TUGAS AKHIR – IS184853

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA HELPDESK UNIT TEKNOLOGI SISTEM INFORMASI PDAM KOTA SURABAYA

INFORMATION TECHNOLOGY PROCESS RISK ASSESSMENT BASED ON COBIT 5 FRAMEWORK AT HELPDESK UNIT OF INFORMATION SYSTEM TECHNOLOGY PDAM SURABAYA

ADITYA SATRIA PUTRA
NRP 0521 15 4000 0004

Dosen Pembimbing
Eko Wahyu Tyas D, S. Kom., MBA
Feby Artwodini, S. Kom., M. T.

Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2019

TUGAS AKHIR – IS184853

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA HELPDESK UNIT TEKNOLOGI SISTEM INFORMASI PDAM KOTA SURABAYA

ADITYA SATRIA PUTRA
NRP 05211540000004

Dosen Pembimbing
Eko Wahyu Tyas D, S.Kom, MBA
Feby Artwodini, S.Kom., M.T.

Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2019

FINAL PROJECT – IS184853

INFORMATION TECHNOLOGY PROCESS RISK ASSESSMENT BASED ON COBIT 5 FRAMEWORK AT HELPDESK UNIT OF INFORMATION SYSTEM TECHNOLOGY PDAM SURABAYA

ADITYA SATRIA PUTRA
NRP 05211540000004

Supervisor
Eko Wahyu Tyas D, S.Kom, MBA
Feby Artwodini, S.Kom., M.T.

Information Systems Department
Faculty of Information and Communication Technology
Institut Teknologi Sepuluh Nopember
Surabaya 2019

LEMBAR PENGESAHAN

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA HELPDESK UNIT TEKNOLOGI SISTEM INFORMASI PDAM KOTA SURABAYA

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi Dan Komunikasi
Institut Teknologi Sepuluh Nopember
Oleh:

ADITYA SATRIA PUTRA
NRP. 0521 15 4000 0004

Surabaya, Juli 2019

KEPALA
DEPARTEMEN SISTEM INFORMASI

Mahendrawathi ER, ST, M.Sc, Ph.D.
NIP 19761011 200604 2 001

LEMBAR PERSETUJUAN

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA HELPDESK UNIT TEKNOLOGI SISTEM INFORMASI PDAM KOTA SURABAYA

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi Dan Komunikasi
Institut Teknologi Sepuluh Nopember

Oleh:

ADITYA SATRIA PUTRA
NRP. 0521 15 4000 0004

Disetujui Tim Penguji: Tanggal Ujian : Juli 2019
Periode Wisuda : September 2019

Eko Wahyu Tyas D, S.Kom, MBA **(Pembimbing I)**

Feby Artwodini, S.Kom, MT. **(Pembimbing II)**

Sholiq, S.T., M.Kom, M.Sa. **(Penguji I)**

Anisah Herdiyanti, S.Kom, M.sc. **(Penguji II)**

PENILAIAN RISIKO PROSES TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 5 PADA *HELPDESK* UNIT TEKNOLOGI SISTEM INFORMASI PDAM KOTA SURABAYA

Abstrak

PDAM Surabaya merupakan unit usaha yang memiliki peran penting dalam memenuhi kebutuhan air bersih masyarakat surabaya yang menerapkan TI untuk membantu dalam pemenuhan tujuan bisnis perusahaan. Salah satu layanan TI yang disediakan adalah manajemen insiden dan pemenuhan permintaan layanan, yang dikelola oleh *helpdesk* unit teknologi sistem informasi. Manajemen insiden dan pemenuhan permintaan layanan adalah proses yang memegang peran penting di perusahaan namun rentan terhadap kesalahan yang bisa menimbulkan beberapa risiko. Karena itu diperlukan identifikasi dan penilaian risiko untuk menghindari permasalahan dalam proses bisnis perusahaan dan meminimalisir kerugian. Untuk mengidentifikasi proses TI, kerangka kerja yang relevan adalah COBIT 5 untuk melakukan manajemen risiko. Risiko diidentifikasi dari proses bisnis *helpdesk* dan kondisi yang ada di dalam organisasi. Data diperoleh dari wawancara dan observasi, kemudian disatukan dengan tujuan ideal berdasarkan COBIT 5 Process DSS02 (Manage Service Request and Incidents). Kemudian Risiko dapat diidentifikasi, dinilai dan dikelola berdasarkan COBIT 5 Process APO12 (Manage risks). Oleh karena itu, keluaran yang diharapkan dari penelitian ini adalah hasil penilaian risiko dan mitigasi berdasarkan kerangka kerja COBIT 5 yang bisa digunakan untuk mengelola risiko.

Kata kunci: Manajemen Insiden, Pengelolaan Permintaan Layanan, Risk Management, COBIT 5

Halaman ini sengaja dikosongkan

INFORMATION TECHNOLOGY PROCESS RISK ASSESSMENT BASED ON COBIT 5 FRAMEWORK AT HELPDESK UNIT OF INFORMATION SYSTEM TECHNOLOGY PDAM SURABAYA

Abstract

PDAM Surabaya is a business unit that has an important role in meeting the needs of Surabaya's clean water. This company implements IT to help meet the company's business goals. One of the IT services provided is incident management and fulfillment of service requests, which are managed by the information system technology helpdesk. Incident management and fulfillment of service requests are processes that play an important role in the company but are vulnerable to problems that can pose several risks. Because of that it needed risk identification and risk assessment to avoid problems in the company's business processes and minimize losses. To identify the IT process, the relevant framework is COBIT 5 to carry out risk management. Risks from helpdesk business processes and conditions that exist within the organization. Data are obtained from interviews and observations, then are integrated with ideal goals based on the COBIT 5 DSS02 Process (Manage Service and Incident Requests). Then the Risk can be identified, assessed and managed based on the COBIT 5 APO12 Process (Manage risk). Therefore, the expected results of this study are the risk assessment result and risk mitigation based on COBIT 5 work that can be used to manage risk.

Keywords: Manajemen Insiden, Pengelolaan Permintaan Layanan, Risk Management, COBIT 5

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas rahmat yang diberikan sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul **"Penilaian Risiko Proses Teknologi Informasi Berdasarkan Kerangka Kerja Cobit 5 pada *Helpdesk* Unit Teknologi Sistem Informasi PDAM Surabaya"** dengan lancar.

Penulis menyadari bahwa Tugas Akhir ini dapat terselesaikan tidak terlepas dari bantuan dan dukungan berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih kepada:

1. Allah SWT. yang senantiasa memberikan petunjuk dan hidayah-Nya sehingga penulis diberikan kekuatan serta kemudahan dalam menyelesaikan Penelitian Tugas Akhir.
2. Eko Wahyu Tyas Darmaningrat, S.Kom, MBA dan Feby Artwodini S.kom, M.T. selaku dosen pembimbing Tugas Akhir yang senantiasa meluangkan waktu untuk memberikan arahan, bimbingan, saran, dukungan serta motivasi selama penyusunan Tugas Akhir
3. Annisah Herdiyanti, S.Kom, M.Sc dan Sholiq, S.T, M.Kom, M.SA selaku dosen penguji yang telah banyak memberi masukan kepada penulis
4. Ayah dan Ibu penulis, atas segala doa, nasehat, kasih sayang, dan dukungan yang diberikan demi kesuksesan penulis
5. Kakak-kakak penulis yaitu Ari, Bayu, Putri dan semua keluarga atas dukungan yang diberikan selama penulis mengikuti perkuliahan di Departemen Sistem Informasi ITS ITS
6. Semua teman-teman Safari ITS yang selalu memberikan semangat, dukungan, dan doa kepada penulis selama masa perkuliahan
7. Direktur utama PDAM Surabaya atas dukungan, ilmu, dan pengalaman dalam melakukan penelitian Tugas Akhir

8. Teman-teman Sistem Informasi ITS 2015 atas segala dukungan dan semangat yang diberikan kepada penulis selama pengerjaan Tugas Akhir
9. Teman-teman fungsionaris UKTK ITS dan KSR ITS yang selama perkuliahan memberikan banyak pembelajaran dan mendukung penulis dalam mengembangkan *softskill* penulis
10. Semua pihak yang turut membantu dalam pelaksanaan Tugas Akhir yang tidak bisa penulis sebutkan satu persatu yang telah memberikan dorongan motivasi, berbagi ilmu dan cerita, serta hal-hal yang membantu penulis dalam mengerjakan penelitian Tugas Akhir.

Besar harapan penulis untuk mendapatkan kritik dan saran yang membangun sehingga Tugas Akhir ini dapat memberikan manfaat bagi semua pihak yang terkait.

Surabaya, Juni 2019

Penulis

DAFTAR ISI

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan

DAFTAR TABEL

BAB I
PENDAHULUAN

Pada bab pendahuluan ini akan membahas terkait latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan relevansi terhadap pengerjaan tugas akhir.

1.1 Latar Belakang

Perusahaan Daerah Air Minum Surabaya atau PDAM Surabaya merupakan unit usaha yang memiliki peran penting dalam pemenuhan kebutuhan air bersih masyarakat Surabaya. PDAM Surabaya memiliki visi menjadi perusahaan air minum modern. Dalam pencapaian visi tersebut, perusahaan memiliki beberapa misi antara lain memastikan pengelolaan keuangan yang transparan untuk kesejahteraan masyarakat, membangun masyarakat yang bijak dalam penggunaan air, menyediakan air minum yang efisien dan berkelanjutan, serta membangun lingkungan kerja yang memperioritaskan integritas dan prestasi [1].

Dalam rangka pencapaian visi dan misinya, PDAM Surabaya menerapkan Teknologi Informasi (TI). Sebagai enabler bisnis, TI akan memberi nilai bagi perusahaan jika tujuan TI selaras dengan tujuan bisnis [2]. Unit layanan Teknologi Sistem Informasi PDAM Surabaya memiliki peran penting untuk keberlangsungan proses bisnis, terutama bagian *helpdesk* yang bertugas untuk mengelola insiden dan pemenuhan permintaan layanan. *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 [3]. *Helpdesk* yang baik juga berfungsi untuk mencatat dan mengklasifikasikan permasalahan yang terjadi serta solusinya sehingga dapat menjadi asset knowledge bagi perusahaan. Namun dalam penerapannya TI tidak selalu berjalan sesuai dengan yang diharapkan, sehingga akan menimbulkan risiko yang dapat merugikan perusahaan.

Risiko proses TI adalah risiko yang terkait dengan TI yakni risiko bisnis yang terkait dengan penggunaan, kepemilikan, pengoperasian, keterlibatan, pengaruh dan penerapan TI dalam suatu organisasi [4]. Sedangkan manajemen risiko mengacu pada budaya proses dan struktur yang diarahkan pada pengelolaan ketidakpastian [5]. Proses pada manajemen risiko terjadi secara sistematis, terus menerus dan diterapkan dalam segala aspek [6]. Dalam konteks organisasi, manajemen risiko diterapkan dalam seluruh bidang yang terdapat dalam organisasi tersebut.

Dalam aktivitas operasional pemberian layanan TI kepada pengguna, tidak jarang *helpdesk* mengalami gangguan dan risiko dalam melakukan aktivitas manajemen insiden, pemenuhan permintaan layanan di luar insiden, maupun penerimaan permintaan akses [7]. Begitu juga dengan *helpdesk* PDAM Surabaya yang selama ini hanya sebatas pada melakukan pencatatan dan penanganan risiko tanpa memberikan penilaian risiko tersendiri terkait pengelolaan layanan dan insiden di PDAM Surabaya, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Oleh karena itu perlu adanya suatu kontrol bagi *helpdesk* untuk memastikan bahwa proses pengelolaan permintaan layanan dan insiden pada *helpdesk* dapat berjalan dengan baik, serta untuk memitigasi risiko pada proses.

Berdasarkan refleksi terhadap permasalahan dari kondisi kekinian yang dialami oleh PDAM Surabaya, penelitian ini bertujuan untuk melakukan manajemen risiko berdasarkan best practice COBIT 5 Domain DSS02 – Manage Service Request and Incident dan APO12 - Manage risk pada *helpdesk* unit Layanan Teknologi Sistem Informasi PDAM Surabaya. Kerangka kerja dan standar yang relevan dengan penelitian ini adalah COBIT 5. kerangka kerja COBIT memberikan gambaran paling detil mengenai strategi dan kontrol dalam pengaturan proses TI yang mendukung keselarasan strategi bisnis dan tujuan TI [8]. Penelitian dengan kerangka kerja COBIT 5 pada PDAM Surabaya juga sudah pernah dilakukan oleh Dyah Retnani Sulistyaningrum dalam pembuatan perangkat audit [9].

COBIT 5 dipilih karena dianggap sesuai dengan kondisi teknologi yang ada pada PDAM Surabaya sekarang karena perusahaan sudah akrab dengan kerangka kerja yang akan digunakan.

Dengan adanya penilaian risiko ini diharapkan dapat mempermudah PDAM Surabaya dalam melakukan manajemen risiko untuk memastikan risiko yang akan dihadapi perusahaan dapat ditangani dengan baik agar tidak mengganggu proses bisnis yang sedang berjalan.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, didapatkan perumusan permasalahan yaitu:

1. Apa saja risiko yang terdapat pada unit *helpdesk* Layanan Teknologi Sistem Informasi PDAM kota Surabaya?
2. Bagaimana hasil pemetaan risiko proses TI yang terdapat pada unit *helpdesk* Layanan Teknologi Sistem Informasi PDAM kota Surabaya berdasarkan COBIT 5?
3. Bagaimana hasil penilaian risiko yang terdapat pada unit *helpdesk* Layanan Teknologi Sistem Informasi PDAM kota Surabaya berdasarkan COBIT 5 sebagai langkah mitigasi risiko?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Studi kasus yang digunakan hanya pada bagian *helpdesk* Layanan Teknologi Sistem Informasi PDAM kota Surabaya.
2. Tidak melakukan identifikasi risiko pada proses selain proses manajemen insiden dan pemenuhan permintaan layanan.
3. Tidak membahas tentang pengelolaan profil risiko.

4. Responden kuisioner pada penelitian ini hanya pada pegawai PDAM kota Surabaya yang merupakan pengguna layanan *helpdesk* unit teknologi sistem informasi.

1.4 Tujuan

Tujuan dilakukannya tugas akhir ini adalah untuk mengetahui hasil penilaian risiko pada proses TI berdasarkan pendekatan COBIT 5 *for Risk* untuk unit *helpdesk* Layanan Teknologi Sistem Informasi PDAM kota Surabaya dan mengetahui hasil pemetaan risiko dengan proses TI pada COBIT 5 Enabling processes sebagai langkah mitigasi.

1.5 Manfaat

Hasil dari penelitian ini diharapkan dapat menjadi acuan dan panduan untuk mengelola risiko serta pedoman untuk mengantisipasi kerugian pada unit *helpdesk* Layanan Teknologi Sistem Informasi PDAM kota Surabaya.

1.6 Relevansi

Penelitian ini berkaitan dengan mata kuliah Manajemen Risiko Teknologi Informasi, Manajemen Layanan Teknologi Informasi, serta Tata kelola Teknologi Informasi. Fokus utama dari Lab MSI adalah optimalisasi dari peran Teknologi Informasi dalam mendukung bisnis/organisasi.

Berdasarkan Tabel 1.1 topik yang digunakan dalam penelitian ini adalah Pengelolaan Risiko TI yang merupakan bagian dari bidang keilmuan yang ada pada Lab MSI.

Tabel 1. 1 MSI Road Maps

Isu strategis dari penelitian lab MSI pada tahun 2016 – 2025	
No	Nama
1	TI sebagai tools Strategi
2	Penerapan E-Government (egov)
3	Manajemen & Perubahan Proyek TI
4	Pengembangan Sistem Informasi

Isu strategis dari penelitian lab MSI pada tahun 2016 – 2025	
5	Kedewasaan Proses TI
6	Pengembangan Layanan TI
7	Penjaminan Mutu Proses TI
8	Pengelolaan Risiko TI
9	IT Productivity Paradox, IT Business Value
10	TI sebagai tools Strategi
11	Penerapan E-Government (egov)

Halaman ini sengaja dikosongkan

BAB II
TINJAUAN PUSTAKA

Pada bab ini akan dijelaskan mengenai penelitian sebelumnya dan dasar teori yang akan dijadikan acuan atau landasan dalam pengerjaan penelitian ini.

2.1 Penelitian Terdahulu

Pada subbab ini akan dijelaskan tentang penelitian terdahulu yang digunakan dalam penelitian ini yang menjelaskan tentang peran COBIT 5 *for Risk* dalam menganalisis risiko dan juga penggunaan domain DSS02 dan APO12 - *Manage risk* dalam manajemen risiko.

Tabel 2. 1 Ringkasan penelitian sebelumnya

Penelitian Ke-1	
Judul Penelitian	Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik) [10]
Penulis; Tahun	Nurfitri Zukhrufatul dan Suprapto; 2018
Deskripsi Umum Penelitian	Penelitian ini menjelaskan tentang permasalahan yang dihadapi oleh PT. Petrokimia Gresik yaitu padatnya proses bisnis yang berjalan di PT. Petrokimia Gresik, mengakibatkan aktivitas pengelolaan risiko menjadi kurang optimal, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Penelitian ini menghasilkan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko-risiko yang tidak diinginkan. Penelitian ini juga menjelaskan tentang subdomain COBIT 5 yang berkaitan dengan penerapan manajemen risiko yaitu subdomain APO12 - *Manage risk*. Sehingga dari penelitian ini diketahui pengelolaan risiko yang telah dicapai PT. Petrokimia Gresik, hasil *capability level* untuk subdomain APO12 pada level 3 (*Established Process*) dan target yang ingin dicapai untuk subdomain APO12 adalah 1 level diatasnya. Dari hasil yang sudah diketahui maka diberikan rekomendasi berupa saran maupun usulan pada proses evaluasi, langkah mitigasi dalam penerapan dan perbaikan manajemen risiko teknologi informasi
Keterkaitan Penelitian	Literatur ini dapat digunakan sebagai acuan dalam melakukan pengerjaan penelitian karena membahas tentang peran APO12 - *Manage risk* pada COBIT 5 dalam manajemen risiko. Serta memberikan pandangan terhadap masalah-masalah apa saja yang akan dihadapi ketika melakukan penilaian risiko di perusahaan.
Penelitian Ke-2	
Judul Penelitian	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 [11].
Penulis; Tahun	Chitra Utami Putri; 2017
Deskripsi Umum Penelitian	Penelitian ini melakukan analisis risiko beserta langkah mitigasinya untuk service desk DPTSI ITS yang berdasarkan pada kerangka kerja COBIT 5 untuk penilaian risiko. Penelitian ini menekankan pada manajemen insiden yang mengacu pada domain DSS02 – *Manage Service Request and Incident* dan APO12 - *Manage risk* di COBIT 5.
Keterkaitan Penelitian	Literatur ini dapat digunakan sebagai pendukung dalam menggunakan framework COBIT 5 karena jurnal ini menggunakan domain DSS02 - *Manage Service Request and Incident* di COBIT 5 dalam menganalisis penilaian risiko. Selain itu penelitian ini juga menjabarkan risiko-risiko pada *service desk* yang telah ditemukan hingga saat ini.
Penelitian Ke-3	
Judul Penelitian	Evaluasi Pengelolaan Risiko Teknologi Informasi(TI) pada Instansi Pemerintah: Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri [12].
Penulis; Tahun	Sigit Samaptoaji; 2014
Deskripsi Umum Penelitian	Penelitian ini menjelasakan tentang penggunaan analisis *risk assessment* dan penentuan strategi atau langkah mitigasi dengan kerangka kerja COBIT dan NIST *Special Publication* 800-30 sehingga menghasilkan dokumen profil risiko teknologi informasi yang dapat dijadikan sebagai masukan atau pertimbangan dalam proses pengambilan keputusan. Penelitian ini juga menjelaskan bagaimana pemberian sebuah nilai pada sebuah risiko sehingga dapat menentukan *inherent risk* dan *residual risk*.
Keterkaitan Penelitian	Literatur ini dapat digunakan sebagai pendukung dalam melakukan penilaian risiko. Dari penilaian tersebut dapat diketahui langkah-langkah yang tepat untuk mitigasi risiko.

Analisa kesenjangan pada ketiga penelitian sebelumnya yang menjadi acuan untuk penelitian ini dapat dilihat pada Tabel 2.2.

Tabel 2. 2 Analisa Gap penelitian sebelumnya

Penelitian Ke-1	Penelitian Ke-2	Penelitian Ke-3
• Penelitian dilakukan di PT. Petrokimia Gresik	• Penelitian dilakukan di DPTSI ITS	• Penelitian dilakukan di Direktorat Jenderal Kependudukan dan

Penelitian Ke-1	Penelitian Ke-2	Penelitian Ke-3
• Standar yang menjadi acuan adalah standar COBIT 5 • Penelitian menggunakan domain COBIT 5 APO 12 *Manage Risk*	• Penilaian risiko berdasarkan metode penilaian COBIT 5 *for Risk* • Penelitian menggunakan domain COBIT 5 APO 12 *Manage Risk*	Pencatatan Sipil Kementerian Dalam Negeri • Standar yang menjadi acuan adalah standar COBIT dan NIST *Special Publication* 800-30
Pendukung: Standar yang digunakan sama yaito COBIT 5	Pendukung: Ruang lingkup yang digunakan sama yaitu pada bagian *helpdesk*	Pendukung: Standar yang digunakan sama yaitu COBIT 5

Penelitian yang Diusulkan: Penilaian Risiko Proses Teknologi Informasi Berdasarkan Kerangka Kerja Cobit 5 Pada *Helpdesk* Unit Teknologi Sistem Informasi PDAM Kota Surabaya
• Penilaian risiko berdasarkan metode penilaian pada COBIT 5 *for Risk* • Menggunakan domain DSS02 – *Manage Service Request and Incident* dan APO12 - *Manage risk* di COBIT 5 • Penilaian dilakukan oleh peneliti dengan cara wawancara, observasi dan studi dokumen

2.2 Dasar Teori

Pada subbab ini akan dijelaskan mengenai teori-teori pendukung untuk penelitian ini.

2.2.1 Risiko

Risiko menurut Kamus Besar Bahasa Indonesia (KBBI) merupakan akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan [13]. Sedangkan menurut pengertian COBIT risiko adalah kemungkinan kerugian, kerusakan atau hancurnya sebuah asset yang disebabkan oleh adanya ancaman karenan terdapat sebuah celah. Risiko adalah sebuah hasil yang tidak diketahui yang mana jarang terjadi dan dapat diukur atau paling tidak dipelajari [14]. Berdasarkan IRM (*Institute of Risk Management*), risiko adalah kombinasi dari kemungkinan kejadian yang tidak pasti dan terdapat konsekuensi atas kejadian tersebut.

2.2.2 Risiko TI

Risiko TI adalah risiko bisnis yang berkaitan erat dengan penggunaan, kepemilikan, operasional, keterlibatan, pengaruh dan adopsi TI di dalam perusahaan [15]. Risiko TI bisa berasal dari berbagai hal yang berkaitan dengan penggunaan teknologi informasi, misalnya terdapat celah pada sumber daya manusia, celah pada hardware, celah pada software, atau celah pada jaringan. Risiko teknologi informasi dibagi menjadi 3 jenis, berdasarkan keputusan yaitu: confidentially, integrity, dan authentication. Terdapat prinsip-prinsip penting dari sebuah rencana keamanan informasi (information security), ialah kerahasian (confidentiality), keutuhan data (integrity) dan ketersediaan (availability). CIA adalah standar yang digunakan banyak pihak untuk mengukur keamanan sebuah sistem. Prinsip-prinsip keamanan informasi, ialah sebagai berikut[16]:

1. Kerahasiaan (*confidentiality*), yaitu membatasi akses informasi hanya bagi pengguna tertentu dan mencegah orang yang tidak berhak memperoleh informasi tersebut. Implementasi konsep *confidentiality* salah satunya adalah *user* ID dan *password* dalam skema otentikasi.
2. Keutuhan data/informasi (*integrity*), yaitu taraf kepercayaan terhadap sebuah informasi. Dalam konsep ini tercakup *data integrity* dan *source integrity*. Keutuhan data terwujud jika data/informasi belum diubah (masih asli), baik perubahan yang terjadi karena kesalahan atau dilakukan sengaja oleh seseorang.
3. Ketersediaan (*availability*), adalah ketersediaan sumber informasi. Jika sebuah sumber informasi tidak tersedia ketika dibutuhkan, bahkan bisa lebih buruk lagi. Ketersediaan ini bisa terpengaruh oleh faktor teknis, faktor alam maupun karena faktor manusia. Meskipun ada tiga faktor yang berpengaruh, tetapi umumnya manusia adalah link paling lemahnya. Karenanya, wajar jika Anda perlu

memperhatikan perlunya menggunakan *tools* untuk data *security*.

Risiko tersebut dapat berupa kerentanan teknologi informasi dari sebuah organisasi dan ancaman teknologi informasi. Risiko TI erat kaitannya dengan keamanan informasi, dimana informasi merupakan aset penting di dalam sebuah organisasi dan apabila terganggu dapat menimbulkan dampak yang signifikan pada proses bisnis organisasi.

2.2.3 Risiko Proses Teknologi Informasi

Proses teknologi informasi merupakan rangkaian kinerja atau aktivitas suatu organisasi dengan menggunakan teknologi dan sistem informasi untuk mencapai tujuan organisasi dan membantu proses bisnis organisasi. Dalam melakukan proses teknologi informasi tentu saja memungkinkan terdapat risiko dimana terdapat kemungkinan terjadinya gangguan dan ancaman bahaya yang muncul ketika proses teknologi informasi berlangsung. Risiko Proses teknologi informasi merupakan gangguan dan ancaman bahaya yang muncul dari serangkaian proses TI yang dimiliki oleh sebuah organisasi [11].

2.2.4 Manajemen Risiko Teknologi Informasi

Manajemen risiko TI adalah proses identifikasi, pengkajian, pengembangan strategi mitigasi dan komunikasi risiko TI yang berpotensi merugikan atau berdampak negatif terhadap organisasi. Mekanisme kontrol dan pengukuran kinerja manajemen risiko TI yang dilakukan oleh semua pihak secara efektif dapat memilih risiko mana yang harus diberi perhatian dan risiko mana yang dapat diterima pada level risiko dan organisasi memfokuskan pada risiko yang benar-benar penting [17]. Menurut *National Institute of Standards and Technology*, manajemen risiko memiliki tiga proses utama yaitu sebagai berikut[18]:

1. *Risk assessment*, adalah proses untuk mengidentifikasi dan mencari dampak risiko sehingga disepakati kontrol mitigasi yang sesuai.

2. *Risk mitigation*, adalah proses untuk mengimplementasikan kontrol yang tepat dalam mengurangi risiko yang sudah diidentifikasi sebelumnya di proses *risk assessment*.
3. *Evaluation and assessment*, adalah proses evaluasi hasil penerapan mitigasi risiko yang sudah dilakukan dan melakukan evaluasi tindak lanjut dengan memberikan panduan agar manajemen risiko berjalan dengan baik.

Manajemen risiko TI bukanlah hal yang mudah, merupakan hal penting untuk menjaga keseimbangan dalam proses manajemen risiko yang cukup sulit dan menghabiskan banyak waktu. Menurut kerangka kerja COBIT 5 *Enabling Process* terdapat empat strategi dalam penanganan risiko yaitu sebagai berikut [14]:

1. Menerima risiko (*acceptance)* adalah risiko yang 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)* adalah upaya perusahaan untuk mengurangi dampak yang mungkin disebabkan oleh risiko yang terjadi. 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)* adalah apabila risiko yang dihadapi terlalu besar dan membawa dampak buruk bagi perusahaan, sehingga perusahaan lebih memilih untuk tidak melakukan aktivitas yang merugikan tersebut karena dapat menimbulkan risiko yang memiliki dampak signifikan.
4. Melakukan transfer risiko (*transference)* adalah apabila risiko yang dihdapi tidak bisa diselesaikan oleh internal perusahaan itu sendiri, sehingga perlu dialihkan kepada pihak ketiga. 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.

2.2.5 *Helpdesk*

Helpdesk system merupakan suatu sistem digunakan untuk penanganan problem management yang mengacu kepada perusahaan tersebut sehingga melalui sistem *ticketing*, *incident* ataupun *problem management* yang diakibatkan oleh IT services perusahaan dapat diidentifikasi dan dikonsolidasikan melalui berbagai media komunikasi yang tersedia di perusahaan, seperti telepon, email, dan juga *web interface*. Sehingga seluruh *incident* ataupun *problem management* dapat ditanggulangi dan diberikan solusinya atas permasalahan yang muncul [19].

2.2.6 Manajemen Insiden

Manajemen insiden dan masalah merupakan bagian dari layanan TI. Insiden adalah sesuatu yang terjadi diluar rencana berupa gangguan yang mengakibatkan pengurangan kualitas terhadap layanan TI. ITIL mendefinisikan manajemen insiden adalah proses untuk menangani semua kasus, termasuk kegagalan, pernyataan keluhan atau gangguan (biasanya

melalui *service desk*), yang dilaporkan oleh pengguna layanan TI [20].

Tujuan utama dari proses Manajemen Insiden adalah untuk mengembalikan layanan secepat mungkin agar beroperasi normal seperti biasa dan meminimalkan dampak yang merugikan operasi bisnis, sehingga memastikan dan mempertahankan ketersediaan layanan dengan kualitas terbaik.

Proses manajemen insiden ITIL terdiri dari [20]:

1. Identifikasi
2. Mencatat
3. kategorisasi
4. Prioritas
5. Diagnosis awal
6. Eskalasi
7. Investigasi dan Diagnosis
8. Resolusi dan *Recovery*
9. Menutup

2.2.7 Kerangka Kerja Manajemen Risiko

Keberhasilan manajemen risiko bergantung 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 [21].

Agar manajemen risiko yang dilakukan dapat berjalan dengan baik, maka dibutuhkan kerangka kerja yang sudah tersertifikasi dan telah diakui secara global dimana mempunyai metode atau panduan yang dapat dijadikan pedoman dalam pembuatan pengelolaan risiko yang ada pada organisasi.

2.2.8 Kerangka Kerja Manajemen Risiko TI

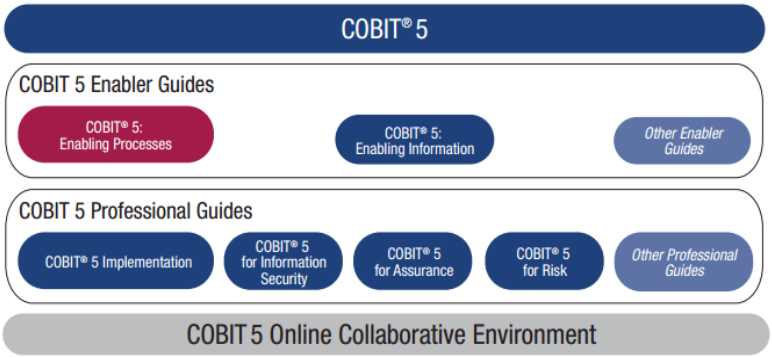
Berikut ini merupakan kerangka kerja manajemen risiko yang umum digunakan berkaitan dengan risiko teknologi informasi:

1. ISO/IEC 27001 dan 27002
   ISO/IEC 27001 merupakan standar yang menetapkan kebutuhan dalam membangun, menerapkan, mempertahankan, dan peningkatan berkelanjutan sebuah sistem manajemen keamanan informasi (SMKI) dalam organisasi yang mencakup penilaian dan perlakuan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi [22].
   Sedangkan ISO 27002 melengkapi konteks dari ISO/IEC 27001. Tujuan dari ISO 27002 ini adalah mengidentifikasi penilaian risiko dan menjelaskan kontrol keamanan informasi yang sesuai. Dimana standar ini digunakan sebagai titik awal penyusunan dan pengembangan Sistem Manajemen Keamanan Informasi (SMKI). Pada standar ini terdapat panduan dalam perencanaan dan implementasi suatu program untuk melindungi aset informasi [23].
2. *Octave*
   OCTAVE (*The Operationally Critical Threat, Asset, and Vulnerability Evaluation*) merupakan metode yang digunakaan sebagai cara untuk mengidentifikasi dan mengevaluasi risiko keamanan informasi dimana berfokus kepada aset dari teknologi informasi yang dimiliki organisasi dalam menerapkan manajemen risiko [24].
3. *COBIT* 5 *for Risk*
   COBIT 5 *for Risk* merupakan panduan COBIT yang dibuat secara khusus untuk melakukan manajemen risiko. Pada COBIT 5 berisi tentang panduan detail dalam mengantisipasi atau memitigasi dampak kerugian bisnis.
   Penelitian ini dipilih menggunakan kerangka kerja COBIT 5 karena risiko yang diidentifikasi berdasarkan proses TI yang terjadi [8]. COBIT 5 *for Risk* menyediakan panduan professional mengenai risiko yaitu diantaranya:

a. Panduan tentang bagaimana menggunakan kerangka kerja COBIT 5 untuk menetapkan tata kelola dan fungsi manajemen risiko untuk perusahaan.
b. Bimbingan dan pendekatan terstruktur tentang bagaimana menggunakan prinsip COBIT 5 untuk mengatur dan mengelola risiko TI.
c. Pemahaman yang jelas tentang penyelarasan COBIT 5 untuk Risiko dengan standar lain yang relevan.

2.2.9 COBIT 5 Enabling Processes

COBIT merupakan singkatan dari *Control Objectives for Information and Related Technology*, merupakan salah satu kerangka kerja (*framework*) dalam mendukung tata kelola teknologi informasi yang dikembagkan oleh sebuah asosiasi *ICASA (Information Systems Audit and Control Association)*. Framework COBIT 5 dibangun berdasarkan 5 prinsip yang dijelaskan secara detail mengenai panduan untuk pengelolaan Teknologi Informasi [14]. Dalam COBIT 5 memiliki *product family* yang digambarkan pada Gambar 2.1.

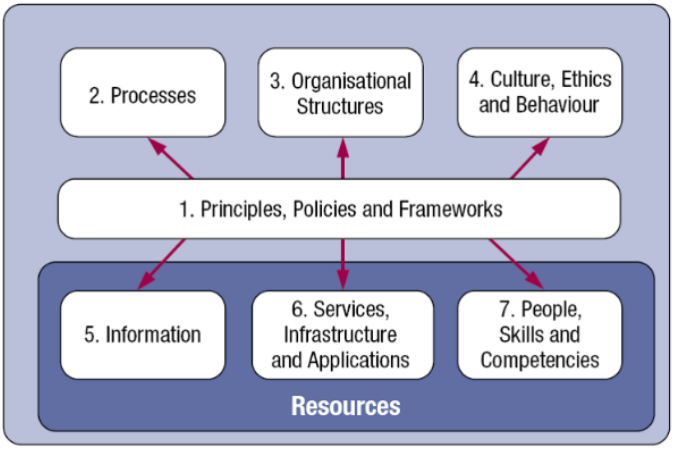


Gambar 2. 1 *COBIT 5 Product Family*

Pada COBIT *Enabler Guides* terdapat produk *enabling process* dan *enabling information*. COBIT *Enabling Process* dapat membantu auditor dan manajer untuk menyambungkan *gap* antara proses bisnis, kebutuhan teknologi informasi, kebutuhan proses, serta risiko TI. Dengan demikian, COBIT 5

dapat mengidentifikasi risiko yang lebih akurat dan dapat menangani risiko tersebut serta merupakan pendekatan yang umum dan berkelanjutan untuk melakukan penilaian terhadap risiko teknologi informasi

COBIT 5 *for Risk* memberikan panduan dan menjelaskan bagaimana masing-masing *enabler* berkontribusi terhadap keseluruhan tata kelola dan pengelolaan fungsi risiko [25]. Pada Gambar 2.2 menunjukkan tujuh kategori *enabler*.



Gambar 2. 2 *Enabler* pada COBIT 5 *for Risk*

1. *Principles, Policies, and Frameworks* merupakan prinsip dan kerangka kerja yang digunakan sebagai petunjuk praktek untuk pelaksanaan manajemen.
2. *Proccess* menjelaskan kumpulan aktivitas yang dilakukan untuk mencapai tujuan dan memiliki outcome yang mendukung tujuan bisnis dan Teknologi Informasi.
3. *Organizational Structures* merupakan pembuat keputusan dalam pelaksanaan manajemen.
4. *Culture, Ethnics, and Behaviour* merupakan kebiasaan dari individu atau kelompok dalam perusahaan baik yang mendukung atau menghambat kesuksesan tata kelola dan manajemen.

5. *Information* dijadikan sebagai kebutuhan untuk memastikan agar organisasi tetap berjalan dan dapat dikelola dengan baik.
6. *Services, Infrastructure, and Applications* menyediakan layanan dan proses teknologi informasi bagi perusahaan.
7. *People, Skills, and Competencies* merupakan sumber daya dalam manajemen dan tata kelola perusahaan yang dibuberkontribusi dalam aktivitas, pembuat keputusan dan perbaikan.

2.2.10 Perspektif Risiko COBIT 5 *for Risk*

COBIT 5 *for Risk* memiliki 2 Perspektif Risiko yaitu perspektif fungsional dan perspektif manajemen. Berdasarkan perspektif fungsional, risiko dideskripsikan sebagai cara untuk membangun dan mempertahankan fungsi risiko pada enterprise dengan menggunakan COBIT 5 *Enabler*. Pada perspektif fungsional risiko, COBIT 5 *for Risk* menyediakan panduan dan mendeskripsikan bagaimana setiap *enabler* dapat berkontribusi pada semua tata kelola dan menajemen pada fungsi risiko. Sedangkan perspektif manajemen melihat pada tata kelola risiko utama, proses manajemen risiko, dan scenario risiko. Perspektif ini mendeskripsikan bagaimana risiko itu dapat dimitigasi dengan menggunakan COBIT 5 *Enabler.*

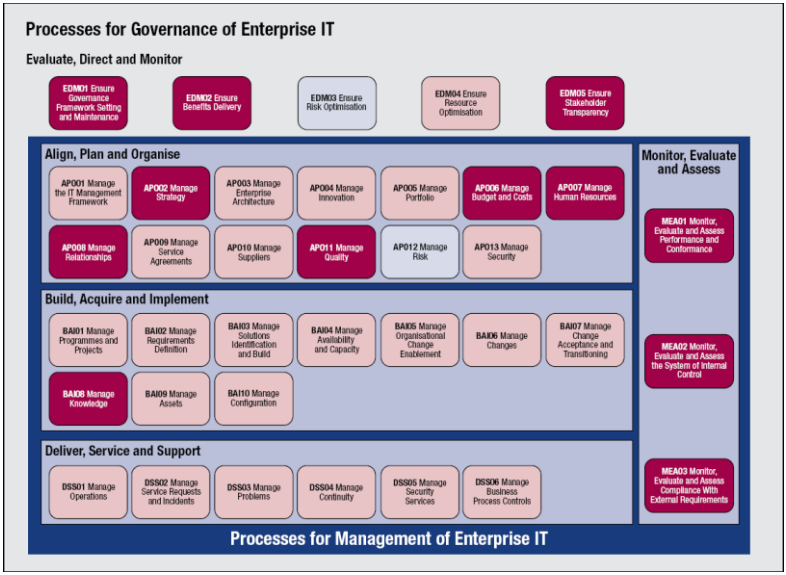
Pada COBIT 5 proses utama yang mendukung perspektif manajemen pada risiko adalah EDM03 *Ensure Risk Optimization* (Memastikan Optimalisasi Risiko) dan APO12 *Manage risk* (Pengelolaan Risiko). Berikut gambaran singkat dari kedua *control objectives* tersebut yang disajikan pada Tabel 2.3 [25].

Tabel 2. 3 Perspektif Manajemen Risiko berdasarkan *COBIT 5 for Risk*

Core Risk Processes	**Justifikasi**
EDM03 Memastikan Optimalisasi Risiko (*Ensure Risk Optimisation*)	Proses ini meliputi pemahaman, artikulasi, dan komunikasi dari *risk appetite* dan *risk tolerance* dan memastikan identifikasi dan manajemen risiko pada nilai perusahaan yang berkaitan dengan penggunaan Teknologi Informasi dan dampaknya. Tujuan dari proses ini adalah mendefinisikan dan mengkomunikasikan thresholds risiko dan memastikan mengetahui keterkaitannya dengan risiko TI. Selain itu, merupakan manajemen yang efektif dan efisien untuk mengelola risiko TI perusahaan
APO12 Pengelolaan Risiko (*Manage risk*)	Proses ini meliputi proses identifikasi yang berkelanjutan, penilaian dan pengurangan risiko TI dengan level toleransi yang ditentukan oleh Manajemen Eksekutif. Manajemen Risiko TI perusahaan harus diintegrasikan dengan ERM. Biaya dan manfaat manajemen risiko harus seimbang dengan mengumpulkan data yang sesuai dan menganalisis risiko, memelihara profil risiko perusahaan dan mengartikulasikan risiko, serta mendefinisikan tindakan manajemen dan merespon risiko.

2.2.11 Domain Kerangka Kerja COBIT 5

Kerangka kerja COBIT 5 terdiri dari 5 domain yang dibagi kedalam 37 proses.



Gambar 2. 3 Proses TI COBIT 5

Masing masing domain berorientasi kepada proses TI. Pada peneletian ini domain yang digunakan untuk menjadi acuan yaitu domain DSS yaitu proses DSS02 - *Manage Service Request and Incidents* terkait manajemen insiden dan permintaan layanan serta domain APO yaitu proses APO12 – *Manage risk* untuk mengidentifikasi dan menilai risiko berdasarkan aktivitas yang ada pada proses DSS02.

2.2.12 DSS02 – Manage Service Request and Incidents

Proses DSS02 (*Manage Service Request and Incidents*) merupakan proses yang berfokus untuk memastikan sebuah respon yang tepat waktu dan efektif pada permintaan pengguna dan resolusi dari semua jenis insiden. Kegiatan dari proses ini adalah memulihkan layanan normal, merekam dan memenuhi permintaan pengguna serta merekam, menyelidiki, mendiagnosa, meningkatkan dan menyelesaikan insiden. Proses DSS02 ini mempunyai 7 subproses, diantaranya [26]:

1. DSS02.01

Merupakan proses untuk mendefinisikan insiden dan layanan permintaan. Kegiatan yang dilakukan adalah mengatur eskalasi insiden dan prosedur, khususnya untuk insiden keamanan dan insiden besar.

2. DSS02.02
   Merupakan proses untuk merekam, mengklasifikasi dan memprioritaskan permintaan dan insiden. Kegiatan yang dilakukan adalah merekam log semua permintaan layanan dan insiden, lalu merekam informasi yang relevan sehingga dapat ditangani secara efektif.
3. DSS02.03
   Merupakan proses untuk memverifikasi, menyetujui dan memenuhi permintaan layanan. Kegiatan yang dilakukan adalah memilih prosedur permintaan yang tepat dan memverifikasi bahwa permintaan layanan memenuhi kriteria permintaan, serta perlu mendapatkan persetujuan jika diperlukan.
4. DSS02.04
   Merupakan proses untuk menyelidiki, mendiagnosa dan mengalokasikan insiden. Kegiatan yang dilakukan adalah mengidentifikasi gejala catatan kejadian, serta menentukan kemungkinan penyebab dan mengalokasikan untuk resolusi.
5. DSS02.05
   Merupakan proses untuk memulihkan dan mengatasi insiden. Kegiatan yang dilakukan adalah melakukan tindakan pemulihan untuk memulihkan TI terkait layanan permintaan dan insiden.
6. DSS02.06
   Merupakan proses untuk menutup permintaan layanan dan insiden. Kegiatan yang dilakukan adalah memverifikasi dengan user yang terkait bahwa permintaan layanan telah terpenuhi atau kejadian telah diselesaikan.
7. DSS02.07
   Merupakan proses untuk melacak status dan menghasilkan laporan. Aktivitas yang dilakukan adalah menganalisa dan melaporkan insiden dan permintaan pemenuhan layanan

untuk memberikan informasi untuk menjadi acuan perbaikan di masa mendatang.

2.2.13 APO12 – *Manage risk*

APO12 – *Manage risk* (mengelola risiko) merupakan salah satu Proses Teknologi Infomasi dalam kerangka kerja COBIT 5 pada domain APO *(Acquisition, Plan, and Organize).* Proses ini menyediakan langkah-langkah terstandar untuk melakukan manajemen risiko dimulai dari mengumpulkan data hingga melakukan mitigasi [14]. Terdapat 6 sub proses dari *APO12 Manage risk* yang didalamnya terdapat aktivitas di setiap sub proses tersebut yang dijadikan sebagai kerangka kerja. Berikut Tabel 2.4 menunjukkan Sub Proses dari APO12-*Manage risk*:

Tabel 2. 4 *Sub Proses APO12 COBIT 5*

Sub Proses	Justifikasi
APO12.01	Mengumpulkan Data
APO12.02	Menganalisis Risiko
APO12.03	Mengelola Profil Risiko
APO12.04	Mengartikulasi Risiko
APO12.05	Menetapkan Portfolio Tindakan Manajemen Risiko
APO12.06	Menanggapi Risiko

2.2.13.1APO12.01 Mengumpulkan Data

Mengidentifikasi dan mengumpulkan data yang relevan sehingga memungkinkan dapat dilakukan identifikasi, analisis, dan pelaporan risiko terkait TI yang efektif. Aktivitas pada APO12.01 adalah sebagai berikut [14]:

1. Menetapkan dan memelihara metode pengumpulan, klasifikasi dan analisis data terkait risiko TI, mengakomodasi berbagai jenis kejadian, mengategorikan risiko TI.
2. Mencatat data yang relevan pada internal perusahaan dan operasi lingkungan eksternal yang dapat berperan signifikan dalam mengelola risiko.
3. Melakukan survei dan analisis histori risiko TI, kehilangan data dan trend eksternal yang tersedia, melalui *event log*, *database*, dan perjanjian industri.

4. Mencatat data pada event risiko yang berdampak atau mungkin berdampak pada nilai/benefit IT, program TI dan *project delivery*, dan/atau operasi TI dan *service delivery*. Menangkap data yang relevan terkait isu, insiden, masalah dan investigasi.
5. Untuk *event* atau kelas yang mirip, atur data yang dikumpulkan dan perhatikan faktor yang memiliki pengaruh. Tentukan faktor yang berkontribusi umum terhadap beberapa *event.*
6. Untuk menentukan kondisi yang spesifik terhadap risiko. Ditentukan dengan menganalisis kondisi *event risk* yang dipengaruhi oleh frekuensi terjadinya risiko dan menentukan kerugian yang besar.
7. Analisis secara rutin dan berkala terhadap *risk event* yang bertujuan untuk mengidentifikasikan isu risiko baru, menyatukan pemahaman internal serta faktor risiko external.

2.2.13.2APO12.02 Menganalisis Risiko

Mengembangkan informasi yang berguna untuk mendukung keputusan risiko yang memperhitungkan relevansi bisnis dari faktor risiko. Aktivitas pada APO12.02 adalah sebagai berikut [14]:

1. Mendefinisikan cakupan dari analisis risiko baik dari segi luas dan kedalamannya. Mempertimbangkan semua faktor risiko dan aset *critical business*. Melakukan *cost benefit analysis* untuk menentukan *scope* analisis risiko
2. Membuat skenario risiko TI secara berkala, termasuk juga skenario yang terdiri dari *cascading* dan/atau tipe ancaman *confidental*. Dan membuat ekspektasi untuk kontrol aktivitas spesifik, kemampuan untuk mendeteksi dan ukuran respon lainnya.
3. Melakukan estimasi frekuensi, besarnya kerugian, dan keuntungan terkait skenario risiko TI. Menghitung semua faktor risiko, evaluasi kontrol operasional yang diketahui dan estimasi level risiko residual.

4. Membandingkan risiko residu dengan *risk tolerance yang* dapat diterima dan identifikasi gejala yang mungkin membutuhkan *risk response*.
5. Mengalisa *cost-benefit* dari potensi *risk response* seperti *avoid*, *reduce/mitigate*, *transfer/share*, dan *accept and exploit/seize*. Ajukan *risk response* yang paling optimal.
6. Spesifikasi *high-level requirements* untuk proyek atau program yang akan mengimplementasikan *risk response* yang telah dipilih. Identifikasi *requirements* dan ekspektasi untuk *key control* yang sesuai untuk respon mitigasi risiko.
7. Validasi hasil analisis risiko sebelum menggunakannya dalam pengambilan keputusan, konfirmasi bahwa analisis sesuai dengan kebutuhan perusahaan dan verifikasi bahwa estimasi telah terukur.

2.2.13.3APO12.03 Mengelola Profil Risiko

Memelihara semua hal yang berkaitan dengan risiko yang sudah diketahui termasuk frekuensi, dampak potensial, dan respon yang diharapkan. Tindakan ini memperhitungkan sumber daya, kemampuan dan aktivitas pengendalian yang dilakukan terkait risiko. Aktivitas pada APO12.03 adalah sebagai berikut [14]:

1. Menerapkan persediaan dalam proses bisnis seperti personil pendukung, aplikasi, infrastuktur, fasilitas, vendor, pemasok, outsource, dan mendokumentasikan ketergantungan pada proses manajemen layanan TI dan sumber daya infrastruktur TI.
2. Menentukan dan menyetujui layanan TI dan sumber daya infrastruktur TI untuk mempertahankan operasi proses bisnis. Menganalisa Ketergantungan dan mengidentifikasi hubungan yang lemah.
3. Membuat skenario risiko agregat menurut kategori, bidang usaha, dan bidang fungsional.
4. Mengambil semua informasi profil risiko secara teratur dan mengkonsolidasikan ke dalam profil risiko gabungan.

5. Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan dapat diidentifikasi serta pemantauan risiko dan tren risiko saat ini.
6. Mengambil informasi tentang kejadian risiko TI yang telah terjadi untuk dimasukkan dalam profil risiko TI perusahaan.
7. Mengumpulkan informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko TI perusahaan.

2.2.13.4APO12.04 Mengartikulasi Risiko

Memberikan informasi yang tepat mengenai kondisi dan peluang terkait TI terkini kepada semua *stakeholder* yang dibutuhkan untuk mendapatkan tanggapan yang tepat. Aktivitas pada APO12.04 adalah sebagai berikut [14]:

1. Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak. Laporan ini dibuat dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Kemudian menyertakan probabilitas dan rentang kerugian atau keuntungan seiring dengan tingkat kepercayaan yang memungkinkan manajemen untuk menyeimbangkan risiko kembali.
2. Menyediakan pembuat keputusan dengan pemahaman tentang skenario terburuk dan paling memungkinkan *(worst-case and most-probable)*, *diligence exposures*, dan reputasi yang signifikan, hukum, atau pertimbangan peraturan.
3. Melaporkan profil risiko saat ini kepada semua pemangku kepentingan, termasuk keefektifan proses manajemen risiko, efektivitas pengendalian, kesenjangan, inkonsistensi, redudansi, status remediasi, dan dampaknya terhadap profil risiko.
4. Review hasil dari objektif penilaian pihak ketiga, audit internal dan *review* penjaminan kualitas, dan memetakan ke dalam profil risiko. *Review* identifikasi *gaps* dan eksposur untuk menentukan kebutuhan analisis risiko tambahan.
5. Secara periodik, untuk area dengan risiko *relative* dan kapasitas paritas risiko, identifikasi berkaitan dengan peluang TI yang memungkinkan penerimaan risiko yang

lebih besar dan meningkatkan pertumbuhan dan kembalinya lebih baik.

2.2.13.5APO12.05 Menetapkan Portfolio Tindakan Manajemen Risiko

Mengelola peluang untuk mengurangi risiko kepada tingkat yang dapat diterima sebagai portofolio. Aktivitas pada APO12.05 adalah sebagai berikut [14]:

1. Mempertahankan kegiatan pengendalian yang ada untuk mengelola risiko dan memungkinkan risiko diambil sesuai dengan *risk appetite* and *tolerance.* Mengklasifikasikan kegiatan pengendalian dan merujuk ke pernyataan risiko TI spesifik dan agregasi risiko TI.
2. Menentukan apakah setiap entitas organisasi memonitor risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolio.
3. Memutuskan setiap proposal proyek untuk mengurangi risiko dan/atau proyek yang memiliki peluang enterprise strategis dengan mempertimbangkan manfaat/biaya, dampak pada profil risiko saat ini dan peraturan yang berlaku

2.2.13.6APO12.06 Menanggapi risiko

Menanggapi kejadian atau risiko secara tepat waktu dengan langkah-langkah efektif untuk membatasi besarnya kerugian dari kejadian terkait TI. Aktivitas pada APO12.06 adalah sebagai berikut [14]:

1. Menyiapkan, mempertahankan, dan menguji rencana dengan mendokumentasikan langkah-langkah spesifik yang harus diambil saat kejadian berisiko yang dapat menyebabkan kejadian operasional atau pembangunan yang signifikan dengan dampak bisnis yang serius. Kemudian memastikan bahwa rencana mencakup jalur eskalasi di seluruh perusahaan.
2. Mengkategorikan insiden dan membandingkan eksposur aktual dengan batas toleransi risiko. Mengkomunikasikan dampak bisnis kepada pengambil keputusan, dan memperbarui profil risiko.

3. Menerapkan rencana respons yang tepat untuk meminimalkan dampak saat insiden risiko terjadi.
4. Memeriksa kejadian di masa lalu yang dapat menimbulkan kerugian dan membuat hilangnya peluang, menentukan penyebabnya. Kemudian mengkomunikasikan penyebab tersebut, kebutuhan respon tambahan, persyaratan dan perbaikan proses kepada pengambil keputusan yang tepat dan memastikan bahwa penyebabnya, persyaratan respon dan perbaikan proses termasuk dalam proses tata kelola risiko.

2.2.14 Penilaian Risiko Berdasarkan COBIT 5 *for Risk*

Penilaian Risiko berdasarkan kerangka kerja COBIT 5 *for Risk* membutuhkan idenfikasi informasi terlebih dahulu terkait risiko seperti tipe risiko, kategori risiko, faktor risiko, skenario risiko, frekuensi dan dampak dari setiap risiko.

2.2.14.1Tipe Risiko

Risiko TI dapat dikategorikan menjadi tiga yaitu sebagai berikut [15]:

1. *IT Benefit/Value Enablement Risk*
   Terkait dengan hilangnya opportunity penggunaan teknologi bagi peningkatan efisiensi dan efektifitas proses bisnis atau sebagai *enabler* bagi inisiatif bisnis baru.
2. *IT Program and Project Deliver Risk*
   Terkait dengan kontribusi teknologi informasi bagi solusi bisnis baru atau memperbaiki solusi bisnis dalam bentuk proyek atau program.
3. *IT Operations and Service Delivery Risk*
   Terkait dengan seluruh aspek kinerja sistem dan layanan teknologi informasi yang dapat merusak atau mereduksi nilai organisasi atau perusahaan.

2.2.14.2Kategori Risiko

Berdasarkan kerangka kerja COBIT 5 *for Risk* terdapat 20 kategori untuk setiap risiko yang diidentifikasi pada Tabel 2.5 berikut [25]:

Tabel 2. 5 Pembagian Kategori Risiko

No	Kategori	Pengertian
1.	*Portfolio establishment and maintenance*	Risiko yang termasuk perencanaan, blueprint,maintenance
2.	*Programme/project lifecycle management*	Risiko yang termasuk manajemen siklus hidup program atau proyek
3.	*IT investment decision making*	Risiko yang terkait pengambilan keputusan investasi TI
4.	*IT expertise and skills*	Risiko yang terkait Keterampilan dan kemampuan TI
5.	*Staff operations*	Risiko yang terkait Staff operasional
6.	*Information*	Risiko yang terkait data dan informasi
7.	*Architecture*	Risiko yang terkait tujuan (visi) dan desain
8.	*Infrastucture*	Risiko yang terkait Infrastruktur
9.	*Software*	Risiko yang terkait Perangkat lunak
10.	*Business ownership of IT*	Risiko yang terkait bisnis TI
11.	*Selection/performance of third-party Supplier*	Risiko yang terkait Pemilihan/performa dari pemasok
12.	*Regulatory compliance*	Risiko yang terkait regulasi organisasi
13.	*Geopolitical*	Risiko yang terkait Geopolitik dan hukum
14.	*Insfrastructure theft or destruction*	Risiko yang terkait pencurian infrastruktur atau perusakan
15.	*Malware*	Risiko yang terkait *virus, worm, malware*
16.	*Logical attacks*	Risiko yang terkait Penyerangan logika
17.	*Industrial action*	Risiko yang terkait Aksi industri
18.	*Environmental*	Risiko yang terkait Lingkungan sekitar
19.	*Acts of Nature*	Risiko terkait Bencana alam
20.	*Innovation*	Risiko terkait Inovasi

2.2.14.3Faktor Risiko

Faktor risiko merupakan kondisi yang mempengaruhi frekuensi dan/atau dampak bisnis dari skenario risiko yang dapat dibedakan dalam dua kategori utama yaitu [25]:

1. Faktor Konstektual

   Faktor konsteksual membedakan risiko berdasarkan tingkat control dari perusahaan yang terbagi menjadi:

   a. Faktor Konstektual Internal

Faktor yang diberlakukan untuk risiko yang berada dibawah kendali perusahaan, meskipun organisasi tidak selalu mudah untuk berubah. Beberapa faktor risiko internal yaitu sasaran dan tujuan perusahaan, kepentingan strategis dari bisnis TI, kompleksitas TI, kompleksitas entitas dan tingkat perubahan, kemampuan manajemen perubahan, model operasional, prioritas strategi, budaya perusahaan, kapasitas finansial.

b. Faktor Konstektual Eksternal
Faktor yang diberlakukan untuk risiko yang berada diluar kendali perusahaan. Beberapa faktor risiko eksternal yaitu faktor pasar dan ekonomi, tingkat perubahan pada siklus hidup produk, industry dan kompetisi, situasi geopolitik, lingkungan regulasi, status dan evolusi teknologi, bentangan ancaman.

2. Kemampuan
Kemampuan seberapa efisien dan efektif perusahaan dinilai dari jumlah aktivitas yang terkait teknologi informasi yang dibedakan menjadi:
   a. Kemampuan manajemen risiko TI
   Mengindikasikan seberapa matang perusahaan dalam melakukan manajemen proses TI. Beberapa faktor kemampuan manajemen risiko TI yaitu tatakelola risiko dan manajemen risiko.
   b. Kemampuan terkait TI
   Mengindikasikan kemampuan *enabler* COBIT 5 terkait TI. Beberapa faktor kemampuan terkait TI yaitu:
   - *Evaluate, direct, and monitor (EDM)*
   - *Align, plan, and organize (APO)*
   - *Build, acquire, and implement (BAI)*
   - *Deliver, service, and support (DSS)*
   - *Monitor, evaluate, and assess (MEA)*

2.2.14.4Skenario Risiko

Skenario risiko TI adalah deskripsi dari kejadian terkait TI yang dapat menimbulkan dampak bisnis ketika atau jika risiko terjadi. Skenario risiko mendeskripsikan kejadian yang

ketika terjadi akan mempunyai dampak yang tidak pasti terhadap pencapaian tujuan perusahaan. Dampak tersebut bisa saja positif atau negatif, sehingga pembuatan skenario risiko terbagi menjadi dua jenis, yaitu skenario positif dan skenario negatif. Skenario risiko merupakan salah satu elemen kunci dari manajemen risiko COBIT 5. Terdapat 2 pendekatan untuk membuat skenario risiko, yaitu [25]:

1. *Top Down*
   Berikut adalah langkah-langkah untuk pendekatan Top-Down:
   a. Mengidentifikasi tujuan bisnis.
   b. Mengidentifikasi risiko TI yang mempunyai dampak terbesar terhadap pencapaian tujan bisnis.
2. *Bottom Up*
   Berikut adalah langkah-langkah untuk pendekatan Bottom-Up:
   a. Mengidentifikasi semua skenario yang ada.
   b. Mengurangi skenario-skenario yang telah teridentifikasi melalui analisis tingkat tinggi.

2.2.14.5Pemetaan Risiko

Risiko yang telah diidentifikasi dapat dipetakan dengan proses yang ada pada COBIT 5 *Enabling Process* sesuai tipe, faktor dan skenario risiko tersebut

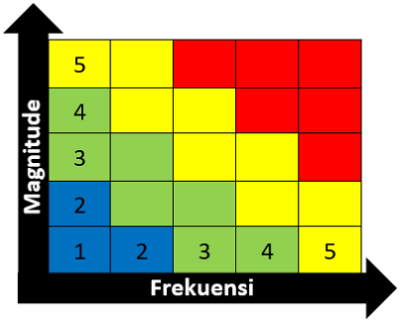
2.2.14.6Level Penilaian Risiko

Berdasarkan kerangka kerja COBIT 5 *for Risk*, penilaian risiko terbagi menjadi dua aspek, yaitu[25]:

1. Aspek Frekuensi
   Penilaian risiko dengan peringkat dan parameter yang dapat disesuaikan dengan konteks organisasi.
2. Aspek Dampak
   Penilaian risiko yang dibagi berdasarkan empat jenis dampak, yaitu:
   a. Produktivitas, penilaian dilihat dari dampak kerugian finansial dari organisasi selama periode tertentu.
   b. Biaya Respon, penilaian dari sisi biaya yang dikeluarkan untuk setiap risiko yang terjadi.

c. Keunggulan Kompetitif, penilaian diukur dari sisi penurunan kepuasan pengguna layanan akibat terjadinya skenario risiko
d. Hukum, penilaian diukur dari biaya denda yang ditanggung akibat terjadinya risiko terkait hokum

Level penilaian risiko didapatkan berdasarkan pemetaan frekuensi dan magnitude dalam matriks warna seperti pada Gambar 2.4.



Gambar 2. 4 Peta Frekuensi dan Magnitude Risiko

Pemetaan tersebut lalu diklasifikasikan dalam tingkatan prioritas seperti pada Gambar 2.5 berikut untuk menentukan tindakan lanjutan terhadap risiko

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

Gambar 2. 5 Level Prioritas Risiko

2.2.15 Mitigasi Risiko

Manajemen risiko memiliki sifar proaktif dalam mengelola dan mengantisipasi risiko sebelum terjadi. Risiko terbagi menjadi dua yaitu positif dan negatif. Risiko negatif dapat membahayakan tujuan proyek, sedangkan risiko positif dapat memberikan dampak positif terhadap proyek. Mitigasi risiko merupakan implementasi sejumlah kontrol IT untuk

mengatasi skenario risiko yang terjadi. Kontrol IT berperan sebagai *enabler* yang disediakan oleh COBIT 5 untuk merespon skenario risiko.

Berikut merupakan respon untuk melakukan mitigasi negatif menurut COBIT 5 [25]:

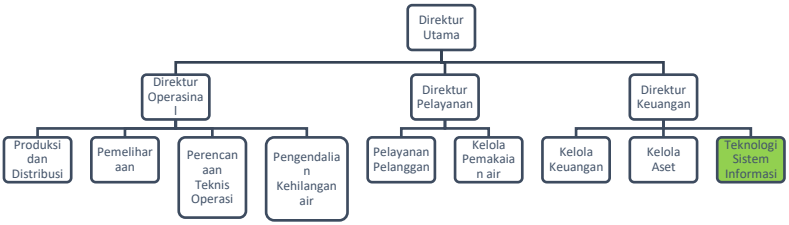
1. *Acceptance*
   Menerima risiko yang sudah diketahui dan tidak dapat dicegah, sehingga perusahaan menerima kerugian, manfaat, atau keuntungan yang mungkin dihasilkan risiko.
2. *Sharing/Transfer*
   Mengalihkan risiko yang sulit untuk ditangani sendiri ke pihak lain.
3. *Avoidance*
   Menghindari risiko yang terlalu besar dengan menhentikan proses dan aktivitas terkait risiko tersebut.
4. *Mitigation*
   Menerapkan kontrol yang sesuai untuk risiko agar mencapai biaya yang efektif.

Berikut merupakan respon untuk melakukan mitigasi positif menurut COBIT 5 [25]:

1. *Exploit*
   Mengeliminasi ketidakpastian dengan memastikan peluang terjadinya risiko.
2. *Enchance*
   Mengalihkan risiko yang sulit untuk ditangani sendiri ke pihak lain.
3. *Share*
   Meningkatkan peluang dengan melibatkan pihak ketiga yang berpotensi untuk menangani, memaksimalkan kemungkinan, meningkatkan manfaat saat risiko terjadi.
4. *Ignore*
   Mengabaikannya peluang terjadinya risiko.

2.2.16 Struktur Organisasi PDAM Kota Surabaya

Struktur Organisasi pada PDAM Kota Surabaya terdapat pada gambar 2.6.



Gambar 2. 6 Struktur Organisasi PDAM Kota Surabaya

Bagian Teknologi Sistem Informasi (TSI) PDAM Surabaya yang dibawahi oleh Direktur Keuangan diberikan tanggung jawab dalam hal pelayanan teknologi informasi perusahaan. Salah satu tanggung jawab dan tugas TSI adalah melayani setiap karyawan di perusahaan mengenai permasalahan di bidang Komputer dan jaringan [27]. Layanan tersebut disebut *service desk* atau *helpdesk.*

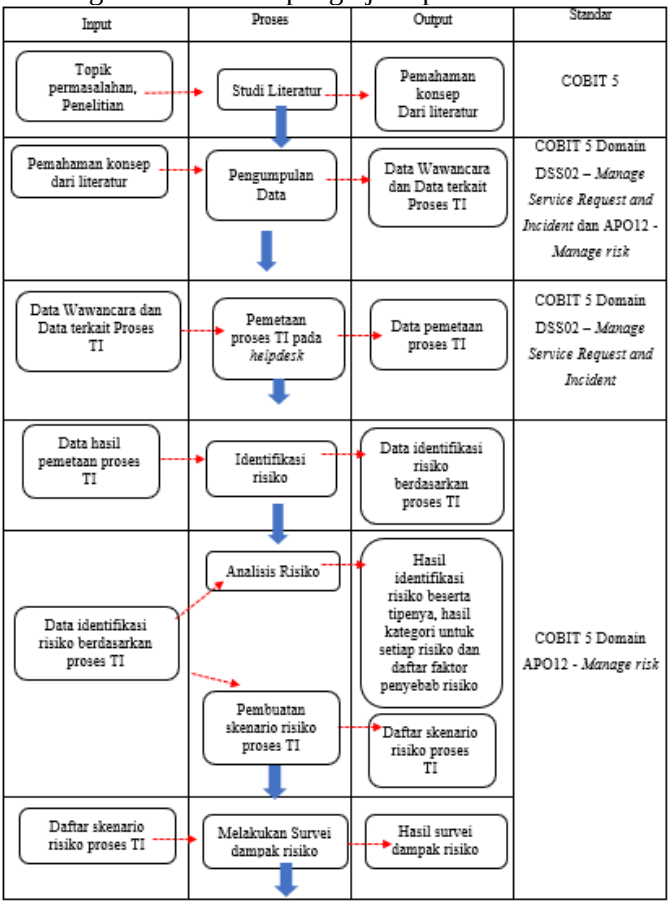
Halaman ini sengaja dikosongkan

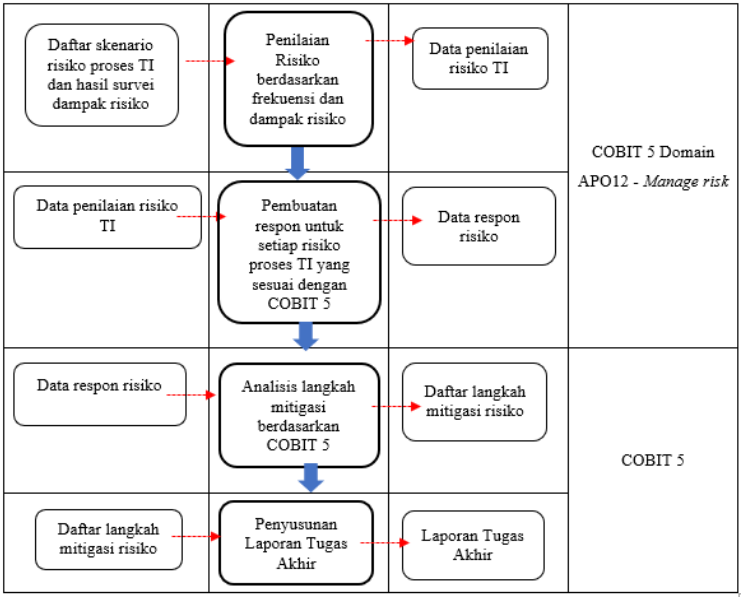
BAB III
METODOLOGI

Untuk mendapatkan hasil yang baik, maka diperlukan langkah-langkah penelitian yang tepat dan runtun. Pada bagian ini akan diuraikan langkah-langkah penelitian yang akan dilakukan oleh peneliti dalam memecahkan permasalahan sehingga penelitian ini dapat diselesaikan dengan baik.

3.1 Diagram Metodologi

Gambar 3.1 merupakan diagram metodologi yang digunakan sebagai acuan dalam pengerjaan penelitian ini.





Gambar 3. 1 Diagram Balok Metodologi

3.1.1 Studi Literatur

Pada tahapan ini dilakukan pengkajian mengenai penelitian yang membahas Manajemen risiko dengan kerangka kerja terstandar COBIT 5 *Enabling Process* dan COBIT 5 *for Risk*. Pustaka yang digunakan yaitu paper, jurnal, dan laporan penelitian.

3.1.2 Pengumpulan Data

Setelah mendapatkan permasalahan dan mengetahui konsep dan kerangka kerja yang di dapat untuk menyelesaikan permasalahan. Selanjutnya dilakukan pengumpulan data yang berkaitan dengan risiko proses teknologi informasi pada *helpdesk* unit TSI PDAM Surabaya dengan melakukan studi dokumen terkait tugas pokok dan fungsi *helpdesk*, observasi dengan melihat kondisi yang sedang berlangsung di ruang kerja *helpdesk* dan wawancara untuk mengidentifikasi permasalahan yang ada, kondisi saat ini dan mengetahui hal – hal yang dibutuhkan untuk melakukan penanganan terkait risiko yang

ada dan akan muncul. Pihak yang akan menjadi narasumber untuk wawancara adalah manajer dan staff unit *helpdesk* unit TSI PDAM Surabaya. Data yang didapatkan adalah data dan informasi terkait proses TI *helpdesk* unit TSI.

3.1.3 Pemetaan Proses TI pada *Helpdesk* dengan COBIT 5

Data yang didapatkan tentunya tidak semuanya seperti yang diinginkan. Oleh karena itu, dibutuhkan pemetaan proses TI pada *helpdesk* untuk memudahkan proses identifikasi risiko. Pemetaan dilakukan dengan memetakan proses pengelolaan permintaan layanan dan insiden pada *helpdesk* unit TSI PDAM untuk dapat mengetahui apakah proses yang dilakukan sudah sesuai dengan *best practice* dari COBIT 5 DSS02 *Manage Service Request and Incidents*.

3.1.4 Identifikasi Risiko

Setelah melakukan pemetaan proses TI *helpdesk* terkait pengelolaan permintaan layanan dan insiden, selanjutnya akan dapat diidentifikasi risiko-risiko apa yang dapat terjadi sesuai per aktivitas yang mengacu kepada kondisi ideal di COBIT 5 sehingga identifikasi risiko juga dilakukan pada Proses TI yang ada pada DSS02 COBIT 5 yang tidak dilakukan di *helpdesk* PDAM Kota Surabaya.

3.1.5 Analisis Risiko

Analisis risiko dilakukan menggunakan domain APO12 *Manage Risk*. Risiko yang sudah diidentifikasi kemudian diolah dalam pembuatan tabel pemetaan risiko dengan tipe risiko yang sesuai. Tipe risiko dapat dimasukan ke dalam tiga kategori, yaitu risiko yang masuk ke manfaat atau nilai risiko TI, operasional dan layanan risiko TI, atau program dan proyek risiko TI.

Setelah membuat daftar risiko berdasarkan tipe risikonya, selanjutnya mengkategorisasikan setiap risiko yang ada untuk memudahkan proses dalam mengidentifikasi risiko. Dibuat tabel hasil identifikasi kategori risiko untuk setiap risiko.

Risiko dikategorikan berdasarkan dua puluh kategori yang ada pada standar COBIT 5 *for Risk*.

Mengacu pada daftar faktor risiko kontekstual pada standar COBIT 5 *for Risk* masing-masing risiko yang sudah diidentifikasi ditentukan faktor-faktor penyebabnya, baik dari faktor internal maupun faktor eksternal. Setelah mengetahui penyebab masing- masing risiko proses TI pada *helpdesk* TSI PDAM dibuatlah tabel faktor penyebab risiko.

Tahap ini memiliki keluaran berupa *risk event* yang merupakan gabungan dari tabel analisis tipe risiko, kategori risiko dan faktor penyebab risiko.

3.1.6 Pembuatan Skenario Risiko Proses TI

Pada tahap ini dilakukan pengelolaan lebih lanjut terhadap daftar risiko yang telah diidentifikasi berdasarkan tipe, kategori dan penyebab, yang telah dipetakan untuk dibuatkan daftar skenario risiko. Pembuatan skenario risiko TI untuk setiap risiko. Skenario risiko dapat dibagi menjadi dua jenis, yaitu jika skenario tersebut memiliki dampak yang baik bagi proses bisnis (skenario positif) dan skenario yang memeiliki dampak yang buruk bagi proses bisnis (skenario negatif).

Langkah-langkah yang dilakukan dalam pembuatan skenario risiko TI adalah:

1. Memperkirakan risiko TI meliputi frekuensi terjadi, besarnya kerugian, dan keuntungan yang dipengaruhi oleh beberapa faktor risiko
2. Memperkirakan jumlah maksimum kerusakan yang terjadi atau keuntungan yang bisa didapatkan
3. Mempertimbangkan jenis-jenis ancaman yang mungkin terjadi
4. Pada skenario risiko TI yang paling penting, lakukan kontrol tertentu. Pada tahap ini kemampuan untuk mendeteksi dan tindakan respon lainnya sangat penting
5. Melakukan evaluasi kontrol dengan mempertimbangkan frekuensi terjadi, besarnya kerugian atau keuntungan

6. Memperkirakan risiko residual dan membandingkannya terhadap risiko yang dapat diterima untuk mengidentifikasi risiko yang mungkin memerlukan respon risiko

Keluaran yang dihasilkan pada tahap ini adalah daftar skenario (dampak) risiko proses TI.

3.1.7 Melakukan Survei Dampak Risiko

Pada tahap ini dilakukan survei dengan mengambil sampel pegawai yang merupakan pengguna layanan unit *helpdesk* unit TSI untuk mengetahui nilai dari dampak risiko terhadap tingkat penurunan kepuasan pengguna dilakukan survei melalui kuisioner. Untuk itu sebelum dilakukan penilaian risiko, dilakukan terlebih dahulu survei untuk mengukur indeks penurunan kepuasan pelanggan,

3.1.8 Penilaian Risiko berdasarkan Frekuensi dan Dampak Risiko

Pada tahap ini dilakukan perhitungan perkiraan frekuensi, besarnya kerugian atau keuntungan yang mungkin didapatkan yang terkait skenario risiko TI dengan memperhitungkan semua faktor risiko. Penentuan nilai frekuensi risiko didapatkan dari hasil wawancara. Besarnya kerugian atau keuntungan yang didapatkan dibedakan menjadi empat menurut COBIT 5 yaitu:

1. Produktivitas, yaitu seberapa besar kerugian atau keuntungan yang dialami organisasi karena risiko.
2. Biaya tanggapan, yaitu besarnya biaya yang dikeluarkan untuk menangani risiko
3. Keunggulan kompetitif, yaitu penurunan kepuasan pelanggan terhadap layanan sistem akibat terjadinya skenario risiko
4. Hukum, yaitu seberapa besar denda yang harus dibayar organisasi dari risiko yang melanggar hukum dan regulasi

Penentuan nilai dampak risiko yaitu keunggulan kompetetif didapatkan dari hasil survei sedangkan penentuan nilai aspek produktivitas, biaya tanggapan dan hukum didapatkan dari hasil wawancara. Perhitungan besarnya keuntungan atau kerugian nantinya akan dihitung dan masing-

masing risiko dikategorisasikan berdasarkan levelnya, yaitu *low risk, medium risk, high risk* dan *very high risk.*

3.1.9 Pembuatan Respon untuk setiap Risiko Proses TI yang sesuai dengan COBIT 5

Setelah mengetahui level risiko, maka dapat dibuat cara penanganan untuk setap risiko yang ada dan diambil yang paling optimal yang dapat dilakukan oleh perusahaan. Berdasarkan COBIT 5 terdapat 4 *risk response* yaitu *avoid* atau risiko yang dapat dihindari, *accept* atau risiko diambil dan diterima oleh perusahaan, *transfer* atau mentransfer risiko ke pihak ketiga, dan *mitigate* atau membuat langkah mitigasi risiko.

3.1.10 Analisis Langkah Mitigasi Risiko berdasarkan COBIT 5

Untuk melakukan analisis langkah mitigasi risiko sebelumnya dilakukan dulu pemetaan risiko berdasarkan tabel respon risiko untuk setiap proses TI, Setelah dilakukan pemetaan risiko dengan ditunjukkan tabel respon risiko untuk setiap proses TI, maka dilakukan analisis langkah mitigasi risiko sesuai dengan respon risiko untuk setiap proses TI berdasarkan aktivitas *key management practices* pada COBIT 5 yang relevan untuk diimplementasikan di perusahaan. Selain itu, langkah mitigasi risiko juga harus mempertimbangkan kemampuan perusahaan dalam melakukan mitigasi risiko.

3.1.11 Penyusunan Laporan Tugas Akhir

Seluruh pelaksanaan ataupun pengerjaan penelitian ini akan didokumentasikan dengan mengikuti format yang berlaku di Jurusan Sistem Informasi ITS.

Di dalam laporan Tugas Akhir akan mencakup :

1. BAB I Pendahuluan
   Pada bab ini akan dijelaskan mulai dari latar belakang, rumusan permasalahan, batasan permasalahan, tujuan dan manfaat pengerjaan penelitian.
2. BAB II Tinjauan Pustaka

Pada bab ini akan dijelaskan mengenai penelitian-penelitian sebelumnya yang telah dilakukan serta teori-teori yang menunjang permasalahan yang dibahas pada penelitian ini

3. BAB III Metodologi
   Pada bab ini akan dijelaskan alur proses dari pengerjaan penelitian mulai dari identifikasi permasalahan sampai pembuatan laporan tugas akhir.
4. BAB IV Perancangan
   Pada bab ini akan dijelaskan mengenai perancangan pengerjaan penegerjaan tugas akhir. Perancangan yang dibuat meliputi perancangan studi kasus dan perancangan terkait hal-hal yang akan dilakukan untuk mengerjakan tugas akhir
5. BAB V Implementasi
   Bab ini berisi tentang implementasi dan penjelasan setiap alur proses yang telah dijabarkan sebelumnya pada metodologi yang digunakan dalam penelitian.
6. BAB VI Hasil dan Pembahasan
   Bab ini berisi analisis dan pembahasan daam penyelesaian permasalahan yang dibahas pada pengerjaan penelitian.
7. BAB VII Kesimpulan dan Saran
   Bab ini berisi kesimpulan dan saran yang ditujukan untuk kelengkapan penyempurnaan penelitian ini.

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Pada bab ini akan dijelaskan mengenai pengumpulan data, metode pengolahan data, dan perancangan terhadap hal-hal yang terkait dengan pengerjaan tugas akhir yang digunakan dalam penilaian risiko di PDAM kota Surabaya.

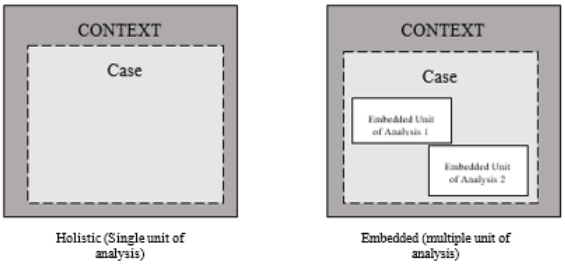
4.1 Perancangan Studi Kasus

Pada bagian ini dilakukan perancangan studi kasus untuk menjelaskan dari studi kasus yang dipilih dan tipe *unit of analysis* yang digunakan.

4.1.1 Tujuan Studi Kasus

Penelitian pada tugas akhir ini bertujuan untuk melakukan penilaian risiko berdasarkan identifikasi risiko terkait proses TI pada *helpdesk* unit TSI PDAM Surabaya menggunakan kerangka kerja COBIT 5. Untuk mencapai tujuan tersebut dalam penelitian tugas akhir ini menggunakan metode wawancara, observasi dan pengkajian dokumen dalam proses penggalian data.

Studi kasus dapat dibagi menjadi dua, yaitu berfokus pada satu kasus (*single-case design*) dan berbagai kasus (*multiple-case design*). Perancangan studi kasus yang digunakan dalam penelitian tugas akhir ini adalah *single-case* design, dimana perancangan single-case design dapat dibagi kedalam dua tipe, yaitu *single unit of analysis* dan *multiple unit of analysis*. Yang ditunjukan pada gambar 4.1.



Gambar 4. 1 Tipe Studi Kasus *Single-Case Design*

Penggunan *single unit of analysis* menghasilkan pemahaman yang lebih dalam untuk subjek yang dianalisis.

Sedangkan multiple unit of analysis menghasilkan bukti yang lebih kuat dengan melakukan perbandingan antara perbedaan dan persamaan antara setiap subjek [28].

Tugas akhir ini menggunakan studi kasus dengan *single unit of analysis*. *Unit of analysis* dalam tugas akhir ini adalah melakukan penilaian risiko terhadap proses TI pada *helpdesk* unit Teknologi Sistem informasi PDAM Surabaya.

4.1.2 *Unit of Analysis*

Unit of analysis yang digunakan oleh penelitian ini adalah identifikasi dan penilaian risiko proses TI yang berada pada proses bisnis *helpdesk* yang berfokus pada manajemen insiden dan pemenuhan permintaan layanan TI di PDAM Surabaya.

4.2 Persiapan Pengumpulan Data

Pada bagian ini dilakukan persiapan pengumpulan data yang dibutuhkan termasuk narasumber yang akan diwawancarai, metode yang digunakan dan uraian rancangan pertanyaan yang akan digunakan dalam wawancara. Pengumpulan informasi terkait PDAM Surabaya akan dilakukan dengan wawancara dengan narasumber terkait.

Wawancara dilakukan dengan narasumber manajer unit Teknologi Sistem Informasi PDAM Surabaya serta staff *helpdesk* unit TSI PDAM. Sedangkan untuk pengkajian dokumen dilakukan pada dokumen yang memiliki informasi terkait manajemen insiden dan pemenuhan permintaaan layanan yang dapat diperoleh dari staff dan unit TSI PDAM Surabaya.

4.3 Pengumpulan Data

Pada bagian ini dilakukan proses pengumpulan data yang dibutuhkan pada penelitian tugas akhir ini. Metode yang dilakukan dalam mengumpulkan data yang dibutuhkan adalah dengan wawancara dengan narasumber terkait, melakukan pengkajian dokumen, serta melakukan survei untuk

menentukan dampak risiko. Tujuan dalam proses pengumpulan data dalam penelitian ini antara lain sebagai berikut:

Tabel 4. 1 Perancangan Metode Tujuan Pengumpulan data

No	Tujuan	Metode
1.	Mengetahui gambaran Struktur Organisasi unit TSI, seperti tupoksi, peran dan tanggung jawab dari unit TSI PDAM Surabaya	Wawancara, Studi Dokumen
2.	Mengidentifikasi insiden dan permintaan layanan	Wawancara, Observasi dan Studi Dokumen
3.	Mengetahui Kondisi kekinian dan kondisi yang diharapkan oleh *helpdesk* unit TSI PDAM Surabaya terkait risiko pada manajemen risiko dan pemenuhan permintaan layanan	Wawancara, Observasi dan Studi Dokumen
4.	Mengetahui risiko yang sering muncul terkait pengelolaan insiden dan pemenuhan permintaan layanan	Wawancara, Studi Dokumen

4.3.1 Wawancara

Wawancara dilakukan untuk mendapatkan informasi langsung dari narasumber. Teknik wawancara yang digunakan ialah wawancara semi terstruktur.

Wawancara yang dilakukan bertujuan untuk memahami proses bisnis yang ada pada *helpdesk* unit Teknologi Sistem Informasi PDAM Surabaya. Dimana narasumber yang berperan atau terlibat langsung dalam proses bisnis *helpdesk* yang akan diwawancarai.

4.3.1.1 Tujuan Wawancara

Wawancara ditujukan kepada *helpdesk* unit Teknologi Sistem Informasi PDAM Surabaya dan dilakukan dengan menggunakan daftar pertanyaan (*interview protocol*). Berikut tujuan wawancara ditampilkan pada Tabel 4.2.

Tabel 4. 2 Tujuan Wawancara

Tujuan Wawancara	Narasumber
• Mengetahui gambaran Struktur Organisasi unit TSI, seperti tupoksi, peran dan tanggung jawab dari unit TSI PDAM Surabaya • Mengetahui proses bisnis yang ada pada *helpdesk* • Mengetahui layanan yang ditangani oleh *helpdesk* • Mengetahui standar acuan yang digunakan oleh *helpdesk* dalam melakukan proses manajemen insiden dan pemenuhan permintaan layanan. • Mengetahui kondisi kekinian dari proses manajemen insiden dan pemenuhan permintaan layanan TI. • Mengetahui risiko yang pernah terjadi di unit TSI. • Mengetahui kondisi sistem informasi *helpdesk* unit TSI. • Mengetahui kesalahan yang sering terjadi pada *helpdesk* saat mengelola insiden dan pemenuhan permintaan layanan • Risiko yang sering muncul dari proses manajemen insiden dan pemenuhan permintaan layanan	Staff *helpdesk* unit Teknologi Sistem Informasi PDAM Surabaya
• Mengetahui kondisi kekinian dari pengelolaan risiko di organisasi • Mengetahui dampak risiko pada proses bisnis sehari-hari organisasi • Mengetahui rencana atau strategi penanganan risiko	Manajer unit Teknologi Sistem Informasi PDAM Surabaya

4.3.1.2 Perancangan *Interview protocol*

Perancangan *interview protocol* adalah perancangan daftar pertanyaan yang akan digunakan agar proses wawancara menjadi tidak bias dan terarah. Dimana *interview protocol* akan digunakan untuk menggali kondisi kekinian organisasi terkait risiko pada *helpdesk* saat mengelola insiden dan pemenuhan permintaan layanan di PDAM Surabaya. Perancangan awal untuk interview procol yaitu mencantumkan informasi terkait

narasumber dan pelaksanaan interview, setelah itu dilanjutkan dengan perancangan daftar pertanyaan dalam *interview protocol*. Berikut isi dari pelaksanaan wawancara dan narasumber yang ditampilkan pada Tabel 4.3.

Tabel 4. 3 Perancangan Narasumber Wawancara

Interview protocol	
Tanggal	10 Maret 2019
Tujuan	Mengetahui kondisi kekinian dari proses bisnis *helpdesk* unit TSI PDAM kota Surabaya
Tempat	PDAM Kota Surabaya
Narasumber	Ari Bimo Sakti
Jabatan	Manajer Unit TSI PDAM Surabaya.

Instrument wawancara pada *interview protocol* dirancang dengan beberapa pertanyaan yang didasarkan pada proses DSS02 Manage Service Requests and Incidents terkait manajemen insiden dan permintaan layanan dan proses APO12 Manage Risks terkait manajemen risiko. interviewer akan mebacakan *interview protocol* kepada narasumber atau ditampilkan ketika wawancara. Interviewer akan mencatat dan merekap respon dari narasumber pada *interview protocol* yang ditampilkan pada Tabel 4.4.

Tabel 4. 4 Perancangan *Interview protocol*

Kategori	**Sasaran: Pengelolaan Manajemen Insiden dan Proses Pemenuhan layanan TI**
Merekam, mengklasifikasikan dan memprioritaskan permintaan dan insiden	Pertanyaan: Bagaimana insiden dan permintaan layanan dicatat?
	Jawaban:

Narasumber ditentukan untuk memudahkan proses dalam melakukan pengumpulan data melalui wawancara. Dalamm menentukan narasumber harus memperhatikan kewenangan dan kapasitas narasumber serta informasi yang

diberikan valid, dan pertanyaan yang relevan dengan narasumber terkait. Berikut narasumber dalam penelitian yang ditampilkan pada Tabel 4.5.

Tabel 4. 5 Narasumber Penelitian

No	Nama	Jabatan
1.	Ari Bimo Sakti	Manajer unit Teknologi Sistem Informasi PDAM kota Surabaya
2.	Alfil Hidayat	Staff *helpdesk* unit Teknologi Sistem Informasi PDAM kota Surabaya
3.	Fitri Qonita	Staff *helpdesk* unit Teknologi Sistem Informasi PDAM kota Surabaya

Setelah melakukan wawancara kepada narasumber yang ada di unit TSI PDAM Surabaya dapat diketahui kondisi kekinian dan kondisi yang diharapkan oleh *helpdesk* unit TSI terkait risiko pada manajemen insiden dan pemenuhan permintaan layanan.

4.3.2 Observasi

Wawancara dilakukan untuk mendapatkan informasi langsung dari narasumber. Teknik wawancara yang digunakan ialah wawancara semi terstruktur. Metode ini dilakukan dengan melakukan pengamatan langsung pada unit Teknologi Sistem Informasi PDAM kota Surabaya. Observasi yang dilakukan bertujuan untuk mendapatkan informasi mengenai kondisi yang nyata yang terjadi dalam proses bisnis *helpdesk* dan informasi tambahan yang dapat dijadikan penunjang dalam penelitian tugas akhir ini. Hasil yang diharapkan dari observasi ini adalah aktivitas-aktivitas dalam DSS02 Manage Service Requests and Incidents terkait manajemen insiden dan permintaan layanan yang sudah dilakukan oleh *helpdesk* unit TSI kota Surabaya.

4.3.3 Pengkajian Dokumen

Pengkajian dokumen adalah metode yang digunakan untuk mendukung informasi yang telah dan belum didapatkan dari hasil wawancara ataupun observasi. Indormasi yang tekait kondisi kekinian *helpdesk* unit TSI PDAM Surabaya seperti struktur organisasi, tupoksi, log aktivitas dan kebijakan terkait dengan manajemen insiden dan pemenuhan permintaan layanan baik dalam bentuk dokumen fisik maupun digital. Pengkajian dokumen juga dapat dijadikan bukti dari wawancara dan observasi yang telah dilakukan.

4.3.4 Survei

Survei melalui kuesioner dilakukan untuk menghitung penurunan kepuasan pelanggan yang merupakan salah satu dampak risiko (magnitude) yaitu competitive advantage. Penurunan kepuasan pelanggan dapat diukur dengan pengisian kuisioner dengan mengambil sampel pegawai yang merupakan pengguna layanan *helpdesk* unit Teknologi Sistem Informasi PDAM Surabaya. Jumlah pegawai di lingkungan PDAM kota Surabaya cukup besar sehingga ruang lingkup dari populasi akan di spesifikasikan untuk pengguna layanan TI dari seluruh pegawai PDAM Surabya yaitu sekitar 1039 Orang. Selanjutnya jumlah populasi ini akan dihitung dengan menggunakan metode slovin, yaitu metode untuk mencari jumlah sampel responden minimal. Berikut merupakan rumus Slovin [28]:

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

Keterangan:
n = Ukuran Sampel.
N = Jumlah Sampel
e = Presentasi Toleransi Kesalahan
sehingga diperoleh

$$n= \frac{1039}{1+1039(0.1)^2}$$

$$n= \frac{1039}{1+10.39}$$

n= 92 orang

Berdasarkan perhitungan tersebut, dengan nilai e = 10% didapatkan sebanyak 92 Orang yang akan menjadi sampel dari populasi sebanyak 1039 Orang. Dalam tahapan ini akan digunakan metode simple random sampling, dimana data yang akan dihasilkan dari kuisioner didapatkan dari 92 responden tersebut.

4.4 Pengolahan Data

Pengolahan data hasil wawancara akan dilakukan dengan mendokumentasikan dengan hasil wawancara interviewer dengan narasumber dengan menggunakan Microsoft Word. Hasil wawancara dengan narasumber dimasukan kedalam tabel hasil wawancara dengan menyusun kalimat agar kalimat menjadi narasi yang dapat lebih mudah dipahami. Kemudian, untuk penilaian risiko aspek frekuensi dan dampak akan dilakukan prioritasi berdasarkan hasil wawancara yang didapat dan survei yang dilakukan. Tools yang akan digunakan ialah Microsoft excel untuk memudahkan dalam perhitungan rata-rata nilai risiko dan pendokumentasian dalam bentuk tabel.

4.5 Analisis Data

Pendekatan analisis dilakukan untuk mengetahui hubungan antara pendekatan yang dilakukan dalam pengerjaan penelitian ini dengan data yang didapat. Analisis yang dilakukan adalah sebagai berikut:

1. Analisis Tugas pokok dan fungsi unit TSI PDAM Surabaya dengan kondisi kekinian dalam proses TI yang ada pada *helpdesk*. Proses ini akan disesuaikan dengan COBIT 5 DSS02 *Manage Service Requests and Incidents* terkait manajemen insiden untuk mengetahui bagaimana proses bisnis yang ada pada *helpdesk* mulai dari awal sampai tahap akhir penutupan proses.
2. Analisis risiko berdasarkan COBIT 5 *for Risk* untuk mengidentidikasi risiko yang mungkin terjadi pada proses manajemen insiden dan permintaan layanan

3. Analisis penilaian risiko berdasarkan COBIT 5 *for Risk* APO12 untuk mengetahui level risiko berdasarkan asper frekuensi dan dampak risiko.
4. Analisis mitigasi risiko untuk mengetahui cara penanganan risiko yang sesuai dengan standar COBIT 5.

4.6 Penilaian Risiko

Penilaian risiko dibuat dengan mengacu kepada template yang ada didalam standar COBIT 5 *for Risk* APO12. Dimana pendekatan proses penilaian risiko yatu dengan melakukan pemetaan risiko terhadap proses di COBIT 5, melakukan analisis risiko, merancang skenario dan melakukan justifikasi dalam penilaian risiko.

4.6.1 Perancangan Pemetaan Risiko Terhadap Proses Di COBIT 5

Risiko yang teridentifikasi dipetakan terhadap proses *helpdesk* terkait manajemen insiden dan pemenuhan permintaan layanan berdasarkan domain DSS02 pada COBIT 5. Berikut perancangan template pemetaan risiko terhadap proses yang ditunjukan pada Tabel 4.6.

Tabel 4. 6 Pemetaan Risiko terhadap Proses DSS02 COBIT5

No	DSS02	Aktivitas DSS02	Risiko	Keterangan
1.	(DSS02.07 – melacak status dan membuat laporan)	Menganalisis insiden dan layanan permintaan dengan mengkategorisasikan tren	Risiko 1	Keterangan 1
2.	(DSS02.07 – melacak status dan membuat laporan)	Membuat dan mendistribusikan laporan berkala atau menyediakan controlled access ke online data	Risiko 2	Keterangan 2

4.6.2 Analisis Risiko

Analisis Risiko berdasarkan tipe risiko, kategori risiko dan faktor risiko.

4.6.2.1 Perancangan Tipe Risiko

Perancangan pemetaan tipe Risiko disajikan dalam Tabel 4.7.

Tabel 4. 7 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	S
2.	Risiko 2	S	S	P

4.6.2.2 Perancangan Kategori Risiko

Perancangan Pemetaan risiko dengan kategori risiko disajikan dalam Tabel 4.8.

Tabel 4. 8 Perancangan Kategori Risiko

No	Risiko	Risk Category TI	Risk ID
1.	Risiko 1	*IT investment decision making*	(IDM1101)
2.	Risiko 2	*Portfolio establishment and maintenance*	(PEM2501)

4.6.2.3 Perancangan Faktor Risiko

Perancangan Pemetaan risiko dengan faktor risiko disajikan dalam Tabel 4.9.

Tabel 4. 9 Perancangan Faktor Risiko

No	Risiko	Faktor Risiko	
		Internal	External
1.	Risiko 1	(Financial Capacity) Penjelasan mengenai faktor risiko	(Regulatory environment) Penjelasan mengenai faktor risiko
2.	Risiko 2	(Culture Of the enterprise) Penjelasan mengenai faktor risiko	(Competitive Environment) Penjelasan mengenai faktor risiko

4.6.3 Perancangan Skenario Risiko

Perancangan Skenario Risiko ditunjukan dalam Tabel 4.10.

Tabel 4. 10 Perancangan Faktor Risiko

No	Risiko	Skenario Risiko	
		Negatif	**Positif**
1.	Risiko 1	Penjelasan Skenario Negatif	Penjelasan Skenario Positif
2.	Risiko 2	Penjelasan Skenario Negatif	Penjelasan Skenario Positif

4.6.4 Perancangan Justifikasi Penilaian Risiko

Penilaian risiko diidentifikasi berdasarkan aspek frekuensi dan dampak dari sebuah risiko, dimana dampak yang diakibatkan dapat dibagi menjadi empat yaitu berdasarkan produktivitas, biaya tanggapan, keunggulan kompetitif dan hukum.

4.6.4.1 Penentuan Nilai Frekuensi

Banyaknya risiko yang terjadi dalam satu periode tertentu disebut frekuensi risiko, biasanya satu periode dihitung dalam satu tahun. Berikut merupakan perancangan penentuan nilai frekuensi berdasarkan parameter banyaknya risiko dalam satu tahun yang disajikan dalam Tabel 4.11.

Tabel 4. 11 Perancangan Justifikasi Frekunsi Risiko

Nilai Frekuensi	Frekuensi Risiko	Keterangan
1	$0{,}01 < N \leq 0.1$	Very Low Risiko yang terjadi lebih dari 0,01 kali dan kurang dari sama dengan 0,1 kali dalam setahun Risiko yang kemungkinan terjadinya sangat rendah
2	$0{,}1 < N \leq 1$	Low Risiko yang terjadi lebih dari 0,1 kali dan kurang dari sama dengan 1 kali dalam setahun

		Risiko yang kemungkinan terjadinya rendah
3	1 < N ≤ 10	Moderate Risiko yang terjadi lebih dari 1 kali dan kurang dari sama dengan 10 kali dalam setahun Risiko yang kemungkinan terjadinya cukup tinggi
4	10 < N ≤ 100	High Frekuensi risiko terjadi lebih dari 10 kali dan kurang dari sama dengan 100 kali dalam setahun Risiko yang kemungkinan terjadinya tinggi
5	100 < N	Very High Frekuensi risiko terjadi lebih dari 100 kali dalam setahun risiko yang kemungkinan terjadinya sangat tinggi

Keterangan: N adalah jumlah terjadinya risiko setiap tahun

4.6.4.2 Penentuan Nilai Dampak

Pengukuran nilai dampak dilihat dari seberapa besar intensitas suatu risiko dalam mempengaruhi proses bisnis didalam organisasi. Dimana dampak dapat dibagi menjadi empat yaitu berdasarkan produktivitas, biaya tanggapan, keunggulan kompetitif dan hukum. Berikut merupakan justifikasi dari nilai dampak yang ditampilkan pada Tabel 4.12.

Tabel 4. 12 Perancangan Justifikasi Dampak Risiko

Nilai Dampak (Magnitude)	**Dampak Risiko**			
	Produktivitas	**Biaya Tanggapan**	**Keunggulan Kompetitif**	**Hukum**
1	0,1% < I ≤ 1%	I ≤ 1 Juta Rupiah	0,5 < I ≤ 1	I ≤ 1 Juta Rupiah
2	1% < I ≤ 3%	1 Juta Rupiah < I ≤ 10 Juta Rupiah	1 < I ≤ 1,5	I ≤ 10 Juta Rupiah
3	3% < I ≤ 5%	10 Juta Rupiah < I ≤	1,5 < I ≤ 2	I ≤ 100 Juta Rupiah

		100 Juta Rupiah		
4	5% < I ≤ 10%	100 Juta Rupiah < I ≤ 500 Juta Rupiah	2 < I ≤ 2,5	I ≤ 500 Juta Rupiah
5	10% < I	500 Juta Rupiah < I	2,5 < I	I > 500 Juta Rupiah

Keterangan: I (Impact) adalah dampak risiko.

Ke-empat aspek tersebut kemudian dihitung rata-ratanya agar memiliki satu nilai dampak. Untuk setiap aspek didapatkan dari studi dokumen dan wawancara kecuali aspek keunggulan kompetitif yang didapatkan dari hasil survei kepuasan pengguna. Berikut penjelasan dari setiap aspek:

1. Produktivitas
   Produktivitas dihitung berdasarkan kerugian presentase (%) secara finansial yang dialami oleh PDAM Surabaya dalam waktu satu periode atau satu tahun.
2. Biaya tanggapan
   Biaya tanggapan adalah biaya yang digunakan oleh perusahaan untuk menangani setiap risiko merugikan yang terjadi.
3. Keunggulan kompetitif
   Keunggulan kompetitif diukur dari penurunan kepuasan pengguna layanan yaitu pegawai PDAM akibat risiko yang terjadi.
4. Berikut merupakan justifikasi dampak risiko berdasarkan keunggulan kompetitif yang disajikan dalam Tabel 4.13.

Tabel 4. 13 Perancangan Justifikasi Dampak Risiko berdasarkan keunggulan kompetitif

Nilai Dampak (Magnitude)	**Dampak Risiko (Keunggulan Kompetitif)**		
	Penurunan Kepuasan	**Rentan Skala Likert (Kuisioner)**	**Keterangan**
1	I ≤ 1	1,00 – 1,50	Sangat Rendah

Nilai Dampak (Magnitude)	Dampak Risiko (Keunggulan Kompetitif)		
	Penurunan Kepuasan	Rentan Skala Likert (Kuisioner)	Keterangan
			Penurunan kepuasan pelanggan yang sangat rendah terhadap layanan
2	$1 < I \leq 1.5$	1,51 – 2,50	Rendah Penurunan kepuasan pelanggan yang rendah terhadap layanan
3	$1,5 < I \leq 2$	2,51 – 3,50	Sedang Penurunan kepuasan pelanggan yang sedang terhadap layanan
4	$2 < I \leq 2,5$	3,51 – 5,50	Tinggi Penurunan kepuasan pelanggan yang Tinggi terhadap layanan
5	$2,5 < I$	4,51 – 1,50	Sangat Tinggi Penurunan kepuasan pelanggan yang sangat Tinggi terhadap layanan

5. Hukum

   Aspek hukum terkait biaya denda yang harus ditanggung oleh perusahaan akibat risiko yang terjadi yang memiliki dampak hukum. Nilai pengukuran nilai dampak berdasarkan biaya denda dalam rupiah yang harus ditanggung oleh perusahaan.

4.6.5 Perancangan Kuisioner Risiko

Berikut merupakan template perancangan kuisioner yang pertanyannya didasari pada scenario risiko yang diajukan untuk pengguna layanan *helpdesk* PDAM Surabaya yang disajikan pada Tabel 4.14.

Tabel 4. 14 Perancangan Kuisioner Risiko

No	Pernyataan	1	2	3	4	5
1.	Pernyataan 1					
2.	Pernyataan 2					
3.	Pernyataan 3					

4.6.5.1 Perancangan Template Pemetaan Kuisioner

Berikut merupakan template pemetaan pernyataan kuisioner dengan risiko berdasarkan persamaan skenario risiko yang disajikan pada Tabel 4.15.

Tabel 4. 15 Perancangan Pemetaan Kuisioner Risiko

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	Positif
1.	Peryantaan Kuisioner 1	Risiko 1	Penjelasan Skenario Negatif	Penjelasan Skenario Positif
		Risiko 2	Penjelasan Skenario Negatif	Penjelasan Skenario Positif

4.6.6 Perancangan Template Penilaian Risiko

Berikut merupakan template penilaian risiko yang meliputi aspek frekuensi dan ke-empat aspek dampak risiko yang disajikan pada Tabel 4.16.

Tabel 4. 16 Perancangan Template Penilaian Risiko

Risk ID	Risiko	Nilai Dampak					Nilai Frekuensi	Level Risiko
		Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Rata-Rata nilai Dampak		
(IDM1101)	Risiko 1	1	1	1	1	1	1	Low
(PEM2501)	Risiko 2	2	1	1	2	1, 5	1	Low

4.6.7 Perancangan Respon Risiko

Berikut merupakan tabel perancangan template untuk respon risiko berdasarkan empat pilihan respon risiko menurut COBIT 5, yaitu risk acceptance, mitigation, avoidance dan transfer yang disajikan dalam Tabel 4.17.

Tabel 4. 17 Perancangan Template respon Risiko

Risk ID	Risiko	Respon
(IDM1101)	Risiko 1	Avoid
(PEM2501)	Risiko 2	Mitigate

4.6.8 Perancangan Mitigasi Risiko

Berikut merupakan tabel perancangan template pemetaan risiko dengan proses TI yang ada pada COBIT 5 untuk dijadikan langkah mitigasi risiko yang disajikan pada Tabel 4.18.

Tabel 4. 18 Perancangan Template mitigasi risiko

Risk ID	Kategori risiko	Risiko	Level risiko	Proses COBIT 5	Langkah Mitigasi
(IES1101)	IT expertise and skill	Risiko 1	Low	APO07 Manage Human Resource	APO07.03 Maintain the skills and competence of Personnel

BAB V
IMPLEMENTASI

Pada bab ini akan dijelaskan tentang implementasi proses dan setiap tahapan di dalam metodologi tugas akhir yang dapat berupa waktu pelaksanaan, hasil dan lampiran terkait yang memuat informasi pencatatan tertentu dengan implementasi proses.

5.1 Proses Pengumpulan Data

Penelitian ini melakukan pengumpulan data yang bertujuan untuk mengidentifikasi dan menganalisa risiko yang berkaitan dengan proses TI yang ada pada *helpdesk* unit TSI PDAM Surabaya yang berhubungan manajemen insiden dan pemenuhan permintaan layanan. Dalam pelaksanaan pengumpulan data dilakukan dengan cara wawancara, observasi dan pengkajian dokumen yang dilakukan dapat dilihat di Lampiran B dan C.

5.1.1 Hasil Wawancara

Berdasarkan perancangan perangkat penggalian data, telah diketahui bahwa yang akan menjadi narasumber adalah staff unit *helpdesk* unit TSI, yaitu Bapak Alfil Hidayat dan Ibu Fitri Qonita serta Manajer unit TSI PDAM Surabaya yaitu Bapak Ari Bimo Sakti. Wawancara telah dilakukan pada Ruang TSI PDAM Surabaya pada tanggal 2 dan 9 Mei 2019.

Berdasarkan proses wawancara dapat diketahui bahwa helpdesk unit TSI PDAM kota Surabaya sudah menggunakan IT dalam melakukan proses bisnis sehari-harinya tetapi masih belum dilakukan identifikasi risiko tersendiri terkait risiko-risiko yang ada pada proses bisnis helpdesk.

Hasil wawancara secara detail dapat dilihat pada Lampiran B.

5.1.2 Hasil Observasi

Hasil dari Observasi yang telah dilakukan terkait proses pada DSS02 COBIT 5 yang sudah dilakukan oleh *helpdesk* PDAM Surabaya dalam proses manajemen insiden dan pemenuhan permintaan layanan.

Berdasarkan hasil observasi dapat diketahui helpdesk sudah banyak melakukan proses TI yang sesuai dengan proses TI ideal yang ada pada DSS02 COBIT 5 tetapi untuk proses-proses yang mengenai analisis tren dan prosedur permintaan belum adanya prosedur dan dokumentasi tersendiri.

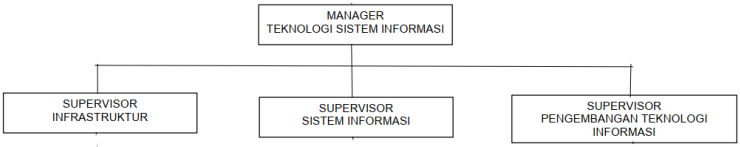
Detail dari hasil observasi dapat dilihat dalam Lampiran C.

5.2 Gambaran Umum Unit Teknologi Sistem Informasi

Unit TSI dipimpin oleh seorang manajer bernama Ari Bimo Sakti yang dibawahnya memiliki tiga bagian yang terdiri atas:

1. Supervisor Infrastruktur
2. Supervisor Sistem Informasi
3. Supervisor Pengembangan Teknologi Informasi

Manajer unit Teknologi Sistem Informasi dipimpin oleh seorang manajer, yang dalam menjalankan tugasnya bertanggung jawab kepada Manajer senior Perencaan dan Pengembangan. Berikut merupakan gambaran struktur organisasi unit TSI PDAM Surabaya yang disajikan dalam gambar 5.1 [29].



Gambar 5. 1 Struktur Organisasi unit TSI

Tugas Pokok dan Fungsi unit TSI

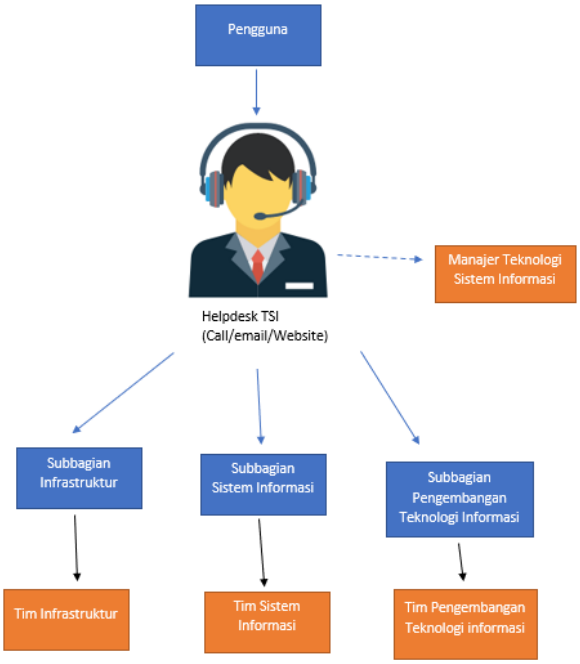
Dalam melaksanakan tugasnya, unit Teknologi Sistem Informasi PDAM Surabaya memnyelenggarakan fungsi [29]:

1. Mengelola dan mengkoordinasikan infrastruktur teknologi informasi yang meliputi penyediaan fasilitas komputer, jaringan komputer, server serta email sistem dan keamanannya.

2. Mengelola dan mengkoordinasikan sistem informasi teknologi yang meliputi perencanaan mapping proses bisnis aplikasi IT, pemeliharaan dan perubahan aplikasi sistem informasi sesuai model dan proses bisnis perusahaan; dan
3. Mengelola dan mengkoordinasikan pengembangan teknologi informasi yang meliputi pembuatan aplikasi dan infrastruktur baru sesuai perkembangan bisnis untuk diterapkan pada perusahaan.

5.2.1 Gambaran Umum *Helpdesk* unit Teknologi Sistem informasi PDAM Surabaya

Helpdesk merupakan salah satu unit yang dimiliki oleh PDAM Surabaya yang menangani berbagai macam permasalahan layanan TI dan keluhan dari para pengguna layanan yang terjadi di lingkungan PDAM Surabaya. Pengguna layanan ini adalah pegwai PDAM Surabaya. Pengguna dapat menyampaikan keluhan dan permasalahan yang dialami kepada *helpdesk* unit TSI melalui sistem informasi *helpdesk* atau datang secara langsung ke ruang unit TSI untuk menyampaikan masalah yang dialami. Permintaan layanan yang ditangani oleh *helpdesk* terkait dengan insiden layanan TI, permintaan layanan TI dan permasalahan infrastruktur IT. Berikut adalah alur layanan (*Helpdesk* Flow) *helpdesk* unit TSI dalam menangani permasalahan dan keluhan yang diterima disajikan dalam gambar 5.2.



Gambar 5. 2 Alur layanan *helpdesk*

Tugas Pokok dan Fungsi unit TSI

Helpdesk dalam kegiatan sehari-harinya memanfaatkan peran TI dengan menggunkan e-mail dan sistem informasi berbasis website untuk menerima laporan maupun permintaan layanan dari pengguna. Berikut merupakan tugas pokok dan fungsi *helpdesk* unit TSI PDAM Surabaya yang disajikan pada Tabel 5.1.

Tabel 5. 1 Tugas Pokok dan fungsi *Helpdesk*

No	Tugas Pokok dan Fungsi
	Manajemen Insiden
1.	Menerima laporan, melakukan pencatatan dan kategorisasi terkait insiden dan keluhan
2.	Mengelola proses manajemen insiden terkait a. Permasalahan akun b. Permasalahan software c. Perbaikan hardware

3.	Melakukan eskalasi insiden ke subbag infrastuktur, sistem informasi atau tim pengembangan teknologi informasi
4.	Mengawasi proses penanganan insiden
5.	Memberikan informasi terkait status laporan kepada pengguna yang melaporkan
6.	Membuat laporan secara berkala terkait insiden yang terjadi
Permintaan Layanan	
1.	Menerima dan mencatat permintaan terkait layanan TI
2.	Melakukan pemenuhan request untuk layanan a. Permintaan data b. Perubahan data c. Perubahan fitur d. Permintaan sistem atau software baru e. Perbaikan hardware

5.3 Risiko Proses TI pada *Helpdesk*

Penentuan risiko Proses TI pada *helpdesk* yang berkaitan dengan proses manajemen insiden dan pemenuhan permintaan layanan dilakukan dengan menganalisis proses TI yang ada pada alur layanan. Dimana risiko yang diidentifikasi merupakan risiko yang diperoleh dari analisis penelitian sebelumnya [28] dan kondisi kekinian dari penggalian informasi mengenai kemungkinan risiko yang akan terjadi melalui proses wawancara, observasi dan studi dokumen. Berikut merupakan daftar pemetaan risiko terhadap proses DSS02 COBIT 5 yang disajikan dalam Tabel 5.2.

Tabel 5. 2 Pemetaan Risiko terhadap Proses DSS02 COBIT5

No	DSS02	Aktivitas	Risiko	Keterangan
1.	DSS02.01 - Menetapkan Skema klasifikasi insiden dan permintaan layanan	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	Kesalahan dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	*Helpdesk* membuat sistem prioritasi dan kategorisasi yang tidak mencakup seluruh layanan TI yang ada atau tidak sesuai dengan kondisi organisasi saat ini
2.		Mendefinisikan bentuk insiden untuk mengetahui	Kegagalan dalam	Adanya server down atau

No	DSS02	Aktivitas	Risiko	Keterangan
		kesalahan untuk membuat resolusi yang efisien dan efektif.	menerima laporan dari pengguna	pemadaam listrik dari pihak PLN yang menyebabkan sistem informasi tidak dapat diakses
3.		Mendefinisikan model permintaan layanan berdasarkan tipe permintaan layanan untuk memungkinkan dilakukan secara mandiri dan layanan yang efisien untuk permintaan yang standar.	Kesalahan dalam menentukan tipe permintaan layanan	Detail Informasi yang diberikan pengguna tidak sesuai dengan masalah yang dialami pengguna
4.		Mendefinisikan peraturan dan prosedur eskalasi insiden, terutama untuk insiden utama dan insiden keamanan.	Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	*Helpdesk* tidak atau lupa memberikan informasi terkait prosedur eskalasi insiden kepada pihak yang melakukan eskalasi
5.		Mendefinisikan pengetahuan permintaan layanan dan kegunaannya.	Kesalahan dalam memahami permintaan pengguna	*Helpdesk* tidak memahami detail informasi dari permintaan pengguna yang diajukan
6.	DSS02.02 - Merekam, mengklasifikasikan dan memprioritaskan permintaan dan insiden	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.	Tidak adanya log insiden atau permintaan layanan TI	Insiden atau permintaan layanan yang masuk tidak tercatat kepada log insiden atau permintaan layanan TI
7.		Untuk memungkinkan analisis tren, diperlukan	Menumpuknya	Permintaan layanan yang

No	DSS02	Aktivitas	Risiko	Keterangan
		klasifikasi permintaan layanan dengan melakukan identifikasi tipe dan kategori dari permintaan tersebut.	permintaan layanan yang masuk	masuk terlalu banyak sehingga *helpdesk* tidak bisa langsung melakukan identifikasi dari permintaan layanan tersebut
8.		Melakukan prioritisasi permintaan layanan berdasarkan definisi layanan dari SLA terhadap proses bisnis perusahaan dan tingkat urgensi.	Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan	*Helpdesk* melakukan kesalahan dalam melakukan prioritasi permintaan layanan
9.			Keterlambatan respon *helpdesk*	Kinerja staff yang lambat menyebabkan *helpdesk* tidak responsif dalam melakukan pengelolaan layanan
10.	DSS02.03 - Melakukan verifikasi, menerima dan memenuhi permintaan layanan	Melakukan verifikasi terhadap hak untuk menggunakan permintaan layanan, jika dimungkinkan, alur proses yang telah didefinisikan dan perubahan standar.	Penyalahgunaan hak akses oleh pengguna	Terdapat penyalahgunaan hak akses untuk permintaan layanan TI
11.		Memperoleh persetujuan finansial dan fungsonal atau tanda tangan, jika dibutuhkan, atau persetujuan otomatis untuk persetujuan dalam perubahan yang standar.	Helpdesk tidak mendapatkan persetujuan finansial atau fungsional	*Helpdesk* tidak mendapatkan persetujuan finansial atau fungsional yang dibutuhkan untuk menangani insiden
12.		Melakukan pemenuhan permintaan dengan cara memilih prosedur permintaan, jika memungkinkan	Pengelolaan pemenuhan permintaan dilakukan	Tidak tersedianya prosedur untuk pengelolaan insiden dan

No	DSS02	Aktivitas	Risiko	Keterangan
		menggunakan menu bantuan mandiri dan model permintaan yang telah dibuat sebelumnya untuk item - item yang sering diminta.	secara tidak konsisten	permintaan layanan
13.	DSS02.04 - Menginvestigasi, mendiagnosa dan mengalokasikan insiden	Mengidentifikasikan dan mendeksripsikan gejala yang relevan untuk mendirikan penyebab yang paling tepat dari insiden tersebut.	Kesalahan *helpdesk* dalam menentukan penyebab dari insiden	*Helpdesk* melakukan kesalahan dalam mendefinisikan gejala yang relevan untuk insiden
14.		Jika insiden tersebut tidak tersedia, buat sebuah log baru.	Terjadinya pengulangan pencatatan untuk insiden yang sama	*Helpdesk* melakukan kesalahan pencatatan untuk insiden yang sama
15.		Menetapkan insiden ke fungsi spesialis.	Kesalahan dalam memilih pihak yang menangani insiden	Pihak yang dieskalasi tidak menguasai cara dari penangan insiden
16.			Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan	Pihak yang dieskalasi terlambat melakukan penanganan insiden
17.	DSS02.05 - Melakukan Penyelesaian dan Pemulihan insiden	Memilih dan menggunakan resolusi insiden yang tepat (*temporary workaround* dan/atau solusi tetap).	Gangguan pada perangkat keras di unit TSI	Hardware yang mendukung penanganan layanan TI tidak dapat digunakan (risiko yang ada saat ini)
18.			Kegagalan dalam menangani insiden	Solusi yang dipilih oleh *helpdesk* tidak dapat digunakan untuk menangani insiden

No	DSS02	Aktivitas	Risiko	Keterangan
				atau permintaan layanan TI
19.		Merekam *workaround* mana yang digunakan untuk melakukan resolusi insiden.	Tidak adanya pencatatan terkait solusi penanganan insiden	Tidak adanya pencatatan mengenai solusi penanganan insiden (risiko yang ada saat ini)
20.		Melakukan aksi pemulihan (jika dibutuhkan).	Penanganan insiden melebihi batas waktu yang disepakati	*Helpdesk* melakukan melakukan kesalahan saat menangani insiden
21.		Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat dipakai sebagai sumber pengetahuan mendatang.	Insiden dan layanan permintaan yang tidak terdokumentasi dengan lengkap	*Helpdesk* tidak membuat laporan penyelesaian insiden dan permintaan layanan dengan semua detail informasi yang lengkap
22.	DSS02.06 - Menutup permintaan layanan dan insiden	Melakukan verifikasi dengan pengguna yang berpengaruh (apabila setuju) bahwa layanan permintaan mereka telah dipenuhi dan diselesaikan dengan baik	Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna	Pengguna merasa tidak puas dengan pelayanan yang telah diberikan
23.		Menutup layanan permintaan dan insiden	Pengguna tidak memberikan konfirmasi terkait status penutupan insiden	Pengguna tidak atau terlambat merespon status penutupan insiden
24.	DSS02.07 - Melacak status dan membuat laporan	Mengawasi dan melacak eskalasi insiden dan resolusi dan penanganan permintaan untuk melakukan progress penyelesaian.	Pihak yang dieskalasi tidak memperbarui status	Pihak yang dieskalasi tidak memberikan status terkait insiden atau

No	DSS02	Aktivitas	Risiko	Keterangan
			mengenai insiden atau permintaan layanan yang ditangani	permintaan layanan
25.			Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi	Insiden atau permintaan layanan tidak terdistribusi kepada pihak yang melakukan eskalasi
26.		Mengidentifikasi informasi stakeholder dan kebutuhan mereka untuk pemenuhan data dan laporan. Idenfitikasi laporan secara berkala.	*Helpdesk* tidak menginformasikan status insiden atau permintaan layanan TI kepada pengguna	Stakeholder tidak memberikan informasi yang lengkap
27.		Menganalisis insiden dan layanan permintaan dengan mengkategorisasikan tren.	Kesalahan pendefinisian tren dalam laporan	*Helpdesk* tidak melakukan pendefinisian tren didalam laporan
28.		Membuat dan mendistribusikan laporan berkala atau menyediakan *controlled access* ke *online data*.	Gangguan terhadap server dan jaringan perusahaan	Terjadi kesalahan dalam mendistribusikan laporan berkala ke online data (risiko yang ada saat ini)

BAB VI
HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan tentang hasil dan pembahasan yang telah didapatkan untuk menjawab rumusan masalah dari penelitian ini.

6.1 Analisis Risiko

Berikut merupakan hasil dari analisis Risiko berdasarkan tipe risiko, kategori risiko dan faktor risiko.

6.1.1 Analisis Tipe Risiko

Pembahasan hasil Analisa tipe risiko dibuat berdasarkan kepentingan tipe skenario risiko tersebut untuk setiap tipe risiko, yaitu tipe 'P' untuk tipe primer atau lebih tinggi, serta tipe 'S' untuk tipe sekunder atau lebih rendah. Berikut merupakan pembagian tipe risiko menjadi tiga, yaitu:

1. *IT Benefit/Value Enablement Risk*
   Apabila risiko terkait dengan hilangnya opportunity penggunaan teknologi bagi peningkatan efisiensi dan efektifitas proses bisnis maka diisi dengan 'P', sedangkan jika tidak terkait maka diisi dengan 'S'.
2. *IT Program and Project Deliver Risk*
   Apabila risiko terkait dengan kontribusi teknologi informasi bagi solusi bisnis baru atau memperbaiki solusi bisnis dalam bentuk proyek atau program maka diisi dengan 'P', sedangkan jika tidak terkait maka diisi dengan 'S'.
3. *IT Operations and Service Delivery Risk*
   Apabila Risiko Terkait dengan aspek kinerja sistem dan layanan teknologi informasi yang dapat merusak atau mereduksi nilai organisasi atau perusahaan maka diisi dengan 'P', sedangkan jika tidak terkait maka diisi dengan 'S'.

Pada tabel 6.1 dibuat tabel tipe risiko berdasarkan hasil wawancara dengan narasumber dari pihak unit TSI PDAM dan analisis risiko pada proses DSS02 COBIT 5 yang dilakukan dalam penelitian ini.

Tabel 6. 1 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 dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	S	S	P
2.	Kegagalan dalam menerima laporan dari pengguna	S	S	P
3.	Kesalahan dalam menentukan tipe permintaan layanan	S	S	P
4.	Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	S	S	P
5.	Kesalahan dalam memahami permintaan pengguna	S	S	P
6.	Tidak adanya log insiden atau permintaan layanan TI	S	S	P
7.	Menumpuknya permintaan layanan yang masuk	S	S	P
8.	Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan	S	S	P
9.	Keterlambatan respon *helpdesk*	S	S	P
10.	Penyalahgunaan hak akses oleh pengguna	S	S	P
11.	Helpdesk tidak mendapatkan	S	S	P

No	Risiko	Tipe Risiko		
		IT Benefit/ Value Enablement Risk	***IT Programme and Project Delivery Risk***	***IT Operations and Service Delivery Risk***
	persetujuan finansial atau fungsional			
12.	Pengelolaan pemenuhan permintaan dilakukan secara tidak konsisten	S	S	P
13.	Kesalahan *helpdesk* dalam menentukan penyebab dari insiden	S	S	P
14.	Terjadinya pengulangan pencatatan untuk insiden yang sama	S	S	P
15.	Kesalahan dalam memilih pihak yang menangani insiden	S	S	P
16.	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan	S	S	P
17.	Gangguan pada perangkat keras di unit TSI	P	S	S
18.	Kegagalan dalam menangani insiden	S	S	P
19.	Tidak adanya pencatatan terkait solusi penanganan insiden	S	S	P
20.	Penanganan insiden melebihi batas waktu yang disepakati	S	S	P
21.	Insiden dan layanan permintaan yang 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***
	terdokumentasi dengan lengkap			
22.	Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna	S	S	P
23.	Pengguna tidak memberikan konfirmasi terkait status penutupan insiden	S	S	P
24.	Pihak yang dieskalasi tidak memperbarui status mengenai insiden atau permintaan layanan yang ditangani	S	S	P
25.	Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi	S	S	P
26.	*Helpdesk* tidak menginformasikan status insiden atau permintaan layanan TI kepada pengguna	S	S	P
27.	Kesalahan pendefinisian tren dalam laporan	S	S	P
28.	Gangguan terhadap server dan jaringan perusahaan	P	S	S

Berdasarkan hasil analisis dari tipe risiko, dapat diketahui bahwa banyak proses bisnis dalam *helpdesk ynag* memiliki risiko bertipe *IT Operations and Service Delivery*

Risk, karena proses-proses manajemen insiden dan pemenuhan permintaan yang ada pada *helpdesk* erat kaitannya dengan aspek kinerja sistem dan layanan teknologi informasi yang dapat merusak atau mereduksi nilai organisasi atau perusahaan. *Helpdesk* juga memiliki 2 risiko terkait dengan hilangnya oportunity TI sebagai peningkatan efisiensi dan efektifitas proses bisnis sehingga kedua risiko tersebut diisikan dengan 'P' (Primer) pada *IT Benefit/Value Enablement Risk* dan semua risiko lainnya diisikan dengan 'P' (Primer) pada *IT Operations and Service Delivery Risk.*

6.1.2 Analisis Kategori Risiko

Pemetaan risiko berdasarkan kategori yang ada pada COBIT 5 dan pemberian ID risiko berdasarkan kategori dan pemetaan risiko yang sebelumnya sudah dilakukan disajikan dalam Tabel 6.2.

Tabel 6. 2 Kategori Risiko

No	Risiko	Risk Category TI	Risk ID
1	Kesalahan dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	*IT expertise and skill*	IE1101
2	Kesalahan dalam menentukan tipe permintaan layanan		IE1302
3	Kesalahan dalam memahami permintaan pengguna		IE1503
4	Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan		IE2304
5	Keterlambatan respon *helpdesk*		IE2305
6	Kesalahan *helpdesk* dalam menentukan penyebab dari insiden		IE4106
7	Kesalahan dalam memilih pihak yang menangani insiden		IE4307
8	Kegagalan dalam menangani insiden		IE5108
9	Kesalahan pendefinisian tren dalam laporan		IE7309
10	Penyalahgunaan hak akses oleh pengguna	*Information*	IF3101

No	Risiko	Risk Category TI	Risk ID
11	Gangguan pada perangkat keras di unit TSI	*Infrastucture*	IS5101
12	Gangguan terhadap server dan jaringan perusahaan	*Logical Attack*	LA7401
13	Pengelolaan pemenuhan permintaan dilakukan secara tidak konsisten	*Regulatory Compliance*	RC3301
14	Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	*Staff Operation*	SO1401
15	Tidak adanya log insiden atau permintaan layanan TI		SO2102
16	Menumpuknya permintaan layanan yang masuk		SO2203
17	Helpdesk tidak mendapatkan persetujuan finansial atau fungsional		SO3204
18	Terjadinya pengulangan pencatatan untuk insiden yang sama		SO4205
19	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan		SO4306
20	Tidak adanya pencatatan terkait solusi penanganan insiden		SO5207
21	Penanganan insiden melebihi batas waktu yang disepakati		SO5308
22	Insiden dan layanan permintaan yang tidak terdokumentasi dengan lengkap		SO5409
23	Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna		SO6110
24	Pengguna tidak memberikan konfirmasi terkait status penutupan insiden		SO6211
25	Pihak yang dieskalasi tidak memperbarui status mengenai insiden atau permintaan layanan yang ditangani		SO7112
26	*Helpdesk* tidak menginformasikan status insiden		SO7213

No	Risiko	Risk Category TI	Risk ID
	atau permintaan layanan TI kepada pengguna		
27	Kegagalan dalam menerima laporan dari pengguna	*Software*	SW1201
28	Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi		SW7101

Berdasarkan hasil analisis dari kategori risiko, dapat diketahui bahwa risiko-risiko paling banyak masuk kategori IT expertise and skill dan staff operation. Karena risiko proses helpdesk memang erat dengan risiko yang disebabkan oleh staff nya.

6.1.3 Analisis Faktor Risiko

Pembahasan hasil Analisa faktor (penyebab) risiko dibuat berdasarkan tipe faktor risiko tersebut, baik faktor internal maupun eksternal. Faktor yang dipilih adalah faktor yang mempengaruhi terjadinya risiko pada proses manajemen insiden dan pemenuhan permintaan layanan. Berikut merupakan hasil dari analisis faktor risiko yang terjadi di *helpdesk* unit TSI PDAM Surabaya yang disajikan pada Tabel 6.3.

Tabel 6. 3 Faktor Risiko

No	Risiko	Faktor Risiko	
		Internal	**External**
1.	Kesalahan dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	**Culture of enterprise** Tidak adanya kebijakan yang khusus yang mengatur tentang pendefinisian pembuatan system kategori insiden atau pemintaan layanan	**Rate of change in the market in which the enterprise operates** Perubahan model bisnis yang terjadi di perusahaan **Regulatory environment** Tidak adanya kebijakan yang jelas terkait

No	Risiko	Faktor Risiko	
		Internal	**External**
			penanganan insiden dan permintaan layanan
2.	Kesalahan dalam menentukan tipe permintaan layanan	**Complexity of IT** Kompleksnya Sistem TI di perusahaan	**Technology Status and evolution** Berkembangnya teknologi yang menyebabkan semakin kompleksnya insiden dan permintaan layanan TI yang dilaporkan.
3.	Kesalahan dalam memahami permintaan pengguna	**Culture of enterprise** Terjadinya kesalahpahaman antara *helpdesk* dengan pelapor terkait insiden atau permintaan layanan yang diajukan	**Technology Status and evolution** Berkembangnya teknologi yang menyebabkan semakin kompleksnya insiden dan permintaan layanan TI yang dilaporkan.
4.	Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan	**Strategic importance of IT in the enterprise** Tidak terdapatnya system prioritasi insiden dan permintaan layanan berdasarkan tingkat urgensi dan dampak yang ditimbulkan dari permintaan	**Regulatory environment** Tidak adanya kebijakan yang jelas terkait prioritasi penanganan insiden dan permintaan layanan

No	Risiko	Faktor Risiko	
		Internal	**External**
		layanan dan insiden. **Culture of enterprise** Tidak adanya kebijakan yang khusus yang mengatur tentang prioritasi insiden atau pemintaan layanan	
5.	Keterlambatan respon *helpdesk*	**Financial Capacity** Usia dari perangkat keras seperti server yang sudah tua **Strategic Priorities** Kesalahan *helpdesk* melakukan prioritasi layanan berdasarkan tingkat urgensi	**Competitive environment** Standar tingkat respon di perusahaan lain yang lebih tinggi yang mempengahuri standar respon dikatakan responsif
6.	Kesalahan *helpdesk* dalam menentukan penyebab dari insiden	**Complexity of IT** Kompleksnya Sistem TI di perusahaan yang menyebabkan *helpdesk* kesulitan menentukan penyebab dari insiden	**Technology Status and evolution** Berkembangnya teknologi yang menyebabkan semakin kompleksnya insiden dan permintaan layanan TI yang dilaporkan.
7.	Kesalahan dalam memilih pihak yang menangani insiden	**Operating model** Pengoperasian proses bisnis perusahaan	**Rate of change in the market in which the enterprise operates**

No	Risiko	Faktor Risiko	
		Internal	**External**
		memiliki model yang rumit **Complexity of IT** Kompleksnya Sistem TI di perusahaan yang menyebabkan *helpdesk* kesulitan melakukan eskalasi insiden	Pengaruh perubahan model bisnis yang terjadi di perusahaan **Regulatory environment** Pengaruh perubahan peraturan yang menyebabkan *helpdesk* kesulitan menentukan pihak yang tepat untuk melakukan eskalasi
8.	Kegagalan dalam menangani insiden	**Operating model** Pengoperasian proses bisnis perusahaan **Complexity of IT** Kompleksnya Sistem TI di perusahaan yang menyebabkan *helpdesk* kesulitan melakukan penanganan insiden **Culture of enterprise** *Helpdesk* tidak melakukan konfirmasi terkait insiden atau permintaan layanan TI kepada pihak yang dieskalasi	**Technology Status and evolution** Berkembangnya teknologi yang menyebabkan semakin kompleksnya insiden dan permintaan layanan TI yang dilaporkan.

No	Risiko	Faktor Risiko	
		Internal	**External**
9.	Kesalahan pendefinisian tren dalam laporan	**Culture of the enterprise** Laporan terkait pengelolaan insiden dan permintaan layanan tidak dilakukan evaluasi dalam suatu pertemuan khusus	**Technology Status and evolution** Berkembangnya teknologi yang menyebabkan semakin kompleksnya insiden dan permintaan layanan TI yang dilaporkan. **Rate of change in the market in which the enterprise operates** Perubahan model bisnis yang terjadi di perusahaan
10.	Penyalahgunaan hak akses oleh pengguna	**The risk management philosopy** Organisasi tidak menyiapkan strategi untuk pencegahan peretasan akun pengguna oleh pihak luar **Culture of the enterprise** Tidak adanya peraturan khusus tentang pergantian password pengguna secara berkala	**Threat landscape** Ancaman dari akun pengguna yang dapat diretas oleh hacker dan disalahgunakan
11.	Gangguan pada perangkat keras di unit TSI	**Financial Capacity**	**Geopolitical environment**

No	Risiko	Faktor Risiko	
		Internal	**External**
		Perusahaan tidak mampu untuk mendatangkan perangkat keras baru karena terbatasnya anggaran. **Financial Capacity** Perusahaan belum memiliki pembangkit listrik sendiri agar tidak terjadi kerusakan perangkat keras yang berasal dari terputusnya arus listrik.	Kondisi perusahaan yang sering mengalami kerusakan perangkat keras karena terjadinya pemadaman listrik dari pihak PLN
12.	Gangguan terhadap server dan jaringan perusahaan	**Culture of the enterprise** Tidak adanya kebijakan mengenai peraturan memakai flashdisk di dialam perusahaan **The risk management philosopy** Organisasi tidak menyiapkan strategi untuk pencegahan dari masuknya virus lewat akses internet	**Threat Landscape** Adanya usaha dari pihak luar untuk meretas perusahaan **Geopolitical environment** Hilangnya koneksi karena antenna Wireless (WAN) bergeser pointingnya karena angin
13.	Pengelolaan pemenuhan permintaan	**Operating model**	**Technology Status and evolution**

No	Risiko	Faktor Risiko	
		Internal	**External**
	dilakukan secara tidak konsisten	Pengoperasian proses bisnis perusahaan memiliki model yang rumit **Complexity of IT** Kompleksnya Sistem TI di perusahaan yang menyebabkan *helpdesk* kesulitan melakukan pengelolaan pemenuhan permintaan	Berkembangnya teknologi yang menyebabkan perubahan yang sering terjadi. **Rate of change in the market in which the enterprise operates** Perubahan model bisnis yang terjadi di perusahaan
14.	Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	**Strategic importance of IT in the enterprise** Tidak tersosialisasinya dengan baik prosedur dari eskalasi insiden kepada pihak-pihak yang terlibat	**Regulatory environment** Tidak adanya peraturan yang jelas terkait pengelolaan permintaan layanan dan insiden.
15.	Tidak adanya log insiden atau permintaan layanan TI	**Complexity of IT** Sistem informasi *helpdesk* yang tidak bisa diakses dan kompleksnya sistem TI yang harus dipahami pengguna **Operating Model** Model operasi yang digunakan dalam pelaporan	**Technology Status and evolution** Berkembangnya teknologi yang menyebabkan perubahan yang sering terjadi. **Competitive environment** Tingginya standar tingkat pelayanan TI di perusahaan lain yang

No	Risiko	Faktor Risiko	
		Internal	**External**
		insiden atau layanan TI masih belum dikuasi oleh pengguna	mempengahuri standar dalam pencataan insiden dan permintaan layanan.
16.	Menumpuknya permintaan layanan yang masuk	**Culture of enterprise** Tidak adanya kebijakan bagi *helpdesk* untuk mencatat dengan lengkap semua permintaan layanan dan insiden dari pengguna yang masuk	**Regulatory environment** Tidak adanya peraturan yang jelas terkait pengelolaan permintaan layanan dan insiden. **Competitive environment** Tingginya standar tingkat pelayanan TI di perusahaan lain yang mempengahuri standar dalam pencataan insiden dan permintaan layanan.
17.	Helpdesk tidak mendapatkan persetujuan finansial atau fungsional	**Financial Capacity** *Helpdesk* tidak mendapat persetujuan finansial dari perusahaan **Strategic importance of IT in the enterprise** *Helpdesk* tidak memiliki prioritas stategis dalam mengelola permintaan layanan dan insiden, terutama	**Regulatory environment** Tidak adanya peraturan yang jelas terkait pengelolaan permintaan layanan dan insiden.

No	Risiko	Faktor Risiko	
		Internal	**External**
		pada saat mendapatkan persetujuan finansial dan fungsional	
18.	Terjadinya pengulangan pencatatan untuk insiden yang sama	**Culture of the enterprise** Laporan terkait pengelolaan insiden dan permintaan layanan tidak dilakukan evaluasi dalam suatu pertemuan khusus	**Competitive environment** Tingginya standar tingkat pelayanan TI di perusahaan lain yang mempengahuri standar dalam pencataan insiden dan permintaan layanan.
19.	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan	**Complexity of IT** Kompleksnya Sistem TI di perusahaan yang menyebabkan *helpdesk* kesulitan melakukan pengelolaan pemenuhan permintaan	**Regulatory environment** Tidak adanya peraturan yang jelas terkait pengawasan dalam pengelolaan permintaan layanan dan insiden.
20.	Tidak adanya pencatatan terkait solusi penanganan insiden	**Operating Model** *Helpdesk* dalam melakukan operasi layanan TI tidak sesuai dengan standar. **Culture of the enterprise** Laporan terkait pengelolaan insiden dan permintaan layanan tidak	**Regulatory environment** Tidak adanya peraturan yang jelas terkait pengawasan dalam pengelolaan permintaan layanan dan insiden. Terutama untuk dokumentasi dari operasi layanan

No	Risiko	Faktor Risiko	
		Internal	**External**
		dilakukan evaluasi dalam suatu pertemuan khusus	terkait insiden dan permintaan layanan TI.
21.	Penanganan insiden melebihi batas waktu yang disepakati	**Financial Capacity** Perusahaan membutuhkan waktu untuk mendapatkan dana untuk menangani insiden **Complexity of IT** Kompleksnya Sistem TI di perusahaan yang menyebabkan *helpdesk* kesulitan melakukan pengelolaan pemenuhan permintaan	**Regulatory environment** Tidak adanya peraturan yang jelas terkait pengawasan dalam pengelolaan permintaan layanan dan insiden
22.	Insiden dan layanan permintaan yang tidak terdokumentasi dengan lengkap	**Culture of the enterprise** Tidak terealisasikannya budaya organisasi tentang kelengkapan dokumen dalam hal pelayanan insiden dan permintaan layanan yang masuk.	**Regulatory environment** Tidak adanya peraturan yang jelas terkait pengawasan dalam pengelolaan permintaan layanan dan insiden. Terutama untuk dokumentasi dari operasi layanan terkait insiden dan permintaan layanan TI.

No	Risiko	Faktor Risiko	
		Internal	**External**
23.	Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna	**Complexity of IT** Kompleksnya Sistem TI di perusahaan yang menyebabkan *helpdesk* kesulitan melakukan pengelolaan pemenuhan permintaan **Culture of the enterprise** Tidak terealisasikannya budaya organisasi tentang pemberian layanan yang berorientasi kepada kepuasan pengguna.	**Competitive environment** Tingginya standar tingkat pelayanan TI di perusahaan lain yang mempengahuri standar dalam penanganan insiden dan permintaan layanan yang mempengaruhi kepuasan pengguna. **Rate of change in the market in which the enterprise operates** Pengaruh perubahan permintaan pengguna yang terjadi pada saat pemenuhan permintaan layanan
24.	Pengguna tidak memberikan konfirmasi terkait status penutupan insiden	**Operating Model** *Helpdesk* dalam melakukan operasi layanan TI tidak sesuai dengan standar.	**Geopolitical environment** Terjadi masalah terkait service pada oracle database yang menyebabkan proses operasi layanan manajemen insiden dan pemenuhan permintaan layanan

No	Risiko	Faktor Risiko	
		Internal	**External**
25.	Pihak yang dieskalasi tidak memperbarui status mengenai insiden atau permintaan layanan yang ditangani	**Operating Model** *Helpdesk* dalam melakukan operasi layanan TI tidak sesuai dengan standar terutama pada saat melakukan eskalasi terkait permintaan layanan dan insiden. **Culture of the enterprise** Tidak terealisasikannya budaya organisasi tentang pemberian layanan yang berorientasi kepada kepuasan pengguna dimana pelapor tidak diberikan status terkait penanganan insiden.	**Regulatory environment** Tidak adanya peraturan yang jelas terkait pengawasan dalam pengelolaan permintaan layanan dan insiden **Technology Status and evolution** *Helpdesk* belum bisa memberikan dan menerima status laporan dalam waktu yang singkat melalui sistem informasi atau teknologi yang ada.
26.	*Helpdesk* tidak menginformasikan status insiden atau permintaan layanan TI kepada pengguna	**Culture of the enterprise** Tidak terealisasikannya budaya organisasi tentang pemberian layanan yang berorientasi kepada kepuasan pengguna dimana pelapor tidak	**Technology Status and evolution** *Helpdesk* belum bisa memberikan dan menerima status laporan dalam waktu yang singkat melalui sistem informasi atau teknologi yang ada.

No	Risiko	Faktor Risiko	
		Internal	**External**
		diberikan status terkait penanganan insiden.	
27.	Kegagalan dalam menerima laporan dari pengguna	**Complexity of IT** Sistem informasi *helpdesk* yang tidak bisa diakses dan kompleksnya sistem TI yang harus dipahami pengguna **Operating Model** Model operasi yang digunakan dalam pelaporan insiden atau layanan TI masih belum dikuasi oleh pengguna	**Threat Landscape** Ancaman serangan kepada sistem yang menyebabkan server down **Geopolitical environment** Terputusnya kabel LAN yang menyebabkan kerusakan pada perulatan jaringan **Technology Status and evolution** Diskpace pada database mencapai treshold
28.	Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi	**Operating Model** *Helpdesk* dalam melakukan operasi layanan TI tidak sesuai dengan standar terutama pada saat melakukan eskalasi terkait permintaan layanan dan insiden	**Threat Landscape** Ancaman serangan kepada sistem yang menyebabkan server down **Technology Status and evolution** Diskpace pada database mencapai treshold

6.2 Skenario Risiko

Skenario Risiko TI dibuat dalam tabel berdasarkan dua jenis skenario, yaitu skenario positif dan skenario risiko negatif yang menjelaskan dampak risiko bila terjadi secara teratur.

Skenario positif menunjukan proses bisnis yang terjadi secara optimal dan baik karena risiko tersebut tidak terjadi dan skenario negatif menunjukan hambatan yang dihadapi di dalam proses bisnis karena dampak dari terjadinya risiko. Berikut merupakan hasil dari pembuatan skenario (dampak) risiko yang terjadi di *helpdesk* unit TSI PDAM Surabaya yang disajikan pada Tabel 6.4.

Tabel 6. 4 Skenario Risiko

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	**Positif**
1.	IE1101	Kesalahan dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	*Helpdesk* kesulitan dalam melakukan penanganan terhadap laporan terkait insiden dan permintaan layanan yang masuk karena insiden tidak dapat dikategorikan dengan tepat.	*Helpdesk* dapat melakukan penanganan terhadap laporan terkait insiden dan permintaan layanan yang masuk dengan lancar sesuai dengan kategori yang tepat dari laporan tersebut.
2.	IE1302	Kesalahan dalam menentukan tipe permintaan layanan	Insiden dan permintaan layanan dieskalasi kepada pihak yang tidak tepat menyebabkan pengelolaan permintaan layanan tidak berjalan dengan lancar.	Insiden dan permintaan layanan dieskalasi kepada pihak yang tepat sehingga laporan dari pengguna bisa diselesaikan dengan tepat dan sesuai waktu yang telah disepakati
3.	IE1503	Kesalahan dalam memahami permintaan pengguna	Penanganan dan pengelolaan insiden atau permintaan	Pengguna merasa puas dengan hasil dari penanganan dan pengelolaan

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	Positif
			layanan yang dilaporkan pengguna dilakukan tidak sesuai harapan pengguna	isiden atau permintaan layanan yang telah dilakukan oleh *helpdesk*
4.	IE2304	Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan	Insiden dengan prioritas lebih tinggi tidak ditangani lebih dulu karena sistem prioritasi yang salah dimana tidak sesuai dengan kondisi perusahaan yang relevan	Penanangan insiden dengan prioritas lebih tinggi didahulukan karena memiliki urgensitas yang tinggi sehingga proses manajemen insiden dan pemenuhan permintaan layanan dapat diselesaikan dengan lancar.
5.	IE2305	Keterlambatan respon *helpdesk*	Proses bisnis layanan TI berjalan dengan lambat dan pengguna tidak mendapatkan kabar terkait status permasalahan yang telah mereka laporkan	Proses bisnis layanan TI dapat berjalan dengan lancar dan tepat waktu karena *helpdesk* melayani pengguna secara responsif
6.	IE4106	Kesalahan *helpdesk* dalam menentukan penyebab dari insiden	Solusi yang digunakan untuk menangani insiden tidak dapat digunakan yang menyebabkan insiden dapat	Insiden dapat diselesaikan sampai akar permasalahan yang membuat pengguna memiliki kepuasan yang

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	Positif
			terjadi lagi di waktu lain	baik terhadap layanan *helpdesk*
7.	IE4307	Kesalahan dalam memilih pihak yang menangani insiden	Proses eskalasi dilakukan kepada pihak yang tidak tepat menyebabkan pengelolaan permintaan layanan tidak berjalan dengan lancar.	Proses eskalasi dilakukan kepada pihak yang tepat sehingga insiden dapat diselesaikan dengan tepat waktu
8.	IE5108	Kegagalan dalam menangani insiden	Insiden ditangani lebih lama dari waktu yang sebelumnya sudah disepakati dan hasil dari penanganan insiden tidak memuaskan pengguna	Insiden dapat diselesaikan dengan solusi yang tepat sehingga insiden dapat diselesaikan tepat waktu dan meningkatkan kepuasan pengguna
9.	IE7309	Kesalahan pendefinisian tren dalam laporan	Insiden yang sering terjadi tidak ditanggapi secara serius oleh *helpdesk* yang menyebabkan masalah yang sama kembali terjadi	Insiden yang sering terjadi dapat dicari akar permasalahannya sehingga dapat mencegah masalah yang sama kembali terjadi
10.	IF3101	Penyalahgunaan hak akses oleh pengguna	Pencurian data dan informasi dapat dilakukan oleh pihak luar dan	Data dan informasi terkait perusahaan selalu aman dan tidak terjadinya

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	Positif
			disalahgunakan secara tidak bertanggung jawab	bocornya informasi kepada pihak luar.
11.	IS5101	Gangguan pada perangkat keras di unit TSI	Proses bisnis pada *helpdesk* menjadi terganggu karena perangkat keras yang digunakan mengalami masalah yang menyebabkan penyelesaian penanganan layanan insiden dan pemenuhan permintaan layanan menjadi terganggu	Operasi layanan terjadi dengan baik dan semua perangkat keras berfungsi dengan baik sehingga *helpdesk* dapat menyelesaikan penanganan layanan insiden dan pemenuhan permintaan layanan dengan baik tanpa adanya masalah.
12.	LA7401	Gangguan terhadap server dan jaringan perusahaan	*Helpdesk* tidak dapat mengakses sistem informasi *helpdesk* ataupun database sehingga proses manajemen insiden dan pemenuhan layanan TI yang ada di *helpdesk* menjadi terkendala dan tidak dapat diselesaikan tepat waktu	*Helpdesk* dapat melakukan semua kegiatan manajemen insiden dan pemenuhan permintaan layanan secara lancar dengan kondisi jaringan dan sistem informasi yang sabil

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	Positif
13.	RC3301	Pengelolaan pemenuhan permintaan dilakukan secara tidak konsisten	*Helpdesk* memiliki kesulitan untuk melakukan pemenuhan permintaan layanan karena tidak adanya prosedur khusus terkait operasi layanan	Proses pengelolaan permintaan dilakukan dengan baik karena mengatur kepada prosedur yang sudah ada
14.	SO1401	Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	Pihak yang dieskalasi tidak mengetahui apa yang harus dilakukan saat ada insiden yang dieskalasikan sehingga pelayanan manajemen insiden dan pemenuhan permintaan layanan yang dilakukan oleh *helpdesk* menjadi terganggu	Pihak yang dieskalasi memahami apa yang perlu dilakukan setelah ada insiden yang dieskalasi sehingga insiden dapat diselesaikan secara tepat waktu
15.	SO2102	Tidak adanya log insiden atau permintaan layanan TI	Proses penangan insiden atau permintaan layanan TI yang masuk tidak dapat dilakukan dengan prosedur yang ada karena laporan tidak tercatat yang	Proses penangan insiden atau permintaan layanan TI dapat berjalan dengan baik serta dokumentasi dari laporan permintaan dapat

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	**Positif**
			memungkinkan permintaan layanan atau insiden tidak terselesaikan.	disimpat dalam direktori khusus.
16.	SO2203	Menumpuknya permintaan layanan yang masuk	Tidak semua perminaan layanan atau insiden dapat diselesaikan dengan tepat waktu karena harus dilakukan prioritasi terlebih dahulu layanan mana yang harus dikerjakan terlebih dahulu oleh *helpdesk*	Permintaan layanan atau insiden dapat diselesaikan dengan tepat waktu dan pendokumentasian yang baik dari laporan penanganan insiden atau permintaan layanan
17.	SO3204	Helpdesk tidak mendapatkan persetujuan finansial atau fungsional	Penangan insiden dan permintaan layanan melebihi batas waktu yang telah disepakati sebelumnya karena *helpdesk* terlambat mendapatkan persetujuan finansial ataupun fungsional yang menyebabkan kepuasan pelanggan menurun	Penanganan insiden dan permintaan layanan dapat diselesaikan dengan baik karena *helpdesk* mendapatkan persetujuan finansial dan fungsional.

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	Positif
18.	SO4205	Terjadinya pengulangan pencatatan untuk insiden yang sama	Laporan insiden atau permintaan layanan memiliki duplikat sehingga pihak yang dieskalasi akan menerima dua laporan insiden yang sama	Laporan insiden atau permintaan layanan terdokumentasi dengan baik dan disimpan dalam direktori khusus
19.	SO4306	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan	Penurunan kepuasan dari pengguna karena insiden yang mereka laporkan diselesaikan dalam waktu yang melebihi kesepakatan sebelumnya	Semua insiden atau permintaan layanan diselesaikan tepat waktu dan proses bisnis dapat berjalan dengan baik
20.	SO5207	Tidak adanya pencatatan terkait solusi penanganan insiden	Tidak dapat dilakukannya penanganan insiden karena kesalahan dalam prosedur yang ada dalam penanganan insiden	Semua insiden atau permintaan layanan dapat dilakukan dengan prosuder yang ada sehingga proses layanan manajemen insiden atau permintaan layanan TI dapat diselesaikan dengan baik tanpa adanya masalah
21.	SO5308	Penanganan insiden melebihi batas waktu yang disepakati	Banyaknya pengguna yang merasa kecewa dengan layanan	Semua insiden atau permintaan layanaan diselesaikan

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	**Positif**
			helpdesk karena aksi pemulihan tidak dilaksanakan dengan sesegera mungkin.	secara tepat waktu yang menyebabkan peningkatan kepuasan pengguna terkait layanan yang diberikan oleh *helpdesk*
22.	SO5409	Insiden dan layanan permintaan yang tidak terdokumentasi dengan lengkap	Tidak adanya bukti dari penanganan insiden dan layanan permintaan yang sudah terdokumentasi sehingga tidak dapat dilakukan analisis tren insiden dan permintaan layanan.	Dokumentasi dari penanganan insiden dan pemenuhan permintaan layanan disimpan dalam direktori khusus dan dapat dilakukan analisis tren terkait insiden dan permintaan layanan.
23.	SO6110	Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna	Pengguna tidak merasa puas dengan layanan yang diberikan oleh *helpdesk* terkait penanganan insiden atau permintaan layanan TI yang dilaporkannya	Pengguna merasa puas dengan kinerja dari *helpdesk* karena sesuai dengan harapan pengguna sehingga dapat meningkatkan kepuasan pengguna terkait layanan manajemen insiden dan permintaan layanan TI pada *helpdesk*.

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	Positif
24.	SO6211	Pengguna tidak memberikan konfirmasi terkait status penutupan insiden	Penutupan insiden akan dilakukan tanpa meminta konfirmasi dari pelapor terkait status selesainya permasalahan yang sebelumnya telah dilaporkan	Penutupan insiden disetujui oleh pelapor dan akan ditutup oleh *helpdesk* setelah meminta feedback kepada pengguna terkait layanan manajemen insiden atau permintaan layanan yang telah diselesaikan
25.	SO7112	Pihak yang dieskalasi tidak memperbarui status mengenai insiden atau permintaan layanan yang ditangani	*Helpdesk* tidak mengetahui status dari pemintaan layanan dan insiden yang sedang ditangani oleh pihak yang dieskalasi karena pihak yang dieskalasi belum atau tidak meberikan kabar terkait insiden atau permintaan layanan yang sedang ditangani	*Helpdesk* dan pengguna mengetahui status dari insiden atau permintaan layanan yang dieskalasi
26.	SO7213	*Helpdesk* tidak menginformasikan status insiden atau permintaan layanan TI kepada pengguna	*Helpdesk* tidak memberikan status kepada pengguna terkait pemintaan layanan dan insiden yang menyebabkan	Pengguna mengetahui status dari laporan yang sebelumnya dia buat dan meningkatnya tingkat kepuasan pengguna

No	Risk ID	Risiko	Skenario Risiko	
			Negatif	**Positif**
			pengguna harus bertanya kembali kepada *helpdesk* terkait status penangan permintaan layanan dan insiden	terhadap layanan *helpdesk*
27.	SW1201	Kegagalan dalam menerima laporan dari pengguna	Sistem informasi *helpdesk* sedang down dan tidak ada laporan yang masuk mengenai permintaan layanan manajemen insiden dan pemenuhan permintaan layanan TI	Sistem informasi *helpdesk* berfungsi dengan baik dan semua permintaan layanan terkait manajemen insiden dan pemenuhan permintaan layanan TI dapat ditangani dengan baik oleh *helpdesk*
28.	SW7101	Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi	Insiden dan permintaan layanan TI yang ada tidak terselesaikan karena tidak ada laporan permintaan penanganan insiden dan permintaan yang masuk kepada pihak yang dieskalasi	Proses operasi layanan berjalan dengan baik dan meningkatnya kepuasan dari pengguna terhadap layanan *helpdesk*.

6.3 Pemetaan Pernyataan Kuisioner dengan Risiko

Pernyataan kuisioner dibuat untuk mewakili dampak dari risiko (skenario risiko) yang dapat muncul untuk mengetahui sejauh mana penurunan kepuasan pelanggan yang terjadi. Pernyataan dikelompokan kepada risiko yang memiliki dampak yang sama atau memiliki banyak kesamaan. Berikut merupakan hasil dari pemetaan risiko yang terjadi di *helpdesk* unit TSI PDAM Surabaya dengan pernyataan pada kuisioner yang disajikan pada Tabel 6.5.

Tabel 6. 5 Pemetaan Pernyataan kuisioner dengan dampak risiko

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	Positif
1.	Saat *helpdesk* tidak memenuhi permintaan layanan dan menangani keluhan sesuai harapan saya, maka kepuasan saya mengalami:	Kesalahan dalam memahami permintaan pengguna	Penanganan dan pengelolaan insiden atau permintaan layanan yang dilaporkan pengguna dilakukan tidak sesuai harapan pengguna	Pengguna merasa puas dengan hasil dari penanganan dan pengelolaan isiden atau permintaan layanan yang telah dilakukan oleh *helpdesk*
		Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan	Insiden dengan prioritas lebih tinggi tidak ditangani lebih dulu karena sistem prioritasi yang salah dimana tidak sesuai dengan kondisi perusahaan yang relevan	Penanangan insiden dengan prioritas lebih tinggi didahulukan karena memiliki urgensitas yang tinggi sehingga proses manajemen insiden dan pemenuhan permintaan layanan dapat diselesaikan dengan lancar.

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	Positif
		Tidak adanya pencatatan terkait solusi penanganan insiden	Tidak dapat dilakukannya penanganan insiden karena kesalahan dalam prosedur yang ada dalam penanganan insiden	Semua insiden atau permintaan layanan dapat dilakukan dengan prosuder yang ada sehingga proses layanan manajemen insiden atau permintaan layanan TI dapat diselesaikan dengan baik tanpa adanya masalah
		Kesalahan dalam memilih pihak yang menangani insiden	Proses eskalasi dilakukan kepada pihak yang tidak tepat menyebabkan pengelolaan permintaan layanan tidak berjalan dengan lancar.	Proses eskalasi dilakukan kepada pihak yang tepat sehingga insiden dapat diselesaikan dengan tepat waktu
		Kesalahan dalam menentukan tipe permintaan layanan	Insiden dan permintaan layanan dieskalasi kepada pihak yang tidak tepat menyebabkan pengelolaan permintaan layanan tidak berjalan dengan lancar.	Insiden dan permintaan layanan dieskalasi kepada pihak yang tepat sehingga laporan dari pengguna bisa diselesaikan dengan tepat dan sesuai waktu yang telah disepakati

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	Positif
2.	Saat *helpdesk* terlambat dalam melakukan respon terhadap laporan saya, maka kepuasan saya mengalami:	Keterlambatan respon *helpdesk*	Proses bisnis layanan TI berjalan dengan lambat dan pengguna tidak mendapatkan kabar terkait status permasalahan yang telah mereka laporkan	Proses bisnis layanan TI dapat berjalan dengan lancar dan tepat waktu karena *helpdesk* melayani pengguna secara responsif
		Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan	Penurunan kepuasan dari pengguna karena insiden yang mereka laporkan diselesaikan dalam waktu yang melebihi kesepakatan sebelumnya	Semua insiden atau permintaan layanan diselesaikan tepat waktu dan proses bisnis dapat berjalan dengan baik
		Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	Pihak yang dieskalasi tidak mengetahui apa yang harus dilakukan saat ada insiden yang dieskalasikan sehingga pelayanan manajemen insiden dan pemenuhan permintaan layanan yang dilakukan oleh	Pihak yang dieskalasi memahami apa yang perlu dilakukan setelah ada insiden yang dieskalasi sehingga insiden dapat diselesaikan secara tepat waktu

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	**Positif**
			helpdesk menjadi terganggu	
		Kegagalan dalam menangani insiden	Insiden ditangani lebih lama dari waktu yang sebelumnya sudah disepakati dan hasil dari penanganan insiden tidak memuaskan pengguna	Insiden dapat diselesaikan dengan solusi yang tepat sehingga insiden dapat diselesaikan tepat waktu dan meningkatkan kepuasan pengguna
3.	Saat *helpdesk* mengabaikan laporan yang saya berikan, maka kepuasan saya mengalami:	Tidak adanya log insiden atau permintaan layanan TI	Proses penangan insiden atau permintaan layanan TI yang masuk tidak dapat dilakukan dengan prosedur yang ada karena laporan tidak tercatat yang memungkinkan permintaan layanan atau insiden tidak terselesaikan.	Proses penangan insiden atau permintaan layanan TI dapat berjalan dengan baik serta dokumentasi dari laporan permintaan dapat disimpat dalam direktori khusus.
		Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi	Insiden dan permintaan layanan TI yang ada tidak terselesaikan karena tidak	Proses operasi layanan berjalan dengan baik dan meningkatnya kepuasan dari pengguna

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	**Positif**
			ada laporan permintaan penanganan insiden dan permintaan yang masuk kepada pihak yang dieskalasi	terhadap layanan *helpdesk*.
4.	Saat *helpdesk* selesai menangani laporan saya melebihi batas waktu yang dijanjikan, maka kepuasan saya mengalami:	Kesalahan dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	*Helpdesk* kesulitan dalam melakukan penanganan terhadap laporan terkait insiden dan permintaan layanan yang masuk karena insiden tidak dapat dikategorikan dengan tepat.	*Helpdesk* dapat melakukan penanganan terhadap laporan terkait insiden dan permintaan layanan yang masuk dengan lancar sesuai dengan kategori yang tepat dari laporan tersebut.
		Penanganan insiden melebihi batas waktu yang disepakati	Banyaknya pengguna yang merasa kecewa dengan layanan *helpdesk* karena aksi pemulihan tidak dilaksanakan dengan sesegera mungkin.	Semua insiden atau permintaan layanaan diselesaikan secara tepat waktu yang menyebabkan peningkatan kepuasan pengguna terkait layanan yang diberikan oleh *helpdesk*

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	Positif
		Helpdesk tidak mendapatkan persetujuan finansial atau fungsional	Penangan insiden dan permintaan layanan melebihi batas waktu yang telah disepakati sebelumnya karena *helpdesk* terlambat mendapatkan persetujuan finansial ataupun fungsional yang menyebabkan kepuasan pelanggan menurun	Penanganan insiden dan permintaan layanan dapat diselesaikan dengan baik karena *helpdesk* mendapatkan persetujuan finansial dan fungsional.
5.	Saat *helpdesk* tidak melakukan verifikasi untuk memastikan bahwa laporan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami:	Pengguna tidak memberikan konfirmasi terkait status penutupan insiden	Penutupan insiden akan dilakukan tanpa meminta konfirmasi dari pelapor terkait status selesainya permasalahan yang sebelumnya telah dilaporkan	Penutupan insiden disetujui oleh pelapor dan akan ditutup oleh *helpdesk* setelah meminta feedback kepada pengguna terkait layanan manajemen insiden atau permintaan layanan yang telah diselesaikan
		Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna	Pengguna tidak merasa puas dengan layanan yang diberikan oleh	Pengguna merasa puas dengan kinerja dari *helpdesk* karena sesuai dengan

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	**Positif**
			helpdesk terkait penanganan insiden atau permintaan layanan TI yang dilaporkannya	harapan pengguna sehingga dapat meningkatkan kepuasan pengguna terkait layanan manajemen insiden dan permintaan layanan TI pada *helpdesk*.
6.	Saat *helpdesk* tidak memberikan status mengenai laporan saya (sedang dikerjakan/selesai), maka kepuasan saya mengalami:	*Helpdesk* tidak menginformasikan status insiden atau permintaan layanan TI kepada pengguna	*Helpdesk* tidak memberikan status kepada pengguna terkait pemintaan layanan dan insiden yang menyebabkan pengguna harus bertanya kembali kepada *helpdesk* terkait status penangan permintaan layanan dan insiden	Pengguna mengetahui status dari laporan yang sebelumnya dia buat dan meningkatnya tingkat kepuasan pengguna terhadap layanan *helpdesk*
		Pihak yang dieskalasi tidak memperbarui status mengenai insiden atau permintaan layanan yang ditangani	*Helpdesk* tidak mengetahui status dari pemintaan layanan dan insiden yang sedang ditangani oleh pihak yang dieskalasi	*Helpdesk* dan pengguna mengetahui status dari insiden atau permintaan layanan yang dieskalasi

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	**Positif**
			karena pihak yang dieskalasi belum atau tidak meberikan kabar terkait insiden atau permintaan layanan yang sedang ditangani	
7.	Saat *helpdesk* tidak menangani akar permasalahan dari permasalahan yang berulang kali saya keluhkan, maka kepuasan saya mengalami:	Insiden dan layanan permintaan yang tidak terdokumentasi dengan lengkap	Tidak adanya bukti dari penanganan insiden dan layanan permintaan yang sudah terdokumentasi sehingga tidak dapat dilakukan analisis tren insiden dan permintaan layanan.	Dokumentasi dari penanganan insiden dan pemenuhan permintaan layanan disimpan dalam direktori khusus dan dapat dilakukan analisis tren terkait insiden dan permintaan layanan.
		Kesalahan pendefinisian tren dalam laporan	Insiden yang sering terjadi tidak ditanggapi secara serius oleh *helpdesk* yang menyebabkan masalah yang sama kembali terjadi	Insiden yang sering terjadi dapat dicari akar permasalahannya sehingga dapat mencegah masalah yang sama kembali terjadi

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	Positif
		Kesalahan *helpdesk* dalam menentukan penyebab dari insiden	Solusi yang digunakan untuk menangani insiden tidak dapat digunakan yang menyebabkan insiden dapat terjadi lagi di waktu lain	Insiden dapat diselesaikan sampai akar permasalahan yang membuat pengguna memiliki kepuasan yang baik terhadap layanan *helpdesk*
8.	Saat layanan pelaporan keluhan dan permintaan pada *helpdesk* tidak mengalami peningkatan, maka kepuasan saya mengalami:	Menumpuknya permintaan layanan yang masuk	Tidak semua perminaan layanan atau insiden dapat diselesaikan dengan tepat waktu karena harus dilakukan prioritasi terlebih dahulu layanan mana yang harus dikerjakan terlebih dahulu oleh *helpdesk*	Permintaan layanan atau insiden dapat diselesaikan dengan tepat waktu dan pendokumentasian yang baik dari laporan penanganan insiden atau permintaan layanan
		Terjadinya pengulangan pencatatan untuk insiden yang sama	Laporan insiden atau permintaan layanan memiliki duplikat sehingga pihak yang dieskalasi akan menerima dua laporan insiden yang sama	Laporan insiden atau permintaan layanan terdokumentasi dengan baik dan disimpan dalam direktori khusus

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	Positif
		Pengelolaan pemenuhan permintaan dilakukan secara tidak konsisten	*Helpdesk* memiliki kesulitan untuk melakukan pemenuhan permintaan layanan karena tidak adanya prosedur khusus terkait operasi layanan	Proses pengelolaan permintaan dilakukan dengan baik karena mengatur kepada prosedur yang sudah ada
9.	Saat saya tidak dapat melakukan pelaporan keluhan dan permintaan kepada *helpdesk* (kesalahan teknis), maka kepuasan saya mengalami:	Kegagalan dalam menerima laporan dari pengguna	Sistem informasi *helpdesk* sedang down dan tidak ada laporan yang masuk mengenai permintaan layanan manajemen insiden dan pemenuhan permintaan layanan TI	Sistem informasi *helpdesk* berfungsi dengan baik dan semua permintaan layanan terkait manajemen insiden dan pemenuhan permintaan layanan TI dapat ditangani dengan baik oleh *helpdesk*
		Gangguan pada perangkat keras di unit TSI	Proses bisnis pada *helpdesk* menjadi terganggu karena perangkat keras yang digunakan mengalami masalah yang menyebabkan penyelesaian penanganan	Operasi layanan terjadi dengan baik dan semua perangkat keras berfungsi dengan baik sehingga *helpdesk* dapat menyelesaikan penanganan layanan insiden dan pemenuhan permintaan layanan dengan

No	Pernyataan	Risiko	Skenario Risiko	
			Negatif	**Positif**
			layanan insiden dan pemenuhan permintaan layanan menjadi terganggu	baik tanpa adanya masalah.
10.	Saat keamanan informasi dari laporan keluhan dan permintaan tidak terlindungi, maka kepuasan saya mengalami:	Penyalahgunaan hak akses oleh pengguna	Pencurian data dan informasi dapat dilakukan oleh pihak luar dan disalahgunakan secara tidak bertanggung jawab	Data dan informasi terkait perusahaan selalu aman dan tidak terjadinya bocornya informasi kepada pihak luar.
		Gangguan terhadap server dan jaringan perusahaan	*Helpdesk* tidak dapat mengakses sistem informasi *helpdesk* ataupun database sehingga proses manajemen insiden dan pemenuhan layanan TI yang ada di *helpdesk* menjadi terkendala dan tidak dapat diselesaikan tepat waktu	*Helpdesk* dapat melakukan semua kegiatan manajemen insiden dan pemenuhan permintaan layanan secara lancar dengan kondisi jaringan dan sistem informasi yang sabil

6.4 Penilaian Risiko

Dalam tahap ini dilakukan penilaian risiko terhadap risiko yang telah dianalisis, penilaian risiko dilakukan berdasarkan perkiraan nilai frekuensi dan dampak risiko terkait dengan skenario risiko TI. Nilai frekuensi didapatkan dari hasil wawancara, sedangkan untuk nilai dampak didapatkan dari survei mengenai penurunan kepuasan pengguna layanan untuk keunggulan kompetetif, sedangkan untuk penentuan nilai dari produktivitas biaya tanggapan dan hukum didapatkan dari hasil wawancara. Hasil Survei secara detail dapat dilihat pada Lampiran E.

Penilaian ini akan digunakan untuk menentukan tingkat level dari sebuah risiko berdasarkan matriks frekuensi dan magnitude risiko. Berikut merupakan hasil dari penilaian risiko yang terjadi di *helpdesk* unit TSI PDAM Surabaya yang disajikan pada Tabel 6.6

Tabel 6. 6 Penilaian Risiko

No	Risk ID	Risiko	Nilai Dampak					Nilai Frekuensi	Level Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Rata-Rata nilai Dampak		
1.	IE1101	Kesalahan dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	1	1	3	1	1.5	1	*Low*
2.	IE1302	Kesalahan dalam menentukan tipe permintaan layanan	1	1	3	1	1.5	2	*Medium*
3.	IE1503	Kesalahan dalam memahami permintaan pengguna	1	1	3	1	1.5	3	*Medium*

No	Risk ID	Risiko	Nilai Dampak					Nilai Frekuensi	Level Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Rata-Rata nilai Dampak		
4.	IE2304	Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan	1	1	3	1	1.5	4	*High*
5.	IE2305	Keterlambatan respon *helpdesk*	1	1	3	1	1.5	2	*Medium*
6.	IE4106	Kesalahan *helpdesk* dalam menentukan penyebab dari insiden	1	1	3	1	1.5	3	*Medium*
7.	IE4307	Kesalahan dalam memilih pihak yang menangani insiden	1	1	3	1	1.5	1	*Low*
8.	IE5108	Kegagalan dalam menangani insiden	1	1	3	1	1.5	2	*Medium*
9.	IE7309	Kesalahan pendefinisian tren dalam laporan	1	1	3	1	1.5	3	*Medium*
10.	IF3101	Penyalahgunaan hak akses oleh pengguna	1	1	4	3	2.25	1	*Medium*
11.	IS5101	Gangguan pada perangkat keras di unit TSI	2	2	3	1	2	4	*High*
12.	LA7401	Gangguan terhadap server dan jaringan perusahaan	1	3	4	1	2.25	2	*Medium*
13.	RC3301	Pengelolaan pemenuhan permintaan dilakukan secara tidak konsisten	1	1	3	1	1.5	1	*Low*
14.	SO1401	Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	1	1	3	1	1.5	1	*Low*
15.	SO2102	Tidak adanya log insiden atau permintaan layanan TI	1	1	3	1	1.5	1	*Low*

No	Risk ID	Risiko	Nilai Dampak					Nilai Frekuensi	Level Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Rata-Rata nilai Dampak		
16.	SO2203	Menumpuknya permintaan layanan yang masuk	1	1	3	1	1.5	1	*Low*
17.	SO3204	Helpdesk tidak mendapatkan persetujuan finansial atau fungsional	1	1	3	1	1.5	3	*Medium*
18.	SO4205	Terjadinya pengulangan pencatatan untuk insiden yang sama	1	1	3	1	1.5	1	*Low*
19.	SO4306	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan	1	1	3	1	1.5	3	*Medium*
20.	SO5207	Tidak adanya pencatatan terkait solusi penanganan insiden	1	1	3.	1	1.5	2	*Medium*
21.	SO5308	Penanganan insiden melebihi batas waktu yang disepakati	1	1	3	1	1.5	3	*Medium*
22.	SO5409	Insiden dan layanan permintaan yang tidak terdokumentasi dengan lengkap	1	1	3	1	1.5	1	*Low*
23.	SO6110	Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna	1	1	3	1	1.5	4	*High*
24.	SO6211	Pengguna tidak memberikan konfirmasi terkait status penutupan insiden	1	1	3	1	1.5	3	*Medium*
25.	SO7112	Pihak yang dieskalasi tidak memperbarui status mengenai insiden	1	1	3	1	1.5	2	*Medium*

No	Risk ID	Risiko	Nilai Dampak					Nilai Frekuensi	Level Risiko
			Produktivitas	Biaya Tanggapan	Keunggulan Kompetitif	Hukum	Rata-Rata nilai Dampak		
		atau permintaan layanan yang ditangani							
26.	SO7213	*Helpdesk* tidak menginformasikan status insiden atau permintaan layanan TI kepada pengguna	1	1	3	1	1.5	1	*Low*
27.	SW1201	Kegagalan dalam menerima laporan dari pengguna	1	1	3	1	1.5	1	*Low*
28.	SW7101	Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi	1	1	3	1	1.5	3	*Medium*

6.5 Penentuan Respon Risiko

Penentuan respon risiko dilakukan setelah melakukan penilaian risiko. Respon yang dipilih berdasarkan respon risiko yang ada pada COBIT 5 yaitu risk acceptance (menerima), mitigation (mitigasi), avoidance (menghindari) dan share/transfer (mengalihkan). Berikut merupakan hasil dari penentutan respon risiko pada *helpdesk* unit TSI PDAM Surabaya yang disajikan pada Tabel 6.7

Tabel 6. 7 Respon Risiko

Risk ID	Kategori Risiko	Risiko	Respon Risiko
IE1101	IT expertise and skill	Kesalahan dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	*Mitigate*
IE1302		Kesalahan dalam menentukan tipe permintaan layanan	*Mitigate*

Risk ID	Kategori Risiko	Risiko	Respon Risiko
IE1503		Kesalahan dalam memahami permintaan pengguna	*Mitigate*
IE2304		Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan	*Mitigate*
IE2305		Keterlambatan respon *helpdesk*	*Mitigate*
IE4106		Kesalahan *helpdesk* dalam menentukan penyebab dari insiden	*Mitigate*
IE4307		Kesalahan dalam memilih pihak yang menangani insiden	*Avoid*
IE5108		Kegagalan dalam menangani insiden	*Mitigate*
IE7309		Kesalahan pendefinisian tren dalam laporan	*Mitigate*
IF3101	Information	Penyalahgunaan hak akses oleh pengguna	*Mitigate*
IS5101	Infrastucture	Gangguan pada perangkat keras di unit TSI	*Transfer*
LA7401	Logical Attack	Gangguan terhadap server dan jaringan perusahaan	*Transfer*
RC3301	Regulatory Compliance	Pengelolaan pemenuhan permintaan dilakukan secara tidak konsisten	*Mitigate*
SO1401	Staff Operation	Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	*Avoid*
SO2102		Tidak adanya log insiden atau permintaan layanan TI	*Mitigate*
SO2203		Menumpuknya permintaan layanan yang masuk	*Mitigate*
SO3204		Helpdesk tidak mendapatkan persetujuan finansial atau fungsional	*Mitigate*
SO4205		Terjadinya pengulangan pencatatan untuk insiden yang sama	*Mitigate*
SO4306		Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan	*Mitigate*

Risk ID	Kategori Risiko	Risiko	Respon Risiko
SO5207		Tidak adanya pencatatan terkait solusi penanganan insiden	*Mitigate*
SO5308		Penanganan insiden melebihi batas waktu yang disepakati	*Mitigate*
SO5409		Insiden dan layanan permintaan yang tidak terdokumentasi dengan lengkap	*Mitigate*
SO6110		Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna	*Mitigate*
SO6211		Pengguna tidak memberikan konfirmasi terkait status penutupan insiden	*Accept*
SO7112		Pihak yang dieskalasi tidak memperbarui status mengenai insiden atau permintaan layanan yang ditangani	*Mitigate*
SO7213		*Helpdesk* tidak menginformasikan status insiden atau permintaan layanan TI kepada pengguna	*Avoid*
SW1201	Software	Kegagalan dalam menerima laporan dari pengguna	*Mitigate*
SW7101		Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi	*Transfer*

6.6 Mitigasi Risiko

Mitigasi risiko ditentukan berdasarkan proses pada COBIT 5 yang relevan untuk menangani risiko dan kemudian dari subdomain proses tersebut diambil aktivitas yang dirasa sesuai untuk menjadi langkah mitigasi. Berikut merupakan hasil dari penentutan langkah mitigasi risiko pada *helpdesk* unit TSI PDAM Surabaya yang disajikan pada Tabel 6.8.

Tabel 6. 8 Mitigasi risiko

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
1	IE1101	Kesalahan dalam pembuatan sistem klasifikasi insiden atau permintaan layanan	*IT expertise and skill*	*Low*	APO07-Manage Human Resource	APO07.04 Evaluate employee job performance – melakukan evaluasi bagi para individu terkait kinerja. Evaluasi dilakukan secara teratur untuk melihat keterampilan dan kompetensi pegawai untuk mencapai tujuan organisasi.	Melakukan evaluasi terkait kinerja secara berkala dan memberikan balik kepada tiap individu untuk lebih berkembang demi mencapai tujuan organisasi
2	IE4307	Kesalahan dalam memilih pihak yang menangani insiden	*IT expertise and skill*	*Low*	DSS01-Manage Operations	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal	Memastikan semua data yang dibutuhkan untuk memproses insiden atau permintaan layanan secara benar sudah tersedia

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
3	RC3301	Pengelolaan pemenuhan permintaan dilakukan secara tidak konsisten	*Regulatory Compliance*	*Low*	DSS01-Manage Operations	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal	Menyusun dan memelihara kebijakan prosedur operasional terkait pengelolaan insiden dan permintaan layanan
4	SO1401	Pihak yang melakukan eskalasi tidak mengetahui prosedur eskalasi insiden	*Staff Operation*	*Low*	DSS01-Manage Operations	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal	Melakukan evaluasi secara teratur terkait impementasi penerapan kebijakan dan prosedur di perusahaan

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
5	SO2102	Tidak adanya log insiden atau permintaan layanan TI	*Staff Operation*	*Low*	DSS01-Manage Operations	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal	Melakukan implementasi kebijakan dan prosedur dalam pengelolaan layanan untuk menunjang proses bisnis
6	SO2203	Menumpuknya permintaan layanan yang masuk	*Staff Operation*	*Low*	DSS01-Manage Operations APO11-Manage Quality	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal APO11.04 Perform Quality monitoring, control and review – melakukan control review dan monitoring terhadap	Melakukan evaluasi secara teratur terkait impementasi penerapan kebijakan dan prosedur di perusahaan Melaksanakan kegiatan pelayanan sesuai prosedur dan kebijakan yang ada untuk menghasilkan pelayanan yang konsisten dan efektif

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
						kulitas proses layanan untuk memantau kepuasan pelanggan sesuai dengan Quality Standard Management	
7	SO4205	Terjadinya pengulangan pencatatan untuk insiden yang sama	*Staff Operation*	*Low*	DSS01-Manage Operations	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal	Menyusun dan memelihara kebijakan prosedur operasional terkait pengelolaan insiden dan permintaan layanan
8	SO5409	Insiden dan layanan permintaan yang tidak terdokumentasi dengan lengkap	*Staff Operation*	*Low*	DSS01-Manage Operations APO11-Manage Quality	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara	Menyusun dan memelihara kebijakan prosedur operasional terkait pengelolaan insiden dan permintaan layanan Melaksanakan kegiatan pelayanan sesuai

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
						konsisten dan andal APO11.04 Perform Quality monitoring, control and review – melakukan control review dan monitoring terhadap kulitas proses layanan untuk memantau kepuasan pelanggan sesuai dengan Quality Standard Management	prosedur dan kebijakan yang ada untuk menghasilkan pelayanan yang konsisten dan efektif
9	SO7213	*Helpdesk* tidak menginformasikan status insiden atau permintaan layanan TI kepada pengguna	*Staff Operation*	*Low*	APO11-Manage Quality	APO11.03 Focus quality management on customer – memfokuskan manajemen kualitas dari layanan dengan kebutuhan pelanggan dan quality management practice yang bertujuan untuk meningkatkan kepuasan pelanggan	Memberikan informasi dan menjaga komunikasi dengan pengguna terkait status laporan yang dilaporkan

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
10	SW1201	Kegagalan dalam menerima laporan dari pengguna	*Software*	*Low*	BAI09 – Manage Assets	BAI09.02 Manage critical assets – Melakukan identifikasi terkait aset-aset yang mendukung proses operasi layanan dan menjaga ketersediaan aset untuk mendukung proses bisnis tersebut	Melakukan penjadwalan maintance untuk menjaga performa sistem Mempersiapkan penggantian jika terjadi kerusakan terkait aset
11	IE1302	Kesalahan dalam menentukan tipe permintaan layanan	*IT expertise and skill*	*Medium*	APO07-Manage Human Resource	APO07.04 Evaluate employee job performance – melakukan evaluasi bagi para individu terkait kinerja. Evaluasi dilakukan secara teratur untuk melihat keterampilan dan kompetensi pegawai untuk mencapai tujuan organisasi.	Melakukan pengembangan performance improvement plan berdasarkan hasil dari kebutuhan training, peningkatan keterampilan SDM dan juga evaluasi

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
12	IE1503	Kesalahan dalam memahami permintaan pengguna	*IT expertise and skill*	*Medium*	BAI02-Manage Requirement Definition	BAI02.01 Define and maintain business functional and technical requirements – Melakukan identifikasi, prioritasi dan spesifikasi informasi yang diperlukan untuk mencapai hasil yang diharapkan dari solusi bisnis	Melakukan validasi terkait kebutuhan yang dibutuhkan untuk pemenuhan layanan Melakukan user acceptance test yang sudah terdokumentasi
13	IE2305	Keterlambatan respon *helpdesk*	*IT expertise and skill*	*Medium*	APO11-Manage Quality	APO11.03 Focus quality management on customer – memfokuskan manajemen kualitas dari layanan dengan kebutuhan pelanggan dan quality management practice yang bertujuan untuk meningkatkan kepuasan pelanggan	Menerapkan standar dalam manajemen kualitas Menjaga stabilisasi respon

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
14	IE4106	Kesalahan *helpdesk* dalam menentukan penyebab dari insiden	*IT expertise and skill*	*Medium*	APO07-Manage Human Resource	APO07.03 Maintain the skills and competencies of personnel – Mendefinisikan sekaligus mengelola keterampilan dan kompetensi yang dibutuhkan oleh tiap personil	Mengadakan review terkait pengembangan skill dan kompetensi terkait manajemen internal dan eksternal Melakukan review succession planning
15	IE5108	Kegagalan dalam menangani insiden	*IT expertise and skill*	*Medium*	APO07-Manage Human Resource	APO07.03 Maintain the skills and competencies of personnel – Mendefinisikan sekaligus mengelola keterampilan dan kompetensi yang dibutuhkan oleh tiap personil	Memberikan akses ke repositori sumber informasi untuk mendukung pengembangan skill dan kompetensi
16	IE7309	Kesalahan pendefinisian tren dalam laporan	*IT expertise and skill*	*Medium*	APO07-Manage Human Resource	APO07.03 Maintain the skills and competencies of personnel – Mendefinisikan sekaligus mengelola keterampilan dan kompetensi yang dibutuhkan oleh tiap personil	Melakukan identifikasi terkait gap antara skill yang dibutuhkan dengan skill yang tersedia saat ini di organisasi untuk dapat mengadakan pelatihan terkait skill

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
							dan kompetensi
17	IF3101	Penyalahgunaan hak akses oleh pengguna	*Information*	*Medium*	DSS05-Manage Security Services	DSS05.04 Manage user identity and logical access – Memastikan bahwa pengguna mempunyai hak akses terkait informasi sesuai dengan kebutuhan bisnisnya	Melakukan otentikasi kepada semua pengguna yang ingin mengakses aset informasi Melakukan review manajemen secara berkala terkait akun dan hak akses yang dimiliki
18	LA7401	Gangguan terhadap server dan jaringan perusahaan	*Logical Attack*	*Medium*	DSS05-Manage Security Services	DSS05.07 Monitor the infrastructure for security-related events – memonitor infrastuktur terkait akses tidak sah dan melakukan manajemen isniden	Melakukan review secara berkala terhadap log kejadian untuk insiden yang mungkin muncul Mendefinisikan prosedur jika terjadi insiden terkait keamanan

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
19	SO3204	Helpdesk tidak mendapatkan persetujuan finansial atau fungsional	*Staff Operation*	*Medium*	DSS01-Manage Operations APO11-Manage Quality	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal APO11.04 Perform Quality monitoring, control and review – melakukan control review dan monitoring terhadap kulitas proses layanan untuk memantau kepuasan pelanggan sesuai dengan Quality Standard Management	Melakukan evaluasi secara teratur terkait impementasi penerapan kebijakan dan prosedur di perusahaan Mengidentifikasi kebutuhan terkait penanganan insiden atau pemenuhan permintaan TI yang dilaporkan oleh pengguna

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
20	SO4306	Pihak yang dieskalasi mengabaikan insiden atau permintaan layanan	*Staff Operation*	*Medium*	APO11-Manage Quality	APO11.04 Perform Quality monitoring, control and review – melakukan control review dan monitoring terhadap kulitas proses layanan untuk memantau kepuasan pelanggan sesuai dengan Quality Standard Management	Melaksanakan kegiatan pelayanan sesuai prosedur dan kebijakan yang ada untuk menghasilkan pelayanan yang konsisten dan efektif
21	SO5207	Tidak adanya pencatatan terkait solusi penanganan insiden	*Staff Operation*	*Medium*	DSS01-Manage Operations	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal	Menyusun dan memelihara kebijakan prosedur operasional terkait pengelolaan insiden dan permintaan layanan

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
22	SO5308	Penanganan insiden melebihi batas waktu yang disepakati	*Staff Operation*	*Medium*	APO11-Manage Quality	APO11.04 Perform Quality monitoring, control and review – melakukan control review dan monitoring terhadap kulitas proses layanan untuk memantau kepuasan pelanggan sesuai dengan Quality Standard Management	Melaksanakan kegiatan pelayanan sesuai prosedur dan kebijakan yang ada untuk menghasilkan pelayanan yang konsisten dan efektif Memverifikasi hasil dari pemenuhan permintaan layanan yang telah dilakukan sudah sesuai dengan kebutuhan dan keinginan pengguna
23	SO6211	Pengguna tidak memberikan konfirmasi terkait status penutupan insiden	*Staff Operation*	*Medium*	APO11-Manage Quality	APO11.03 Focus quality management on customer – memfokuskan manajemen kualitas dari layanan dengan kebutuhan pelanggan dan quality management practice yang bertujuan untuk meningkatkan kepuasan pelanggan	Mengidentifikasi kriteria penerimaan kualitas layanan dari pengguna dengan menyelaraskannya dengan kualitas TI yang ada.

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
24	SO7112	Pihak yang dieskalasi tidak memperbarui status mengenai insiden atau permintaan layanan yang ditangani	*Staff Operation*	*Medium*	DSS01-Manage Operations	DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal	Melakukan evaluasi secara teratur terkait impementasi penerapan kebijakan dan prosedur di perusahaan
25	SW7101	Tidak adanya laporan insiden yang dieskalasi melalui sistem informasi	*Software*	*Medium*	BAI09 – Manage Assets	BAI09.02 Manage critical assets – Melakukan identifikasi terkait aset-aset yang mendukung proses operasi layanan dan menjaga ketersediaan aset untuk mendukung proses bisnis tersebut	Mendefinisikan kebijakan dan prosedur jika terjadi kegagalan dalam mengakses sistem operasi
26	IE2304	Kesalahan dalam menentukan prioritasi insiden atau permintaan layanan	*IT expertise and skill*	*High*	APO07-Manage Human Resource DSS01-Manage Operations	APO07.04 Evaluate employee job performance – melakukan evaluasi bagi para individu terkait kinerja. Evaluasi dilakukan secara teratur	Menetapkan skema prioritasi insiden atau permintaan layanan sesuai tingkat layanan. Memastikan ketersediaan dari sumber daya seperti

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
						untuk melihat keterampilan dan kompetensi pegawai untuk mencapai tujuan organisasi. DSS01.01 Perform Operational Procedures – Menjalankan dan juga melakukan pemeliharaan terkait kebijakan, prosedur operasional dan tugas operasional secara konsisten dan andal	SDM dan infrastruktur. Menyusun dan memelihara kebijakan prosedur operasional terkait pengelolaan insiden dan permintaan layanan
27	IS5101	Gangguan pada perangkat keras di unit TSI	*Infrastructure*	*High*	BAI09 – Manage Assets	BAI09.03 Manage the asset life cycle – Melakukan manajemen terkait siklus hidup dari aset agar didapatkan penggunaan yang efektif dan efisien.	Memantau usia dari aset yang digunakan dan mempersiapkan rencana pergantian perangkat keras secara berkala Secara teratur memantau performa perangkat keras dalam proses bisnis perusahaan

No	Risk ID	Risiko	Kategori Risiko	Level risiko	Proses COBIT 5	Justifikasi	Langkah Mitigasi
28	SO6110	Pemenuhan permintaan TI yang tidak sesuai keinginan pengguna	*Staff Operation*	*High*	APO11-Manage Quality	APO11.03 Focus quality management on customer – memfokuskan manajemen kualitas dari layanan dengan kebutuhan pelanggan dan quality management practice yang bertujuan untuk meningkatkan kepuasan pelanggan	Meminta feedback kepada pengguna terkait pelayanan yang telah dilakukan Memverifikasi hasil dari pelayanan yang telah dilakukan dengan kepuasan pengguna

Halaman ini sengaja dikosongkan

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini akan dijelaskan tentang Kesimpulan dan saran yang bermanfaat untuk perbaikan atau masukan yang bermanfaat untuk penelitian selanjutnya.

7.1 Kesimpulan

Kesimpulan yang didapat adalah:

1. Teridentifikasi sejumlah 28 risiko dari proses DSS02 Manage Service Request and Incidents pada COBIT 5, yang dimana pada aktivitas DSS02.01 - Menetapkan Skema klasifikasi insiden dan permintaan layanan memiliki risiko paling banyak berjumlah 5 (lima) dikarenakan *helpdesk* memiliki kerentanan dalam melakukan klasifikasi terkait insiden dan laporan permintaan layanan yang masuk.
2. Berdasarkan penilaian risiko yang dilakukan dari 28 risiko diketahui bahwa 3 risiko dengan level tinggi, 15 dengan level sedang dan 10 risiko dengan level rendah. Dengan risiko yang memiliki nilai tinggi adalah kesalahan dalam menentukan prioritasi insiden atau layanan, Gangguan pada perangkat keras di unit TSI dan pemenuhan permintaan TI yang tidak sesuai dengan keinginan pengguna.
3. Hasil dari survei menunjukan bahwa dampak dari risiko yang paling signifikan terhadap penurunan kepuasan pengguna adalah ketika keamanan informasi dari laporan keluhan dan permintaan tidak terlindungi.
4. Hasil dari mitigasi risiko menunjukan pemetaan proses TI COBIT 5 yang paling sesuai untuk langkah mitigasi risiko, diidentifikasi 11 proses mitigasi risiko berdasarkan COBIT 5, yaitu:
   a. APO07.03 *Maintain the skills and competencies of personnel*
   b. APO07.04 *Evaluate employee job performance*
   c. APO11.03 *Focus quality management on customer*

d. APO11.04 *Perform Quality monitoring, control and review*
e. BAI09.02 *Manage critical assets*
f. DSS01.01 *Perform Operational Procedures*
g. DSS05.04 *Manage user identity and logical access*
h. DSS05.07 *Monitor the infrastructure for security-related events*
i. BAI02.01 *Define and maintain business functional and technical requirements*
j. BAI09.02 *Manage critical assets*
k. BAI09.03 *Manage the asset life cycle*

7.2 Saran

Saran Penulis kepda peneliti selanjutnya yang akan melakukan penelitian serupa adalah sebagai berikut:

1. Dalam penelitian ini proses pengumpulan data terkait proses bisnis *helpdesk* dan tugas pokok dan fungsinya dilakukan dengan cara wawancara, survei dan observasi peneliti. Proses survei dilakukan dengan sampel seluruh pengguna yang ada tanpa memperhatikan terlebih dahulu kepentingan kebutuhan pengguna tersebut terkait layanan *helpdesk*, maka dari itu sebaiknya dilakukan identifikasi terlebih dahulu bagian atau divisi mana saja dari sampel yang sebaiknya dijadikan fokus untuk survei.
2. Penentuan langkah mitigasi risiko didapatkan berdasarkan pemetaan proses TI COBIT 5 yang paling sesuai dengan risiko, diharapkan untuk penelitian selanjutnya menggunakan metode lain yang lebih detail dan sistematis dalam menunjukan langkah mitigasi risiko untuk keberlangsungan bisnis bagi organisasi.

DAFTAR PUSTAKA

[1] PDAM Surya Sembada Kota Surabaya, "Visi Misi PDAM," PDAM Surya Sembada Kota Surabaya, 2019.[Online]. Available: http://pdam-sby.go.id/. [Accessed: 27-Feb-2019]

[2] H. M. Jogiyanto , "Sistem Tatakelola Teknologi Informasi," Yogyakarta: Andi, 2011.

[3] ITIL v3, ITIL Version 3: Service Operation, Buckinghamshire: Office of Government Commerce, 2011.

[4] Murahartawaty, W.I Chandra and A. Ibnu, "Audit Penerapan Teknologi Informasi Berbasis Risiko dengan Framework Cobit versi 4.1 di perguruan tinggi XYZ," *Jurnal Rekayasa Sistem & Industri, vol. 1, no. 1, pp. 106-113,2014*.

[5] D. Cooper, S. Grey, G. Raymond and P. Walker, "Project Risk Management Guidelines: Managing Risk in large Projects and Complex Procurements,"Chichester, West Sussex: John Wiley & Sons Ltd., 2004.

[6] P.Hopkin, "Fundamentals of Enterprise Risk Management Understanding, Evaluating, and Implementing Effective Risk Management," London: Kogan Page, 2017.

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

[8] 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.

[9] 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.

[10] N. Z. Firdaus and Suprapto, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus: PT. Petrokimia Gresik,"J-ptiik, vol.2, no. 1, pp.91-100, 2018.

[11] C. U. Putri, "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, "Surabaya: Institut Teknologi Sepuluh Nopember(ITS), 2017.

[12] Sigit Samaptoaji, "Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri," Jakarta: Universitas Indonesia, 2014. [Online]. Available: https://lib.ui.ac.id/. [Accessed: 03-Mar-2019].

[13] Badan Pengembangan dan Pembinaan Bahasa Kementrian Pendidikan dan Kebudayaan, "Arti kata risiko - Kamus Besar Bahasa Indonesia(KBBI) Online," *http://www.kbbi.web.id,* 2019. [Online]. Available: http://www.kbbi.web.id/risiko. [Accessed: 03-Mar-2019].

[14] ISACA, COBIT 5 Enabling Process. R. Meadows: ISACA, 2012.

[15] ISACA, *The Risk IT FrameWork*. USA: ISACA, 2009.

[16] Knight, "Risk, Uncertainty, and Profit," *BioData Min.*, vol. 10, no. 1, pp. 1–17, 2017.

[17] Westerman, George and Richard Hunter, "IT Risk: Turning Business Threats Into Competitive Advantage," Harvard Business School Press, 2007.

[18] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, Revision 1, 2011.

[19] F. Syukriah, "Evaluasi Pemanfaatan IT *Helpdesk* dan manajemen,"*Vol 2, 2007*.

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

[21] A. Amri, "Kerangka Kerja Manajemen Risiko," Institut Teknologi Bandung, 2015. [Online]. Available: http://blogs.itb.ac.id/. [Accessed: 03-Mar-2019].

[22] ISO, "ISO/IEC 27001:2013," 2013. [Online]. Available: http://www.iso.org/standard/54534.html. [Accessed: 03-Mar-2019].

[23] M. A. Ramadhana, "Pembuatan Perangkat Audit Internal TI Berbais Resiko Menggunakan ISO / IEC 27002:2007 Pada Proses Pengelolaan Data Studi Kasus Digital Library ITS," 2007.

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

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

[26] ISACA, Process Reference Guide Exposure Draft, USA: ISACA, 2011.

[27] O.S Reza, "Tata Kelola Teknologi Informasi Berdasarkan Framework Cobit 4.1 pada Perusahaan Daerah Air Minum Surabaya," Surabaya: stikom, 2017.

[28] Sugiyono, "Metode Penelitian Kuantitatif, Kualitatif dan R&D," Bandung: Afabeta, 2011.

[29] PDAM Surabaya, "Struktur Organisasi dan Tata Kerja Perusahaan Daerah Air Minum Surya Sembada Kota Surabaya" Surabaya, 2017

Halaman ini sengaja dikosongkan

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 Unit Teknologi Sistem Informasi PDAM Surabaya.

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 masingmasing *helpdesk* di Unit TSI PDAM Surabaya?
Struktur Organisasi *helpdesk*	2. Seperti apa bentuk *helpdesk* pada Unit Teknologi Informasi (TSI) PDAM Surabaya? Bagaimana struktur organisasinya?
Tugas pokok fungsi *helpdesk*	3. Apakah tugas pokok dan fungsi dari *helpdesk* di Unit Teknologi Sistem Informasi (TSI) PDAM Surabaya?
Proses bisnis *helpdesk*	4. Bagaimana proses bisnis *helpdesk* sehariharinya?
	5. Apakah *helpdesk* sudah memanfaatkan peran TI dalam menjalankan proses bisnis sehariharinya? 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, mengklasifik asikan dan memprioritа skan 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 mengalokasi kan 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 dan pemulihan insiden insiden	1. Bagaimana pengambilan suatu solusi pemulihan insiden ditentukan? 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 itu disimpan?
Kategori	**Sasaran: Kondisi Sistem Informasi *Helpdesk* Unit Teknologi Informasi (TSI) PDAM Surabaya.**
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.

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.

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

INTERVIEW PROTOCOL 1

Tanggal	02 Maret 2019
Tujuan	Untuk mendapatkan informasi terkait kondisi kekinian dari proses bisnis *helpdesk* dalam menangani insiden maupun layanan di Unit Teknologi Informasi (TSI) PDAM Surabaya.
Tempat	PDAM Kota Surabaya
Narasumber	Fitri Qonita dan Alfil Hidayat
Jabatan	Staff *Helpdesk* Unit TSI PDAM Surabaya.

NO	Pertanyaan	Jawaban
1.	Apakah peran dan tanggung jawab masing-masing *helpdesk* di Unit Teknologi Informasi (TSI) PDAM Surabaya?	Menangani permintaan layanan TI terkait perubahan data, permintaan data, perubahan fitur, pembuatan sistem baru dan perbaikan hardware
2.	Seperti apa bentuk *helpdesk pada* Unit Teknologi Informasi (TSI) PDAM Surabaya? Bagaimana struktur organisasinya?	*Helpdesk* merupakan salah satu unit yang dimiliki oleh PDAM Surabaya yang menangani berbagai macam permasalahan layanan TI dan keluhan dari para pengguna layanan yang terjadi di lingkungan PDAM Surabaya. 
3.	Apakah tugas pokok dan fungsi dari *helpdesk* di Unit Teknologi Informasi (TSI) PDAM Surabaya?	Melakukan operasi layanan terkait insiden dan manajemen pemenuhan permintaan layanan TI
4.	Bagaimana proses bisnis *helpdesk* sehariharinya?	*Helpdesk* menerima laporan dari user terkait permasalahan yang sedang

		user hadapi atau permintaan terkait layanan TI setelah itu *helpdesk* akan melakukan eskalasi insiden kepada pihak yang bertanggung jawab terkait permintaan. Setelah permintaan selesai *helpdesk* akan melakukan verifikasi kepada user terkait penyelesaian permintaan dan jika user telah setuju maka permintaan akan ditutup
5.	Apakah *helpdesk* sudah memanfaatkan peran TI dalam menjalankan proses bisnis sehariharinya? Bagaimana bentuk pemanfaatan TI tersebut?	Sudah, *helpdesk* memanfaatkan telepon, email dan sistem informasi.
6.	Bentuk layanan dan proses TI apa saja yang ditangani oleh *helpdesk*?	Perubahan data, permintaan data, perubahan fitur aplikasi dan pengadaan perangkat keras
7.	Bagaimana alur atau prosedur pelaporan insiden maupun permintaan layanan?	User mengisi form, mengirim lewat email atau datang langsung ke unit TSI dan menyampaikan terkait permintaan yang dia inginkan atau permasalahan yang sedang dia alami setelah itu akan dilakukan eskalasi kepada bagian yang menanganinya
8.	Apa saja insiden yang sering terjadi pada layanan-layanan tersebut? Dan bagaimana penanganannya?	Permintaan data terkait organisasi dan perubahan fitur didalam aplikasi
9.	Hal-hal apa saja yang dirasa masih kurang dalam pengelolaan insiden dan permintaan layanan?	Untuk permintaan yang datang dari form

10.	Apakah proses pengelolaan insiden dan pemenuhan permintaan layanan sudah mengacu pada standar tertentu?	Sudah ada
11.	Bagaimana suatu insiden di deteksi?	Datang dari laporan user
12.	Bagaimana proses pemenuhan layanan dilakukan?	Untuk layanan yang urgent dilakukan secara langsung sedangkan permintaan yang memiliki urgensi biasa dilakukan sesuai kebijakan prioritasi yang ada
13.	Apakah terdapat suatu klasifikasi/kategorisasi insiden dan pemenuhan layanan secara lengkap?	Sudah melalui sistem informasi
14.	Bagaimana suatu insiden diidentifikasi dalam suatu klasifikasi/kategori?	Sesuai laporan dari user dalam mendefinisikan tipe layanan
15.	Bagaimana insiden dan permintaan layanan di catat?	Form dari user disimpan di excel dan dimasukan ke repositori khusus
16.	Apakah pencatatan tersebut disimpan dalam satu direktori khusus?	Iya didalam direktori khusus di dalam sistem informasi
17.	Apakah terdapat suatu sistem informasi khusus dalam pencatatan insiden?	ada
18.	Detail informasi apasajakah yang dicatat dalam data insiden dan pemenuhan permintaan layanan?	Identitas pelapor, deskripsi permintaan, tanggal diajukan, tanggal diterima dan SLA.
19.	Apakah terdapat sistem prioritasi insiden dan pemenuhan layanan? Kriteria apa saja yang digunakan dalam memprioritaskan insiden dan pemenuhan layanan permintaan?	Ada, prioritas dari identitas pelapor dan dari kompleksitas permintaan yang datang.

20.	Apakah terdapat daftar prioritas khusus untuk insiden dan permintaan yang terjadi?	Ada
21.	Tipe insiden dan pemenuhan layanan seperti apa yang memerlukan eskalasi? Apakah eskalasi fungsional atau hierarki?	Untuk permintaan yang diluar kapabilitas *helpdesk* dilakukan eskalasi fungsional
22.	Bagaimana eskalasi insiden tersebut dilakukan?	Dilakukan dengan telpon atau melalui sistem informasi.
23.	Apakah terdapat prosedur khusus dalam menangani insiden dan memenuhi permintaan layanan?	Ada prosedur dalam menangani insiden dan permintaan layanan
24.	Apakah diperlukan persetujuan fungsional untuk menangani insiden dan memenuhi permintaan layanan?	Untuk hal-hal yang berdampak besar bagi organisasi diperlukan persetujuan fungsional
25.	Ketika insiden terjadi (terdapat suatu laporan dari pengguna), apakah dilakukan diagnosa awal untuk menentukan gejala penyebab masalah?	Iya dilakukan
26.	Apakah dilakukan aktivitas investigasi dan diagnosa terhadap insiden yang terjadi? Bagaimana investigasi dan diagnosa insiden tersebut biasanya dilakukan?	Iya contohnya dapat dilakukan dengan meremote komputer dari pengguna
27.	Bagaimana pengambilan suatu solusi pemulihan insiden ditentukan?	Untuk insiden yang sudah terjadi tidak perlu didiskusikan
28.	Apakah solusi tersebut diuji terlebih dahulu?	Iya
29.	Apakah terdapat SOP khusus untuk melakukan pemulihan/penyelesaian insiden ?	Belum ada SOP khusus untuk menyelesaikan insiden
30.	Berapa lama biasanya suatu insiden atau layanan diselesaikan?	Untuk permintaan yang tidak kompleks dapat dilakukan dibawah 1 minggu sedangkan untuk permintaan yang kompleks

		bisa dilakukan lebih dari satu minggu
31.	Bagaimana suatu insiden dan permintaan layanan ditutup?	Dilakukan verifikasi ke user melalui telepon dan ketika user sudah puas maka permintaan akan ditutup
32.	Apakah solusi yang diberikan divalidasi ke pengguna (pelapor) insiden dan peminta layanan?	Iya
33.	Apakah eskalasi insiden dan penanganan layanan diawasi?	Iya, user juga dapat meminta status terkait laporan
34.	Apakah dibuatkan laporan terkait permintaan layanan dan insiden tersebut?	Iya
35.	Dimana laporan itu disimpan?	Di direktori khusus didalam server internal
36.	Apakah terdapat suatu sistem informasi *helpdesk* untuk mengelola insiden dan pengelolaan permintaan layanan?	Ada
37.	Adakah permasalahan yang pernah terjadi terkait sistem informasi *helpdesk*?	Permasalahan seperti kinerja database yang lambat, kegagalan koneksi, serangan terhadap komputer server dan kerusakan dari perangkat keras yang digunakan
38.	Siapa saja yang menjadi admin/bertanggung jawab/pengelola sistem informasi *helpdesk*?	Staff *helpdesk* yang menjadi admin adalah bapak Alfil.
39.	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*)?	*Hardware, web, network, people*

40.	Apakah pernah dilakukan identifikasi risiko terkait sistem informasi *helpdesk*?	Belum pernah

INTERVIEW PROTOCOL 2

Tanggal	02 Maret 2019
Tujuan	Untuk mendapatkan detail informasi terkait kesalahan dan risiko yang kerap muncul dari proses pengelolaan insiden dan pemenuhan permintaan layanan.
Tempat	PDAM Kota Surabaya
Narasumber	Fitri Qonita dan Alfil Hidayat
Jabatan	Staff *Helpdesk* Unit TSI PDAM Surabaya.

NO	Pertanyaan	Jawaban
1.	Dari pemanfaatan peran TI, apakah sering terjadi kesalahan pada saat *helpdesk* mengelola insiden dan memenuhi permintan layanan?	Untuk insiden cukup jarang tetapi untuk permintaan layanan cukup banyak
2.	Kesalahan apa yang paling sering terjadi pada saat mengelola insiden dan memenuhi permintan layanan?	Tidak memahami penerimaan user
3.	Seberapa fatal kesalahan yang pernah dilakukan?	Belum terlalu fatal
4.	Proses apa yang paling rentan terjadi kesalahan atau menimbulkan risiko?	Saat menerima permintaan dari user dan proses perubahan data
5.	Apakah selama ini kesalahan dan risiko yang terjadi dicatat dan disimpan?	iya untuk risiko
6.	Jika ya, apakah terdapat pengkategorisasian risiko? Bagaimana pengkategorisasiannya?	Tidak ada pengkategorasisan risiko
7.	Dari penjabaran kesalahan dan risiko tersebut, apakah risiko tersebut disebabkan oleh faktor internal dan eksternal? Bagaimana penjabarannya	Dijabarkan kedua faktor tersebut terhadap risiko
8.	Seberapa berpengaruh risiko-risiko yang terjadi tersebut terhadap proses bisnis *helpdesk*?	Cukup berpengaruh terhadap proses bisnis

9.	Seberapa sering (frekuensi) risiko-risiko tersebut terjadi?	Risiko yang paling sering terjadi seperti mati listrik memiliki frekuensi yang tinggi dan dampak yang besar karena *helpdesk* harus mengulang pekerjaan yang telah dia lakukan
10.	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)	Belum pernah ada perhitungan tersendiri untuk aspek-aspek tersebut
11.	Apakah terdapat standar atau acuan dalam menilai risiko yang ada?	ada

INTERVIEW PROTOCOL 3

Tanggal	10 Maret 2019
Tujuan	Untuk mendapatkan detail informasi terkait rencana lanjutan dalam menangani dan mengantisipasi terjadinya risiko.
Tempat	PDAM Kota Surabaya
Narasumber	Ari Bimo Sakti
Jabatan	Manajer Unit TSI PDAM Surabaya.

NO	Pertanyaan	Jawaban
1.	Bagaimana pengelolaan/manajemen risiko jika terdapat risiko yang terjadi?	Tidak ada pengelolaan yang tertulis terkait

		dengan risiko yang belum pernah ditemui
2.	Apakah proses pengelolaan risiko tersebut sudah mengacu pada standar tertentu?	Sudah
3.	Seberapa fatal dampak risiko terhadap proses bisnis sehari-hari organisasi?	Untuk risiko yang terjadi di *helpdesk* tidak terlalu fatal dampaknya bagi proses bisnis
4.	Risiko mana yang memberikan dampak paling signifikan terhadap proses bisnis organisasi?	Risiko terkait padamnya listrik atau downtime dari database atau server
5.	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)	Belum pernah ada perhitungan tersendiri untuk aspek-aspek tersebut
6.	Seperti apa bentuk rencana atau strategi untuk menangani risiko?	Rencana strategi untuk menangani bencana atau strategi dibuat untuk menghindari terjadinya risiko
7.	Bagaimana rencana strategi tersebut dibuat?	melihat faktor yang menyebabkan risiko tersebut
8.	Berdasarkan acuan standar apa rencana atau strategi tersebut dibuat?	ISO
9.	Siapa saja yang berperan dalam melakukan aksi tersebut?	Seluruh bagian dari unit TSI ikut berperan

10.	Apakah terdapat suatu proses mitigasi risiko tersendiri? Berdasarkan acuan standar apa mitigasi tersebut dibuat?	Sudah tetapi belum mengacu kepada standar tertentu
11.	Strategi apa yang dirasa paling sesuai terhadap kondisi organisasi?	Strategi untuk mempertahankan proses bisnis, mempertahankan kepuasan pengguna dan menghindari terjadinya risiko.

Halaman ini sengaja dikosongkan

LAMPIRAN C - Hasil Observasi

No	DSS02	Aktivitas	Dilakukan	Keterangan
1	DSS02.01 - Menetapkan Skema klasifikasi insiden dan permintaan layanan	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	√	*Helpdesk* sudah melakukan kategorisasi insiden dan prioritasi insiden berdasarkan tingkat urgensinya
2		Mendefinisikan bentuk insiden untuk mengetahui kesalahan untuk membuat resolusi yang efisien dan efektif.	√	Insiden sudah di definisikan jenis dan solusi penananganannya
3		Mendefinisikan model permintaan layanan berdasarkan tipe permintaan layanan untuk memungkinkan dilakukan secara mandiri dan layanan yang efisien untuk permintaan yang standar.	√	Model permintaan sudah terdefinisikan berdasarkan jenisnya
4		Mendefinisikan peraturan dan prosedur eskalasi insiden, terutama untuk insiden utama dan insiden keamanan.	-	Belum ada kebijakan atau prosedur untuk eskalasi insiden
5		Mendefinisikan pengetahuan permintaan layanan dan kegunaannya.	√	Pengetahuan permintaan layanan dan kegunaannya sudah terdefinisikan
6	DSS02.02 - Merekam, mengklasifikasikan dan	Menetapkan dan mendefinisikan klasifikasi permintaan layanan dan skema prioritisasi beserta kriteria untuk pendaftaran masalah,	√	Semua informasi terkait permintaan dan insiden sudah dicatat baik melalui sistem

	memprioritaskan permintaan dan insiden	melakukan pencatatan semua permintaan dan insiden serta semua informasi yang terkait, sehingga bisa di tangani secara efektif dan laporan tersebut bisa dipelihara.		informasi atau laporan langsung
7		Untuk memungkinkan analisis tren, diperlukan klasifikasi permintaan layanan dengan melakukan identifikasi tipe dan kategori dari permintaan tersebut.	√	*Helpdesk* sudah melakukan identifikasi dari tipe dan kategori permintaan layanan
8		Melakukan prioritisasi permintaan layanan berdasarkan definisi layanan dari SLA terhadap proses bisnis perusahaan dan tingkat urgensi.	√	Sudah ada sistem prioritasi berdasarkan tingkat urgensitas layanan
9	DSS02.03 - Melakukan verifikasi, menerima dan memenuhi permintaan layanan	Melakukan verifikasi terhadap hak untuk menggunakan permintaan layanan, jika dimungkinkan, alur proses yang telah didefinisikan dan perubahan standar.	√	*Helpdesk* sudah melakukan verifikasi kepada pengguna tentang hak menggunakan permintaan
10		Memperoleh persetujuan finansial dan fungsonal atau tanda tangan, jika dibutuhkan, atau persetujuan otomatis untuk persetujuan dalam perubahan yang standar.	√	*Helpdesk* sudah melakukan pengajuan finansial dan fungsional jika dibutuhkan
11		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.	-	Belum adanya prosedur atau alur tertulis yang diterapkan di perusahaan

12	DSS02.04 - Menginvestigasi, mendiagnosa dan mengalokasikan insiden	Mengidentifikasikan dan mendeksripsikan gejala yang relevan untuk mendirikan penyebab yang paling tepat dari insiden tersebut.	√	*Helpdesk* sudah melakukan identifikasi terkait gejala dari insiden
13		Jika insiden tersebut tidak tersedia, buat sebuah log baru.	√	*Helpdesk* membuat dokumentasi jika insiden tersebut tidak tersedia
14		Menetapkan insiden ke fungsi spesialis.	√	Sudah dilakukan eskalasi fungsional terkait insiden
15	DSS02.05 - Melakukan Penyelesaian dan Pemulihan insiden	Memilih dan menggunakan resolusi insiden yang tepat (*temporary workaround* dan/atau solusi tetap).	√	Sudah dilakukan pemilihan resolusi insiden sesuai dengan kebutuhan.
16		Merekam *workaround* mana yang digunakan untuk melakukan resolusi insiden.	-	Belum dilakukan pencatatan terkait workaround yang digunakan
17		Melakukan aksi pemulihan (jika dibutuhkan).	√	Sudah dilakukan aksi pemulihan jika dibutuhkan
18		Mendokumentasikan resolusi insiden dan menilai apakah resolusi tersebut dapat dipakai sebagai sumber pengetahuan mendatang.	√	Sudah ada dokumentasi terkait pelaporan insiden
19	DSS02.06 - Menutup permintaan layanan dan insiden	Melakukan verifikasi dengan pengguna yang berpengaruh (apabila setuju) bahwa layanan permintaan mereka telah dipenuhi dan diselesaikan dengan baik	√	*Helpdesk* sudah melakukan user acceptance test setelah layanan permintaan dipenuhi
20		Menutup layanan permintaan dan insiden	√	Sudah dilakukan penutupan layanan

				permintaan dan insiden
21	DSS02.07 - Melacak status dan membuat laporan	Mengawasi dan melacak eskalasi insiden dan resolusi dan penanganan permintaan untuk melakukan progress penyelesaian.	-	Belum adanya pengawasan terkait insiden yang dieskalasi
22		Mengidentifikasi informasi stakeholder dan kebutuhan mereka untuk pemenuhan data dan laporan. Idenfitikasi laporan secara berkala.	√	Sudah dilakukan identifikasi informasi terkait pemenuhan data dan laporan.
23		Menganalisis insiden dan layanan permintaan dengan mengkategorisasikan tren.	-	Belum dilakukan analisis dan kategorisasi tren
24		Membuat dan mendistribusikan laporan berkala atau menyediakan *controlled access* ke *online data*.	√	Sudah dibuatnya direktori khusus terkait laporan berkala di server internal perusahaan

LAMPIRAN D - Form Kuisioner

KUESIONER KEPUASAN PENGGUNA TERHADAP LAYANAN *HELPDESK* PDAM KOTA SURABAYA

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* PDAM Kota Surabaya.

Nama :

Divisi :

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)

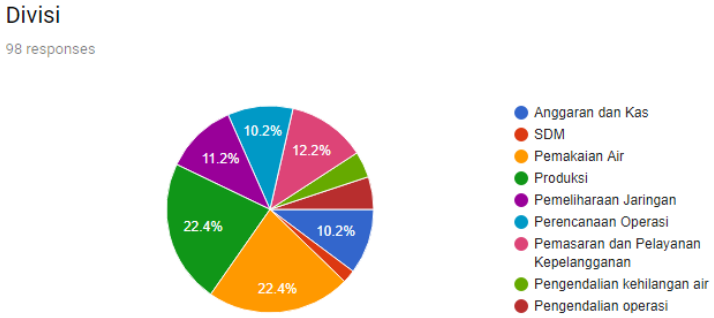
No.	Pernyataan	1	2	3	4	5
1	Saat *helpdesk* tidak memenuhi permintaan dan menangani keluhan sesuai harapan saya, maka kepuasan saya mengalami:					
2	Saat *helpdesk* terlambat dalam melakukan respon terhadap laporan saya, maka kepuasan saya mengalami:					
3	Saat *helpdesk* mengabaikan laporan yang saya berikan, maka kepuasan saya mengalami:					
4	Saat *helpdesk* selesai menangani laporan saya melebihi batas waktu yang dijanjikan, maka kepuasan saya mengalami:					

5	Saat *helpdesk* tidak melakukan verifikasi untuk memastikan bahwa laporan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami :					
6	Saat *helpdesk* tidak memberikan status mengenai laporan saya (sedang dikerjakan/selesai), maka kepuasan saya mengalami:					
7	Saat *helpdesk* tidak menangani akar permasalahan dari permasalahan yang berulang kali saya keluhkan, maka kepuasan saya mengalami:					
8	Saat layanan pelaporan keluhan dan permintaan pada *helpdesk* tidak mengalami peningkatan, maka kepuasan saya mengalami:					
9	Saat saya tidak dapat melakukan pelaporan keluhan dan permintaan kepada helpdesk (kesalahan teknis), maka kepuasan saya mengalami:					
10	Saat keamanan informasi dari laporan keluhan dan permintaan tidak terlindungi, maka kepuasan saya mengalami:					

LAMPIRAN E - Hasil Survei

a. Demografi data

Informasi terkait responden mengenai jumlah responden tiap bagian yang menjadi sampel dalam penelitian ini. Responden yang dituju adalah pengguna layanan *helpdesk* unit TSI PDAM Surabaya. Berikut merupakan data yang didapat dari survei yang dilakukan:



Dengan rincian:

- 22.4% dari divisi pemakaian air
- 22.4% dari divisi produksi
- 12.2% dari divisi pemasaran dan pelayanan kepelangganan
- 11.2% dari divisi pemeliharaan jaringan
- 10.2% dari divisi perencanaan operasi
- 10.2% dari divisi anggaran dan kas
- 5.1% dari divisi pengendalian operasi
- 4.1% dari divisi pengendalian kehilangan air
- 2% dari divisi SDM

b. Analisis Hasil Survei

Peneletian ini memaanfaatkan skala likert dengan lima poin dari 1-5 yang dijelaskan dalam tabel berikut

Nilai Skala likert	Rentan Nilai	Keterangan
1	98 - 176,4	Penurunan sangat sedikit
2	176,5 - 254,8	Penurunan sedikit
3	254,9 - 333,2	Netral
4	333,3 - 411,6	Penurunan tinggi
5	411,7 - 490	Penurunan sangat tinggi

Berikut adalah hasil survei yang diambil dari total 98 responden.

NO	Pernyataan	Jumlah Jawaban					Total Sampel	Total nilai	Keterangan
		1	2	3	4	5			
1.	Saat *helpdesk* tidak memenuhi permintaan layanan dan menangani keluhan sesuai harapan saya, maka kepuasan saya mengalami:	6	31	30	22	9	98	294	Netral
2.	Saat *helpdesk* terlambat dalam melakukan respon terhadap laporan saya, maka kepuasan saya mengalami:	9	18	38	19	14	98	305	Netral

3.	Saat *helpdesk* mengabaikan laporan yang saya berikan, maka kepuasan saya mengalami:	7	24	16	32	19	98	326	Netral
4.	Saat *helpdesk* selesai menangani laporan saya melebihi batas waktu yang dijanjikan, maka kepuasan saya mengalami:	5	21	25	39	8	98	318	Netral
5.	Saat *helpdesk* tidak melakukan verifikasi untuk memastikan bahwa laporan saya telah terpenuhi sesuai harapan, maka kepuasan saya mengalami:	4	15	36	26	17	98	331	Netral
6.	Saat *helpdesk* tidak memberikan status mengenai laporan saya (sedang dikerjakan/selesai), maka kepuasan saya mengalami:	9	22	26	31	10	98	305	Netral
7.	Saat *helpdesk* tidak menangani akar	5	21	22	33	17	98	330	Netral

	permasalahan dari permasalahan yang berulang kali saya keluhkan, maka kepuasan saya mengalami:								
8.	Saat layanan pelaporan keluhan dan permintaan pada *helpdesk* tidak mengalami peningkatan, maka kepuasan saya mengalami:	14	24	30	20	10	98	282	Netral
9.	Saat saya tidak dapat melakukan pelaporan keluhan dan permintaan kepada *helpdesk* (kesalahan teknis), maka kepuasan saya mengalami:	6	17	24	35	16	98	332	Netral
10.	Saat keamanan informasi dari laporan keluhan dan permintaan tidak terlindungi, maka kepuasan saya mengalami:	6	18	23	31	20	98	335	Penurunan tinggi

BIODATA PENULIS

Aditya Satria Putra atau akrab disapa “Adit” sebagai penulis merupakan putra Bungsu dari Bapak Bambang Purwanto dan Ibu Yuliawati yang lahir di Bogor pada tanggal 04 Desember 1997. Penulis merupakan anak keempat dari 4 bersaudara.

Penulis menempuh pendidikan formal di SDN Nanggewer 1 Bogor (2003-2009), SMPN 5 Bogor (2009-2012), SMA 3 Bogor (2012-2015), dan memilih untuk melanjutkan ke jenjang sarjana di Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember (ITS). Semasa perkuliahan, penulis aktif berorganisasi di Unit Kegiatan Mahasiswa (UKM) KSR PMI ITS selama kurang lebih 3 tahun dan mampu menjadi staff logistik pada tahun 2016-2017 selama berkegiatan di UKM KSR PMI ITS. Penulis juga turut melampiaskan minat di bidang kesenian dengan mengikuti UKM Unit Kegiatan Tari dan Mahasiswa ITS. Penulis juga pernah menjabat sebagai staff Tim Event pada tahun 2017-2018 selama aktif berorganisasi di UKM Unit Kegiatan Tari dan Mahasiswa ITS. Di luar, penulis juga aktif berkegiatan sosial di lingkup kota Surabaya.

Di akhir masa kuliah, penulis mengambil minat bidang Manajemen Sistem Informasi (MSI) di Departemen Sistem Informasi. Segala pertanyaan dan saran mengenai Tugas Akhir ini dapat dikirimkan melalui email ke p.adityasatria@gmail.com.