standar kepuasan pengguna.
28.	Ketidakjelasan status insiden atau permintaan layanan	***Operating model-*** Model pengoperasian *helpdesk*tidak tersentralisasi, di mana apabila pelaporan telah	***Technology status and evolution-*** *Helpdesk*tidak memiliki teknologi/sistem informasi yang dapat

No	Risiko	Faktor Risiko	
		Internal	**Eksternal**
		dieskalasi ke bagian teknisi atau pemasok pemenuhan permintaan dan penanganan inisden, maka pengguna/pelapor layanan langsung berhubungan dengan pihak bersangkutan sedangkan *helpdesk* tidak memiliki akses komunikasi langsung kepada pengguna. Terkait perubahan status pemenuhan permintaan dan penanganan insiden yang dilakukan tidak didistribusikan kembali kepada *helpdesk* atau pengguna sehingga menimbulkan ketidakjelasan status.	mengakomodasi dalam distribusi atau pengembalian status pelaporan permintaan layanan dan insiden sehingga dapat diakses oleh seluruh pengguna TI baik oleh *helpdesk*, pelapor dan teknisi.
29.	Kesalahan pendefinisian tren dalam laporan	***Culture of the enterprise-*** Tidak terdapat rapat pertemuan atau evaluasi yang membahas laporan pengelolaan permintaan layanan dan insiden.	***Technology status and evolution-*** Tuntutan perkembangan TI dalam mengevaluasi tren permintaan dan insiden.

No	Risiko	Faktor Risiko	
		Internal	Eksternal
30.	Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan	***Complexity of IT***- Sistem tidak dapat mendistribusikan laporan secara otomatis dan merata. ***Culture of enterprise***- Tidak terdapat rapat pertemuan atau evaluasi yang membahas laporan pengelolaan permintaan layanan dan insiden	***Regulatory environment***- Tidak ada kebijakan dan prosedur terkait laporan pengelolaan permintaan layanan dan insiden.
31.	Bocornya laporan kepada pihak lain	***Complexity of IT***- Sistem penyimpanan laporan tidak memiliki kompleksitas keamanan yang tinggi. ***The risk management philosopy***- Organisasi tidak menyiapkan strategi untuk mencegah celah keamanan terhadap data atau aset kritis lain.	***Threat landscape***- Ancaman serangan sistem untuk mengambil data yang dapat dimasuki pihak yang berwenang.

Berdasarkan hasil analisis Tabel 6.6 diatas, dapat diketahui bahwa:

1. Faktor (penyebab) internal mayoritas disebabkan oleh ***complexity of IT***, dimana risiko disebabkan karena

kompleksnya sistem TI dan namun pengetahuan dan keterampilan para SDM TI kurang memadai dan belum terbiasa.

2. Faktor (penyebab) internal lain yang cukup banyak mempengaruhi ialah c***ulture of the enterprise,*** dimana risiko disebabkan karena belum terkelolanya kebijakan atau prosedur khusus organisasi (Sub Direktorat Layanan TSI) dalam menyediakan pelayanan TI, khususnya dalam hal manajemen insiden dan permintaan layanan TI serta pengelolaan risiko TI.
3. Faktor (penyebab) internal lain yang cukup banyak mempengaruhi ialah ***strategic importance of IT in the enterprise***, dimana risiko disebabkan karena perusahaan tidak memiliki strategi yang baik dalam memanfaatkan TI, seperti tidak adanya pengarahan, kebijakan atau pelatihan yang mendukung staff dala memberikan pelayanan.
4. Faktor (penyebab) eksternal mayoritas disebabkan oleh ***regulatory environment,*** dimana risiko disebabkan karena perusahaan tidak memiliki peraturan atau kebijakan tertulis terkait pengelolaan insiden dan pemenuhan permintaan layanan TI.
5. Faktor (penyebab) eksternal lain yang cukup banyak mempengaruhi ialah ***technology status and evolution,*** dimana risiko disebabkan karena perkembangan teknologi dan seni (IPTEKS) yang belum terlalu dipahami dan dikuasai oleh elemen organisasi.

Jika di gabung, hasil dari analisis tipe risiko, kategori risiko dan faktor (penyebab) risiko dapat menjadi sebuah *risk event*.

6.4 Pembuatan Skenario Risiko

Selanjutnya dilakukan pembuatan skenario risiko TI atau dampak risiko bila terjadi secara teratur berdasarkan dua jenis, yaitu skenario positif dan skenario negatif. Skenario positif berisikan dampak apabila risiko tersebut tidak terjadi, sehingga mendeskripsikan proses bisnis yang dapat berjalan lancar dan optimal. Sedangkan skenario negatif berisikan dampak apabila

risiko terjadi, sehingga menghasilkan sebuah gangguan atau hambatan terhadap proses bisnis. Berikut skenario risiko TI ditampilkan pada Tabel 6.7.

Tabel 6.7 Skenario Risiko

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
1.	Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan permintaan layanan	Penanganan insiden dapat dilakukan dengan tepat dan sesuai sehingga memudahkan apabila ingin di eskalasi sesuai kategori permasalahannya.	Penanganan insiden dan permintaan layanan terhambat karena data tidak sesuai sehingga dan membutuhkan waktu lebih lama untuk menyelesaikannya.
2.	Kesalahan *entry* data dari pengguna (pelapor)	Pengguna mengisikan data laporan insiden atau permintaan layanannya dengan tepat dan lengkap sehingga identifikasi dan penanganan insiden dapat berjalan dengan lancar, sesuai dan tepat waktu.	Terdapat kesalahan pengisian data, data dan informasi yang ada tidak relevan sehingga identifikasi dan penanganan insiden menjadi terhambat dan membutuhkan waktu lebih lama.
3.	Kegagalan akses sistem *e-ticket*	Pengguna dapat mengandalkan sistem e-ticket untuk membuat laporan insiden dan permintaan layanan, serta unit *helpdesk* dapat menerima dan mengelola laporan dari pengguna dengan tepat	Menumpuk-nya pelaporan melalui sistem manual (*e-mail* dan telepon), serta *helpdesk* tidak dapat melacak status pelaporan yang sedang ditangani.

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
4.	Kesalahan memahami permintaan pengguna	Laporan permintaan layanan dan insiden dapat dipenuhi sesuai dengan harapan pengguna dimana selesai tepat waktu, tidak ada penambahan sumber daya dan biaya sehingga memenuhi SLA.	Laporan permintaan layanan dan insiden tidak terpenuhi sesuai dengan harapan pengguna dimana tidak selesai tepat waktu, ada penambahan sumber daya dan biaya sehingga memenuhi SLA.
5.	*Helpdesk* lupa atau tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	Proses penanganan insiden khususnya pada proses eskalasi berjalan lancar karena prosedur sudah jelas.	Pihak yang dieskalasi kesulitan dalam menangani insiden yang dialokasikan sehingga proses penanganan terhambat dan membutuhkan waktu lebih lama.
6.	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk	Data atau *log* insiden tercatat lengkap sehinga memudahkan identifikasi dan penanganan insiden atau permintaan layanan TI.	*Helpdesk* atau teknisi kesulitan dalam mengidentifikasi dan menangani insiden atau permintaan layanan TI karena mengabaikan pencatatan insiden sehingga data tidak lengkap.
7.	Kesalahan pengalokasian kategorisasi atau	Penanganan dan pendistribusian insiden dapat	Penanganan dan pendistribusian insiden tidak

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
	prioritas insiden dan permintaan layanan	berjalan lancar karena data kategorisasi relevan dengan pendistribusian pihak yang akan menangani. Selain itu penanganan insiden didahulukan yang memiliki urgensitas tinggi dan dampak besar karena sistem prioritas yang tepat sehingga sesuai dengan harapan pelanggan.	sesuai karena data kategorisasi yang tidak relevan. Selain itu penanganan insiden yang prioritas rendah didahulukan karena sistem prioritas yang salah dimana tidak sesuai dengan harapan pelanggan.
8.	Keterlambatan respon *helpdesk*	Proses bisnis layanan TI berjalan dengan baik karena *helpdesk* cepat tanggap dalam melayani pengguna sehingga kepuasan pengguna meningkat.	Banyaknya komplain dari pengguna layanan dikarenakan keluhan mereka tidak langsung (terlambat) ditangani sehingga proses bisnis layanan menjadi terhambat.
9.	Penyalahgunaan hak akses permintaan layanan TI	Organisasi tidak mengalami kerugian baik finansial dikarenakan pemenuhan permintaan layanan sesuai sebagaimana prosedurnya, serta data (aset kritis)	Kerugian organisasi terhadap pemenuhan permintaan di luar hak pengguna, baik kehilangan data (aset kritis), maupun kerugian finansial.

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
		organisasi tidak terancam oleh pihak tidak berwenang.	
10.	*Helpdesk* tidak mengajukan persetujuan finansial dan fungsional yang dibutuhkan	Proses penanganan insiden berjalan lancar dan dapat selesai tepat waktu karena telah disetujui baik secara fungsional maupun finansial jika membutuhkan biaya khusus.	Proses penanganan insiden terhambat karena belum adanya persetujuan finansial atau fungsional dari pihak manajemen sehingga tidak dapat dilanjutkan atau di *pending* terlebih dahulu sehingga membutuhkan waktu lebih lama.
11.	Prosedur pengelolaan insiden tidak tersedia secara tertulis	Proses pengelolaan insiden dan permintaan layanan berjalan dengan tepat karena mengacu pada prosedur.	*Helpdesk* atau teknisi kesulitan atau melakukan insiden hanya berdasarkan pengalaman saja karena tidak adanya prosedur khusus.
12.	Kesalahan mendiagnosa gejala insiden	Proses eksekusi penangana insiden berjalan lancar dikarenakan diagnosa yang tepat, sehingga solusi yang diberikan juga sesuai.	Proses eksekusi penanganan insiden terhambat dikarenakan diagnosa yang salah, dimana pemilihan solusinya juga tidak tepat. sehingga tidak

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
			sesuai dengan harapan pengguna
13.	Kesalahan pencatatan (*logging)* insiden atau permintaan layanan	Proses penanganan insiden dan permintaan layanan TI berjalan dengan baik dan tepat sesuai data dan informasi terkait yang dicatat sesuai harapan pengguna.	Proses penanganan insiden menjadi tidak tepat dikarenakan adanya kesalahan pada saat menuliskan identitas pelapor, kategori insiden, nama insiden, pihak yang menangani sehingga tidak sesuai dengan harapan pengguna.
14.	*Log* insiden atau permintaan layanan TI tidak lengkap	Proses penanganan insiden dapat berjalan dengan lancar dan tepat waktu serta dapat dilakukan analisis tren insiden dan permintaan layanan karena *log* berisikan lengkap terkait data pelapor, kategori, tanggal, pihak yang menangani, tingkat kritis dan status sesuai dengan pelaporan yang masuk ke sistem segera dapat dikelola. Serta log disimpan dalam	Proses penanganan insiden menjadi terhambat serta tidak dapat dilakukan analisis tren insiden dan permintaan layanan karena *log* yang ada tidak lengkap dimana tidak mencakup data pelapor, data insiden, tanggal kejadian, tingkat kritis, status penanganan. Serta log tidak disimpan dalam sebuah direktori khusus.

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
		sebuah direktori khusus.	
15.	Kesalahan melakukan distribusi (eskalasi) insiden atau permintaan layanan TI	Laporan insiden atau permintaan layanan dialokasikan ke pihak yang tepat sehingga dapat tertangani dengan baik.	Laporan insiden atau permintaan layanan masuk ke pihak yang tidak menguasai dimana tidak sesuai dengan harapan pengguna.
16.	Pihak yang di eskalasi melakukan kesalahan penanganan insiden atau permintaan layanan TI	Pelaporan permintaan dan insiden dapat diidentifikasi dan ditangani dengan tepat oleh teknisi atau *helpdesk*.	Pihak yang menangani pelaporan mengalami kesulitan dalam mengidentifikasi dan memberikan solusi permintaan layanan dan insiden sehingga hasilnya tidak tepat dan tidak sesuai dengan harapan pengguna.
17.	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan TI yang masuk	Pelaporan permintaan layanan dan insiden segera dikerjakan dengan benar dan tepat waktu oleh pihak yang dieskalasi.	Banyaknya komplain dari pengguna karena laporan insiden dan permintaan layanannya yang diabaikan.
18.	Sistem yang mendukung penanganan layanan TI tidak berfungsi	Proses penanganan insiden yang membutuhkan sistem TI tetap berjalan lancar sehingga membantu memudahkan	Proses penanganan insiden yang membutuhkan sistem TI pendukung menjadi terhambat sehingga

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
		helpdesk dalam menyelesaikan laporan.	penangannya tidak selesai tepat waktu.
19.	Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI	Insiden ditangani dengan tepat dan memenuhi kepuasan pengguna.	Insiden tidak ditangani dengan tepat sehingga membutuhkan waktu lebih dan kepuasan pengguna menurun.
20.	Kesalahan dalam melakukan eksekusi penanganan insiden atau pemenuhan layanan TI	Insiden terlapor ditangani dan keadaan normal dikembalikan seperti harapan pengguna. Permintaan layanan yang diajukan pengguna dapat dipenuhi sesuai harapan dan memuaskan pengguna.	Insiden tidak terselesaikan dan permintaan layanan tidak dipenuhi sesuai harapan pengguna.
21.	Penanganan insiden atau permintaan layanan TI melebihi batas waktu yang disepakati	Proses bisnis layanan berjalan dengan baik serta meningkatnya kepuasan pengguna.	Banyaknya komplain pengguna layanan karena insiden tidak diselesaikan sesuai kesepakatan.
22.	Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap	Dapat dilakukan analisis tren insiden dan permintaan layanan karena laporan penyelesaian insiden lengkap	Tidak dapat dilakukan analisis tren insiden dan permintaan layanan karena laporan penyelesaian

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
		terdokumentasi sesuai harapan pengguna dan disimpan dalam sebuah direktori khusus.	insiden lengkap dan disimpan dalam sebuah direktori khusus. Selain itu juga tidak ada bukti penyelesaian insiden yang terdokumentasi.
23.	Ketidakpuasan pengguna terhadap layanan yang diberikan	Berkurangnya komplain pengguna dan meningkatkan kepercayaan pengguna terhadap layanan helpdesk.	Pengguna kecewa sehingga tidak menggunakan layanan *helpdesk* lagi.
24.	Pengguna enggan memberikan *feedback* layanan TI	Helpdesk bisa meningkatkan kinerjanya berdasarkan kritik dan saran dari pengguna.	Helpdesk tidak ada gambaran mengenai kritik dan saran pengguna sebagai masukan untuk meningkatkan kinerjanya.
25.	Pengguna tidak menyetujui status penutupan insiden	Penutupan insiden disetujui oleh pengguna karena sudah sesuai dengan harapan pengguna sehingga dapat meningkatkan kepuasan pengguna.	Pengguna tidak puas terhadap kinerja yang diberikan oleh *helpdesk* terkait penanganan insiden atau permintaan layanan TI yang diajukannya.
26.	Pengguna tidak diinformasikan mengenai penutupan insiden	Pengguna selalu mendapatkan informasi terkini terkait insiden atau permintaan layanan	Pengguna tidak mengetahui apakah insiden atau permintaan layanannya sudah

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
		TI yang diajukannya dimana hal ini dapat meningkatkan kepuasan pengguna terhadap pelayanan yang diberikan *helpdesk*.	selesai ditangani dan ditutup dimana hal ini dapat menurunkan kepuasan pengguna terhadap kinerja *helpdesk*.
27.	Pengguna tidak merespon penutupan insiden atau permintaan layanan TI	Penutupan insiden disetujui oleh pengguna karena sudah sesuai dengan harapan pengguna sehingga dapat meningkatkan kepuasan pengguna.	Penutupan insiden akan ditutup secara otomatis oleh *helpdesk* tanpa mengetahui tingkat kepuasan pengguna.
28.	Ketidakjelasan status insiden atau permintaan layanan	Baik pengguna/pelapor layanan, *helpdesk*, maupun teknisi mengetahui status permintaan layanan dan insiden dengan jelas sehingga laporan permintaan layanan dan insiden dapat segera dikelola dengan efektif.	Pengguna tidak mengetahui apakah permintaan layanan dan insiden telah ditanggapi, sedang ditangani, atau selesai ditangani sehingga pengguna/pelapor harus bertanya kembali ke *helpdesk*. Sedangkan *helpdesk* juga berisiko tidak mengetahui status permintaan layanan dan insiden yang sedang ditangani oleh teknisi

No	Risiko	Skenario Risiko	
		Skenario Positif	**Skenario Negatif**
			(ketika telah alokasi / eskalasi dilakukan).
29.	Kesalahan pendefinisian tren dalam laporan	Tepat dalam mengidentifikasi insiden yang berubah status menjadi *problem* untuk segera diperbaiki hingga akar masalah sehingga dapat menghindari masalah yang berulang.	Insiden terjadi berulang namun tidak diidentifikasi sebagai *problem* untuk menghindari masalah yang berulang.
30.	Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan	Manajemen organisasi dapat mengevaluasi hasil pengelolaan permintaan layanan dan insiden berdasarkan laporan yang telah didistribusikan.	Tidak adanya perubahan yang lebih baik terhadap evaluasi layanan pengelolaan permintaan layanan dan insiden.
31.	Bocornya laporan kepada pihak lain	Data dan informasi yang kritis selalu terjaga keamanannya dan hanya pihak yang berwenang yang dapat mengaksesnya.	Data dan informasi yang kritis diketahui dan dapat disalahgunakan oleh pihak yang tidak berwenang.

6.5 Pemetaan Risiko terhadap Pertanyaan Kuesioner

Untuk memudahkan perhitungan hasil kuesioner, dilakukan pemetaan risiko dengan pertanyaan kuesioner yang sudah dibuat sebelum nantinya melakukan penilaian risiko. Pemetaan risiko dengan pertanyaan kuesioner dikategorikan berdasarkan persamaan dampak (skenario) risiko. Berikut merupakan pemetaan risiko dengan pertanyaan kuesioner berdasarkan dampak risiko yang disajikan pada Tabel 6.8.

Tabel 6.8 Pemetaan Risiko terhadap Pertanyaan Kuesioner

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
K01	Ketika *helpdesk* tidak memenuhi permintaan dan menangani keluhan sesuai harapan saya, maka kepuasan saya mengalami:	Kesalahan memahami permintaan pengguna	Laporan permintaan layanan dan insiden dapat dipenuhi sesuai dengan harapan pengguna dimana selesai tepat waktu, tidak ada penambahan sumber daya dan biaya sehingga memenuhi SLA.	Laporan permintaan layanan dan insiden tidak terpenuhi sesuai dengan harapan pengguna dimana tidak selesai tepat waktu, ada penambahan sumber daya dan biaya sehingga memenuhi SLA.
		Kesalahan pengalokasian kategorisasi atau	Penanganan dan pendistribusian insiden dapat berjalan lancar	Penanganan dan pendistribusian insiden tidak sesuai

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
		prioritas insiden dan permintaan layanan	karena data kategorisasi relevan dengan pendistribusian pihak yang akan menangani. Selain itu penanganan insiden didahulukan yang memiliki urgensitas tinggi dan dampak besar karena sistem prioritas yang tepat sehingga sesuai dengan harapan pelanggan.	karena data kategorisasi yang tidak relevan. Selain itu penanganan insiden yang prioritas rendah didahulukan karena sistem prioritas yang salah dimana tidak sesuai dengan harapan pelanggan.
		Prosedur pengelolaan insiden tidak tersedia secara tertulis	Proses pengelolaan insiden dan permintaan layanan berjalan dengan tepat karena mengacu pada prosedur.	*Helpdesk* atau teknisi kesulitan atau melakukan insiden hanya berdasarkan pengalaman saja karena tidak adanya prosedur khusus.

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
		Kesalahan pencatatan (*logging)* insiden atau permintaan layanan	Proses penanganan insiden dan permintaan layanan TI berjalan dengan baik dan tepat sesuai data dan informasi terkait yang dicatat sesuai harapan pengguna.	Proses penanganan insiden menjadi tidak tepat dikarenakan adanya kesalahan pada saat menuliskan identitas pelapor, kategori insiden, nama insiden, pihak yang menangani sehingga tidak sesuai dengan harapan pengguna.
		Log insiden atau permintaan layanan TI tidak lengkap	Proses penanganan insiden dapat berjalan dengan lancar dan tepat waktu serta dapat dilakukan analisis tren insiden dan permintaan layanan karena *log* berisikan lengkap terkait data pelapor, kategori,	Proses penanganan insiden menjadi terhambat serta tidak dapat dilakukan analisis tren insiden dan permintaan layanan karena *log* yang ada tidak lengkap dimana tidak

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
			tanggal, pihak yang menangani, tingkat kritis dan status sesuai dengan pelaporan yang masuk ke sistem segera dapat dikelola. Serta log disimpan dalam sebuah direktori khusus.	mencakup data pelapor, data insiden, tanggal kejadian, tingkat kritis, status penanganan. Serta log tidak disimpan dalam sebuah direktori khusus.
		Kesalahan melakukan distribusi (eskalasi) insiden atau permintaan layanan TI	Laporan insiden atau permintaan layanan dialokasikan ke pihak yang tepat sehingga dapat tertangani dengan baik.	Laporan insiden atau permintaan layanan masuk ke pihak yang tidak menguasai dimana tidak sesuai dengan harapan pengguna.
		Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI	Insiden ditangani dengan tepat dan memenuhi kepuasan pengguna.	Insiden tidak ditangani dengan tepat sehingga membutuhkan waktu lebih dan kepuasan pengguna menurun.

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
		Kesalahan dalam melakukan eksekusi penanganan insiden atau pemenuhan layanan TI	Insiden terlapor ditangani dan keadaan normal dikembalikan seperti harapan pengguna. Permintaan layanan yang diajukan pengguna dapat dipenuhi sesuai harapan dan memuaskan pengguna.	Insiden tidak terselesaikan dan permintaan layanan tidak dipenuhi sesuai harapan pengguna.
		Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap	Dapat dilakukan analisis tren insiden dan permintaan layanan karena laporan penyelesaian insiden lengkap terdokumentasi sesuai harapan pengguna dan disimpan dalam sebuah direktori khusus.	Tidak dapat dilakukan analisis tren insiden dan permintaan layanan karena laporan penyelesaian insiden lengkap dan disimpan dalam sebuah direktori khusus. Selain itu juga tidak ada bukti

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
				penyelesaian insiden yang terdokumentasi.
		Ketidakpuasan pengguna terhadap layanan yang diberikan	Berkurangnya komplain pengguna dan meningkatkan kepercayaan pengguna terhadap layanan helpdesk.	Pengguna kecewa sehingga tidak menggunakan layanan *helpdesk* lagi.
		Pengguna tidak menyetujui status penutupan insiden	Penutupan insiden disetujui oleh pengguna karena sudah sesuai dengan harapan pengguna sehingga dapat meningkatkan kepuasan pengguna.	Pengguna tidak puas terhadap kinerja yang diberikan oleh *helpdesk* terkait penanganan insiden atau permintaan layanan TI yang diajukannya.
		Pihak yang di eskalasi melakukan kesalahan penanganan	Pelaporan permintaan dan insiden dapat diidentifikasi dan ditangani dengan tepat	Pihak yang menangani pelaporan mengalami kesulitan dalam mengidentifikasi dan

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
		insiden atau permintaan layanan TI	oleh teknisi atau *helpdesk*.	memberikan solusi permintaan layanan dan insiden sehingga hasilnya tidak tepat dan tidak sesuai dengan harapan pengguna.
		Kesalahan mendiagnosa gejala insiden	Proses eksekusi penangana insiden berjalan lancar dikarenakan diagnosa yang tepat, sehingga solusi yang diberikan juga sesuai.	Proses eksekusi penanganan insiden terhambat dikarenakan diagnosa yang salah, dimana pemilihan solusinya juga tidak tepat. sehingga tidak sesuai dengan harapan pengguna
K02	Ketika *helpdesk* terlambat dalam merespon laporan saya, maka kepuasan saya mengalami:	Keterlambatan respon *helpdesk*	Proses bisnis layanan TI berjalan dengan baik karena *helpdesk* cepat tanggap dalam melayani	Banyaknya komplain dari pengguna layanan dikarenakan keluhan mereka tidak

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
			pengguna sehingga kepuasan pengguna meningkat.	langsung (terlambat) ditangani sehingga proses bisnis layanan menjadi terhambat.
K03	Ketika *helpdesk* mengabaikan laporan saya, maka kepuasan saya mengalami:	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk	Data atau *log* insiden tercatat lengkap sehinga memudahkan identifikasi dan penanganan insiden atau permintaan layanan TI.	*Helpdesk* atau teknisi kesulitan dalam mengidentifikasi dan menangani insiden atau permintaan layanan TI karena mengabaikan pencatatan insiden sehingga data tidak lengkap.
		Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan TI yang masuk	Pelaporan permintaan layanan dan insiden segera dikerjakan dengan benar dan tepat waktu oleh pihak yang dieskalasi.	Banyaknya komplain dari pengguna karena laporan insiden dan permintaan layanannya yang diabaikan.

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
K04	Ketika *helpdesk* selesai menangani laporan saya di luar batas waktu yang dijanjikan, maka kepuasan saya mengalami:	Penanganan insiden atau permintaan layanan TI melebihi batas waktu yang disepakati	Proses bisnis layanan berjalan dengan baik serta meningkatnya kepuasan pengguna.	Banyaknya komplain pengguna layanan karena insiden tidak diselesaikan sesuai kesepakatan.
		Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan permintaan layanan	Penanganan insiden dapat dilakukan dengan tepat dan sesuai sehingga memudahkan apabila ingin di eskalasi sesuai kategori permasalahannya.	Penanganan insiden dan permintaan layanan terhambat karena data tidak sesuai sehingga dan membutuhkan waktu lebih lama untuk menyelesaikannya.
		Kesalahan *entry* data dari pengguna (pelapor)	Pengguna mengisikan data laporan insiden atau permintaan layanannya dengan tepat dan lengkap sehingga identifikasi dan	Terdapat kesalahan pengisian data, data dan informasi yang ada tidak relevan sehingga identifikasi dan penanganan

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
			penanganan insiden dapat berjalan dengan lancar, sesuai dan tepat waktu.	insiden menjadi terhambat dan membutuhkan waktu lebih lama.
		Helpdesk tidak mengajukan persetujuan finansial dan fungsional yang dibutuhkan	Proses penanganan insiden berjalan lancar dan dapat selesai tepat waktu karena telah disetujui baik secara fungsional maupun finansial jika membutuhkan biaya khusus.	Proses penanganan insiden terhambat karena belum adanya persetujuan finansial atau fungsional dari pihak manajemen sehingga tidak dapat dilanjutkan atau di *pending* terlebih dahulu sehingga membutuhkan waktu lebih lama.
		Sistem yang mendukung penanganan layanan TI tidak berfungsi	Proses penanganan insiden yang membutuhkan sistem TI tetap berjalan lancar sehingga membantu	Proses penanganan insiden yang membutuhkan sistem TI pendukung menjadi terhambat

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
			memudahkan *helpdesk* dalam menyelesaikan laporan.	sehingga penangannya tidak selesai tepat waktu.
		Helpdesk lupa atau tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	Proses penanganan insiden khususnya pada proses eskalasi berjalan lancar karena prosedur sudah jelas.	Pihak yang dieskalasi kesulitan dalam menangani insiden yang dialokasikan sehingga proses penanganan terhambat dan membutuhkan waktu lebih lama.
K05	Ketika *helpdesk* tidak melakukan verifikasi kepuasan saya untuk memastikan bahwa laporan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami :	Pengguna tidak diinformasikan mengenai penutupan insiden	Pengguna selalu mendapatkan informasi terkini terkait insiden atau permintaan layanan TI yang diajukannya dimana hal ini dapat meningkatkan kepuasan pengguna terhadap	Pengguna tidak mengetahui apakah insiden atau permintaan layanannya sudah selesai ditangani dan ditutup dimana hal ini dapat menurunkan kepuasan pengguna

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
			pelayanan yang diberikan *helpdesk*.	terhadap kinerja *helpdesk*.
		Pengguna tidak merespon penutupan insiden atau permintaan layanan TI	Penutupan insiden disetujui oleh pengguna karena sudah sesuai dengan harapan pengguna sehingga dapat meningkatkan kepuasan pengguna.	Penutupan insiden akan ditutup secara otomatis oleh *helpdesk* tanpa mengetahui tingkat kepuasan pengguna.
K06	Ketika *helpdesk* tidak memberi informasi status laporan saya (sedang direspon/selesai ditangani/telah ditutup), maka kepuasan saya mengalami:	Ketidakjelasan status insiden atau permintaan layanan	Baik pengguna/pelapor layanan, *helpdesk*, maupun teknisi mengetahui status permintaan layanan dan insiden dengan jelas sehingga laporan permintaan layanan dan insiden dapat segera dikelola dengan efektif.	Pengguna tidak mengetahui apakah permintaan layanan dan insiden telah ditanggapi, sedang ditangani, atau selesai ditangani sehingga pengguna/pelapor harus bertanya kembali ke *helpdesk*. Sedangkan *helpdesk* juga berisiko tidak

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
				mengetahui status permintaan layanan dan insiden yang sedang ditangani oleh teknisi (ketika telah alokasi / eskalasi dilakukan).
K07	Ketika *helpdesk* tidak menangani masalah yang berulang kali saya keluhkan hingga akar permasalahan, maka kepuasan saya mengalami:	Kesalahan pendefinisian tren dalam laporan	Tepat dalam mengidentifikasi insiden yang berubah status menjadi *problem* untuk segera diperbaiki hingga akar masalah sehingga dapat menghindari masalah yang berulang.	Insiden terjadi berulang namun tidak diidentifikasi sebagai *problem* untuk menghindari masalah yang berulang.
K08	Ketika *helpdesk* tidak mengalami peningkatan dalam melayani permintaan dan keluhan saya, maka kepuasan saya mengalami:	Pengguna enggan memberikan *feedback* layanan TI	Helpdesk bisa meningkatkan kinerjanya berdasarkan kritik dan saran dari pengguna.	Helpdesk tidak ada gambaran mengenai kritik dan saran pengguna sebagai masukan untuk

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
				meningkatkan kinerjanya.
		Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan	Manajemen organisasi dapat mengevaluasi hasil pengelolaan permintaan layanan dan insiden berdasarkan laporan yang telah didistribusikan.	Tidak adanya perubahan yang lebih baik terhadap evaluasi layanan pengelolaan permintaan layanan dan insiden.
K09	Ketika sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak dapat saya akses, maka kepuasan saya mengalami:	Kegagalan akses sistem *e-ticket*	Pengguna dapat mengandalkan sistem e-ticket untuk membuat laporan insiden dan permintaan layanan, serta unit *helpdesk* dapat menerima dan mengelola laporan dari pengguna dengan tepat	Menumpuk-nya pelaporan melalui sistem manual (*e-mail* dan telepon), serta *helpdesk* tidak dapat melacak status pelaporan yang sedang ditangani.
K10	Ketika keamanan informasi pada sistem *e-ticket* (*website* untuk pelaporan keluhan dan	Bocornya laporan kepada pihak lain	Data dan informasi yang kritis selalu terjaga keamanannya dan hanya	Data dan informasi yang kritis diketahui dan dapat

ID	Pernyataan	Risiko	Skenario Risiko	
			Skenario Positif	Skenario Negatif
	permintaan) tidak terlindungi, maka kepuasan saya mengalami:		pihak yang berwenang yang dapat mengaksesnya.	disalahgunakan oleh pihak yang tidak berwenang.
		Penyalahgunaan hak akses permintaan layanan TI	Organisasi tidak mengalami kerugian baik finansial dikarenakan pemenuhan permintaan layanan sesuai sebagaimana prosedurnya, serta data (aset kritis) organisasi tidak terancam oleh pihak tidak berwenang.	Kerugian organisasi terhadap pemenuhan permintaan di luar hak pengguna, baik kehilangan data (aset kritis), maupun kerugian finansial.

6.6 Penilaian Risiko

Pada tahap penilaian risiko TI berdasarkan perkiraan frekuensi dan dampaknya besarnya keuntungan atau kerugian yang terkait dengan skenario risiko TI. Penentuan nilai frekuensi risiko didapatkan dari hasil wawancara, sedangkan penentuan nilai dampak risiko yaitu keunggulan kompetitif didapatkan dari hasil kuesioner, sedangkan penentuan nilai aspek produktivitas, biaya tanggapan dan hukum didapatkan dari hasil wawancara. Perhitungan rata-rata penilaian risiko untuk keseluruhan peringkat dampak mengikuti aturan pembulatan desimal, dimana apabila nilai desimal dibawah 0.5 maka akan dibulatkan ke angka dibawah satu digit, sedangkan apabila nilai desimal diatas 0.5, maka akan dibulatkan ke angka diatas satu digit. Berikut hasil penilaian risiko TI yang telah dipetakan menjadi level penilaian risiko ditampilkan pada Tabel 6.9.

Tabel 6.9 Penilaian Frekuensi dan Dampak Risiko

No	Kategori Risiko TI	ID Risiko	Risiko	Frekuensi	Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Rata-rata Peringkat Dampak	Level Risiko
1.	*IT expertise and skill*	IES001	Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan	1	1	1	3	1	1.5	*Low*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
			permintaan layanan							
2.	*IT expertise and skill*	IES002	Kesalahan memahami permintaan pengguna	3	1	1	4	1	1,75	*Medium*
3.	*IT expertise and skill*	IES003	Kesalahan pengalokasian kategorisasi atau prioritas insiden dan permintaan layanan	1	1	1	4	1	1,75	*Low*
4.	*IT expertise and skill*	IES004	Keterlambatan respon *helpdesk*	4	1	1	4	1	1,75	*High*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
5.	*IT expertise and skill*	IES005	Pihak yang di eskalasi melakukan kesalahan penanganan insiden atau permintaan layanan TI	1	1	1	4	1	1,75	*Low*
6.	*IT expertise and skill*	IES006	Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI	2	1	1	4	1	1,75	*Medium*
7.	*IT expertise and skill*	IES007	Kesalahan dalam melakukan eksekusi	2	1	1	4	1	1,75	*Medium*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
			penanganan insiden atau pemenuhan layanan TI							
8.	*IT expertise and skill*	IES008	Kesalahan pendefinisian tren dalam laporan	3	1	1	3	1	1,5	*Medium*
9.	*IT expertise and skill*	IES009	Kesalahan mendiagnosa gejala insiden	2	1	1	4	1	1,75	*Medium*
10.	*Staff operation (human error and malicious intent)*	SOH001	Kesalahan *entry* data dari pengguna (pelapor)	3	1	1	3	1	1,5	*Medium*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tangga pan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Perin gkat Damp ak	Level Risiko
11.	*Staff operation (human error and malicious intent)*	SOH002	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk	2	1	1	4	1	1,75	*Medium*
12.	*Staff operation (human error and malicious intent)*	SOH003	*Helpdesk* lupa atau tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	4	1	1	3	1	1,5	*Medium*
13.	*Staff operation (human*	SOH004	*Helpdesk* tidak mengajukan persetujuan	1	1	1	3	1	1,5	*Low*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
	error and malicious intent)		finansial dan fungsional yang dibutuhkan							
14.	*Staff operation (human error and malicious intent)*	SOH005	Kesalahan pencatatan (*logging)* insiden atau permintaan layanan	3	1	1	4	1	1,75	*Medium*
15.	*Staff operation (human error and malicious intent)*	SOH006	*Log* insiden atau permintaan layanan TI tidak lengkap	3	1	1	4	1	1,75	*Medium*
16.	*Staff operatio*	SOH007	Kesalahan melakukan	3	1	1	4	1	1,75	*Medium*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
	n (human error and maliciou s intent)		distribusi (eskalasi) insiden atau permintaan layanan TI							
17.	*Staff operatio n (human error and maliciou s intent)*	SOH00 8	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan TI yang masuk	1	1	1	4	1	1,75	*Low*
18.	*Staff operatio n (human error and maliciou s intent)*	SOH00 9	Penanganan insiden atau permintaan layanan TI melebihi batas	4	1	1	3	1	1,5	*Medium*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
			waktu yang disepakati							
19.	*Staff operation (human error and malicious intent)*	SOH010	Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap	3	1	1	4	1	1.75	*Medium*
20.	*Staff operation (human error and malicious intent)*	SOH011	Ketidakpuasan pengguna terhadap layanan yang diberikan	4	1	1	4	1	1,75	*High*
21.	*Staff operation (human*	SOH012	Pengguna enggan memberikan	4	1	1	3	1	1,5	*Medium*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
	error and malicious intent)		*feedback* layanan TI							
22.	*Staff operation (human error and malicious intent)*	SOH013	Pengguna tidak menyetujui status penutupan insiden	4	1	1	4	1	1,75	*High*
23.	*Staff operation (human error and malicious intent)*	SOH014	Pengguna tidak diinformasikan mengenai penutupan insiden	3	1	1	3	1	1,5	*Medium*
24.	*Staff operatio*	SOH015	Pengguna tidak merespon	4	1	1	3	1	1,5	*Medium*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
	n (human error and maliciou s intent)		penutupan insiden atau permintaan layanan TI							
25.	*Staff operatio n (human error and maliciou s intent)*	SOH01 6	Ketidakjelasan status insiden atau permintaan layanan	4	1	1	3	1	1,5	*Medium*
26.	*Staff operatio n (human error and maliciou s intent)*	SOH01 7	Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan	2	1	1	3	1	1,5	*Low*

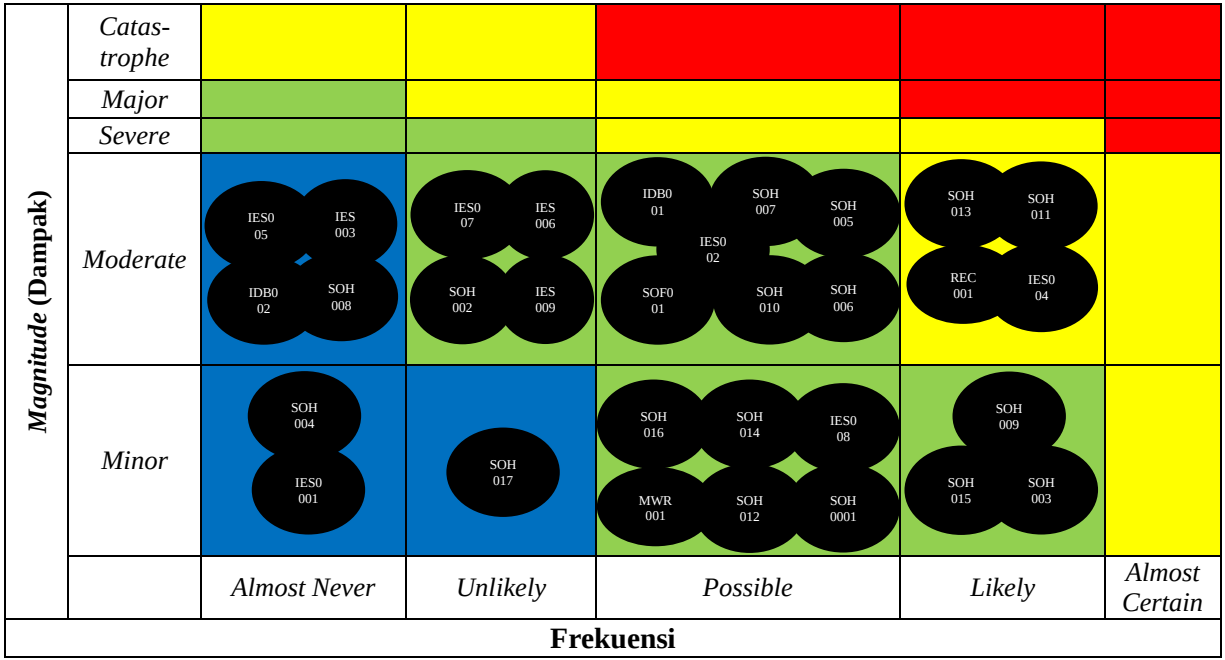
No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tangga pan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Perin gkat Damp ak	Level Risiko
27.	*Information (data,breanch: damage,leakage and access)*	IDB001	Penyalahgunaan hak akses permintaan layanan TI	3	1	1	4	1	1,75	*Medium*
28.		IDB002	Bocornya laporan pada pihak lain	1	1	1	4	1	1,75	*Low*
29.	*Software*	SOF001	Kegagalan akses sistem e-ticket	3	1	1	4	1	1,75	*Medium*
30.	*Regulatory Compliance*	REC001	Prosedur pengelolaan insiden tidak tersedia secara tertulis	4	1	1	4	1	1,75	*High*

No	Kategori Risiko TI	ID Risiko	Risiko	Fre-kuensi	Produkti-vitas	Biaya Tanggapan	Keung-gulan Kompe-titif	Hu-kum	Rata-rata Peringkat Dampak	Level Risiko
31.	*Malware*	MWR001	Sistem yang mendukung penanganan layanan TI tidak berfungsi	3	1	1	3	1	1,5	*Medium*

Berdasarkan hasil penilaian risiko diatas, maka dapat diketahui bahwa:

1. Risiko yang memiliki level *high*:
   - Paling banyak berasal dari kategori *staff operations* (*human error and malicious intent*) yaitu sebanyak 2 (dua) risiko.
   - 1 (satu) risiko level *high* lain berasal dari *regulatory compliance*.
   - 1 (satu) risiko level *high* lain lagi berasal dari kategori *IT expertise and skills*.
2. Risiko yang memiliki level *medium:*
   - Paling banyak berasal dari kategori *staff operations* (*human error and malicious intent*) yaitu sebanyak 12 (dua belas) risiko.
   - 5 (lima) risiko level *medium* lain berasal dari kategori *IT expertise and skills*.
   - 1 (satu) risiko level *high* lain berasal dari kategori *malware*.
   - 1 (satu) risiko berlevel *medium* lain berasal dari kategori *information (data,breanch: damage,leakage and access)*.
   - 1 (satu) risiko level *low* lain berasal dari kategori *software*.
3. Risiko yang memiliki level *low:*
   - Paling banyak berasal dari kategori *IT expertise and skils* dan *staff operations* dimana masing-masing terdiri dari 3 (tiga risiko).
   - 1 (satu) risiko level *low* lain berasal dari kategori *information (data,breanch: damage,leakage and access)*.

Berikut merupakan persebaran letak risiko berdasarkan frekuensi dan dampak (*magnitude*) nya yang disajikan melalui *Risk Scatter* pada Bagan 6.1



Bagan 6.1 ***Risk Scatter***

Berdasarkan *risk scatter* diatas, dapat dilihat persebaran risiko mayoritas berada kategori *medium* dan paling sedikit berada pada kategori *high*. Selanjutnya untuk melakukan mitigasi risiko, perlu dilakukan prioritas risiko. Prioritas dapat ditentukan berdasarkan hasil penilaian risiko. Jika hasil penilaian risiko yang cukup tinggi maka risikonya akan diprioritaskan untuk aksi mitigasi. Sementara itu risiko lainnya yang tidak berada pada kategori *high* maka dapat ditentukan oleh nilai frekuensi dengan mempertimbangkan dampak risiko agar dapat diprioritaskan untuk aksi mitigasi risiko.

6.7 Penentuan Respon Risiko

Setelah melakukan penilaian risiko, selanjutnya dilakukan tahap pemberian respon risiko. Berikut merupakan tabel penentuan pilihan respon risiko berdasarkan COBIT 5, yaitu *risk acceptance* (diterima), *mitigation* (mitigasi), *avoidance* (dihindari), *share/transfer* (dialihkan) yang disajikan pada Tabel 6.10.

Tabel 6.10 Respon Risiko

No.	Risiko	Respon Risiko
•	Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan permintaan layanan	*Mitigate (Treat)*
•	Kesalahan *entry* data dari pengguna (pelapor)	*Mitigate (Treat)*
•	Kegagalan akses sistem *e-ticket*	*Transfer*
•	Kesalahan memahami permintaan pengguna	*Mitigate (Treat)*
•	*Helpdesk* lupa atau tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	*Mitigate (Treat)*
•	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk	*Mitigate (Treat)*
•	Kesalahan pengalokasian kategorisasi atau prioritas insiden dan permintaan layanan	*Mitigate (Treat)*
•	Keterlambatan respon *helpdesk*	*Mitigate (Treat)*

No.	Risiko	Respon Risiko
•	Penyalahgunaan hak akses permintaan layanan TI	*Mitigate (Treat)*
•	*Helpdesk* tidak mengajukan persetujuan finansial dan fungsional yang dibutuhkan	*Avoid*
•	Prosedur pengelolaan insiden tidak tersedia secara tertulis	*Mitigate (Treat)*
•	Kesalahan mendiagnosa gejala insiden	*Mitigate (Treat)*
•	Kesalahan pencatatan (*logging)* insiden atau permintaan layanan	*Mitigate (Treat)*
•	*Log* insiden atau permintaan layanan TI tidak lengkap	*Mitigate (Treat)*
•	Kesalahan melakukan distribusi (eskalasi) insiden atau permintaan layanan TI	*Avoid*
•	Pihak yang di eskalasi melakukan kesalahan penanganan insiden atau permintaan layanan TI	*Transfer*
•	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan TI yang masuk	*Transfer*
•	Sistem yang mendukung penanganan layanan TI tidak berfungsi	*Transfer*
•	Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI	*Mitigate (Treat)*
•	Kesalahan dalam melakukan eksekusi penanganan insiden atau pemenuhan layanan TI	*Mitigate (Treat)*
•	Penanganan insiden atau permintaan layanan TI melebihi batas waktu yang disepakati	*Mitigate (Treat)*
•	Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap	*Mitigate (Treat)*
•	Ketidakpuasan pengguna terhadap layanan yang diberikan	*Mitigate (Treat)*
•	Pengguna enggan memberikan *feedback* layanan TI	*Take*
•	Pengguna tidak menyetujui status penutupan insiden	*Mitigate (Treat)*
•	Pengguna tidak diinformasikan mengenai penutupan insiden	*Avoid*
•	Pengguna tidak merespon penutupan insiden atau permintaan layanan TI	*Take*

No.	Risiko	Respon Risiko
•	Ketidakjelasan status insiden atau permintaan layanan	*Mitigate (Treat)*
•	Kesalahan pendefinisian tren dalam laporan	*Mitigate (Treat)*
•	Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan	*Mitigate (Treat)*
•	Bocornya laporan kepada pihak lain	*Mitigate (Treat)*

6.8 Analisis Langkah Mitigasi Risiko berdasarkan Pemetaan Proses COBIT 5

Setelah risiko selesai diidentifikasi, maka dapat ditentukan langkah mitigasi dimana pada penelitian ini menggunakan pemetaan dengan proses TI COBIT 5 kemudian diambil beberapa aktivitas *key management practices* yang relevan untuk diimplementasikan organisasi. Berikut merupakan analisis proses TI COBIT 5 yang sesuai berdasarkan kategori risiko berserta justifikasi pemetaannya yang disajikan pada Tabel 6.11.

Tabel 6.11 Analisis Pemetaan Kategori Risiko dengan Proses TI COBIT 5

No.	Kategori	Justifikasi Kategori	Proses TI COBIT 5 yang Sesuai	Justifikasi Pemetan dengan Proses TI COBIT 5
1.	*IT expertise and skills* (Ketrampilan dan kemampuan TI)	Risiko yang berhubungan dengan ketrampilan dan kemampuan TI SDM	APO07 *Manage Human Resource*	Proses ini memberikan pendekatan terstruktur untuk memastikan penataan dan penempatan SDM secara optimal, pendefinisian peran dan tanggung jawab kinerja, evaluasi kinerja, pemberian penghargaan (*reward*), serta perencanaan pertumbuhan dan pembelajaran (*learning and growth*) untuk memastikan optimalisasi kinerja SDM untuk mencapai tujuan organisasi. Risiko yang berhubungan dengan keterampilan dan kemampuan TI (*IT expertise and skills*) SDM membutuhkan mitigasi berupa

No.	Kategori	Justifikasi Kategori	Proses TI COBIT 5 yang Sesuai	Justifikasi Pemetan dengan Proses TI COBIT 5
				pengadaan pelatihan untuk meningkatkan kemampuan dan keterampilan SDM serta mengadakan evaluasi kinerja untuk mengukur kemampuannya agar sesuai tujuan organisasi.
2.	*Staff operations (human error and malicious intent)* (Staff operasional (kesalahan dan niat buruk manusia))	Risiko yang berhubungan dengan kesalahan staff operasional seperti yang tidak disengaja (*human error*) atau kesalahan yang disengaja	DSS01 *Manage Operations*	Proses ini meliputi pelaksanaan kegiatan operasional dengan menyusun, mengembangkan dan menerapkan kebijakan khusus dan prosedur operasional yang telah ditetapkan. Tujuannya ialah memberikan pelayanan operasional TI yang optimal. Risiko yang berhubungan dengan kesalahan *staff* bisa diminimalisir dengan cara menetapkan dan mengimplementasikan kebijakan beserta prosedur operasional agar proses bisnis lebih terstruktur, dan berjalan seragam.

No.	Kategori	Justifikasi Kategori	Proses TI COBIT 5 yang Sesuai	Justifikasi Pemetan dengan Proses TI COBIT 5
			APO11 *Manage Quality*	Proses ini mendefinisikan kriteria kualitas, penggunaan standar kualitas serta pemantauannya untuk memastikan layanan yang diberikan organisasi memenuhi kriteria kualitas serta meningkatkan kepuasan *stakeholder* dengan memenuhi kebutuhannya. Risiko yang berhubungan dengan kesalahan *staff* akan berdampak pada hasil atau layanan yang diberikan kepada *stakeholder* atau *customer*, sehinga dapat dimitigasi dengan selalu menerapkan standar kualitas pelayanan demi meningkatkan kepuasan pelanggan.

No.	Kategori	Justifikasi Kategori	Proses TI COBIT 5 yang Sesuai	Justifikasi Pemetan dengan Proses TI COBIT 5
3.	*Information (data breach: damage, leakage and access)* (Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses))	Risiko yang berhubungan dengan data dan informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses)	DSS05 *Manage Security Services*	Proses ini meliputi perlindungan aset informasi perusahaan sesuai kebijakan keamanan informasi untuk menghindari terjadinya risiko yang berhubungan dengan keamanan informasi. Tujuanya ialah meminimalkan dampak bisnis dari kerentanan keamanan informasi. Risiko yang berhubungan dengan data dan informasi harus dikelola karena kedua hal tersebut merupakan aset kritis sehingga perlu dilindungi sesuai standar keamanan informasi.
4.	*Software* (Perangkat lunak)	Risiko yang berhubungan dengan perangkat lunak	BAI09 *Manage Assets*	Proses ini meliputi pengelolaan aset TI melalui siklus hidup mereka untuk memastikan bahwa penggunaannya memberikan nilai pada perusahaan, dapat diandalkan mendukung kemampuan layanan tujuan bisnis, terlindungi secara fisik dan logikal. Risiko yang berhubungan dengan aset TI seperti *hardware* dan *software* dapat
5.	*Malware* (Virus)	Risiko yang berhubungan dengan virus, *worm*, *malware*		

No.	Kategori	Justifikasi Kategori	Proses TI COBIT 5 yang Sesuai	Justifikasi Pemetan dengan Proses TI COBIT 5
				di mitigasi dengan cara memberikan perlindungan dan pemeliharaan aset.
6.	*Regulatory compliance* (Pemenuhan regulasi)	Risiko yang berhubungan dengan regulasi organisasi	DSS01 *Manage Operations*	Proses ini meliputi pelaksanaan kegiatan operasional dengan menyusun, mengembangkan dan menerapkan kebijakan dan prosedur operasional yang telah ditetapkan. Tujuannya ialah memberikan pelayanan operasional TI yang optimal. Risiko yang berhubungan dengan pemenuhan regulasi organisasi dapat di mitigasi dengan cara mengimplementasikan penatakelolaan TI yaitu dengan menyusun dan menerapkan kebijakan dan prosedur operasional agar proses bisnis lebih terstruktur, dan berjalan seragam.

Berdasarkan analisis pada Tabel 6.11 diatas, dapat diketahui langkah mitigasi yang sesuai dengan kategori risiko. Maka berikut merupakan analisis langkah mitigasi yang dibuat berdasarkan prioritas level risiko, dimana untuk risiko berlevel *high* dibuat detail per aktivitas untuk meminimalisir dampak kerugian organisasi.

Sedangkan untuk risiko berlevel *medium* dan *low* dilakukan pemetaan terhadap *key management practices* COBIT 5 yang sesuai yang disajikan pada Tabel 6.12.

Tabel 6.11 Analisis Langkah Mitigasi Risiko berdasarkan Pemetaan Proses COBIT 5

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
1.	*Staff operation (human error and malicious intent)*	SOH011	Ketidakpuasan pengguna terhadap layanan yang diberikan	*High*	APO11 *Manage Quality*	**APO11.03** ***Focus quality management on customers*** **-** Memfokuskan manajemen kualitas untuk meningkatkan kepuasan pelanggan dengan mengidentifikasi kebutuhan pelanggan dan menyelaraskannya dengan *quality management practices*. - Identifikasi kebutuhan utama pelanggan. - Identifikasi kriteria penerimaan kualitas pelanggan dengan menyelaraskannya terhadap standar kualitas TI.
2.	*Staff operation (human error and malicious intent)*	SOH013	Pengguna tidak menyetujui status penutupan insiden	*High*		

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						- Melaksanakan pelayanan sesuai kebutuhan dan kriteria penerimaan pelanggan. - Memverifikasi hasil pelayanan terhadap kepuasan pelanggan. - Secara teratur meminta *feedback* pelanggan untuk meningkatkan pelayanan. - Menerapkan standar manajemen kualitas. - Memberikan stabilisasi respon - Menjaga komunikasi dan memberikan informasi terbaru terkait laporan yang diajukannya. - Secara berkala lakukan survei kepuasan pelanggan

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						dan pertimbangkan hasilnya untuk meningkatkan kinerja pelayanan.
3.	*IT expertise and skill*	IES004	Keterlambatan respon *helpdesk*	*High*	APO07 *Manage Human Resource*	**APO07.04 *Evaluate employee job performance* -** Lakukan evaluasi kinerja individu secara teratur terhadap untuk melihat ketercapaian tujuan tujuan organisasi dengan melihat keterampilan dan kompetensi pegawai serta pelaksanaan peran dan tanggung jawab pegawai**..** Aktivitas: - Menetapkan skema prioritasi sesuai tingkat kritikal layanan.

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						- Melakukan pengawasan dan pemantauan berkala terkait kinerja operasional. - Memastikan ketersediaan sumber daya seperti infrastruktur, SDM. - Melakukan evaluasi kinerja pegawai secara menyeluruh dan rutin. - Memberikan *feedback* terkait kinerja tiap individu sesuai dengan ketercapaian tujuan organisasi. - Memberikan *reward* atas komitmen yang tepat, pengembangan kompetensi dan pencapaian keberhasilan suatu tujuan kinerja yang tentunya harus diterapkan

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						secara konsisten dan sejalan dengan kebijakan organisasi - Mengembangkan *Performance Improvement Plan* berdasarkan hasil evaluasi, maupun kebutuhan training dan peningkatan keterampilan SDM. - Menetapkan standar manajemen kualitas
4.	*Regulatory Compliance*	REC001	Prosedur pengelolaan insiden tidak tersedia secara tertuli	*High*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan kebijakan dan prosedur operasional serta tugas operasional secara andal dan konsisten.

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						- Susun, kembangkan dan pelihara kebijakan beserta prosedur operasional pengelolaan insiden dan permintaan layanan. - Implementasikan kebijakan dan prosedur untuk menunjang keefektifan proses bisnis. - Lakukan evaluasi berkala terkait keefektifkan penerapan kebijakan dan prosedur.
5.	*Staff operation (human error and malicious intent)*	SOH009	Penanganan insiden atau permintaan layanan TI melebihi batas waktu yang disepakati	*Medium*	APO11 *Manage Quality*	**APO11.04** ***Perform quality monitoring, control and reviews*** **-** Memantau kualitas proses dan layanan secara berkelanjutan seperti yang didefinisikan oleh QMS

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
6.	*Staff operation (human error and malicious intent)*	SOH015	Pengguna tidak merespon penutupan insiden atau permintaan layanan TI	*Medium*		(*Quality Management Standard*). Mendefinisikan, merencanakan dan melaksanakan pengukuran untuk memantau kepuasan pelanggan dengan kualitas sesuai dengan QMS. Aktivitas: - Mengidentifikasi kebutuhan pelanggan dan kriteria penerimaan kualitasnya. - Melaksanakan pelayanan sesuai kebijakan, prosedur dan jadwal yang telah dibuat secara konsisten dan efektif. - Mengkomunikasikan kepada pelanggan terkait informasi terkini yang

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						menghambat proses pelayanan. - Memverifikasi penanganan yang diberikan terhadap kebutuhan dan kriteria penerimaan kualitas pelanggan.
7.	*Staff operation (human error and malicious intent)*	SOH003	*Helpdesk* lupa atau tidak menginformasikan prosedur eskalasi insiden kepada pihak yang melakukan eskalasi	*Medium*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan kebijakan dan prosedur operasional serta tugas operasional secara andal dan konsisten. - Susun, kembangkan dan pelihara kebijakan dan prosedur operasional pengelolaan insiden dan permintaan layanan.

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						- Implementasikan kebijakan dan prosedur untuk menunjang keefektifan proses bisnis. - Lakukan evaluasi berkala terkait keefektifkan penerapan kebijakan dan prosedur.
8.	*IT expertise and skill*	IES002	Kesalahan memahami permintaan pengguna	*Medium*	BAI02 *Manage Requirements Definition*	**BAI02.01** ***Define and maintain business functional and technical requirements*** **-** Mengidentifikasi, memprioritaskan, dan menspesifikkan informasi bisnis, fungsional, teknis, dan control requirements yang meliputi ruang lingkup / pemahaman dari semua inisiatif yang diperlukan untuk

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						mencapai hasil yang diharapkan dari solusi bisnis.
9.	*Staff operation (human error and malicious intent)*	SOH005	Kesalahan pencatatan (*logging)* insiden atau permintaan layanan	*Medium*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures* -** Memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten.
10.	*Staff operation (human error and malicious intent)*	SOH006	*Log* insiden atau permintaan layanan TI tidak lengkap	*Medium*		
11.	*Staff operation (human error and*	SOH007	Kesalahan melakukan distribusi (eskalasi) insiden atau permintaan layanan TI	*Medium*		

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
	malicious intent)					
12.	*Information (data,breanch: damage,leakage and access)*	IDB001	Penyalahgunaan hak akses permintaan layanan TI	*Medium*	DSS05 *Manage Security Services*	**DSS05.04** ***Manage user identity and logical access*** **-** Memastikan bahwa semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnisnya dan melakukan koordinasi dengan unit bisnis yang mengelola hak akses dalam proses bisnis.
13.	*Software*	SOF001	Kegagalan akses sistem e-ticket	*Medium*	BAI09 *Manage Assets*	**BAI09.02** ***Manage critical assets*** **-** Identifikasi aset kritis yang memberikan kemampuan layanan dan mengambil langkah-langkah untuk memaksimalkan keandalan dan ketersediaan aset untuk mendukung kebutuhan bisnis.

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
14.	*Staff operation (human error and malicious intent)*	SOH012	Pengguna enggan memberikan *feedback* layanan TI	*Medium*	APO11 *Manage Quality*	**APO11.04** ***Perform quality monitoring, control and reviews*** **-** Memantau kualitas proses dan layanan secara berkelanjutan seperti yang didefinisikan oleh QMS (*Quality Management Standard*). Mendefinisikan, merencanakan dan melaksanakan pengukuran untuk memantau kepuasan pelanggan dengan kualitas sesuai dengan QMS.
15.	*Staff operation (human error and malicious intent)*	SOH014	Pengguna tidak diinformasikan mengenai penutupan insiden	*Medium*	APO11 *Manage Quality*	**APO11.04** ***Perform quality monitoring, control and reviews*** **-** Memantau kualitas proses dan layanan secara berkelanjutan seperti yang didefinisikan oleh QMS (*Quality Management*

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						Standard). Mendefinisikan, merencanakan dan melaksanakan pengukuran untuk memantau kepuasan pelanggan dengan kualitas sesuai dengan QMS.
16.	*IT expertise and skill*	IES008	Kesalahan pendefinisian tren dalam laporan	*Medium*	APO07 *Manage Human Resource*	**APO07.03** ***Maintain the skills and competencies of personnel*** - Mendefinisikan dan mengelola keterampilan dan kompetensi yang dibutuhkan personil.
17.	*Malware*	MWR001	Sistem yang mendukung penanganan layanan TI tidak berfungsi	*Medium*	BAI09 *Manage Assets*	**BAI09.02** ***Manage critical assets*** - Identifikasi aset kritis yang memberikan kemampuan layanan dan mengambil langkah-langkah untuk memaksimalkan keandalan

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						dan ketersediaan aset untuk mendukung kebutuhan bisnis.
18.	*IT expertise and skill*	IES006	Kesalahan dalam memilih solusi penanganan insiden atau permintaan layanan TI	*Medium*	BAI02 *Manage Requirements Definition*	**BAI02.02** ***Perform a feasibility study and formulate alternative solutions*** - Melakukan studi kelayakan solusi alternatif potensial, menilai kelayakannya dan pilih yang dianggap paling relevan.
19.	*IT expertise and skill*	IES007	Kesalahan dalam melakukan eksekusi penanganan insiden atau pemenuhan layanan TI	*Medium*	APO07 *Manage Human Resource*	**APO07.03** ***Maintain the skills and competencies of personnel*** - Mendefinisikan dan mengelola keterampilan dan kompetensi yang dibutuhkan personil.
20.	*IT expertise and skill*	IES009	Kesalahan mendiagnosa gejala insiden	*Medium*	APO07 *Manage Human Resource*	**APO07.03** ***Maintain the skills and competencies of personnel*** - Mendefinisikan dan mengelola keterampilan

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
						dan kompetensi yang dibutuhkan personil.
21.	*Staff operation (human error and malicious intent)*	SOH001	Kesalahan *entry* data dari pengguna (pelapor)	*Medium*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten.
22.	*Staff operation (human error and malicious intent)*	SOH016	Ketidakjelasan status insiden atau permintaan layanan	*Medium*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten.
23.	*Staff operation (human*	SOH002	*Helpdesk* tidak mencatat insiden atau	*Medium*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
	error and malicious intent)		permintaan layanan TI yang masuk			kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten.
24.	*Staff operation (human error and malicious intent)*	SOH010	Laporan penyelesaian insiden atau permintaan layanan TI tidak lengkap	*Medium*		
25.	*Staff operation (human error and malicious intent)*	SOH017	Laporan pengelolaan insiden dan permintaan layanan tidak terdistribusikan	*Low*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten.

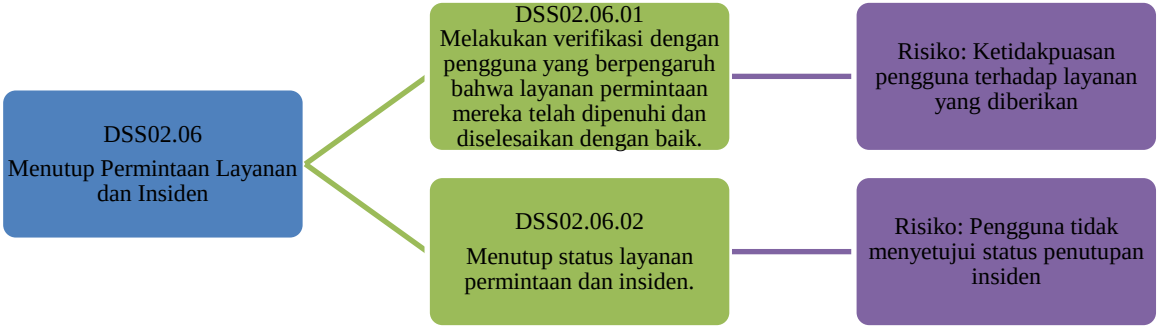
No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
26.	*IT expertise and skill*	IES003	Kesalahan pengalokasian kategorisasi atau prioritas insiden dan permintaan layanan	*Low*	APO07 *Manage Human Resource*	**APO07.03** ***Maintain the skills and competencies of personnel*** - Mendefinisikan dan mengelola keterampilan dan kompetensi yang dibutuhkan personil.
27.	*IT expertise and skill*	IES005	Pihak yang di eskalasi melakukan kesalahan penanganan insiden atau permintaan layanan TI	*Low*		
28.	*Information (data,breanch: damage,leakage and access*	IDB002	Bocornya laporan pada pihak lain	*Low*	DSS05 *Manage Security Services*	**DSS05.06** ***Manage sensitive documents and output devices*** - Membangun pengamanan fisik yang memadai, melakukan praktik pemeliharaan aset TI sensitif, seperti bentuk dokumen rahasia, surat berharga, printer tujuan khusus atau token keamanan.

No	Kategori Risiko TI	ID Risiko	Risiko	Level Risiko	Pemetaan Proses COBIT 5	Langkah Mitigasi Berdasarkan Aktivitas COBIT 5
29.	*Staff operation (human error and malicious intent)*	SOH008	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan TI yang masuk	*Low*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten.
30.	*Staff operation (human error and malicious intent)*	SOH004	*Helpdesk* tidak mengajukan persetujuan finansial dan fungsional yang dibutuhkan	*Low*	DSS01 *Manage Operations*	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten.
31.	*IT expertise and skill*	IES001	Kesalahan pembuatan sistem kategorisasi atau sistem prioritas insiden dan permintaan layanan	*Low*	APO07 *Manage Human Resource*	**APO07.03 *Maintain the skills and competencies of personnel*** - Mendefinisikan dan mengelola keterampilan dan kompetensi yang dibutuhkan personil.

6.8.1 Pemetaan Risiko dengan Proses TI Helpdesk

Berikut merupakan pemetaan risiko level *high* dengan proses TI *helpdesk* yang disajikan pada Bagan dibawah.

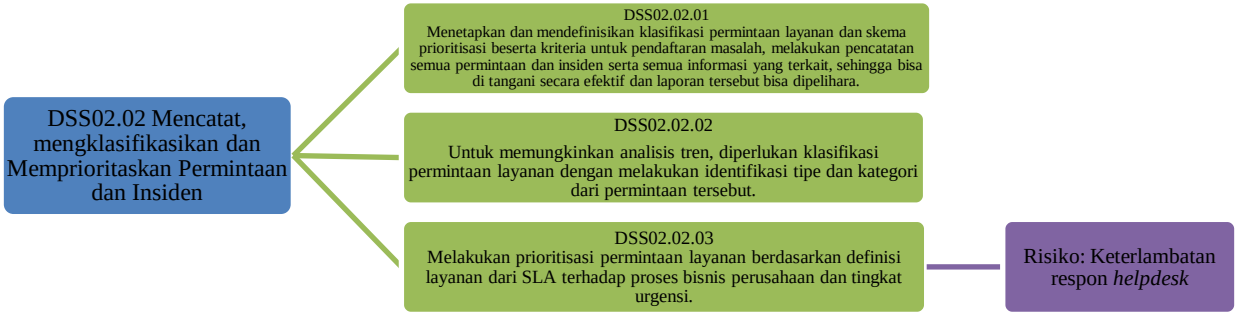
1. Risiko: Ketidakpuasan pengguna terhadap layanan yang diberikan dan pengguna tidak menyetujui status penutupan insiden.



Bagan 6.2 Pemetaan Risiko High 1 dan 2

Dapat diketahui bahwa pada aktivitas melakukan verifikasi penanganan layanan dapat terjadi risiko bahwa pelanggan atau pengguna tidak puas terhadap layanan yang diberikan. Selain itu pada aktivitas menutup status layanan permintaan dan insiden dapat diketahui bahwa pengguna tidak menyetujui status perubahan tersebut.

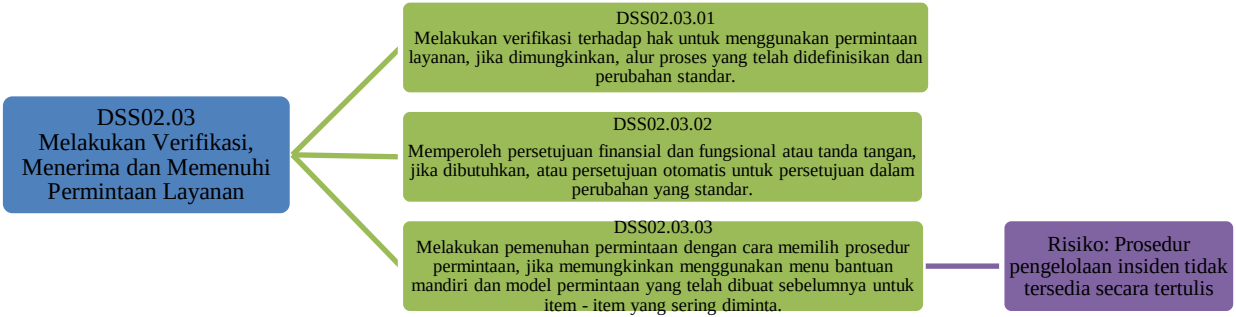
2. Risiko: Keterlambatan respon *helpdesk*



Bagan 6.3 Pemetaan Risiko High 3

Dapat diketahui bahwa pada proses DSS02.02 Mencatat, mengklasifikasikan dan Memprioritaskan Permintaan dan Insiden terutama pada proses melakukan prioritisasi permintaan layanan terhadap proses tingkat urgensi terdapat risiko keterlambatan respon *helpdesk*.

3. Risiko: Prosedur pengelolaan insiden tidak tersedia secara tertulis



Bagan 6.4 Pemetaan Risiko High 4

Dapat diketahui bahwa pada proses melakukan verifikasi dan memenuhi permintaan layanan terdapat aktivitas melakukan pemenuhan layanan sesuai prosedur, namun terdapat risiko bahwa prosedur pengelolaan insiden tidak tersedia secara tertulis.

6.8.2 *Risk Management Plan*

Berdasarkan hasil mitigasi risiko yang berlevel *high*, kemudian di identifikasi penanggung jawab risiko yang sesuai. Berikut hasilnya pada Tabel 6.12.

Tabel 6.12 Risk Management Plan

Aktivitas	Risiko	Mitigasi	Penanganggung Jawab
DSS02.06.01 -Melakukan verifikasi dengan pengguna yang berpengaruh bahwa layanan permintaan mereka telah dipenuhi dan diselesaikan dengan baik	Ketidakpuasan pengguna terhadap layanan yang diberikan	**APO11.03** ***Focus quality management on customers*** **-** Memfokuskan manajemen kualitas untuk meningkatkan kepuasan pelanggan dengan mengidentifikasi kebutuhan pelanggan dan menyelaraskannya dengan *quality management practices*. - Identifikasi kebutuhan utama pelanggan. - Identifikasi kriteria penerimaan kualitas pelanggan dengan menyelaraskannya terhadap standar kualitas TI.	Kepala Divisi

Aktivitas	Risiko	Mitigasi	Penanganggung Jawab
		- Melaksanakan pelayanan sesuai kebutuhan dan kriteria penerimaan pelanggan. - Memverifikasi hasil pelayanan terhadap kepuasan pelanggan. - Secara teratur meminta *feedback* pelanggan untuk meningkatkan pelayanan. - Menerapkan standar manajemen kualitas. - Memberikan stabilisasi respon - Menjaga komunikasi dan memberikan informasi terbaru terkait laporan yang diajukannya. - Secara berkala lakukan survei kepuasan pelanggan dan pertimbangkan hasilnya untuk meningkatkan kinerja pelayanan.	
DSS02.06.02 - Menutup status layanan permintaan dan insiden.	Pengguna tidak menyetujui status penutupan insiden		

Aktivitas	Risiko	Mitigasi	Penanganggung Jawab
DSS02.02.03 - Melakukan prioritisasi permintaan layanan berdasarkan definisi layanan dari SLA terhadap proses bisnis perusahaan dan tingkat urgensi.	Keterlambatan respon *helpdesk*	**APO07.04** ***Evaluate employee job performance*** **-** Lakukan evaluasi kinerja individu secara teratur terhadap untuk melihat ketercapaian tujuan tujuan organisasi dengan melihat keterampilan dan kompetensi pegawai serta pelaksanaan peran dan tanggung jawab pegawai.. Aktivitas: - Menetapkan skema prioritasi sesuai tingkat kritikal layanan. - Melakukan pengawasan dan pemantauan berkala terkait kinerja operasional. - Memastikan ketersediaan sumber daya seperti infrastruktur, SDM. - Melakukan evaluasi kinerja pegawai secara menyeluruh dan rutin. - Memberikan *feedback* terkait kinerja tiap individu sesuai dengan ketercapaian tujuan organisasi.	Kepala Divisi dan diawasi oleh Kepala Subdirektorat

Aktivitas	Risiko	Mitigasi	Penanganggung Jawab
		- Memberikan *reward* atas komitmen yang tepat, pengembangan kompetensi dan pencapaian keberhasilan suatu tujuan kinerja yang tentunya harus diterapkan secara konsisten dan sejalan dengan kebijakan organisasi - Mengembangkan *Performance Improvement Plan* berdasarkan hasil evaluasi, maupun kebutuhan training dan peningkatan keterampilan SDM. - Menetapkan standar manajemen kualitas	
DSS02.03.03 - Melakukan pemenuhan permintaan dengan cara memilih prosedur permintaan, jika memungkinkan menggunakan menu bantuan mandiri dan model permintaan yang telah dibuat sebelumnya	Prosedur pengelolaan insiden tidak tersedia secara tertulis	**DSS01.01 *Perform Operational Procedures*** - Memelihara dan menjalankan kebijakan dan prosedur operasional serta tugas operasional secara andal dan konsisten. - Susun, kembangkan dan pelihara kebijakan beserta prosedur operasional pengelolaan insiden dan permintaan layanan.	Pihak Manajemen Sub Direktorat Layanan dan Teknologi Informasi; Kepala Sub Direktorat dan Kepala Divisi

Aktivitas	Risiko	Mitigasi	Penanganggung Jawab
untuk item - item yang sering diminta		- Implementasikan kebijakan dan prosedur untuk menunjang keefektifan proses bisnis. - Lakukan evaluasi berkala terkait keefektifkan penerapan kebijakan dan prosedur.	

Berdasarkan hasil *Risk Management Plan* diatas dengan melakukan *fit in* kondisi organisasi dengan standar, bagian organisasi yang dapat ditambah tupoksinya ialah bagian diatas *helpdesk* yaitu Kepala Divisi, karena Kepala Divisi memiliki tugas pokok fungsi untuk melaksanakan tugas khusus dari pimpinan atau dapat memperdetail tugas pokok fungsi dari Kepala Divisi.

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini merangkum hasil akhir dari pembuatan tugas akhir menjadi sebuah kesimpulan dan dilengkapi dengan saran-saran untuk perbaikan ataupun penelitian lanjutan. Kesimpulan merupakan rangkuman dari hasil analisis dan penilaian risiko. Sedangkan saran merupakan usulan atau rekomendasi peneliti terhadap hasil tugas akhir untuk perbaikan ataupun penelitian lanjutan.

7.1 Kesimpulan

Berdasarkan hasil penilaian risiko yang sudah dilakukan pada proses TI unit *helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi dengan menggunakan kerangka kerja COBIT 5 maka dapat disimpulkan bahwa:

1. Dari sejumlah 31 (tiga puluh satu) risiko yang teridentifikasi dari proses DSS02 *Manage Service Requests and Incidents* COBIT 5, paling banyak terpetakan dengan aktivitas DSS02.04 – Menginvestigasi, Mendiagnosa dan Mengalokasikan Insiden dikarenakan rentannya terjadi kesalahan pada *helpdesk* dalam melakukan identifikasi dan mendiagnosa gejala dan penyebab insiden dan permintaan layanan.
2. Semua risiko masuk ke dalam tipe *IT Operations and Service Delivery Risk*, dikarenakan risiko hanya terkait dengan kegiatan operasional unit *helpdesk* Subdirektorat Layanan DPTSI dimana terkait dengan stabilitas operasional, ketersediaan, perlindungan dan pemulihan layanan TI, sehingga risiko dapat membawa kerugian atau pengurangan nilai perusahaan.
3. Dari risiko yang teridentifikasi:
   - Risiko level *high* dan *medium* paling banyak berasal dari kategori *staff operations (human error and malicious intent*), dimana risiko terjadi akibat kelalaian dan kesalahan *staff* yang disengaja maupun tidak disengaja.

- Risiko level *low* paling banyak berasal dari kategori *IT expertise and skills*, dimana risiko terjadi akibat kurang memadainya pengetahuan dan keterampilan TI SDM.

4. Dampak yang ditekankan ialah aspek penurunan kepuasan pengguna dikarenakan ke-tiga aspek lainnya fokus kepada finansial, sedangkan DPTSI bukan merupakan organisasi yang berorientasi pada profit.
5. Setelah dilakukan survei, kategori pertanyaan kuesioner yang memiliki dampak paling signifikan terhadap penurunan kepuasan pelanggan ialah ketika *helpdesk* melakukan pengabaian pada laporan insiden atau permintaan layanan yang diajukan pengguna layanan.
6. Risiko yang paling signifikan dengan nilai tertinggi berada pada 4 (empat) risiko kategori *high* yang memiliki nilai penilaian sama. Ke-empat risiko tersebut ialah keterlambatan respon *helpdesk*, prosedur pengelolaan insiden tidak tersedia secara tertulis , ketidakpuasan pengguna terhadap layanan yang diberikan, Pengguna tidak menyetujui status penutupan insiden dimana memiliki nilai frekuensi yang tinggi dan dampak penurunan kepuasan pengguna yang besar.
7. Dikarenakan mayoritas risiko berasal dari kategori *staff operations* dan *IT expertise and skills*, maka pemetaan proses TI COBIT 5 yang paling sesuai ialah proses DSS01 *Manage Operations* untuk langkah mitigasi risiko kategori *staff operations*, dimana proses ini berisikan serangkaian aktivitas untuk membuat dan mengimplementasikan prosedur tertulis yang ditujukan untuk meminimalisir kesalahan operasional *staff*. Serta proses APO07 *Manage Human Resource* untuk langkah mitigasi risiko kategori *IT expertise and skills*, dimana proses ini berisikan serangkaian aktivitas untuk meningkatkan kemampuan dan keterampilan *staff* untuk melakukan pekerjaannya.
8. Berdasarkan hasil analisis mitigasi risiko, diperlukan re-struktur organisasi demi mengoptimalkan pelaksanaan

proses bisnis karena tugas pokok dan fungsi Sub Direktorat Layanan Teknologi dan Sistem Informasi belum spesifik.

7.2 Saran

Adapun saran yang dapat diberikan agar bisa dijadikan rekomendasi untuk penelitian selanjutnya yaitu:

1. Proses APO12 *Manage Risks* COBIT 5 memiliki 7 (tujuh) rangkaian aktivitas, dimana pada penelitian ini hanya menggunakan 2 (dua) aktivitas pertama yaitu sampai pada aktivitas APO12.02 Menganalis Risiko, diharapkan penelitian selanjutnya bisa meneruskan hingga aktivitas APO12.07 Merespon Risiko.
2. Dikarenakan keterbatasan waktu, penelitian ini hanya mengambil sampel mahasiswa untuk mengisi kuesioner penurunan kepuasan pengguna layanan. Diharapkan kuesioner penelitian risiko *helpdesk* Sub Direktorat Layanan TSI DPTSI selanjutnya terkait penurunan kepuasan pengguna layanan dapat mengambil sampel yang lebih banyak dengan memasukkan kategori dosen, karyawan dan mahasiswa karena ke-tiganya merupakan pengguna layanan DPTSI.
3. Nilai toleransi kegagalan metode slovin (*e*) untuk survei selanjutnya diharapkan dapat memakai nilai yang lebih rendah dari 0.15 agar responden yang ditargetkan lebih banyak sehingga hasilnya bisa lebih *reliable*.
4. Sesuai dengan analisis mitigasi risiko, diharapkan Subdirektorat Layanan dapat memperbaiki tugas pokok dan fungsi struktur organisasi. Berdasarkan hasil usulan diatas, bagian yang perlu ditambahkan tupoksinya iala Kepala Divisi.
5. Untuk penelitian selanjutnya, diharapkan dapat membuat dokumen prosedur mitigasi risiko yang lebih rinci dan tersistematis dimana dokumen mendeskripsikan detail langkah mitigasi untuk risiko yang berdampak besar bagi organisasi.

"Halaman ini sengaja dikosongkan"

DAFTAR PUSTAKA

[1] Direktorat Pengembangan Teknologi dan Sistem Informasi ITS, "Tentang DPTSI," Direktorat Pengembangan Teknologi dan Sistem Informasi ITS, 2016. [Online]. Available: http://dptsi.its.ac.id/. [Diakses 1 Oktober 2016].

[2] ITIL V3, ITIL Version 3 : Service Operation, Buckinghamshire: Office of Goverment Commerce, 2011.

[3] I. Desy, B. Cahyo dan H. Maria, "Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effect Analysis di Divisi TI Bank XYZ Surabaya," *Seminar Nasional Sistem Informasi Indonesia,* p. 1, 2014.

[4] M. Labombang, "Manajemen Risiko dalam Proyek Konstruksi," *SMARTek (Sipil, Mesin, Arsitektur, Elektro),* pp. 1-2, 2011.

[5] Glasgow Caledonian University, "Risk Management Strategy," London.

[6] G. Stoneburner, A. Goguen dan A. Feringa, Risk Management Guide for Information Technology Systems (Recommendations of the National Institute of Standards and Technology)., U.S. Department Of Commerce, 2002.

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

[8] R. K. Candra, I. Atastina dan Y. Firdaus, "Audit Teknologi Informasi menggunakan Framework COBIT 5 Pada Domain DSS (Delivery, Service, and Support) (Studi Kasus : iGracias Telkom University)," *Eproc,* vol. I, p. 2, 2015.

[9] R. Stup, "Standard Operating Procedures: Managing The Human Variables," *National Mastitis Council Regional Meeting Proceedings,* 2002.

[10] D. R. Indah, Harlili dan A. Firdaus, "Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk," *International Conference on Computer Science and Engineering,* 2014.

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

[12] O. Illoh, S. Aghili dan S. Butakov, "Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates," *Research Gate*, 2015.

[13] KBBI, Kamus Besar Bahasa Indonesia, 2008.

[14] C. A. Williams dan R. M. Heins, Risk Management and Insurance, New York: McGraw-Hill, 1976.

[15] A. Damodaran, Investment Valuation: Tools and Techniques for Determining the Value of Any Asset, John Wiley & Sons, 2002.

[16] H. Darmawi, Manajemen Risiko, Jakarta: Bumi Aksara, 2005.

[17] J. M. Griffin dan M. L. Lemmon, "Book–to–market Equity, Distress Risk, and Stock Returns," *The Journal of Finance*, vol. 5, p. 57, 2002.

[18] A. Salim, Asuransi dan Manajemen Risiko, Jakarta: Raja Grafindo Persada, 2007.

[19] S. Djojosoedarso, Prinsip – Prinsip Manajemen Risiko Asuransi, Jakarta: Penerbit Salemba Empat, 2003.

[20] APB Indonesia, "Risiko Positif (Peluang)," APB Indonesia, 2016. [Online]. Available: http://www.apb-group.com/risiko-positif-peluang/. [Diakses 19 January 2017].

[21] E. Widya, "Pengendalian Sistem Informasi Berdasarkan Komputer," Ekowiner, April 2015. [Online]. Available: http://www.ekowiner.web.id/. [Diakses 10 November 2016].

[22] Teknologi Informasi dan Komunikasi, "Mengelola Risiko Teknologi Informasi," Teknologi Informasi dan Komunikasi, May 2016. [Online]. Available: http://www.teknologiinformasidankomunikasi.com/. [Diakses 22 September 2016].

[23] ISACA, COBIT 5 for Risk, Rolling Meadows: ISACA, 2013.

[24] ISACA, COBIT 5 Enabling Processes, Rolling Meadows: ISACA, 2012.

[25] W. F. Smith, Principles Materials Science Engineering, New York: McGraw-Hill Companies, 1990.

[26] B. Djohanputro, Manajemen Risiko Korporat, Jakarta: PPM Manajemen, 2008.

[27] J. Liebowitz dan K. Wright, "Does Measuring Knowledge Make "Cents"? Expert Systems with Application," vol. II, p. 17, 1999.

[28] R. H. Clough dan G. A. Sears, Constructing Contracting, New York: John Willey & Sons Inc., 1999.

[29] AS/NZS ISO 31000, "Risk Management - Principles and Guidelines," International Standard, New Zealand, 2009.

[30] A. Affandi, "Memorandum Akhir Jabatan Ketua LPTSI," Lembaga Pengembangan Teknologi dan Sistem Informasi, Surabaya, 2016.

[31] Office of Government Commerce (OGC), ITIL Service Operation, The Stationary Office, 2007.

[32] Megawati dan K. Surendro, "Usulan Tata Kelola Manajemen Insiden dan Masalah Berdasarkan Kombinasi COBIT 4.1 dan ITIL V3," *Seminar Nasional Aplikasi Teknologi Informasi (SNATI),* p. 3, 2012.

[33] Tutorials Point, "Incident Management and Request Fulfillment," Tutorials Point, 2016. [Online]. Available: https://www.tutorialspoint.com. [Diakses 16 October 2016].

[34] Tutorials Point, "Access Management," Tutorials Point, [Online]. Available: https://www.tutorialspoint.com. [Diakses 14 November 2016].

[35] T. P. Silitonga dan A. H. N. Ali, "Sistem Manajemen Insiden pada Program Manajemen Helpdesk dan Dukungan TI Berdasarkan Framework ITIL V3 (Studi Kasus: Biro Teknologi Informasi BPK-RI)," *Seminar Nasional Informatika,* 2010.

[36] C. Kusuma, "Membedah Anatomi ISO 31000: 2009 Risk Management – Principles and Guidelines," July 2014.

[Online]. Available: http://crmsindonesia.org/. [Diakses 26 April 2016].

[37] AS/NZS ISO 31000, Risk Management -- Principles and Guidelines, New Zealand: International Standard, 2009.

[38] E. E. Putri, Pengaruh Komisaris Independen, Komite Manajemen Risiko, Reputasi Auditor dan Konsentrasi Kepemilikan terhadap Pengungkapan Enterprises Risk Management (Dimensi COSO ERM Framework), Ciputat: Universitas Islam Negeri Syarif Hidayatullah, 2013.

[39] ISO/IEC 27001, "Information technology — Security techniques — Information security management systems — Requirements," 2013. [Online]. Available: http://www.iso27001security.com/. [Diakses 26 April 2016].

[40] ISO/IEC 27002, "ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls," 2013. [Online]. Available: http://www.iso27001security.com/. [Diakses 26 April 2016].

[41] C. J. Alberts dan A. Dorofee, Managing Information Security Risks: The Octave Approach, Boston: Addison-Wesley Longman Publishing Co., Inc., 2002.

[42] F. Adikara, "Implementasi Tata Kelola Teknologi Informasi Perguruan Tinggi Berdasarkan COBIT 5 pada Laboratorium Rekayas Perangkat Lunak Universitas Esa Unggul," *Seminar Nasional Sistem Informasi Indonesia*, p. 132, 2013.

[43] W. V. Grembergen dan S. D. Haes, "Moving From IT Governance to Enterprise Governance," *ISACA Journal*, 2009.

[44] D. Hillson, "Effective Strategies for Exploiting Opportunities," *Project Management Professional Solutions Limited*, 2001.

[45] R. K. Yin, Case Study Research Design and Methods Fourth Edition, International Educational adn Professional Publisher, 1984.

[46] C. Schell, "The Value of the Case Study as a Research Strategy," *Manchester Business School*, p. January, 1992.

[47] D. P. Hasmarini dan A. Yuniawan, "Pengaruh Keadilan Prosedural dan Distributif terhadap Kepuasan Kerja dan Komitmen Aktif," *Jurnal Bisnis Strategi*, vol. XVII, no. 1, p. 99, 2008.

[48] Institut Teknologi Sepuluh Nopember, "Peraturan Rektor Nomor 10 Tahun 2016 Tentang OTK ITS," Institut Teknologi Sepuluh Nopember, Surabaya, 2016.

[49] Direktorat Pengembangan Teknologi dan Sistem Informasi, "Proses Bisnis DPTSI V3," Direktorat Pengembangan Teknologi dan Sistem Informasi, Surabaya, 2016.

"Halaman ini sengaja dikosongkan"

BIODATA PENULIS

Penulis bernama lengkap Chitra Utami Putri, yang biasa dipanggil Chitra, merupakan anak pertama dari dua bersaudara yang dilahirkan di Kota Jakarta pada tanggal 27 Oktober 1995. Penulis menempuh 12 tahun masa pendidikan formal di Kota Jakarta. Riwayat pendidikan penulis dimulai pada tahun 2001 di SDN Pisangan Timur 01 Pagi, SMPN 236 Jakarta pada tahun 2007, dan SMAN 103 Jakarta pada tahun 2010. Pada tahun 2013, penulis meneruskan Pendidikan Tinggi Negeri dengan merantau ke Kota Surabaya, yaitu di Jurusan Sistem Informasi FTIf, Institut Teknologi Sepuluh Nopember Surabaya dan terdaftar dengan NRP 5213100193.

Selama menjadi mahasiswa, penulis aktif sebagai anggota aktif di Himpunan Mahasiswa Sistem Informasi (HMSI). Penulis juga aktif berorganisasi di HMSI sebagai staff Departemen Dalam Negeri kepengurusan 2014/2015, ITS EXPO 2014 sebagai staff Display, dan berbagai kepanitiaan. Penulis melanjutkan berorganisasi di HMSI sebagai Sekretaris Departemen Dalam Negeri kepengurusan 2015/2016 serta melanjutkan ITS EXPO 2015 sebagai staff ahli Pasar Kreatif. Ketertarikan penulis pada bidang manajemen risiko 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 PT Pertamina Pusat, Gambir, Jakarta Pusat. Penulis dapat dihubungi melalui e-mail chitrautm@gmail.com.

LAMPIRAN A – INTERVIEW PROTOCOL

INTERVIEW PROTOCOL 1

Tujuan Interview	:	Untuk mendapatkan informasi terkait kondisi kekinian dari proses bisnis *helpdesk* dalam menangani insiden maupun layanan di Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI.
Tanggal	:	24 November 2016
Waktu	:	09.30 – 10.30 WIB
Lokasi	:	Dilo (Digital Innovation Lounge) ITS
Narasumber	:	Bapak Jainul Arifin, Ibu Mudjiatin, Ibu Widiyaningsih, dan Ibu Wiwin Rochmawati.
Jabatan	:	Staff *Helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi

Notes:

- ✓ Perkenalan diri
- ✓ Mengucapkan terima kasih atas kesempatannya
- ✓ Menjelaskan durasi wawancara
- ✓ Sasaran :
  - Proses bisnis *helpdesk*
  - Struktur organisasi *helpdesk*
  - Layanan yang ditangani *helpdesk*
  - Tugas pokok fungsi *helpdesk*
  - Visi misi *helpdesk*
  - Standar acuan *helpdesk*
  - Pengelolaan manajemen insiden dan pemenuhan permintaan layanan TI.
  - Sistem Informasi *helpdesk*

Kategori	Sasaran: Proses bisnis, struktur organisasi, tugas pokok fungsi, visi misi dan layanan yang ditangani *helpdesk*
Proses bisnis *helpdesk*	1. Apakah peran dan tanggung jawab masing-masing *helpdesk* di subdir layanan DPTSI?
Struktur Organisasi *helpdesk*	2. Seperti apa bentuk *helpdesk* pada Subdirektorat Layanan Teknologi dan Sistem Informasi Teknologi Informasi (DPTSI) ITS? Bagaimana struktur organisasinya?
Tugas pokok fungsi *helpdesk*	3. Apakah tugas pokok dan fungsi dari *helpdesk* di Subdirektorat Layanan Teknologi dan Sistem Informasi Teknologi Informasi (DPTSI) ITS?
Proses bisnis *helpdesk*	4. Bagaimana proses bisnis *helpdesk* sehari-harinya?
	5. Apakah *helpdesk* sudah memanfaatkan peran TI dalam menjalankan proses bisnis sehari-harinya? Bagaimana bentuk pemanfaatan TI tersebut?
Layanan TI *helpdesk*	6. Bentuk layanan dan proses TI apa saja yang ditangani oleh *helpdesk*?
	7. Bagaimana alur atau prosedur pelaporan insiden maupun permintaan layanan?
	8. Apa saja insiden yang sering terjadi pada layanan-layanan tersebut? Dan bagaimana penanganannya?
	9. Hal-hal apa saja yang dirasa masih kurang dalam pengelolaan insiden dan permintaan layanan?
Standar acuan *helpdesk*	10. Apakah proses pengelolaan insiden dan pemenuhan permintaan layanan sudah mengacu pada standar tertentu?
Kategori	**Sasaran: Pengelolaan Manajemen Insiden dan Proses Pemenuhan Layanan TI**
Menetapkan skema klasifikasi insiden dan layanan permintaan	1. Bagaimana suatu insiden di deteksi? 2. Bagaimana proses pemenuhan layanan dilakukan? 3. Apakah terdapat suatu klasifikasi/kategorisasi insiden dan pemenuhan layanan secara lengkap?

	4. Bagaimana suatu insiden diidentifikasi dalam suatu klasifikasi/kategori?
Merekam, mengklasifikasikan dan memprioritaskan permintaan dan insiden	1. Bagaimana insiden dan permintaan layanan di catat? 2. Apakah pencatatan tersebut disimpan dalam satu direktori khusus? 3. Apakah terdapat suatu sistem informasi khusus dalam pencatatan insiden? 4. Detail informasi apasajakah yang dicatat dalam data insiden dan pemenuhan permintaan layanan? 5. Apakah terdapat sistem prioritasi insiden dan pemenuhan layanan? Kriteria apa saja yang digunakan dalam memprioritaskan insiden dan pemenuhan layanan permintaan? 6. Apakah terdapat daftar prioritas khusus untuk insiden dan permintaan yang terjadi? 7. Tipe insiden dan pemenuhan layanan seperti apa yang memerlukan eskalasi? Apakah eskalasi fungsional atau hierarki? 8. Bagaimana eskalasi insiden tersebut dilakukan?
Melakukan verifikasi, menerima dan memenuhi permintaan layanan	1. Apakah terdapat prosedur khusus dalam menangani insiden dan memenuhi permintaan layanan? 2. Apakah diperlukan persetujuan fungsional untuk menangani insiden dan memenuhi permintaan layanan?
Menginvestigasi, mendiagnosa dan mengalokasikan insiden	1. Ketika insiden terjadi (terdapat suatu laporan dari pengguna), apakah dilakukan diagnosa awal untuk menentukan gejala penyebab masalah? 2. Apakah dilakukan aktivitas investigasi dan diagnosa terhadap insiden yang terjadi? Bagaimana investigasi dan diagnosa insiden tersebut biasanya dilakukan?
Melakukan penyelesaian	1. Bagaimana pengambilan suatu solusi pemulihan insiden ditentukan?

dan pemulihan insiden insiden	2. Apakah solusi tersebut diuji terlebih dahulu? 3. Apakah terdapat SOP khusus untuk melakukan pemulihan/penyelesaian insiden ? 4. Berapa lama biasanya suatu insiden atau layanan diselesaikan?
Menutup permintaan layanan dan insiden.	1. Bagaimana suatu insiden dan permintaan layanan ditutup? 2. Apakah solusi yang diberikan divalidasi ke pengguna (pelapor) insiden dan peminta layanan?
Melacak status dan membuat laporan	1. Apakah eskalasi insiden dan penanganan layanan diawasi? 2. Apakah dibuatkan laporan terkait permintaan layanan dan insiden tersebut? 3. Dimana laporan terkait insiden dan permintaan layanan tersebut disimpan?
Kategori	**Sasaran: Kondisi Sistem Informasi *Helpdesk* Subdirektorat layanan DPTSI.**
Sistem Informasi *Helpdesk*	1. Apakah terdapat suatu sistem informasi *helpdesk* untuk mengelola insiden dan pengelolaan permintaan layanan?
Sistem Informasi *Helpdesk*	2. Adakah permasalahan yang pernah terjadi terkait sistem informasi *helpdesk*?
Sistem Informasi *Helpdesk*	3. Siapa saja yang menjadi admin/bertanggung jawab/pengelola sistem informasi *helpdesk* ? (daftar perbagian staff dan peran serta tanggungjawab masing-masing)
Sistem Informasi *Helpdesk*	4. Apa saja komponen sistem informasi (*hardware, software, data, network, people, prosedur*) yang berkaitan dengan pengelolaan manajemen insiden dan proses pengelolaan permintaan layanan (sistem informasi *helpdesk*)?
Sistem Informasi *Helpdesk*	5. Apakah pernah dilakukan identifikasi risiko terkait sistem informasi *helpdesk*?

***INTERVIEW PROTOCOL* 2**

Tujuan Interview	:	Untuk mendapatkan detail informasi terkait kesalahan dan risiko yang kerap muncul dari proses pengelolaan insiden dan pemenuhan permintaan layanan.
Tanggal	:	24 November 2016
Waktu	:	09.30 – 10.30 WIB
Lokasi	:	Dilo (Digital Innovation Lounge) ITS
Narasumber	:	Bapak Jainul Arifin, Ibu Mudjiatin, Ibu Widiyaningsih, dan Ibu Wiwin Rochmawati.
Jabatan	:	Staff *Helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi

Notes:

- ✓ Perkenalan diri
- ✓ Mengucapkan terima kasih atas kesempatannya
- ✓ Menjelaskan durasi wawancara
- ✓ Sasaran :
  - Kesalahan yang kerap terjadi pada *helpdesk* saat mengelola insiden dan memenuhi permintaan layanan.
  - Risiko TI yang muncul dari proses pengelolaan insiden dan pemeuhan permintaan layanan.

Kategori	**Sasaran: Kesalahan pada *helpdesk* saat mengelola insiden dan memenuhi permintaan layanan**
Kesalahan umum *helpdesk*	1. Dari pemanfaatan peran TI, apakah sering terjadi kesalahan pada saat *helpdesk* mengelola insiden dan memenuhi permintan layanan?

Kesalahan umum *helpdesk*	2. Kesalahan apa yang paling sering terjadi pada saat mengelola insiden dan memenuhi permintan layanan?
Kesalahan umum *helpdesk*	3. Seberapa fatal kesalahan yang pernah dilakukan?
Kategori	**Sasaran: Risiko yang muncul dari proses pengelolaan insiden dan pemenuhan permintaan layanan.**
Mengumpulkan Data	1. Proses apa yang paling rentan terjadi kesalahan atau menimbulkan risiko? 2. Apakah selama ini kesalahan dan risiko yang terjadi dicatat dan disimpan? 3. Jika ya, apakah terdapat pengkategorisasian risiko? Bagaimana pengkategorisasiannya? 4. Dari penjabaran kesalahan dan risiko tersebut, apakah risiko tersebut disebabkan oleh faktor internal dan eksternal? Bagaimana penjabarannya?
Menganalisis Risiko	1. Seberapa berpengaruh risiko-risiko yang terjadi tersebut terhadap proses bisnis *helpdesk*? 2. Seberapa sering (frekuensi) risiko-risiko tersebut terjadi? 3. Apakah risiko yang terjadi tersebut menimbulkan dampak yang merugikan? Jika ya, bagaimana? Apakah mempengaruhi keempat 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) 4. Apakah terdapat standar atau acuan dalam menilai risiko yang ada?

***INTERVIEW PROTOCOL* 3**

Tujuan Interview	:	Untuk mendapatkan detail informasi terkait rencana lanjutan dalam menangani dan mengantisipasi terjadinya risiko.
Tanggal	:	7 Desember 2016
Waktu	:	17.00
Lokasi	:	Aula Jurusan Sistem Informasi ITS
Narasumber	:	Hanim Maria Astuti S.Kom., M.Sc
Jabatan	:	Kepala Subdirektorat Layanan Teknologi dan Sistem Informasi

Notes:

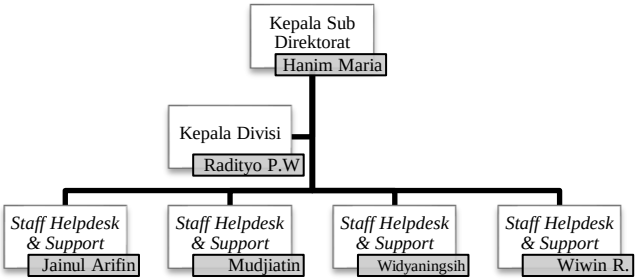
- ✓ Perkenalan diri
- ✓ Mengucapkan terima kasih atas kesempatannya
- ✓ Menjelaskan durasi wawancara
- ✓ Sasaran :
  - Kondisi kekinian organisasi terhadap risiko yang terjadi
  - Rencana atau strategi dalam menangani risiko.

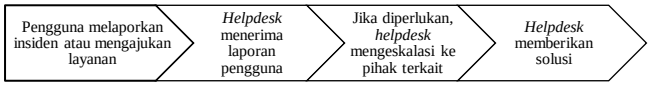
Kategori	**Sasaran: Kondisi kekinian organisasi terhadap risiko yang terjadi**
Pengelolaan Risiko	1. Bagaimana pengelolaan/manajemen risiko jika terdapat risiko yang terjadi?
	2. Apakah proses pengelolaan risiko tersebut sudah mengacu pada standar tertentu?
Dampak Risiko	3. Seberapa fatal dampak risiko terhadap proses bisnis sehari-hari organisasi?
	4. Risiko mana yang memberikan dampak paling signifikan terhadap proses bisnis organisasi?
	5. Bagaimana dampak terjadinya risiko terhadap ke-empat aspek berikut:

	• 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)
Kategori	**Sasaran: Rencana atau strategi dalam menangani risiko.**
Rencana atau strategi penaganan risiko	1. Seperti apa bentuk rencana atau strategi untuk menangani risiko? 2. Bagaimana rencana strategi tersebut dibuat? 3. Berdasarkan acuan standar apa rencana atau strategi tersebut dibuat? 4. Siapa saja yang berperan dalam melakukan aksi tersebut? 5. Apakah terdapat suatu proses mitigasi risiko tersendiri? Berdasarkan acuan standar apa mitigasi tersebut dibuat? 6. Strategi apa yang dirasa paling sesuai terhadap kondisi organisasi?

LAMPIRAN B – HASIL WAWANCARA

HASIL INTERVIEW 1

No	URAIAN
1	**Pertanyaan:** Apakah peran dan tanggung jawab masing-masing *helpdesk* di subdir layanan DPTSI?
	Jawaban: • Ibu Mudjiyatin sebagai *helpdesk* terkait pengelolaan e-mail dan komplain pengguna serta sebagai administrator umum • Ibu Wiwin Rochmawati sebagai *helpdesk* terkait website, domain dan hosting • Bapak Jainul Arifin sebagai *helpdesk* terkait pengelolaan e-mail dan komplain pengguna serta sebagai administrator umum • Ibu Widyaningsih sebagai *helpdesk* terkait manajemen user, SIM dan Office365
2	**Pertanyaan:** Seperti apa bentuk *helpdesk* pada Subdirektorat Layanan Teknologi dan Sistem Informasi Teknologi Informasi (DPTSI) ITS? Bagaimana struktur organisasinya?
	Jawaban: *Helpdesk* subdir layanan DPTSI terdiri dari empat karyawan, dimana masing-masing karyawan memiliki peran dan tanggung jawabnya masing-masing seperti yang disebutkan diatas. Semua karyawan *helpdesk* dinaungi oleh Kepala Divisi yaitu Bapak Radityo Prasetianto Wibowo dan dipimpin oleh Kepala Sub direktorat yaitu Ibu Hanim Maria Astuti. Berikut merupakan struktur organisasinya. 

No	URAIAN
3	**Pertanyaan:** Apakah tugas pokok dan fungsi dari helpdesk di Subdirektorat Layanan Teknologi dan Sistem Informasi Teknologi Informasi (DPTSI) ITS?
	Jawaban: Lihat tupoksi/*jobdesk* di SKP
4	**Pertanyaan:** Bagaimana proses bisnis *helpdesk* sehari-harinya?
	Jawaban: Proses bisnis dimulai ketika ada pengguna yang melaporkan insiden maupun mengajukan layanan permintaan, kemudian *helpdesk* menerima laporan tersebut. Kemudian jika *helpdesk* tidak bisa menangani permintaan yang diajukan pengguna, *helpdesk* akan mengeskalasikan permintaan tersebut ke bagian terkait yang lebih ahli. Kemudian pengguna akan langsung berhubungan dengan pihak bidang tersebut. Jika pengguna sudah berhubungan dengan pihak bidang tersebut, *helpdesk* tidak lagi terlibat dengan pengguna tersebut. Berikut merupakan bagan proses bisnis *helpdesk* sehari-harinya. 
5	**Pertanyaan:** Apakah *helpdesk* sudah memanfaatkan peran TI dalam menjalankan proses bisnis sehari-harinya? Bagaimana bentuk pemanfaatan TI tersebut?
	Jawaban: Ya sudah, mulai awal tahun 2016 *helpdesk* sudah mengimplementasikan sistem *e-ticket* berbasis *web* yang sudah dapat diakses oleh pengguna untuk mengajukan permintaan layanan maupun melaporkan insiden. Selain itu pengguna juga bisa melaporkan permintaan maupun insiden ke email *helpdesk*.
6	**Pertanyaan:** Bagaimana alur atau prosedur pelapora insiden maupun permintaan layanan?

No	URAIAN
	Jawaban: 8. Pengguna melaporkan insiden maupun permintaan layanan TI nya melalui telepon, *e-mail*, maupun sistem *e-ticket*. 9. *Helpdesk* menerima laporan permintaan pengguna. 10. Jika *helpdesk* yang menerima laporan tersebut tidak dapat menangani permasalahan tersebut, maka *helpdesk* akan mengeskalasikan permintaan pengguna ke pihak *helpdesk* yang terkait bidangnya. Selanjutnya pengguna akan berhubungan langsung dengan *helpdesk* bidang terkait untuk menyelesaikan permintaannya. 11. *Helpdesk* yang menyelesaikan permasalahan akan mencatat permintaan pengguna. 12. *Helpdesk* yang menyelesaikan permasalahan memberikan solusi pada pengguna. 13. *Helpdesk* memverifikasi solusi dan kepuasan pengguna terkait penyelesaian permasalahan pengguna. 14. Pengguna memberikan umpan balik terkait penyelesaian permintaannya. 15. Insiden maupun permintaan layanan TI tersebut ditutup.
7	**Pertanyaan:** Apa saja insiden yang sering terjadi pada layanan-layanan tersebut? Dan bagaimana penanganannya?
	Jawaban: Yang paling sering terjadi adalah masalah jaringan internet, pengguna lupa password *e-mail*, permintaan tambah kuota *e-mail*, masalah SIM akademik (integra). Untuk penangnannya biasanya melakukan perbaikan teknis oleh *helpdesk* bidang jaringan, mereset *password* dan penambahan kuota *e-mail* oleh admin, dan menunggu sampai *server* integra kembali pulih.
8	**Pertanyaan:** Siapa yang biasanya bertugas menangani insiden tersebut?
	Jawaban:

No	URAIAN
	Biasanya alurnya user melapor pada bagian layanan TSI. Nantinya permasalahan didistribusikan ke bagian terkait bidangnya, misalkan ketika permasalahan pada aplikasi telah diselesaikan bagian pengembangan, ketika ada terjadi permasalahan teknis dan jaringan, bagian layanan TSI langsung melaporkan pada bagian infrastruktur.
9	**Pertanyaan:** Apakah proses pengelolaan insiden dan pemenuhan permintaan layanan sudah mengacu pada standar tertentu?
	Jawaban: Awalnya mengacu pada standar ISO 2008, namun tidak semuanya diimplementasikan, rata-rata pengelolaan insiden dan layanan hanya berdasarkan pengalaman *helpdesk* dalam menangani insiden dan layanan.
10	**Pertanyaan:** Hal-hal apa saja yang dirasa masih kurang dalam pengelolaan insiden dan permintaan layanan?
	Jawaban: Pengelolaan insiden di *helpdesk* subdir layanan DPTSI ini masih memiliki banyak kekurangan, dari segi: - Pengguna, kadang pengguna tidak mau diajak bekerja sama, misal tidak mau memberikan umpan balik atau memvalidasi status penutupan insiden. - SDM, masing-masing bagian layanan hanya dikelola oleh 1 orang saja. - Tidak terdapat prosedur yang mengacu pada standar acuan khusus dalam menangani insiden dan layanan.
11	**Pertanyaan:** Bagaimana suatu insiden di deteksi?
	Jawaban: Terdapat *software* khusus yang dimiliki ITS untuk mendeteksi insiden (pantau.its)
12	**Pertanyaan:** Bagaimana proses pemenuhan layanan dilakukan?
	Jawaban: Sesuai alur yang disebutkan pada poin pertanyaan 6.
13	**Pertanyaan:** Bagaimana suatu insiden diidentifikasi dalam suatu klasifikasi/kategori?

No	URAIAN
	Jawaban: Tidak ada pengkategorisasian khusus, hanya berdasarkan permasalahannya, seperti kategori *e-mail*, SIM, jaringan, aset/infrastruktur.
14	**Pertanyaan:** Bagaimana insiden dan permintaan layanan di catat?
	Jawaban: Biasanya permasalahan yang melalui *e-mail* maupun sistem *e-ticket* hanya di *capture* kemudian disimpan dalam dokumen *helpdesk* masing-masing. Namun jika pengajuan permintaan melalui telepon biasanya tidak dicatat.
15	**Pertanyaan:** Apakah pencatatan tersebut disimpan dalam satu direktori khusus?
	Jawaban: Jika melalui sistem *e-ticket*, sudah terdapat direktori database khusus untuk menyimpan histori dari pengajuan layanan oleh pengguna. Namun jika melalui *e-mail* dan telepon tidak ada direktori penyimpanan khusus.
16	**Pertanyaan:** Detail informasi apasajakah yang dicatat dalam data insiden dan pemenuhan permintaan layanan?
	Jawaban: Nama insiden, pihak yang melaporkan dan tanggal kejadian.
17	**Pertanyaan:** Apakah terdapat sistem prioritasi insiden dan pemenuhan layanan? Kriteria apa saja yang digunakan dalam memprioritaskan insiden dan pemenuhan layanan permintaan?
	Jawaban: Ya, namun hanya berdasarkan tingkat kritikalitas/urgensitas dari insiden maupun layanan TI yang diajukan. Jika insiden tersebut berdampak signifikan makan akan di dahulukan, jika pengguna hanya menanyakan informasi terkait layanan maka bisa dinomorduakan.
18	**Pertanyaan:** Apakah terdapat daftar prioritas khusus untuk insiden dan permintaan yang terjadi?

No	URAIAN
	Jawaban: Tidak, hanya berdasarkan tingkat kedaruratan permintaan saja.
19	**Pertanyaan:** Tipe insiden dan pemenuhan layanan seperti apa yang memerlukan eskalasi? Apakah eskalasi fungsional atau hierarki?
	Jawaban: Tipe eskalasi sesuai dengan kebutuhan dan tingkat keparahan insiden. Jika insiden memerlukan pihak lain yang lebih ahli di bidangnya (dalam kasus ini ialah bidang pengembangan dan bidang infrastruktur & jaringan), maka akan dilakukan tipe eksalasi fungsional. Jika insiden membutuhkan persetujuan manajemen apabila terkait biaya dan waktu yang lama, maka akan dilakukan eskalasi hierarki kepada Kepala Subdirektorat Layanan TSI.
20	**Pertanyaan:** Bagaimana eskalasi insiden tersebut dilakukan?
	Jawaban: - Jika eskalasi fungsional, maka pendistribusian akan dilakukan melalui telepon, *e-mail* atau percakapan langsung ke pihak bidang terkait. - Jika eskalasi hierarki, maka dibutuhkan pengajuan surat untuk meminta persetujuan pihak manajemen yang lebih tinggi.
21	**Pertanyaan:** Apakah terdapat prosedur khusus dalam menangani insiden dan memenuhi permintaan layanan?
	Jawaban: Tidak ada, semua penanganan hanya didasarkan pada pengalaman dan *by request* saja.
22	**Pertanyaan:** Apakah diperlukan persetujuan fungsional untuk menangani insiden dan memenuhi permintaan layanan?
	Jawaban: Ya, apabila tingkat keparahan insiden tinggi atau membutuhkan biaya khusus maka akan membutuhkan persetujuan pihak manajemen, namun pada kasus ini, *helpdesk* hanya membantu mengajukan persetujuannya saja

No	URAIAN
	sesuai prosedur ITS, tidak sampai membantu mengeksekusi pembeliannya. Sedangkan apabila hanya sebatas pendistribusian fungsional, tidak membutuhkan persetujuan khusus.
23	**Pertanyaan:** Ketika insiden terjadi (terdapat suatu laporan dari pengguna), apakah dilakukan diagnosa awal untuk menentukan gejala penyebab masalah?
	Jawaban: Ya, yaitu dengan penggalian lebih dalam terkait permasalahan yang diajukan dengan menanyakan detailnya kepada pengguna.
24	**Pertanyaan:** Apakah dilakukan aktivitas investigasi dan diagnosa terhadap insiden yang terjadi? Bagaimana investigasi dan diagnosa insiden tersebut biasanya dilakukan?
	Jawaban: Jika insiden kecil sebatas penggalian informasi yang detail untuk mencari penyebab insiden tersebut. Namun jika insiden besar, maka *helpdesk* akan mencari dan menganalisis akar permasalahannya sendiri.
27	**Pertanyaan:** Bagaimana pengambilan suatu solusi pemulihan insiden ditentukan?
	Jawaban: Dengan menganalsisis penyebab permasalahan tersebut, lalu dicarikan solusi yang sesuai.
28	**Pertanyaan:** Apakah solusi tersebut diuji terlebih dahulu?
	Jawaban: Tidak, karena hanya melihat berdasarkan pengalaman saja.
29	**Pertanyaan:** Apakah terdapat SOP khusus untuk melakukan pemulihan/penyelesaian insiden ?
	Jawaban: Tidak.
30	**Pertanyaan:**

No	URAIAN
	Berapa lama biasanya suatu insiden atau layanan diselesaikan?
	Jawaban: - Jika permintaan kecil seperti *reset password*, maka hanya membutuhkan waktu kurang dari 5 menit. - Jika permasalahan koneksi jaringan maka membutuhkan waktu paling lama 1 jam. - Jika permintaan atau insiden menyangkut penggantian aset yang membutuhkan biaya, maka membutuhkan waktu mencapai berbulan-bulan karena proses pengajuan dana sangat rumit.
31	**Pertanyaan:** Bagaimana suatu insiden dan permintaan layanan ditutup?
	Jawaban: Biasanya membutuhkan persetujuan pengguna, jika melalui *e-mail*, maka pengguna ditanyakan secara langsung. Sedangkan jika melalui sistem *e-ticket*, pengguna diminta menutup insiden tersebut apabila merasa puas dan tidak membutuhkan pelayanan lagi, namun apabila pengguna tidak menutup melebihi batas waktu yang ditentukan, maka insiden atau layanan akan ditutup secara otomatis. Namun semua penutupan insiden tidak dibuatkan pelaporan khusus.
32	**Pertanyaan:** Apakah solusi yang diberikan divalidasi ke pengguna (pelapor) insiden dan peminta layanan?
	Jawaban: Ya, dengan cara meminta umpan balik terkait kepuasan pengguna.
33	**Pertanyaan:** Apakah eskalasi insiden dan penanganan layanan diawasi?
	Jawaban: Untuk fungsional tidak semuanya diawasi, namun untuk hierarki diawasi oleh kasubdir bahkan rektor.
34	**Pertanyaan:** Apakah dibuatkan laporan terkait permintaan layanan dan insiden tersebut?
	Jawaban: Tidak dibuatkan laporan khusus.

No	URAIAN
35	**Pertanyaan:** Dimana laporan terkait insiden dan permintaan layanan tersebut disimpan?
	Jawaban: Tidak ada.
36	**Pertanyaan:** Apakah terdapat suatu sistem informasi helpdesk untuk mengelola insiden dan pengelolaan permintaan layanan?
	Jawaban: Ya, layanan sistem *e-ticket* berbasis *web* tersebut.
37	**Pertanyaan:** Adakah permasalahan yang pernah terjadi terkait sistem informasi *helpdesk*?
	Jawaban: Terkadang masih dijumpai beberapa *error/bug*, seperti waktu/tanggal yang tidak sesuai.
38	**Pertanyaan:** Siapa saja yang menjadi admin/bertanggung jawab/pengelola sistem informasi *helpdesk*? (daftar perbagian staff dan peran serta tanggungjawab masing-masing)
	Jawaban: Administrator umum sistem *e-ticket* adalah Bapak Jainul Arifin. Nantinya keluhan yang masuk akan didistrubusikan/dieskalasi kepada *helpdesk* terkait bidangnya.
39	**Pertanyaan:** Apa saja komponen sistem informasi (*hardware, software, data, network, people, prosedur*) yang berkaitan dengan pengelolaan manajemen insiden dan proses pengelolaan permintaan layanan (sistem informasi helpdesk)?
	Jawaban: *Hardware, web, network, people*.
40	**Pertanyaan:** Apakah pernah dilakukan identifikasi risiko terkait sistem informasi helpdesk?
	Jawaban: Belum pernah.

HASIL INTERVIEW 2

No	URAIAN
1	**Pertanyaan:** Dari pemanfaatan peran TI, apakah sering terjadi kesalahan pada saat *helpdesk* mengelola insiden dan memenuhi permintan layanan?
	Jawaban: Sering, namun hanya kesalahan-kesalahan kecil, seperti salah mengklik tombol, salah menginput tanggal.
2	**Pertanyaan:** Kesalahan apa yang paling sering terjadi pada saat mengelola insiden dan memenuhi permintan layanan?
	Jawaban: Salah mengklik tombol sistem, salah memilih pihak untuk mengeskalasi, lupa mendokumentasikan insiden.
3	**Pertanyaan:** Seberapa fatal kesalahan yang pernah dilakukan?
	Jawaban: Tidak pernah ada yang fatal jika dari sisi *helpdsk*.
4	**Pertanyaan:** Proses apa yang paling rentan terjadi kesalahan atau menimbulkan risiko?
	Jawaban: Proses terkait pengelolaan *e-mail*, integra, sistem *e-ticket* dan SIM.
5	**Pertanyaan:** Apakah selama ini kesalahan dan risiko yang terjadi dicatat dan disimpan? Jika ya, apakah terdapat pengkategorisasian risiko? Bagaimana pengkategorisasiannya?
	Jawaban: Tidak pernah ada pencacatan dan penyimpanan histori risiko, maka tidak ada pengkategorisasian risiko.
6	**Pertanyaan:** Dari penjabaran kesalahan dan risiko tersebut, apakah risiko tersebut disebabkan oleh faktor internal dan eksternal? Bagaimana penjabarannya?
	Jawaban: Sebagian risiko disebabkan oleh *helpdesk* (internal) namun hanya kesalahan-kesalahan kecil, sedangkan kesalahan atau

No	URAIAN
	risiko kebanyakan disebabkan oleh teknis (internal) dan pengguna (eksternal).
7	**Pertanyaan:** Seberapa berpengaruh risiko-risiko yang terjadi tersebut terhadap proses bisnis helpdesk?
	Jawaban: Tidak berpengaruh signifikan, hanya beberapa yang menyebabkan kerugian finansial yang berdampak signifikan namun jarang terjadi.
8	**Pertanyaan:** Seberapa sering (frekuensi) risiko-risiko tersebut terjadi?
	Jawaban: Jika hanya kesalahan kecil seperti *human error* dan teknis sering terjadi, namun jika menimbulkan kerugian finansial jarang terjadi.
9	**Pertanyaan:** Apakah risiko yang terjadi tersebut menimbulkan dampak yang merugikan? Jika ya, bagaimana? Apakah mempengaruhi keempat 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: • Produktivitas → Dampak ini berpengaruh jika risiko berhubungan dengan pergantian aset organisasi yang membutuhkan biaya. • Biaya tanggapan → Tidak ada biaya khusus • Keunggulan kompetitif → Biasanya penuruan kepuasan pengguna hanya dilihat dari umpan balik mereka setelah permintaannya dipenuhi. • Hukum → Belum ada risiko yang melanggar hukum secara internal, namun risiko eskternal seperti *hacker* melanggar hukum UU ITE.

No	URAIAN
10	**Pertanyaan:** Apakah terdapat standar atau acuan dalam menilai risiko yang ada?
	Jawaban: Tidak ada.

HASIL INTERVIEW 3

No	URAIAN
1	**Pertanyaan:** Bagaimana pengelolaan/manajemen risiko jika terdapat risiko yang terjadi?
	Jawaban: Tidak ada pengelolaan yang tertulis, antisipasi sudah dilakukan namun tidak tertulis sehingga identifikasi tidak komprehensif.
2	**Pertanyaan:** Apakah proses pengelolaan risiko tersebut sudah mengacu pada standar tertentu?
	Jawaban: Belum mengacu pada standar apapun, karena belum pernah dilakukan identifikasi penilaian risiko.
3	**Pertanyaan:** Seberapa fatal dampak risiko terhadap proses bisnis sehari-hari organisasi?
	Jawaban: Sebuah risiko dikatakan fatal apabila mengurangi efisiensi waktu dan menurunkan kepuasan pelanggan DPTSI.
4	**Pertanyaan:** Risiko mana yang memberikan dampak paling signifikan terhadap proses bisnis organisasi?
	Jawaban: Risiko yang paling memakan waktu dan menurunkan kepuasan pelanggan.
5	**Pertanyaan:** • Bagaimana dampak terjadinya risiko terhadap ke-empat aspek berikut: • Produktivitas → rugi pendapatan selama satu tahun (%)

No	URAIAN
	• Biaya tanggapan → beban terkait dengan mengelola kejadian yang merugikan (Rp) • Keunggulan kompetitif → penurunan kepuasan pengguna (indeks) • Hukum→kepatuhan terhadap peraturan-denda (Rp)
	Jawaban: • Produktivitas → tidak ada rugi pendapatan yang khusus mengacu pada *helpdesk* maupun sub direktorat layanan • Biaya tanggapan → jika dari sisi subdir layanan, tidak pernah mengeluarkan biaya tanggapan. • Keunggulan kompetitif → banyak pengguna yang merasa tidak puasa apabila layaanannya tidak dipenuhi sesuai yang diharapkan • Hukum→ belum ada risiko terkait denda
6	**Pertanyaan:** Seperti apa bentuk rencana atau strategi untuk menangani risiko?
	Jawaban: Rencana strategi untuk menangani risiko dibuat untuk meminimalisir dampak, contohnya dampak meminimalisir keamanan informasi. Contoh: email mahasiswa ITS yang memiliki periode *lifetime*, dibatasi hanya bisa aktif saat ia masi menjadi mahasiswa (*gross period*), setelah 6 bulan kelulusan maka *e-mail* akan tomatis di non aktifkan, lalu pembatasan hak akses (*Single Sign On*/SSO), menggunakan prinsip SEMPRA (*Single Entry for Many Purposes*)
7	**Pertanyaan:** Bagaimana rencana strategi tersebut dibuat?
	Jawaban: Dalam bentuk keputusan melalui kesimpulan permasalahan dalam sebuah rapat manajemen.
8	**Pertanyaan:** Berdasarkan acuan standar apa rencana atau strategi tersebut dibuat?

No	URAIAN
	Jawaban: Hanya berdasarkan pengalaman dan pertimbangan kejadian-kejadian dan kesalahan dimasa lalu.
9	Siapa saja yang berperan dalam melakukan aksi tersebut?
	Jawaban: Pihak manajemen dan seluruh elemen organisasi ikut menerapkannya.
10	**Pertanyaan:** Apakah terdapat suatu proses mitigasi risiko tersendiri? Berdasarkan acuan standar apa mitigasi tersebut dibuat?
	Jawaban: Mitigasi risiko belum pernah dibuat secara tertulis dan belum mengacu pada standar apa pun.
10	**Pertanyaan:** Strategi apa yang dirasa paling sesuai terhadap kondisi organisasi?
	Jawaban: Strategi untuk mengurangi dampak keamanan informasi, strategi untuk mempertahankan kepuasan pengguna dan mengefisiensikan waktu.

LAMPIRAN C – HASIL OBSERVASI

Tujuan Observasi : Menganalisis proses TI *helpdesk* dengan melakukan pemetaan dengan proses ideal pada domain DSS02 *Manage Service Requests and Incidents* COBIT 5.
Tanggal : 24 November 2016
Waktu : 09.30 – 10.30 WIB
Lokasi : Dilo (Digital Innovation Lounge) ITS
Narasumber : Bapak Jainul Arifin, Ibu Mudjiatin, Ibu Widiyaningsih, dan Ibu Wiwin Rochmawati.
Jabatan : Staff *Helpdesk* Subdirektorat Layanan Teknologi dan Sistem Informasi

DSS02.01			
No.	**Aktivitas DSS02.01 – Menetapkan skema klasifikasi insiden dan layanan permintaan**	**Dilakukan**	**Keterangan**
1.	Menetapkan dan mendefinisikan klasifikasi permintaan layanan dan skema prioritisasi beserta kriteria untuk pendaftaran masalah, untuk memastikan pendekatan yang konsisten dalam menangani, menginformasikan pengguna dan melakukan analisis tren.	√	Pengguna bisa melakukan pelaporan permintaan layanan dan insiden dari user (pengguna) ke *helpdesk* melalui *e-mail*, telepon atau sistem *e-ticket*. *Helpdesk* subdir layanan DPTSI sudah melakukan pengkategorisasian insiden untuk membantu proses pendistribusian atau eskalasi penanganan layanan. Selain itu *helpdesk* juga

DSS02.01			
No.	**Aktivitas DSS02.01 – Menetapkan skema klasifikasi insiden dan layanan permintaan**	**Dilakukan**	**Keterangan**
			sudah melakukan prioritasi insiden didasarkan pada tingkat urgensitasnya
2.	Mendefinisikan bentuk insiden untuk mengetahui kesalahan untuk membuat resolusi yang efisien dan efektif.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan pendefinisian insiden untuk mengetahui jenis dan solusi yang akan dilakukan kedepannya.
3.	Mendefinisikan model permintaan layanan berdasarkan tipe permintaan layanan untuk memungkinkan dilakukan secara mandiri dan layanan yang efisien untuk permintaan yang standar.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan penefinisian model permintaan layanan berdasarkan jenisnya namun tidak terdapat daftar kategorisasi yang ditetapkan.
4.	Mendefinisikan peraturan dan prosedur eskalasi insiden, terutama untuk insiden utama dan insiden keamanan.	-	*Helpdesk* subdir layanan DPTSI tidak menetapkan peraturan maupun prosedur dalam melakukan eskalasi insiden.
5.	Mendefinisikan pengetahuan permintaan layanan dan kegunaannya.	√	*Helpdesk* subdir layanan DPTSI sudah menfefinisikan pengetahuan permintaan layanan melalui penggalian informasi dan komunikasi kepada pengguna terkait insiden maupun permintaan layanan yang diajukan.

DSS02.02			
No.	**Aktivitas DSS02.02 – Mencatat, mengklasifikasikan dan Memprioritaskan Permintaan dan Insiden**	**Dilakukan**	**Keterangan**
1.	Menetapkan dan mendefinisikan klasifikasi permintaan layanan dan skema prioritisasi beserta kriteria untuk pendaftaran masalah, melakukan pencatatan semua permintaan dan insiden serta semua informasi yang terkait, sehingga bisa di tangani secara efektif dan laporan tersebut bisa dipelihara.	√	*Helpdesk* subdir layanan DPTSI mencatat permintaan dan keluhan yang masuk dengan cara *meng-capture e-mail* maupun laporan dari *e-ticket* yang masuk.
2.	Untuk memungkinkan analisis tren, diperlukan klasifikasi permintaan layanan dengan melakukan identifikasi tipe dan kategori dari permintaan tersebut.	-	*Helpdesk* subdir layanan DPTSI sudah melakukan klasifikasi permintaan layanan dan insiden serta prioritasinya, meskipun belum ada penetapan terstandar dan tertulis yang mengacu pada standar. Namun *helpdesk* tidak melakukan analisis tren .
3.	Melakukan prioritisasi permintaan layanan berdasarkan definisi layanan dari SLA terhadap proses bisnis perusahaan dan tingkat urgensi.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan sistem prioritasi berdasarkan tingkat urgensitas layanan dan insiden yang masuk.

DSS02.03			
No.	**Aktivitas DSS02.03 – Melakukan Verifikasi, Menerima dan Memenuhi Permintaan Layanan**	**Dilakukan**	**Keterangan**
1.	Melakukan verifikasi terhadap hak untuk menggunakan permintaan layanan, jika dimungkinkan, alur proses yang telah didefinisikan dan perubahan standar.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan verifikasi kepada pengguna dengan cara memberikan edukasi terkait alur penanganan insiden.
2.	Memperoleh persetujuan finansial dan fungsonal atau tanda tangan, jika dibutuhkan, atau persetujuan otomatis untuk persetujuan dalam perubahan yang standar.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan pengajuan finansial dan fungsional kepada pihak manajemen seperti ke kepada subdirektorat, jika insiden maupun layanan yang masuk membutuhkannya.
3.	Melakukan pemenuhan 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.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan pemenuhan permintaan dengan memilih alur dan prosedur yang sesuai dengan bidang permasalahan meskipun tidak ada alur tertulis yang ditetapkan.

DSS02.04			
No.	**Aktivitas DSS02.04 – Menginvestigasi, Mendiagnosa dan Mengalokasikan Insiden**	**Dilakukan**	**Keterangan**
1.	Mengidentifikasikan dan mendeksripsikan gejala yang relevan untuk mendirikan penyebab yang paling tepat dari insiden tersebut.	√	*Helpdesk* subdir layanan DPTSI sudah menganalisis gejala yang relevan untuk menentukan penyebab sebelum solusi yang akan digunakan.
2.	Jika insiden tersebut tidak tersedia, buat sebuah log baru.	√	*Helpdesk* subdir layanan DPTSI sudah membuat dokumentasi insiden baru meskipun tidak berbentuk *log*.
3.	Menetapkan insiden ke fungsi spesialis.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan eskalasi ke fungsi spesialis yaitu dengan mendistribusikan penanganan insiden dan layanan kepada *helpdesk* yang lebih menguasai bidang terkait.

DSS02.05			
No.	**Aktivitas DSS02.05 – Melakukan Penyelesaian dan Pemulihan Insiden**	**Dilakukan**	**Keterangan**
1.	Memilih dan menggunakan resolusi insiden yang tepat (*temporary workaround* dan/atau solusi tetap).	√	*Helpdesk* subdir layanan DPTSI sudah melakukan pemilihan resolusi insiden sesuai dengan kebutuhan penanganan.

DSS02.05			
No.	**Aktivitas DSS02.05 – Melakukan Penyelesaian dan Pemulihan Insiden**	**Dilakukan**	**Keterangan**
2.	Merekam *workaround* mana yang digunakan untuk melakukan resolusi insiden.	-	*Helpdesk* subdir layanan DPTSI tidak mencatat solusi, melainkan langsung mengimplementasikannya.
3.	Melakukan aksi pemulihan (jika dibutuhkan).	√	*Helpdesk* subdir layanan DPTSI sudah melakukan aksi pemulihan sesuai dengan penyebab dan kebutuhan penanganan insiden.
4.	Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat dipakai sebagai sumber pengetahuan mendatang.	√	*Helpdesk* subdir layanan DPTSI sudah mendokumentasikan solusi insiden sebagai bentuk penyelesaian penanganan insiden dan layanan, namun belum ada format laporan khusus untuk mendokumentasikan insiden.

DSS02.06			
No.	**Aktivitas DSS02.06 – Menutup Permintaan Layanan dan Insiden**	**Dilakukan**	**Keterangan**
1.	Melakukan verifikasi dengan pengguna yang berpengaruh (apabila setuju) bahwa layanan permintaan mereka telah dipenuhi dan diselesaikan dengan baik.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan verifikasi terlebih dahulu dengan pengguna sebelum menutup insiden dan layanan yang sudah selesai ditangani. Pengguna dimintai *feedback* terkait penanganan dan pelayanan

DSS02.06			
No.	**Aktivitas DSS02.06 – Menutup Permintaan Layanan dan Insiden**	**Dilakukan**	**Keterangan**
			yang diberikan oleh *helpdesk* lalu menanyakan status insiden terkait validasi penutupan insiden.
2.	Menutup layanan permintaan dan insiden.	√	*Helpdesk* subdir layanan DPTSI menutup permintaan insiden dan layanan dengan memberikan status kepada masing-masing insiden dan layanan.

DSS02.07			
No.	**Aktivitas DSS02.07 – Melacak Status dan Membuat Laporan**	**Dilakukan**	**Keterangan**
1.	Mengawasi dan melacak eskalasi insiden dan resolusi dan penanganan permintaan untuk melakukan progress penyelesaian.	-	*Helpdesk* subdir layanan DPTSI tidak melakukan pengawasan dan penanganan kepada pengguna yang dieskalasikan ke bagian lain, karena hal tersebut menjadi tanggung jawab pihak yang menangani.
2.	Mengidentifikasi informasi stakeholder dan kebutuhan mereka untuk pemenuhan data dan laporan. Idenfitikasi laporan secara berkala.	√	*Helpdesk* subdir layanan DPTSI sudah melakukan penggalian informasi kepada pengguna terkait penanaganan insiden
3.	Menganalisis insiden dan layanan permintaan dengan mengkategorisasikan tren.	-	*Helpdesk* subdir layanan DPTSI tidak melakukan analisis dan kategorisasi tren.

DSS02.07			
No.	**Aktivitas DSS02.07 – Melacak Status dan Membuat Laporan**	**Dilakukan**	**Keterangan**
4.	Membuat dan mendistribusikan laporan berkala atau menyediakan *controlled access* ke *online data*.	-	*Helpdesk* subdir layanan DPTSI membuat laporan terkait penanganan insiden namun tidak menyediakan *controlled access* ke *online data* agar pihak lain dapat mengakses laporan tersebut.

LAMPIRAN D – KUESIONER PENURUNAN KEPUASAN PENGGUNA TERHADAP LAYANAN HELPDESK DPTSI

Tujuan: Kuisioner berikut dilakukan untuk tujuan penelitian Tugas Akhir Jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember (ITS) dalam melihat tingkat penurunan kepuasan pengguna terhadap layanan *helpdesk* 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 (Tinggi)
5 = Penurunan Sangat Banyak (Sangat Tinggi)

No.	Pernyataan	1	2	3	4	5
1	Ketika *helpdesk* tidak memenuhi permintaan dan menangani keluhan					

No.	Pernyataan	1	2	3	4	5
	sesuai harapan saya, maka kepuasan saya mengalami:					
2	Ketika *helpdesk* terlambat dalam merespon laporan saya, maka kepuasan saya mengalami:					
3	Ketika *helpdesk* mengabaikan laporan saya, maka kepuasan saya mengalami:					
4	Ketika *helpdesk* selesai menangani laporan saya di luar batas waktu yang dijanjikan, maka kepuasan saya mengalami:					
5	Ketika *helpdesk* tidak melakukan verifikasi kepuasan saya untuk memastikan bahwa laporan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami :					
6	Ketika *helpdesk* tidak memberi informasi status laporan saya (sedang direspon/selesai ditangani/telah ditutup), maka kepuasan saya mengalami:					
7	Ketika *helpdesk* tidak menangani masalah yang berulang kali saya keluhkan hingga akar permasalahan, maka kepuasan saya mengalami:					
8	Ketika *helpdesk* 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:					

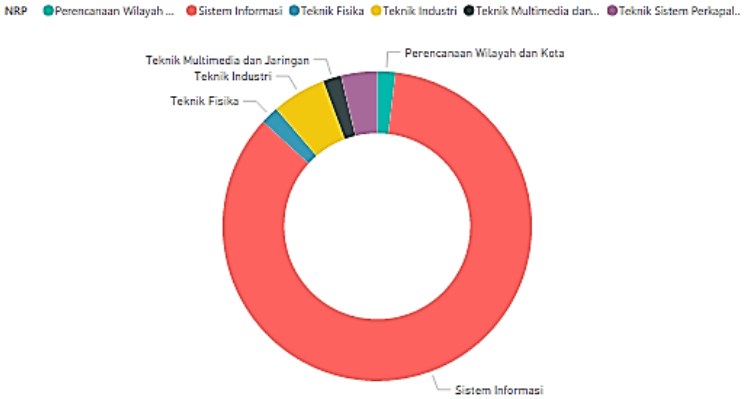
LAMPIRAN E – HASIL KUESIONER (ANALISIS STATISTIK DESKRIPTIF)

Tujuan Kuesioner	:	Mengetahui tingkat penurunan kepuasan pengguna terhadap dampak kinerja *helpdesk* terkait pengelolaan insiden dan permintaan layanan TI pada Subdirektorat Layanan Teknologi dan Sistem Informasi DPTSI ITS
Tanggal Pengisian Kuesioner	:	28 Desember 2016 – 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 *helpdesk* Sub Direktorat Layanan DPTSI, dimana sebagian besar yang menggunakan layanan ialah mahasiswa. Berikut merupakan jurusan responden (mahasiswa Institut Teknologi Sepuluh Nopember).

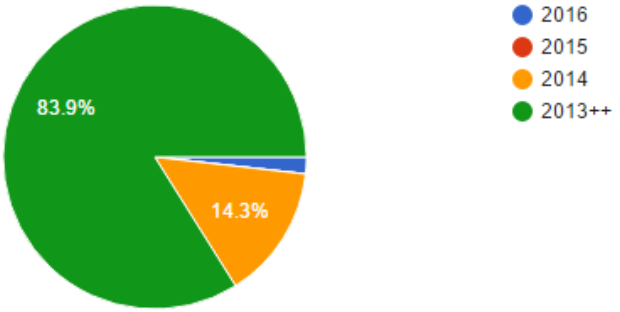


Berdasarkan grafik diatas, dapat diketahui bahwa:

- 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



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 merupakan rentan skala likert yang digunakan untuk melihat hasil respon kuesioner.

Nilai Skala Likert Kuesioner	Keterangan Skala Likert	Rentan Nilai
1	Penurunan Sangat Sedikit	1,00 – 1,50
2	Penurunan Sedikit	1,51 – 2,50
3	Netral	2,51 – 3,50
4	Penurunan Banyak (Tinggi)	3,51 – 4,50
5	Penurunan Sangat Banyak (Sangat Tinggi)	4,51 – 5,00

Berikut merupakan rekap hasil kuesioner yang diambil dari total 53 responden.

ID	Pertanyaan	Jumlah Jawaban Responden					Total	Mean	Keterangan
		1	2	3	4	5			
K01	Ketika *helpdesk* tidak memenuhi permintaan dan menangani keluhan sesuai harapan saya, maka kepuasan saya mengalami:	0	7	5	33	8	53	3.8	Penurunan Banyak (Tinggi)
K02	Ketika *helpdesk* terlambat dalam merespon laporan saya, maka kepuasan saya mengalami:	0	12	7	25	9	53	3.6	Penurunan Banyak (Tinggi)
K03	Ketika *helpdesk* mengabaikan laporan saya, maka kepuasan saya mengalami:	1	2	3	24	23	53	4.2	Penurunan Banyak (Tinggi)
K04	Ketika *helpdesk* selesai menangani laporan saya di luar batas waktu yang dijanjikan, maka kepuasan saya mengalami:	3	15	10	22	3	53	3.1	Netral
K05	Ketika *helpdesk* tidak melakukan verifikasi kepuasan saya untuk memastikan bahwa laporan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami :	7	12	15	17	2	53	2.9	Netral

ID	Pertanyaan	Jumlah Jawaban Responden					Total	Mean	Keterangan
		1	2	3	4	5			
K06	Ketika *helpdesk* tidak memberi informasi status laporan saya (sedang direspon/selesai ditangani/telah ditutup), maka kepuasan saya mengalami:	0	15	9	24	5	53	3.3	Netral
K07	Ketika *helpdesk* tidak menangani masalah yang berulang kali saya keluhkan hingga akar permasalahan, maka kepuasan saya mengalami:	2	10	14	20	7	53	3.4	Netral
K08	Ketika *helpdesk* tidak mengalami peningkatan dalam melayani permintaan dan keluhan saya, maka kepuasan saya mengalami:	1	14	14	20	4	53	3.2	Netral
K09	Ketika sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak dapat saya akses, maka kepuasan saya mengalami:	1	5	9	23	15	53	3.9	Penurunan Banyak (Tinggi)
K10	Ketika keamanan informasi pada sistem *e-ticket* (*website* untuk pelaporan keluhan dan permintaan) tidak terlindungi, maka kepuasan saya mengalami:	0	5	14	21	13	53	3.8	Penurunan Banyak (Tinggi)