TUGAS AKHIR – KS141501

AUDIT MANAJEMEN INSIDEN PADA UNIT TEKNOLOGI SISTEM INFORMASI MENGGUNAKAN COBIT 5 DSS02 PADA PDAM SURYA SEMBADA KOTA SURABAYA

AUDIT INCIDENT MANAGEMENT IN UNIT TECHNOLOGY INFORMATION SYSTEM USING COBIT 5 DSS02 IN PDAM SURYA SEMBADA SURABAYA CITY

ADHISKA PUTRI MAHARANI
NRP 05211440000099

Dosen Pembimbing
Ir.Khakim Ghozali, M.MT

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

TUGAS AKHIR – KS141501

AUDIT MANAJEMEN INSIDEN PADA UNIT TEKNOLOGI SISTEM INFORMASI MENGGUNAKAN COBIT 5 DSS02 PADA PDAM SURYA SEMBADA KOTA SURABAYA

ADHISKA PUTRI MAHARANI
NRP 05211440000099

Dosen Pembimbing
Ir.Khakim Ghozali, M.MT

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

FINAL PROJECT – KS141501

AUDIT INCIDENT MANAGEMENT IN UNIT TECHNOLOGY INFORMATION SYSTEM USING COBIT 5 DSS02 IN PDAM SURYA SEMBADA SURABAYA CITY

ADHISKA PUTRI MAHARANI
NRP 05211440000099

Supervisors
Ir.Khakim Ghozali, M.MT

INFORMATION SYSTEMS DEPARTMENT
Information and Communication Technology Faculty
Sepuluh Nopember Institut of Technology
Surabaya 2018

LEMBAR PENGESAHAN

AUDIT MANAJEMEN INSIDEN PADA UNIT TEKNOLOGI SISTEM INFORMASI MENGGUNAKAN COBIT 5 DSS02 PADA PDAM SURYA SEMBADA 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:

ADHISKA PUTRI MAHARANI
NRP. 05211440000099

Surabaya, Juli 2018

KETUA
DEPARTEMEN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

AUDIT MANAJEMEN INSIDEN PADA UNIT TEKNOLOGI SISTEM INFORMASI MENGGUNAKAN COBIT 5 DSS02 PADA PDAM SURYA SEMBADA 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 :

ADHISKA PUTRI MAHARANI

NRP. 05211440000099

Disetujui Tim Penguji : Tanggal Ujian : Juli 2018
Periode Wisuda : September 2018

Ir.Khakim Ghozali, M.MT (Pembimbing I)

Dr. Apol Pribadi, ST.MT (Penguji I)

Anisah Herdiyanti, S.Kom, M.Sc., ITIL (Penguji II)

AUDIT MANAJEMEN INSIDEN PADA UNIT TEKNOLOGI SISTEM INFORMASI MENGGUNAKAN COBIT 5 DSS02 PADA PDAM SURYA SEMBADA KOTA SURABAYA

Nama Mahasisiwa	**:**	**Adhiska Putri Maharani**
NRP	**:**	**05211440000099**
Departemen	**:**	**Sistem Infromasi**
Dosen Pembimbing	**:**	**Ir.Khakim Ghozali, M.MT**

ABSTRAK

Penelitian ini membahas mengenai pembuatan Audit Manajemen Insiden Pada Unit Teknologi Sistem Informasi Menggunakan COBIT 5 DSS02 Pada Service Desk pada PDAM Surya Sembada Kota Surabaya. PDAM Surya Sembada Kota Surabaya merupakan salah satu unit usaha milik daerah, yang bergerak dalam distribusi air bersih bagi masyarakat umum. PDAM terdapat disetiap provinsi,kabupaten, dan kotamadya di seluruh Indonesia.Sebagai salah satu BUMD atau bisa disebut Badan Usaha Milik Negara yang memiliki keterkaitan dalam bidang IT pada setiap proses bisnis yang ada, tidak jarang juga menimbulkan gangguan atau insiden yang mengakibatkan menurunnya kualitas layanan pada service desk unit teknologi system informasi PDAM Surya Sembada Kota Surabaya.Karena belum adanya perangkat yang digunakan untuk melakukan audit service desk berdasarkan COBIT 5 menggunakan best practice pada service desk mereka.

Tujuan untuk penelitian ini melakukan Audti Sistem Informasi yang baik dan mudah digunakan diperlukan analisis baik internal maupun external pada pihak service desk PDAM Surya Sembada agar dapat membantu pengembangan TI secara optimal sesuai best practice dan dapat dijalankan sesuai dengan standart. Agar dapat mencapai tujuan tersebut, dilakukan beberapa langkah. pertama dengan melakukan pemetaan proses dan control objective yang menghasilkan analisis kondisi

kekinian pada service desk menggunakan COBIT 5 kedua dil-akukan pengumpulan data terkait risiko. Ketiga mengumpulka data terkait risiko yang. Keempat,akan dianalisis risikonya.Kelima akan dilakukan pemetaan risiko dan control objective untuk diverifikasi untuk menghasilkan temuan audit yang keenam,akan ditentukan tingkat risikonya berdasarkan best practice dan akan dihasilkan rekomendasi dari hasil temuan audit.

Hasil dari tugas akhir ini adalah sebuah dokumen Audit service standart pada service desk PDAM Surya Sembada yang disusun berdasarkan best practice COBIT 5.

Kata Kunci: Audit, Servce Desk, Cobit 5, Insiden

AUDIT INCIDENT MANAGEMENT IN UNIT TECHNOLOGY INFORMATION SYSTEM USING COBIT 5 DSS02 IN PDAM SURYA SEMBADA SURABAYA CITY

Name	**:**	**Adhiska Putri Maharani**
NRP	**:**	**05211440000099**
Departement	**:**	**Sistem Infromasi**
Supervisior	**:**	**Ir.Khakim Ghozali, M.MT**

ABSTRACT

This research discuss about Audit Incident Management In Unit Technology Information System Using COBIT 5 DSS02 in PDAM Surya Sembada Surabaya. PDAM Surya Sembada Surabaya is one of the regional owned business units, which is engaged in air distribution for the general public. PDAMs in every province, district, and city throughout Indonesia. As one of the BUMD or can be called State-Owned Enterprises that have interrelations in the field of IT in every existing process, not infrequently also cause problems. desk service unit of information system technology PDAM Surya Sembada Kota Surabaya.Karena no body to conduct audit service desk based on COBIT 5 using best practice at their service desk.

The purpose of the program that performs a good and easy to use Good Information System audit both internally and externally on the Surya Sembada PDAM service desk in order to assist the development of IT optimally according to best practice and can be run in accordance with the standards. To achieve that goal, several steps are taken. first by performing the process and controlling the objectives that resulted in the current state of the service table using the second COBIT 5 conducted with respect to the relevant data. Thirdly collect risk-related data. Fourth, the risks will be analyzed. Fifth will mapping and

goal control to identify the six audit findings, the level of risk will be determined based on best practice and will result in recommendations from audit findings.

The result of this final project is the standard document of Audit service at PDAM Surya Sembada service desk which is based on best practice COBIT 5.

Keywords: Audit, Servce Desk, Cobit 5, Incident

KATA PENGANTAR

Bismillahirohmanirrohim

Puji Syukur Kepada Allah SWT karena atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan buku tugas akhir dengan judul
"**AUDIT MANAJEMEN INSIDEN PADA UNIT TEKNOLOGI SISTEM INFORMASI MENGGUNAKAN COBIT 5 DSS02 PADA PDAM SURYA SEMBADA KOTA SURABAYA**" yang merupakan satu syarat kelulusan pada Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember Surabaya.
Selama masa pengerjaan Tugas Akhir ini, penulis telah memperoleh banyak bantuan, bimbingan dan petunjuk dari berbagai pihak. Maka dari itu, dalam kesempatan ini penulis akan menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

- Terima kasih kepada Allah SWT, yang telah memberikan kesehatan, kemudahan, kelancaran, dan kesempatan untuk penulis hingga dapat menyelesaikan Tugas Akhir ini.
- Kedua orangtua, kakak, sahabat dan seluruh keluarga yang selalu hadir dan senantiasa mendoakan dan memberikan kasih sayang serta semangat tiada henti untuk menyelesaikan Tugas Akhir.
- Bapak Dr. Ir. Aris Tjahyanto, M.Kom, selaku Ketua Departemen Sistem Informasi ITS, yang telah menyediakan fasilitas terbaik untuk kebutuhan penelitian mahasiswa.
- Bapak Ir.Khakim Gozali, M.MT Selaku Dosen Pembimbing yang telah banyak meluangkan waktu untuk membimbing mengarahkan dann mendukung dalam penyelesaian Tugas Akhir.
- Bapak Dr. Apol Pribadi,ST.MT dan Ibu Anisah Herdiyanti,S.Kom,M.Sc.,ITIL selaku dosen penguji saya yang telah memberikan saya masukan sejak seminar proposal hingga siding tugas akhir selesai.

- Ibu Hanim Maria Astuti, S.Kom,M.Sc selaku dosen wali yang telah memberikan arahan terkait perkuliahan di Departemen Sistem Informasi.
- Seluruh dosen pengajar beserta staf dan karyawan di Departemen Sistem Informasi, FTIK ITS Surabaya yang telah memberikan ilmu dan bantuan kepada penulis selama 8 semester ini.
- Terima kasih untuk Mbak Icha dan Mas Adim yang sudah membantu menyelesaikan masalah dan memberikan saya semangat untuk tetap melanjutkan tugas akhir.
- Teman-teman seperjuangan laboratorium MSI dan OSIRIS yang selalu memberikan dukungan kepada kita semua yang sedang berjuang.
- Sahabat sahabat angkatan D14 yang selalu mendukung dan memberikan semanagat positif, memberikan canda tawa, susah duka untuk penulis dalam menjalani perkuliahan ini khussusnya yang selalu ada dari awal, Fufu, Khai, Lia, Icak, Gusti,Galih, Nina, Kiki, dan Lita.
- Sahabat kesayangan yang selalu ada selama 7 tahun, Eunike,Shafira,Sandra,Rininta,Farhana,Shieta,Roro,Apip yang sama sama sedang berjuang
- Terunutuk saudara saya Erica Octavia yang juga sama–sama berjuang di UNS dalam menempuh tugas akhir.

Penulis menyadari bahwa Tugas Akhir ini masih belum sempurna dan memiliki banyak kekurangan di dalamnya. Dan oleh karena itu, penulis meminta maaf atas segala kesalahan yang dibuat penulis dalam buku Tugas Akhir ini. Penulis membuka pintu selebar-lebarnya kepada pihak-pihak yang ingin memberikan kritik, saran, masukan, dan penelitian selanjutnya yang ingin menyempurnakan karya, dan Tugas Akhir ini. Semoga buku Tugas Akhir ini bermanfaat bagi seluruh pembaca.

Surabaya, Juli 2018

Adhiska Putri Maharani

DAFTAR ISI

LEMBAR PENGESAHAN 1
LEMBAR PERSETUJUAN 2
ABSTRAK v
ABSTRACT vii
KATA PENGANTAR ix
DAFTAR ISI xi
DAFTAR GAMBAR xv
DAFTAR TABEL xvii
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Perumusan Masalah 3
1.3. Batasan Pengerjaan Tugas Akhir 3
1.4. Tujuan Tugas Akhir 4
1.5. Manfaat Tugas Akhir 4
1.6. Relevansi 5
BAB II TINJAUAN PUSTAKA 7
2.1. Studi Sebelumnya 7
2.2. Dasar Teori 8
2.2.1. Audit 8
2.2.1.1. Audit Sistem Informasi 9
2.2.1.2. Pengertian Audit Berbasis Risiko 9
2.2.1.3. Program Audit 10
2.2.1.4. Perangkat Audit 11
2.2.1.5. Jenis Audit 12
2.2.2. Analisis Risiko TI 13
2.2.3. Kerangka Kerja Analisis Risiko 14
2.2.4. COBIT 5 For Risk 14
2.2.4.1. Mengumpulkan Data 16
2.2.4.2. Menganalisis Risiko 17
2.2.4.3. Cobit 5 DSS02 Mengelola Permintaan Layanan dan Insiden 19
2.2.5. Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya 22
BAB III METODOLOGI PENELITIAN 25

3.1 Metodologi Penelitian 25
3.2 Tahapan Perancangan Perangkat Audit 26
3.2.1. Melakukan Pemetaan Proses dan Control Objective 26
3.3 Tahap Analisis 26
3.3.1. Mengumpulkan Informasi Terkait Risiko TI..... 26
3.3.2. Menganalisis Risiko 27
3.3.2.1. Membuat Skenario Risiko TI 27
3.3.2.2. Melakukan Penilaian Risiko TI..... 27
3.4 Tahap Pembuatan Perangkat Audit 27
3.4.1. Melakukan Pemetaan Risiko dan Control Objective 28
3.4.2. Membuat Perangkat Audit..... 28
3.5. Tahap Pembuatan Hasil..... 28
3.5.1. Verifikasi Dokumen Perangkat Audit 28
3.6. Tahap Mencari Hasil Temuan 29
3.7. Penentuan Tingkat Risiko 29
3.8. Menyusun Rekomendasi dari Hasil Temuan 29
3.9. Jadwal Kegiatan 30
BAB IV PERANCANGAN 33
4.1. Perancangan Studi Kasus 33
4.1.1. Unit Of Analysis..... 36
4.2. Persiapan Pengumpulan Data..... 36
4.3. Metode Pengelolaan Data..... 38
4.4. Pendekatan Analisis 39
BAB V IMPLEMENTASI 41
5.1. Proses Pelaksanaan Penulisan 41
5.2. Gambaran Umum Unit TSI..... 42
5.3. Gambaran Umum Pengelolaan Insiden Unit TSI ... 45
5.4. Proses Manajemen Insiden Berdasarkan Standard . 46
5.5. Pendefinisian Kemungkinan dan Tingkat Dampak Risiko..... 47
5.6. Pemetaan Control Objective..... 56
5.7. Analisis Risiko 61
5.8. Perangkat Audit yang Digunakan..... 69
5.9. Gambaran dan Rintangan 72
BAB VI HASIL DAN PEMBAHASAN 73

6.1. Hasil Temuan Audit 73
6.2. Rekomendasi Hasil Perbaikan 78
BAB VII KESIMPULAN DAN SARAN 81
7.1. Kesimpulan 81
DAFTAR PUSTAKA 85
BIODATA PENULIS 87
LAMPIRAN A: Interview Protocol A-1
LAMPIRAN B: Hasil Wawancara B-1
LAMPIRAN C: Pemetaan Key Management Practice C-1
LAMPIRAN D: Analisis Risiko D-1
LAMPIRAN E: Hasil Temuan E-1
LAMPIRAN F: Hasil Rekomendasi F-1
LAMPIRAN G: Bukti Temuan Audit G-1

DAFTAR GAMBAR

Gambar 2. 1 Proses Audit ISO 19001 10
Gambar 2. 2 Proses Mengelola Risiko (sumber: Cobit 5) 16
Gambar 2. 3 Peta Risiko 4 Wilayah 19
Gambar 2. 4 Manajemen Insiiden Pada COBIT 5 (Sumber: ISACA,COBIT 5: Enabling Process) 20
Gambar 3. 1 Metodologi Penelitian 25
Gambar G. 1 Web Application Service Desk Catatan Log Insiden F-1
Gambar G. 2 Bukti Dokumen SLA G-2
Gambar G. 3 Bukti Dokumen SLA G-3
Gambar G. 4 Penanggung Jawab Insiden G-4
Gambar G. 5 Penutupan Pelaporan Insiden G-5
Gambar G. 6 Tingkat Prioritas Pada System Log G-6
Gambar G. 7 Penutupan Penanganan Insiden G-7
Gambar G. 8 Prosedur Perawatan dan Perbaikan Hardware G-8
Gambar G. 9 Dokumen SOP SMM ISO 9001 Instruksi Kerja G-13
Gambar G. 10 Prosedur Perawatan dan Perbaikan Software . G-19
Gambar G. 11 Posedur Backup Data G-23
Gambar G. 12 Prosedur Permintaan/Perubahan Data G-26
Gambar G. 13 Instruksi Kerja Pelaksanaan Back Up Data G-30
Gambar G. 14 Instruksi Kerja Back Up Data G-35
Gambar G. 15 Prosedur Perbaikan Device Sewa G-37

DAFTAR TABEL

Tabel 2. 1 Penelitian Sebelumnya (1) 7
Tabel 2. 2 Penelitian Sebelumnya (1) 8
Tabel 2. 3 Penilaian Risiko Berdasarkan Frekuensi [6] 17
Tabel 2. 5 Peta Risiko 4 Wilayah 19
Tabel 3. 1 Jadwal Pelaksanaan Tugas Akhir 31
Tabel 5. 1 Tugas Pokok dan Fungsi Bagian Pengembang TI 42
Tabel 5. 2 Tugas Pokok dan Fungsi Bagian Sistem Informasi 43
Tabel 5. 3 Tugas Pokok dan Fungsi Bagian Infrastruktur 44
Tabel 5. 4 Proses Pengelolaan Insiden dalam COBIT 5 47
Tabel 5. 5 Tingkat Dampak Risiko [6] 48
Tabel 5. 6 Daftar Risiko Pengelolaan Insiden Unit TSI..... 50
Tabel 5. 7 Pemetaan Key Management Practice 57
Tabel 5. 8 Control Objective 60
Tabel 5. 9 Analisis Risiko Berdasarkan Aset 62
Tabel 5. 10 Analisis Risiko 66
Tabel 5. 11 Petunjuk Pengisian Template Audit Report..... 71
Tabel 6. 1 Kriteria Dampak 74
Tabel 6. 2 Hasil Temuan Berdasarkan CO 75
Tabel 6. 3 Hasil Temuan Berdasarkan Kriteria Dampak 76
Tabel 6. 4 Hasil Rekomendasi Perbaikan 78
Tabel 7. 1 Tingkat Risiko 82
Tabel 7. 2 Hasil Kriteria Dampak..... 83

BAB I
PENDAHULUAN

Pada bagian bab ini akan dijelaskan latar belakang, rumusan masalah, batasan masalah,tujuan,manfaat yang diperoleh yang ingin dicapai dalam pengerjaan penelitian ini yang akan saya jadikan bahan Tugas Akhir.

1.1. Latar Belakang

Dalam era sekarang, persaingan dalam dunia bisnis dan usaha semakin meningkat dan menambah permasalahan yang dihadapi oleh manajemen risiko perusahaan. PDAM (Perusahaan Daerah Air Minum) merupakan salah satu unit usaha milik daerah, yang bergerak dalam distribusi air bersih bagi masyarakat umum. PDAM terdapat disetiap provinsi, kabupaten, dan kotamadya di seluruh Indonesia.

PDAM Surya Sembada Kota Surabaya memiliki misi salah satunya memberikan layanan prima bagi pelanggan dan berkelanjutan bagi pemangku kepentingan dengan diwujudkannya penyediaan infrastruktur teknologi dan aplikasi yang dapat digunakan untuk mendukung proses bisnis layanan tersebut. Dalam penerapan yang dilakukan terkadang perangkat yang dioperasikan mengalami gangguan atau insiden yang mengganggu proses bisnis. sSmua permintaan yang berkaitan dengan insiden dari aplikasi maupun infrastruktur akan dicatat oleh unit teknologi system informasi melalui service desk. Servie desk merupakan suatu unit fungsional yang menghubungkan antara unit teknologi sisem informasi dengan semua user aplikasi dan infrastruktur yang ada di PDAM yang menjadi tujuan akhir manajemen insiden yaitu memberikan penyelesaian permintaan layanan dan resolusi dari insiden yang tercatat dengan cepat dan tepat[1].

Berdirinya PDAM Surya Sembada Kota Surabaya merupakan penginggalan jaman belanda, dimana pembentukan sebagai BUMD berdasarkan, Peraturan Daerah No.7 tahun 1976 tanggal

30 Maret 1976, dan disahkan dengan surat keputusan Gubernur Kepala Daerah Tingkat I Jawa Timur pada tanggal 06 Nopember 1976 dan diundangkan dalam Lembaaran Daerah Kotamadya Daerah Tingkat II Surabaya tahun 1976 seri C pada tanggal 23 Nopember 1976.[2] Suatu unit fungsional pada suatu system layanan berfungsi sebagai penghubung antara unit teknologi system informasi dengan semua pengguna layanan TI yang ada pada PDAM dan harus memberikan respon yang baik dan efektif agar pemenuhan permintaan berjalan dengan cepat dan tepat[3].

Dalam aktivitas operasional PDAM tidak sedikit mengalami gangguan atau insiden yang mengakibatkan menurunnya kualitas pelayanan yang diberikan. Oleh karena itu terdapat unit service desk yang bertugas menangani berbagai macam keluhan insiden dan memenuhi berbagai bentuk permintaan layanan TI pada PDAM Surya Sembada Kota Surabaya[4]. Karena masih adanya keterbatasan untuk melakukan pencatatan dan penanganan dalam memberikan prioritas dan klasifikasi terhadap permintaan layanan dan insiden sehingga dapat menyebabkan kesalahan mengambil keputusan dalam penanganannya. Gangguan resiko yang terjadi mengakibatkan penurunan kualitas performa pada service desk yang membutuhkan suatu control terhadap proses pengelolaan permintaan layanan dan insiden pada service desk dilaksanakan dengan baik, serta memitigasi risiko pada proses.

Berdasarkan latar belakang yang saya jelaskan, penelitian tugas akhir ini bertujuan untuk menghasilkan dokumen audit service desk dengan menggunakan manajemen insiden pada service desk unit teknologi system informasi yang disesuaikan dengan prosedur operasional layanan pada unit service desk, Dalam pembuatan perangkat audit berbasis risiko ini, langkah pertama penulis akan melakukan pemetaan control objective pada Service Desk Unit TSI berdasarkan perangkat audit yang sudah pernah dibuat oleh peneliti terdahulu dengan proses pengelolaan permintaan layanan dan insiden. Berdasarkan best prac-

tice COBIT 5 yang nantinya akan disesuaikan dengan kebutuhan dan kesesuaian PDAM. Selanjutnya dilakukan analisis risiko teknologi informassi berbasis proses pada service desk menggunakan kerangka kerja COBIT 5 for Risk yang akan digunakan untuk melakukan verifikasi berdasarkan best practice dan persetujuan perangkat audit juga bisa menjadi temuan audit untuk dianalisis dengan tingkat risikonya dan akan diberikan rekomendasi sesuai dengan kebijakan perusahaan. Dengan adanya penelitian ini diharapkan PDAM Surya Sembada Surabaya dapat meningkatkan performa kualitas layanan terhadap pemberian layanan TI dan mengurangi permasalahan layanan TI sehingga dapat memberikan nilai secara prima untuk pengguna layanan.

1.2. Perumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan, maka rumusan masalah dari tugas akhir ini, yaitu:

1. Apa saja risiko teknologi system informasi yang terdapat pada service desk PDAM Surya Sembada Kota Surabaya.
2. Bagaimana hasil penilaian risiko teknologi system informasi.
3. Apa saja Control Objective yang dapat memitigasi risiko yang ada.
4. Bagaimana bentuk perangkat yang digunakan dalam control objective yang dibuat.
5. Bagaimana rekomendasi yang diberikan berdasarkan hasil temuan Audit Service Desk Unit TSI.

1.3. Batasan Pengerjaan Tugas Akhir

Dari permasalahan yang disebutkan pada perumusan masalah diatas, batasan pemasalahan dalam tugas akhir ini adalah:

1. Tugas Akhir ini dilakukan di PDAM Surya Sembada Kota Surabaya.

2. Kebutuhan teknologi informasi pada penelitian ini hanya berdasarkan yang berkaitan dengan divisi teknologi system informasi pada unit teknologi system informasi PDAM.
3. Metode yang digunakan untuk penelitian adalah wawancara dan observasi dengan menggunakan refrensi model yang telah dibuat dalam penelitian mahasiswa S1 Sistem Informasi ITS.
4. Hasil dari tugas akhir ini adalah sebuah *dokumen audit* yang bisa dijadikan panduan untuk kedepannya.

1.4. Tujuan Tugas Akhir

Tujuan yang hendak dicapai dalam pengerjaan tugas akhir ini adalah:

1. Untuk meningkatka kualitas dan performa Service Desk
2. Mengetahui risiko yang terdapat pada PDAM Surya Sembada Kota Surabaya
3. Mengetahui Control Objective yang digunakan untuk mitigasi risiko dalam melakukan audit pada service desk PDAM.
4. Menghasilkan dokumen audit untuk control objective yang digunakan dalam melakukan audit pada service desk PDAM.
5. Mendapatkan temuan audit yang akan dijadikan rekomendasi untuk PDAM.

1.5. Manfaat Tugas Akhir

Manfaat yang diberikan dengan adanya tugas akhir ini adalah sebagai berikut:

1.5.1. Manfaat Perusahaan

Tugas akhir ini diharapkan dapat membantu PDAM Surya Sembada Kota Surabaya dalam membuat dokumen Audit untuk bahan evaluasi pengembangan dan refrensi perangkat organisasi dalam melakukan audit internal terhadap pengelolaan

terkait insiden secara tepat agar kualitas manajemen TI bisa meningkat dan mencapai kepuasan yang diinginkan.

1.5.2.Manfaat Bagi Mahasiswa

Adanya penelitian ini sebagai refrensi dalam bidang audit teknologi informasi/system informasi khususnya pada pembuatan dokumen dan juga menambah wawasan auditor khususnya mengenai Audit Sistem Informasi.

1.5.3.Bagi Penelitian Berikutnya

Tugas akhir ini diharapkan dapat memberikan motivasi dan gambaran bagi peneliti lain untuk melakukan Audit Sistem Informasi pada PDAM Surya Sembada Kota Surabaya.

1.6. Relevansi

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

(Halaman ini sengaja dikosongkan)

BAB II
TINJAUAN PUSTAKA

Dalam Bab ini, akan dijelaskan mengenai penelitian terdahulu dan landasan teori yang digunakan sebagai acuan dalam pengerjaan tugas akhir. Penelitian terdahulu merupakan suatu penelitian yang pernah dilakukan oleh peneliti-peneliti sebelumnya yang diguanakan sebagai acuan tugas akhir. Landasan teori merupakan teori-teori yang berhubungan dengan pengerjaan tugas akhir.

2.1. Studi Sebelumnya

Pada sub bab ini akan diterangkan mengenai beberapa penelitian terdahulu yang telah dilakukan dan memiliki relevansi dengan tugas akhir ini. Penelitian terdahulu tersebut dapat dilihat pada **Error! Reference source not found.** dan **Error! Reference source not found.**.

Tabel 2. 1 Penelitian Sebelumnya (1)

Nama Peneliti	Devi Fitrianah dan Yudho Giri Sucahyo
Judul Penelitian	*Audit Sistem Informasi/Teknologi Informasi Dengan Kerangka Kerja Cobit Untuk Evaluasi Manajemen Teknologi Informasi di Universitas XYZ* [5].
Penjelasan Singkat	Penelitian ini membahas mengenai bagaimana mempertahankan integritas informasi yang disimpan dan diolah untuk meningkatkan keefektifan penggunaan teknologi informasi serta mendukung efisiensi dalam organisasi dan bertujuan untuk melakukan pemetaan terhadap tahap audit TI beserta control yang kemudian diaplikasikan ke suatu perusahaan, yaitu Universitas XYZ yang digunakan sebagai acuan adalah COBIT-ISACA dengan

	menggunakan 210 detailed control objective.. dan menghasilkan rekomendasi untuk manajemen TI yang lebih baik.
Hasil Penelitian	Hasil dari penelitian ini dengan menggunakan metode COBIT sebagai kerangka kerja audit dan ITIL

Tabel 2. 2 Penelitian Sebelumnya (1)

Nama Peneliti	Sarah Putri Ramadhani, Anisah herdiyanti, Hanim Maria Astuti
Tahun Penelitian	2017
Judul Penelitian	*Pembuatan Perangkat Audit Berbasis Risiko Berdasarkan COBIT 5 dan Service Desk Standard Pada Service Desk* [6]
Penjelasan Singkat	Pada penelitian in membahas tentang pembuatan perangkat audit untuk mengembangkan audit pada service desk DPTSI yang dibuat berdasarkan control objective pada service desk standard yang dipetakan dengan proses pada best practice COBIT 5 Domain DSS02 Manage Service Request and incident dan menghasilkan dokumen perangkat audit beserta panduan penggunaannya.
Hasil Penelitian	Hasil penelitian ini menggunakan metode berdasarkan best practice COBIT 5 domain DSS02

2.2. Dasar Teori

Pada sub bab ini akan dijabarkan mengenai dasar teori yang digunakan untuk mendukung pengerjaan tugas akhir ini.

2.2.1. Audit

Audit adalah pemeriksaan sistematis yang menghasilkan analisa, pengujian bukti dan konfirmasi (Cannon,2011) [7]. Menurut Arens dan Loe, Definisi audit sendiri menurut ICASA

proses yang sudah berstruktur atau sudah sistematis secara individu berkualitas dan berkompeten terhadap apa yang akan dievaluasi dan diperoleh bukti secara obyektif dengan tujuan dapat memberikan pendapat dan melaporkan sejauh mana proses itu akan diimplementasikan.

- Menurut Arnes dan Loebbecke, Audit adalah akumulasi dan evaluasi dari data yang didapatkan atau informasi yang didapatkan untuk menentukan dan melaporkan kesesuaian antara informasi yang telah ditentukan dan harus dilakukan oleh seseorang yang berkompeten dan independen[8].
- Menurut Prof L,R.Dicksee Audit adalah pemeriksaan dokumen keuangan dimana fakta dan informasi yang didapatkan mencerminkan hubungan timbal balik yang dilakukan sudah sesuai atau belum[9].

2.2.1.1. Audit Sistem Informasi

Audit Sistem Informasi menurut Riananto Sarno dalam bukunya ”Audit Sistem/Teknologi adalah aktivitas audit yang diakukan untuk memastikan pengelolaan sistem informasi yang sudah terarah dalam kerangka audit untuk perbaikan yang dilakukan pada kerangka perbaikan berkelanjutan dan penyesuaian terhadap kepatutan apakah sistem yang dijalankan sesuai atau tidak dengan standard yang berlaku[10].

2.2.1.2. Pengertian Audit Berbasis Risiko

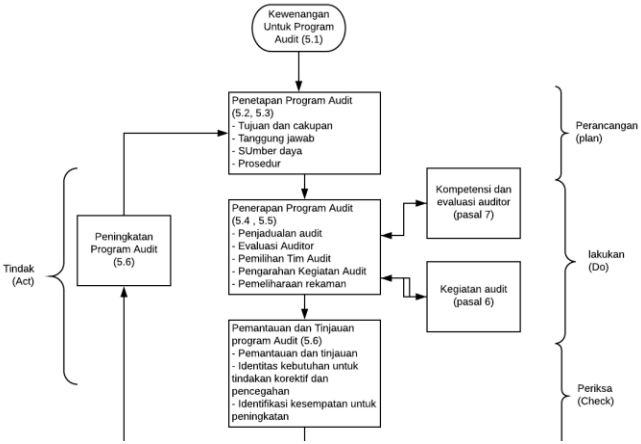
Audit berbasis risiko merupakan aktivitas yang dilakukan auditor yyang bertujuan untuk mendukung hasil atau pencapaian tujuan suatu organisasi yang sudah ditetapkan dengan melihat semua aspek pendukung yang dapat menghambat pencapaian tujuan atau disebut sebagai risiko. Pemahaman *Penilaian Risiko* sangat membantu auditor dalam merencanakan akktivitas audit dengan cara memperhatikan apa yang terjadi didalam sebuah perusahaan terhadap suatu risiko yang terjadi dan bagaimana

kendali operasional internal yang sudah dimiliki oleh perusahan itu sendiri.

2.2.1.3. Program Audit

Beberapa Pengertian mengenai program audit bisa didefinisikan seperti pada poin dibawah ini:

1. Berdasarkan IS/ISO 19011:2011 audit program dapat membantu proses audit menjadi lebih efisien dan efektif. Terdapat informasi dan sumber daya yang dibutuhkan untuk audit antara lain seperti dibawah ini [11]:
    1. Tujuan (objective) untuk program audit dan audit individual
    2. Prosedur program audit
    3. Kriteria audit
    4. Metode audit
    5. Pemilihan tim audit
    6. Sumber daya yang dibutuhkan, meliputi travel dan akomodasi
    7. Proses untuk menangani kerahasiaan, keamanan informasi, kesehatan dan keselamatan, dan hal yang berkaitan.



Gambar 2. 1 Proses Audit ISO 19001

2. Audit program bisa juga berupa pendefinisian prosedur secara rinci dengan mempertimbangkan penilaian dari tingkat risiko. Berdasarkan tingkat spesifikasi sebuah program audit tergantung pada kelengkapan audit yang akan dijalankan, bisa berdasarkan pada tingkat dokumentasi dan pengalaman dari sebuah tim audit. Beberapa yang bisa digunakan dalam program audit diantaranya[12]:
    - Prosedur audit yang digunakan
    - Referensi lain seperti tujuan audit, waktu dan sampling atau contoh
    - Set instruksi atau panduan untuk tim audit
    - Penentuan ukuran dan dasar seleksi untuk masing masing area
    - Alat monitoring dan pencatat pelaksanaan audit yang sesuai.

2.2.1.4. Perangkat Audit

Perangkat *audit* merupakan sebuah alat yang dapat digunakan atau difungsikan sebagaimana untuk membantu proses audit agar lebih efektif dan efisien. Dengan adanya perangkat audit, auditor atau orang yang sedang mengaudit bisa menjalankan audit sesuai dengan tujuan dan memastikan semua proses audit sudah dilakukan dengan baik dan benar[13].
Berdasarkan IS/ISO 19011:2011 pembuatan dokumen audit ini merupakan pembuatan dokumen kerja yang terdapat didalam penulisannya merupakan pembuatan perangkat audit yang akan digunakan oleh tim audit untuk mengumpulkan dan menganalisa relevansi informasi dan bukti yang bisa didapatkan berdasarkan analisa yang akan dicatat pada laporan audit [11].
Berikut ini beberapa penjelasan singkat mengenai perangkat audit yang akan dibuat pada penulisan ini mengacu pada IS/ISO 19011:2011 [11]:

1. Daftar Cek
   Merupakan pengujian yang dilakukan secara real dengan mengecheck apakah prosedur yang sudah dilakukan dengan baik atau tidak. Daftar cek ini dibuat berdasarkan prosedur yang sudah sesuai dengan standart.
2. Audit Report atau Laporan Temuan Audit
   Dibuat berdasarkan kebutuhan pencatatan daftar temuan,hasil *evaluasi data* auditor,data penanggung jawab,solusi,catatan dari pihak managemen organisasi dan laporan pendukung lainnya.
3. Panduan atau Formulir Penggunaan *Perangkat Audit*
   Merupakan formulir atau template untuk melakukan pencatatan informasi dari bukti pendukung, temuan audit dan hasil pertemuan bersama tim audit.

Dalam penelitian ini akan menghasikan dua dokumen, yaitu:

a. Dokumen Perangkat Audit – berisi tentang prosedur Audit, Daftar Cek, dan Laporan Temuan Audit.
b. Dokumen Panduan Penggunaan Perangkat Audit – berisi tentang langkah-langkah dan tata-cara penggunaan dokumen perangkat audit.

2.2.1.5. Jenis Audit

Menurut Abdul Halim, dilihat dari sisi luas pemeriksaan dan untuk siapa audit dilaksanakan, audit dapat dikelompokan menjadi tigass jenis golongan audit, diantaranya sebagai berikut [12]:

1. *Audit Internal* – suatu control organisasi yang mengukur dan mengevaluasi efektivitas organisasi. Informasi yang akan dihasilkan dan akan ditujukan untuk manajemen organisasi sebuah organisasi. Pelaksanakan audit secara *internal* dilakukan oleh auditor internal dan merupakan karyawan organisasi tersebut yang berfungsi untuk membantu meningkatkan efisiensi dan efektivitas kegiatan perusahaan yang dikelola.

2. *Audit Eksternal* – suatu control social yang memberikan jasa untuk memenuhi kebutuhan informasi untuk pihak luar perusahaan yang diaudit. Pelaksanakan audit secara eksternal dilakukan oleh auditor dari pihak luar perusahaan yang independen dan telah terferivikasi atau telah diakui oleh pihak berwenang untuk melaksanakan tugas tersebut. Auditor eksternal pada umumnya dibayar oleh manajemen perusahaan yang sedang diaudit.
3. *Audit Sektor Publik* – suatu kontrol atas organisasi pemerintahan yang memberikan jasanya pada masyarakat, seperti pemerintah pusat ataupun pemerintah daerah. *Audit* dapat mencakup audit laporan keuangan,audit kepatuhan dan audit operasional. Pelaksanakan audit secara internal dilakukan oleh auditor pemerintah dan dibayar oleh pemerintah.

2.2.2. Analisis Risiko TI

Risiko merupakan peristiwa yang tidak pasti atau kondisi yang jika terjadi akan memiliki efek pada setidaknya sebuah proyek [15]. Menurut ISO (*International Standard Operation*), risiko SI/TI adalah suatu potensi yang memiliki ancaman cukup besar yang bisa tereksploitasi kerentanan dari asset atau gabungan asset yang bisa menyebabkan kerugian bagi sebuah organisasi [16].

Manajemen Risiko TI merupakan proses pengidentifikasian, penilaian dan prioritas risiko yang bertujuan sebagai pengoordinasian sumber daya perusahaan agar lebih tepat sasaran untuk meminimalkan kemungkinan terjadinya kesalahan atau risiko dan menimbulkan

Dampak yang berlebihan, proses analisis risiko merupakan tahap bagian dari aktivitas manajemen risiko TI yang terbagi menjadi tahap identifikasi, penilaian, dan prioritas risiko [17].

2.2.3. Kerangka Kerja Analisis Risiko

Kerangka kerja membantu untuk menganalisis risiko secara efektif melalui penerapan proses pada berbagai tingkat dan dalam konteks tertentu dalam sebuah organisasi maupun di perusahaan. Tujuan kerangka kerja manajemen risiko adalah untuk memastikan informasi risiko yang didapatkan dari proses manajemen risiko digunakan untuk memenuhi akuntabilitas pada semua tingkat organisasi yang berhubungan satu sama lain. Agar analisis yang dilakukan berhasil, maka kerangka kerja yang digunakan harus tersertifikasi dan memiliki metode atau landasan yang bisa dijadikan dasar pedoman pengelolaan risiko yang sesuai dengan kesepakatan dari perusahaan[18]. Banyak best practice yang bisa digunakan untuk kerangka kerja dalam melakukan analisis risiko dalam proses manajemen risiko, seperti ISO 31000, COSO ERM dan Cobit 5 for risk memiliki kerangka kerja penilaian risiko namun ISO dan COSO ERM memiliki kekurangan dalam mengidentifikasi risiko berdasarkan apa yang dipengaruhi sasaran tujuan sebuah organisasi, bukan berdasarkan proses dan aktivitas [19].

2.2.4. COBIT 5 For Risk

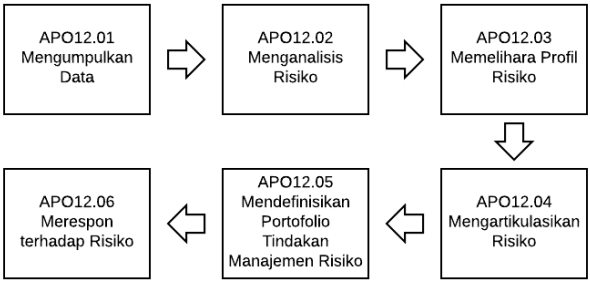
COBIT 5 for Risk adalah panduan kerangka kerja yang dibuat untuk mengatur/mengelola risiko TI didalam sebuah organisasi/perusahaan. COBIT 5 for Risk mendefinisikan bagaimana proses manajemen risiko utama dalam mengidentifikasi, menganalisis dan merespon risiko aktivitas risiko pada penelitian ini berfokus pada praktik sesuai kerangka kerja COBIT 5 for Risk domain APO12 Manage Risk. Sedangkan COBIT 5 sebuah kerangka kerja yang dibuat berdasarkan 5 prinsip dasar dimana kerangka kerja yang dibuat lebih detail termasuk juga panduan yang dapat digunakan untuk melakukan manajemen dan tata kelola perusahaan TI [3].

COBIT 5 Goal Cascade adalah sebuah mekanisme untuk menerjemahkan kebutuhan stakeholder ke dalam data yang spesifik , mudah dilakukan dan bisa sesuai dengan permintaan perusahaan yang berhubungan dengan TI untuk mencapai tujuan

yang diinginkan. COBIT 5 Goal Enabler terdapat 4 bagian diantaranya adalah [3]:

1. *Stakeholder Needs Cascade to Enterprise Goals*
   Tujuan perusahaan yang menggunakan Balanced Scorecard (BSC), dimana BSC berfungsi sebagai penentu dalam mempresentasikan pemetaan tujuan perusahaan.
2. *Stakeholder Drivers Influencer Stakeholder Needs*
   Sesuatu yang dapat mempengaruhi kebutuhan stakeholder dalam perubahan strategi, perubahan lingkungan bisnis dan proses.
3. *Enterprise Goals Cascade to IT-related Goals*
   Pencapaian tujuan yang akan menjadi outcome yang sudah dipetakan berdasarkan IT BSC dan It-related goals, yang sudah dilakukan sebanyak tujuh belas pemetaan didalam COBIT 5.
4. IT-related Goals Cascade to Enabler Goals
   Tujuan TI adalah tujuan sebuah perusahan untuk bisa berhasil, terdapat beberapa hal yang perlu diperhatikan, seperti:
   - Prinsip, kebijakan dan kerangka kerja
   - Proses
   - Struktur organisasi
   - Kebudayaan, etika dan kebiasaan
   - Informasi
   - Layanan, infrastruktur, dan aplikasi
   - Orang, kemampuan dan Kompetensi

Aktivitas manajemen risiko pada penelitian ini focus terhadap praktik sesuai keerangka kerja COBIT 5 for Risk domain APO12 Manage Risk. Dimana dalam kerangka kerja COBIT 5 for risk memiliki beberapa proses yang mendefinisikan pengelolaan risiko TI, berikut alur proses mengelola risiko [18]:



Gambar 2. 2 Proses Mengelola Risiko (sumber: Cobit 5)

Pada pembuatan perangkat Audit berbasis risiko, hanya dilakukan proses APO12.01 mengumpulkan data dan APO12.02 menganalisis risiko. Berikut penjelasan proses dan aktivitas pada tahap mengumpulkan data dan menganalisis risiko.

2.2.4.1. Mengumpulkan Data

Pada tahap mengumpulkan data dalam penelitian ini melakukan survei dan analisis histori risiko TI dan pengalaman kerugian data yang tersedia secara eksternal dan trend. Kemuddian dilakukan pembuatan daftar risiko dan menentukan tipe risiko yang didokumentasikan dalam risk event dan menentukan tipe risiko berdasarkan pada type of risk yang dibagi menjadi tiga kategori yaitu:

- *IT benefit/ Value enablement risk*
  Tipe risiko yang dimana dapat kesempatan untuk menggunakan teknologi dalam meningkatkan efisiensi atau efektifitas bisnis proses dan sebagai enabler untuk membuat bisnis baru.
- *IT program and project delivery risk*
  Tipe risiko yang berkontribusi TI untuk memperbarui atau meningkatkan solusi bisnis dalam bentuk proyek dan program.
- *IT operations and service delivery risk*

Tipe risiko yang berhubungan dengan stabilitas operasional, ketersediaan dan pemulihan layanan TI yang berdampak kehancuran atau penurunan value.

Kemudian menentukan kategori risiko dan menentukan faktor risiko dimana dipengaruhi berdaarkan suatu kondisi dimana frekuensi dan dampak bisnis terhadap scenario risiko.

2.2.4.2. Menganalisis Risiko

Pada tahap menganalisis risiko akan dilakukan pembuatan dan pembaruan skenario risiko TI, yang nantinya akan dikembangkan menjadi aktivitas kontrol yang lebih spesifik. Pada tahap ini dilakukan pemuatan scenario berdasarkn dua jenis yaitu skenario positif dan skenario negatif. Skenario positif kemungkinan risiko TI tidak terjadi begitu pun sebaliknya jika skenario negatife menunjukan risiko TI terjadi. Kemudian dalam menganalisis risiko juga bisa melakukan penilaian risiko berdasarkan perkiraan dan dampak untuk setiap risiko, berdasarkan perkiraan frekuensi dan dampak hasil setiap level. [20]

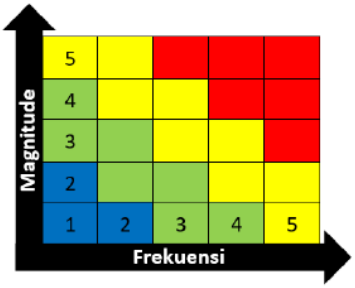
Tabel 2. 3 Penilaian Risiko Berdasarkan Frekuensi [6]

Peringkat Frekuensi	Frekuensi Skenario	Keterangan
1	N≤ 0,1	Very Low - Kemungkinan risiko rendah - Kemungkinan kegagalan terjadi kurang dari 0,1 kali dalam satu tahun
2	0,1 < N ≤ 1	Low - Kemungkinan scenario risiko rendah - Mungkin terjadi dalam beberapa keadaan - Frekuensi kegagalan terjadi lebih dari 0,1 kali dan sama dengan 1 kali dalam satu tahun

Peringkat Frekuensi	Frekuensi Skenario	Keterangan
3	1 < N ≤ 10	Moderate - Kemungkinan scenario risiko terjadi cukup tinggi - Terjadi pada beberapa keadaan (kadang-kadang) - Frekuensi terjadi lebih dai 1 dan kurang dari sama dengan 10 kali dalamm satu tahun
4	10 < N ≤ 100	High - Kemungkinan scenario risiko terjadi tinggi - Kemungkinan terjadi pada sebagian besar keadaan - Frekuensi kegagalan terjadi lebih dari 10 kali dan kurang dari sama dengan 100 kali dalam satu tahun
5	100 < N	Very High - Scenario risiko sangat tinggi dan tidak bisa dihindari - Selalu terjadi pada sebagian besar keadaan - Frekuensi terjadinya kegagalan sangat tinggi, yaitu lebih dari 100 kali dalam satu tahun

Keterangan: N adalah jumlah terjadinya scenario risiko tiap tahun.

Pada analisis risiko juga bisa ditentukan berdasarkan penilaian risiko berdasarkan frekuensi dan dampak risiko TI. Didapatkan prioritas risiko berdasarkan level penilaian risiko melalui pemetaan pada suatu peta risiko yang dibagi menjadi empat wilayah warna. Berikut penggambaran peta risiko[3].



Gambar 2. 3 Peta Risiko 4 Wilayah

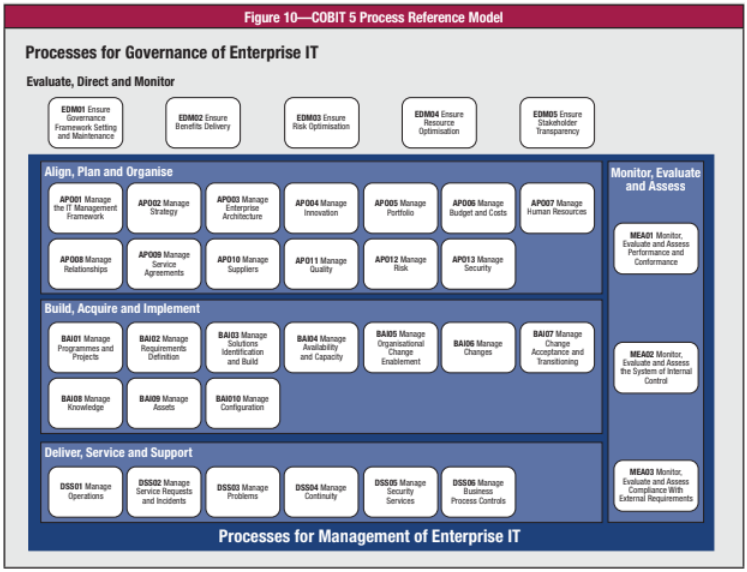
Pemetaan frekuensi dan magniture berdasarkan empat wilayah warna kemudian diklasifikasikan berdasarkan level prioritas kegagalan yang memerlukan penanganan lanjut, berikut pemetaan level prioritas risiko.

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

Tabel 2. 4 Peta Risiko 4 Wilayah

2.2.4.3. Cobit 5 DSS02 Mengelola Permintaan Layanan dan Insiden

Manajemen insiden yang ada di COBIT 5 fokus pada domain *Deliver, Service and Support (DSS)* yang ke dua yaitu Manage Service Request and Incident. Dimana didalam domain tersebut memiliki beberapa proses yang berjalan di dalamnya, DSS02 sendiri menyediakan standarisasi respon yang efektif dan efisien untuk request dari pengguna dan memberika solusi untuk semua jenis insiden agar bisa memenuhi kebutuhan layanan dengan baik [3].



Gambar 2. 4 Manajemen Insiiden Pada COBIT 5 (Sumber: ISACA,COBIT 5: Enabling Process)

Terdapat tujuh proses yang ada didalam DSS02 yang juga akan dijadikan sebagai kontrol dalam pembuatan perangkat audit dalam penulisan ini:

- DSS02.01: Memodifikasi insiden dan skema klasifikasi permintaan layanan
- Menetapkan model insiden terhadap error yang diketahui untuk meningkatkan efektifitas dan efisiensi penyelesaian masalah.
- Menetapkan dan mendefinisikan insiden dan klasifikasi permintaan layanan dan skema prioritas memastikan pendekatan yang konsisten dalam mennginfokan kepada pengguna dan melakukan analisis tren.
- Menetapkan model permintaan layanan berdasarkan tiga permintaan layanan untuk meningkatkan layanan yang bersifat mandiri dan efisien.

- Menetapkan aturan dan prosedur peningkatan insiden khususnya pada insiden keamanan Menetapkan sumber pengetahuan mengenai insiden dan permintaan dan prosedurnya.

- DSS02.02: Mencatat, mengklasifikasi dan memprioritaskan permintaan dan insiden

- Mencatat semua permintaan layanan dan insiden serta merkam semua informasi yang relevan.
- Analisis tren, klasifikasi permintaan layanan dan insiden dengan mengidentifikasi tipe dan kategori
- Pelayanan service dan insiden berdasarkan SLA

- DSS02.03: Memverifikasi, menyetujui dan memenuhi permintaan layanan

- Melakukan verifikasi untuk menggunakan permintaan layanan, jika dimungkingkan, alur proses yang telah didefinisikan dan perubahan standar.
- Memperoleh persetujuan finansial dan fungsional atau tanda tangan, jika dibutuhkan atau persetujuan otomatis untuk persetujuan dalam perubahan yang standar
- Pemenuhan permintaan layanan dengan cara memilih prosedur permintaan, jika memungkinkan menggunakan menu bantuan mandiri dan model permintaan yang telah dibuat sebelumnya.

- DSS02.04: Menginvestigasikan, mendiagnosis dan mengalokasikan insiden

- Mengidentifikasi dan mendeskripsikan gejala untuk menetapkan penyebab yang terjadi. Merefrensikan sumber pengetahuan yang tersedia (error dan permasalahan yang muncul) untuk mengidentifikasi penyelesaian insiden.
- Mencatat permasalahan baru jika masalah terkait sudah diketahui dan tidak ada kesalahan maka akan disetujui berdasarkan kriteria untuk pendaftaran masalah.
- Menetapkan insiden fungsi spesialis jika keahlian yang lebih dalam diperlukan dan melibatkan level manajemen jika dibutuhkan.

- DSS02.05: Menyelesasikan dan memulihkan insiden

- Memilih dan menerapkan penyelesaian insiden yang sesuai.
- Merekam apakah workaround digunakan untuk pencatatan insiden.
- Melaksanakan aksi pemulihan jika dibutuhkan.
- Mendokumentasikan penyelesaian insiden dan menilai jika penyelesaian dapa digunakan untuk sumber pengetahuan kedepannya.

- DSS02,06: Menutup Permintaan Layanan dan Insiden

- Melakukan verifikasi kepuasan permintaan layanan dan penyelesaian insiden terhadap pengguna yang terlibat.
- Menutup permintaan layanan dan insiden.

- DSS02.07: Melacak Status dan membuat Laporan

- Memantau dan menelusuri peningkatan insiden dan prosedur permintaan pengelolaan untuk menuju penyelesaian masalah.
- Melakukan identifikasi stakeholders dari informasi dan kebutuhan data atau laporan serta mengidentifikasi frekuensi dan perantara laporan
- Menganalisis insiden dan permintaan layanan berdasarkan kategori dan tipe untuk menetapkan trend dan mengidentifikasi pola masalah yang berulang. Menggunakan informasi sebagai input dalam perencanaan peningkatan berlanjut.
- Membuat dan mendistribusikan laporan secara tepat waktu atau menyediakan akses data secara online.

2.2.5. Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya

PDAM Surya Sembada Kota Surabaya merupakan salah satu unit usaha milik daerah yang bergerak dibidang distribusi air bersih bagi masyarakat yang tinggal di wilayah Surabaya dan sekitarnya yang diawasi langsung atau dimonitoring oleh pihak eksekutif maupun legislatif daerah. *Unit Teknologi Sistem Informasi* adalah salah satu unit yang terdapat 3 bagian yang memiliki fungsi dasar sebagai sebuah unit yang bertugas untuk

menjalankan siklus pengembangan teknologi system informasi, yaitu *Seksi Pengembangan TI, Seksi Sistem Informasi dan Seksi Infrastruktur*. Unit ini menangani langsung beberapa system dan aplikasi operasional yang dijalankan oleh PDAM Surya Sembada. Beberapa contohnya antara lain. *Aplikasi Customer Service, Call Center, Aplikasi loket untuk pembayaran tagihan air. Android Pengecekan No. rekening, Aplikasi Hubungan Langganan dan masih banyak lagi*. Unit ini selalu menangani segala gangguan pada system PDAM yang terkait langsung dengan teknologi system informasi.

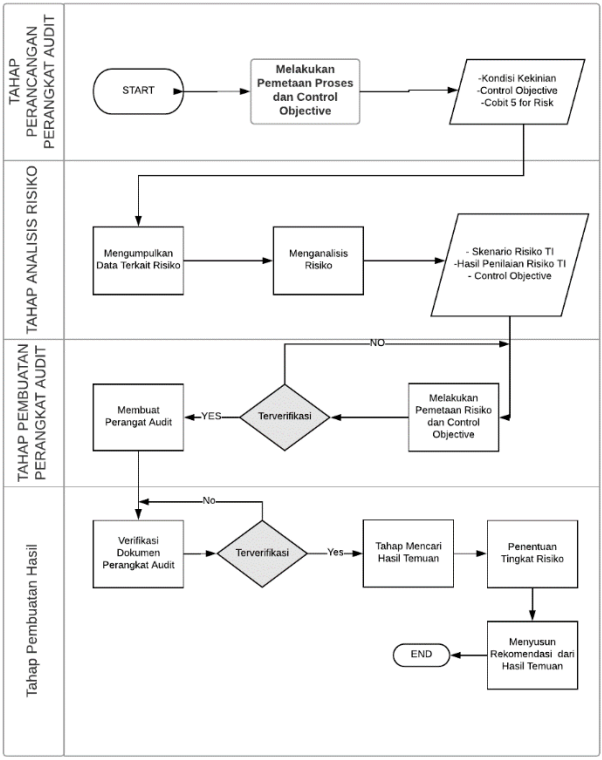
(Halaman ini sengaja dikosongkan)

BAB III
METODOLOGI PENELITIAN

Pada bab ini akan dijelaskan mengena alur metode penelitian yang akan dilakukan oleh peneliti dalam melakukan penelitian ini. Metode penelitian ini juga digunakan sebagai pedoman untuk melaksanakan penelitian agar terarah dan sistematis.

3.1 Metodologi Penelitian

Diagram Metodologi dari Tugas Akhir ini dapat dilihat pada **Gambar 3.1.**



Gambar 3. 1 Metodologi Penelitian

3.2 Tahapan Perancangan Perangkat Audit

Pada tahap ini, adalah tahap awal dalam melakukan aktivitas sebelum membuat perangkat audit berbasis risiko. Tahap ini dilakukan untuk mendapatkan control objective yang digunakan untuk menyusun dokuman perangkat audit. Pada tahap ini juga akan diakukan aktivitas pemetaan proses dan control objective. Namun penulis akan menggunakan perangkat audit yang sudah pernah dilakukan oleh peneliti sebelumnya dan penulis melakukan modifikasi perangkat.

3.2.1. Melakukan Pemetaan Proses dan Control Objective

Dalam penelitian pada tahap perancangan audit adalah tahap awal penulis melakukan aktivitas pembuatan dokumen risiko. Tahap ini dilakukan untuk mendapatkan data yang dibutuhkan untuk mendapat control objective yang sesuai dan akan digunakan untuk menyusun dokumen audit.

3.3 Tahap Analisis

Tahap kedua dalam penelitian ini adalah tahap dimana penulis melakukan dua tahapan proses yaitu tahap mengumpulkan data terkait risiko dan tahap menganalisis risiko.

3.3.1. Mengumpulkan Informasi Terkait Risiko TI

1. Wawancara, dilakukan secara langsung kepada staf service desk yang bertugas secara langsung dalam operasional maupun teknis layanan teknologi informasi di PDAM Surya Sembada. Metode ini digunakan untuk memperoleh informasi kondisi kekinian oeganisasi terkait proses pengelolaan layanan dan insiden pada unit service desk.
2. Survei , dilakukan untuk mengumpulkan data terkait dampak penurunan kepuasan pengguna layanan terhadap scenario risiko yang mungkin terjadi.
3. Studi Literatur (dokumen), dilakukan menggunakan berbagai sumber pustaka atau dokumen. Pada tahapan ini penulis mengumpulkan data terkait risiko TI pada service

desk dari penelitian manajemen risiko TI pada manajemen layanan TI

3.3.2. Menganalisis Risiko

Pada tahap menganalisis risiko dilakukan pengolahan daftar risiko yang sudah diketahui dari hasil wawancara dan survei dari sumber terkait. Pada tahap ini akan dilakukan pemetaan risiko terhadao proses service desk, membuat scenario risiko TI dan melakukan penilaian risiko TI.

3.3.2.1. Membuat Skenario Risiko TI

Aktivitas ini dilakukan untuk membuat dan memperbarui scenario risiko TI secara teratur, termasuk scenario untuk risiko yang tidak terduga, dan akan dijadikan aktivitas control yang lebih spesifik. Pada tahap ini dilaukan pembuatan scenario berdasarkan dua jenis yaitu scenario positif dan negative.

3.3.2.2. Melakukan Penilaian Risiko TI

Penilaian risiko TI dilakukan berdasarkan perkiraan frekuensi dan besarnya keuntungan atau kerugian (magnitude) yang terkait dengan scenario risiko TI. Berdasarkan frekuensi dan magnitude akan didapatkan hasil level setiap risiko ntuk dikelompokan menjadi prioritas risiko TI. Hasil yang dikeluar-kan pada tahapan ini berupa risk register berdasarkan hasil penilaian risiko TI berdasarkan prioritas risiko.

3.4 Tahap Pembuatan Perangkat Audit

Pada tahap ketiga dalam pengerjaan penelitian adalah tahap pembuatan perangkat audit. Didalam tahap ini yang digunakan adalah data dari control objective dan table risk yang telah didapatkan. Pada tahap ini, penulis melakukan dua tahapan proses diantaranya tahap pemetaan risiko dan control objective serta tahap pembuatan perangkat audit.

3.4.1. Melakukan Pemetaan Risiko dan Control Objective

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

3.4.2. Membuat Perangkat Audit

Merupakan tahap penyusunan perangkat audit untuk control objective yang telah dipetakan terhadap risiko TI yang ada. Tahapan ini memiliki aktivitas, yaitu pembuatan dokumen perangkat audit. Namun disini saya menggunakan template perangkat audit yang sudah ada maka saya langsung mencari hasil temuan berdasarkan control objective yang sudah saya temukan.

3.5. Tahap Pembuatan Hasil

Pada tahap terakhir dalam pengerjaan penelitian ini adalah tahap pembahasan hasil. Dimana pada tahap ini, penulis telah berfokus pada verifikasi perangkat audit yang telah didapatkan dari tahapan sebelumnya.

3.5.1. Verifikasi Dokumen Perangkat Audit

Tahap verifikasi perangkat audit dilakukan ketika dokumen perangkat audit selesai dibuaat. Verifikasi dilakukan oleh Kepala TI PDAM Surya Sembada dengan cara menyesuaikan dokumen audit yang dibuat oleh penulis dengan pendekatan best practice yang digunakan. Pada tahapan ini tidak menutup kemungkinan akan ada perbaikan. Pada tahapan ini dilakukan pemenuhan kebutuhan berdasarkan proses dan control objective.

3.6. Tahap Mencari Hasil Temuan

Tahap mencari hasil temuan audit dilakukan ketika dokumen sudah diverifikasi dan telah dirangkum selama proses pengerjaan lapangan. Penulis akan menyimpulkan dan memperoleh keyakinan bahwa temuan yang sudah dirangkum sudah dijalankan sesuai prosedur dan bisa diolah kembali yang akan diberikan tingkatan risiko dan rekomendasi. Untuk melengkapi pembuatan dokumen audit. Maka diperlukan template audit yang akan dibuat yaitu berbentuk template yang nantinya akan berisi tata cara pengisian temuan-temuan yang didapatkan dari proses audit dan resolusi dari temuan audit yang berisikan konten-konten yang telah disesuaikan berdasarkan control yang telah sesuai dengan prosedur audit.

3.7. Penentuan Tingkat Risiko

Penentuan tingkat risiko dilakukan berdasarkan dari hasil temuan dan besarnya keungungan atau kerugian yang berkaitan dengan scenario risiko TI untuk menadapatkan tingkatan risiko yang valid, yang akan didapatkan hasil level setiap risiko untuk kemudian dikelompokan menurut prioritas risiko TI. Hasil keluaran dari penentuan tingkat risiko adalah tabel tingkat risiko berdasarkan hasil temuan audit.

3.8. Menyusun Rekomendasi dari Hasil Temuan

Pada penyusunan rekomendasi dari hasil audit merupakan solusi atau saran alternative untuk menyelesaikan/mengatasi masalah yang ada pada service desk PDAM Surya Sembada yang didapatkan dari hasil temuan audit. Rekomendasi bersifat fisible, operasional, spesifik dan mengidentifikasi subjek yang bertanggung jawab untuk ditindak lanjuti. Kesimpulan atau pendapat harus menempatkaaan berbagai temuan audit dalam perspektif yang didasarkan dari temuan audit secara keseluruhan. Manajemen dan auditor berkewajiban untuk memperhatikan atau memberikan tanggapan atas temuan audit. Auditor internal juga ikut mendiskusikan temuan audit beserta

rekomendasinya agar terhindar dari kesalahpahaman perbedaan pendapat.

3.9. Jadwal Kegiatan

Dalam proses pengerjaan tugas akhir ini terdapat jadwal pengerjaan. Berikut ini merupakan tabel rincian jadwal kegiatan selama penelitian tugas akhir berlangsung

No	Kegiatan	Bulan 1				Bulan 2				Bulan 3			
	Studi Literatur												
	Perancangan Audit												
	Pemetaan proses dan control objective												
	Menganalisis Risiko												
	Membuat perangkat audit												
	Verifikasi dokumen peranngkat audit												
	Tahap mencari Hasil temuan												
	Penentuan tingkat risiko												

No	Kegiatan	Bulan 1					Bulan 2					Bulan 3	
	Menyusun Rek-omendasi hasil temuan												
	Penyusunan Laporan Tugas Akhir												

Tabel 3. 1 Jadwal Pelaksanaan Tugas Akhir

(Halaman ini sengaja dikosongkan)

BAB IV
PERANCANGAN

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

4.1. Perancangan Studi Kasus

Penelitian ini bertujuan untuk menggunakan sebuah studi kasus. Seperti sebagaimana yang diterapkan dalam suatu perusahaan tertentu, yaitu studi kasus PDAM Surya Sembada Kota Surabaya. Harapannya dokumen hasil audit tersebut dapat digunakan oleh auditor internal untuk melakukan pengendalian internal. Penggunaan studi kasus merupakan suatu hal yang sangat penting untuk menggali data dan informasi yang diperlukan pada service desk suatu perusahaan/ organisasi sebagaimmana pengertian dan pentingnya penggunaan sebuah studi kasus menurut para ahli, diantaranya adalah:

1. Yin (2003) menawarkan suatu pengertian yang berbeda mengapa kita harus menggunakan studi kasus dalam melakukan penulisan, dikarenakan sebuah studi kasus adalah suatu metode unik untuk mengamati sebuah topik empiris yang dilakukan berdasarkan satu prosedur yang telah dibuat sebelumnya. Penulisan studi kasuss memiliki kode unik karena hanya mengobservasi area geografis yang sangat kecil atau suatu objek menarik secara mendalam [21].
2. Studi kasus dalam penulisan merupakan sebuah aktivitas pengamatan yang berfokus untuk mendeskripsikan, memahami, memprediksi ataupun mengontrol sebuah individu [22].
3. Sykes (1990) mengatakan bahwa tidak mudah dalam mendapatkan jenis-jenis informasi tertentu yang sulit bahkan tidak mungkin didapatkan selain dengan menggunakan studi kasus [23].

Didalam melakukan sebuah penulisan penting dalam menentukan dan memilih studi kasus yang tepat. Dalam pemilihannya terdapat tiga kategori studi kasus yang dijelaskan oleh Yin [20], diantaranya adalah:

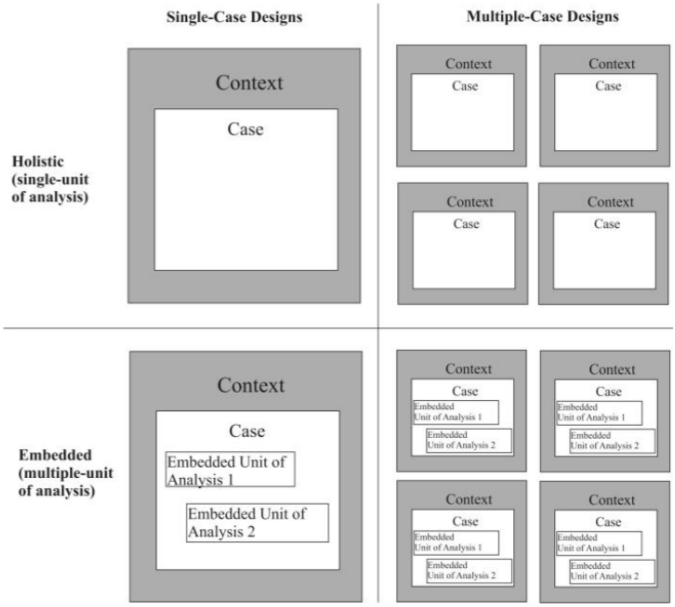
- Studi kasus deskriptif (*descriptive*) bertujuan untuk menggambarkan suatu fenomena yang biasanya berbentuk narasi, yang biasanya harus dimulai dengan mendeskripsikan teori untuk mendukung suatu fenomena tertentu.
- Studi kasus explanatory bertujuan untuk menjelaskan fenomena dalam kata secara jelas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

Pada penulisan ini, tujuan penulis menggunakan studi kasus adalah agar penulis fokus dengan ekplorasi. Pertimbangan dengan pemilihan katogori ekplorasi ini adalah penulis ingin lebih melakukan ekplorasi lebih mendalam pada pengelolaan manajemen insiden pada Unit Teknologi Sistem Informasi pada studi kasus sebuah perusahaan milik pemerintah yang menyediakan sebuah layanan yaitu PDAM Surya Sembada Kota Surabaya.Dengan melakukan pemiihan studi kasus ini akan memudahkan penulis dalam melakukan perancangan penulisan yang akan mempermudah untuk mendapatkan data yang dibutuhkan selama melakukan penulisan.

Dalam melakukan penulisan menurut Yin langkah selanjutnya yang dapat dilakukan adaah dengan melakukan perancangan penulisan. Perancangan yang akan dilakukan untuk membantu penulis dalam memahami dan menentukan tujuan pemilihan studi kasus, persiapan

pengumpulan data untuk kebutuhan penulisan, menentukan metode bagaimana untuk mengolah data hingga menentukan pendekatan untuk melakukan analisis mendalam mengenai data yang nantinya akan digunakan pada proses penulisan [20].

Dalam memilih studi kasus ada dua tipe analisis yaitu *single-case design* dan *multiple-case design*. Terdapat perbedaan antara kedua tipe jika digunakan untuk penulisan, *single-case design* merupakan tipe studi kasus dimana penulis harus lebih perhatian terhadap kasus dan lebih fokus terhadap metode yang digunakan didalam penulisannya. *Single-case design* cukup banyak digunakan pada penulisan dengan kasus yang unik, kritis, menguji kebenaran suatu teori dan mengekplorasi kondisi tertentu pada suatu studi kasus. Sedangkan *multiple-case design* merupakan tipe yang menggunakan lebih dari satu studi kasus yang bertujuan untuk membandingkkan beberapa studi kasus yang ada dan bertujuan untuk melakukan replikasi temuan pada seluruh studi kasus yang ada. Perbedaan pada kedua tipe ini terletak pada jumlah unit of analysis yang digunakan seperti terlihat pada Gambar 7 Type Unit Of Analysis.



Gambar 4. 1 7 Type Unit Of Analysis (Book: A Case Study Methodology) [21]

4.1.1. Unit Of Analysis

Didalam studi kasus yang telah ditentukan, penulis memilih PDAM Surya Sembada Kota Surabaya menjadi studi kasus penulisan. Dimana *Unit of Analysis* telah ditentukan oleh penulis yang merupakan analisis pemetaan untuk mengetahui proses pengelolaan insiden layanan service desk dimana pengelolaan insiden ini akan dilakukan eksplorasi lebih lanjut unuk membantu menemukan hasil temuan pada Unit TSI.

4.2. Persiapan Pengumpulan Data

Pada tahap pengumpulan data dan informasi, peneliti membutuhkan data dan informasi untuk mengetahui kondisi kekinian dan kondisi harapan dari proses pengelolaan permintaan layanan dan insiden pada service sdesk PDAM Surya Sembada Kota Surabaya. Didalam bagian ini akan dibahas bagaimana

metode yang akan digunakan untuk pengumpulan data pada studi kasus penulisan pada pengerjaan tugas akhir ini, penulis menggunakan beberapa metode untuk mengumpulkan data yang dibutuhkan, diantaranya adalah wawancara, observasi dan dokumen. Dari beberapa metode yang digunakan oleh penulis tersebut akan menghasilkan interview protocol pada **LAMPIRAN A** nantinya akan mendasari penulis untuk melakukan wawancara dan observasi.

Berikut penjelasan mengenai metode pengumpulan data yang akan digunakan oleh penulis:

1. *Wawancara*

   Wawancara merupakan aktivitas untuk mengganti informasi dari seseorang untuk suatu tujuan tertentu. Dimna dalam wawancara ini akan dilakukan untuk orang-orang yang memegang kendali terhadap service desk perusahaan, diantaranya adalah staff TSI didalam melakukan teknik ini penulis kan mewawancarai Bapak Tatang Nurlillah Satria Pratama Unit TSI yang berkaitan langsung dengan pengelolaan insiden. Namun tidak semua staff akan diwawancarai melainkan hanya supervisor pada unit TSI dan staff pengguna aplikasi. Wawancara ini dilakukan untuk mendapatkan informasi mengenai kondisi kekinian pengelolaan insiden pada Unit TSI yang meliputi bagaimana alur pengelolaan indsiden mulai dari tahapan pencatatan hingga penanganan dan juga siapa saja yang memegang kendali dan tanggung jawab pada service desk dan setiap insiden yang terjadi.

2. *Observasi*

   Pada tahap kedua adalah observasi melakukan secara keseluruhan teknik pelaporan mulai dari pencatatan manual, telfon, hingga web application service desk untuk mengetahui alur dan proses pengelolaan manajemen insiden. Observasi ini dilakukan untuk mendapatkan data yang akurat mengenai pengelolaan

insiden dengan juga melihat log pencatatan hingga penanganan insiden.

3. *Dokumen*
   Pada tahap ketiga adalah dengan melakukan analisis terhadap beberapa dokumen yang salah satunya adalah log insiden. Dari beberapa teknik pengumpulan data yang akan dilakukan dalam penulisan ini, berikut beberapa detail data yang ingin didapatkan selama proses penelitian:
   - Tugas pokok dan tanggung jawab utama unit TSI yang didalamnya terbagi menjadi bagian utama yaitu bagian Sistem Informasi, bagian Pengembangan SI, dan bagian Infrastruktur.
   - Kondisi seputar pelayanan pada service desk terkait tujuan dan tanggung jawab setiap divisi,
   - Dokumen log Insiden atau daftar list insiden yang berasalh dari web application service desk
   - Dokumen pendukung lain untuk melengkapi evidence dalam pembuatan perangkat audit
   - Dokumen standart yang digunakan dalam melakukan penelitian yaitu dokumen standard COBIT 5

Di dalam teknik pengumpulan data ini terdapat banyak informasi dan data yang harus didapatkan. Dimana data dan informasi ini akan dipertanggung jawabkan pada pidak manajemen PDAM Surya Sembada pada akhir penulisan dalam bentuk dokumen luaran berupa perangkat audit.

4.3. Metode Pengelolaan Data

Metode pengelolaan data pada penulisan ini terdapat dua metode yang digunakan, metode pertama adalah dengan melakukan pennulisan ulang hasil wawancara yang terdapat pada catatan hasil wawancara yang disalin pada aplikasi Mi-

crosoft Word. Metode ini dilakukan agar mempermudah penulis untuk melakukan pengolahan analisis pada hasil wawancara dengan pihak-pihak terkait. Metode pengelolaan data yang digunakan yaitu dengan cara melakukan analisis deskriptif dari data yang didapatkan dengan memaparkannya ke dalam tabel sehingga data menjadi lebih mudah untuk dipahami. Sedangkan data yang didapatkan secara observasi dilakukan pencatatan terhadap hasil pengamatan.

4.4. Pendekatan Analisis

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

- Analisis kondisi kekinian pengelolaan manajemen insiden pada service desk. Analisis ini dilakukan untuk mengetahui bagaimana alur dan proses pengelolaan manajemen insiden mulai dari tahapan hingga penanganan serta siapa saja yang memegang tanggung jawa pada setiap insiden. Alur yang terdapat pada proses ini akan digunakan dalam proses pemetaan dengan COBIT 5
- Analisis pemetaan terhadap kondisi kekinian pada pengelolaan insiden terhadap pengelolaan insiden berdasarkan COBIT 5 untuk mendapatkan daftar proses yang akan digunakan dalam pemetaan *control objective.*
- Analisis pemetaan untuk menentukan *control objective* yang disesuaikan dengan COBIT 5
- Analisis pendektan manajemen rissiko berdasarkan *control objective* untuk mencari kemungkinan risiko yang akan terjadi selama pengelolaan insiden tersebut.
- Analisis penilaian risiko berdasarkan *risk register* yang telah diidentifikasi berdasarka *control objective* untuk menentukan prioritass tingkat kepentingan perangkat audit.

(Halaman ini sengaja dikosongkan)

BAB V
IMPLEMENTASI

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

5.1. Proses Pelaksanaan Penulisan

Pada bab pelaksanaan penulisan ini, akan dibahas mengenai hasil perancangan studi kasus yang didapatkan melalui wawancara berserta dengan daftar data dan informasi yang sudah didapatkan. Berdasarkan perancangan studi kasus yang telah dilakukan berdasarkan kriteria yang telah ditetapkan pada ahap persiapan pengumpulan data, maka narasumber yang diwawancara adalah Bapak Aditya sebagai staff bagian Tata Usaha, Ibu Ira sebagai staff kelola kinerja perusahaan dan Bapak Nurlillah Satria Pratama sebagai supervisor Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya.Wawancaa mengenai kondisi kekinian pengelolaan insiden pada *service desk* dilakukan lebih dari 3 kali. Hasil wawancara tersebut secaara singkat akan dijelaskan pada poin dibawah ini:

1. Pengelolaan service desk dilakukan dengan menggunakan web application service desk.
2. Pelaporan insiden dan permintaan menggunakan tiga saluran yaitu web application, form pelaporan insiden dan telepon.
3. Pengelolaan insiden pada service desk unit TSI bertujuan untuk memulihkan insiden yang terjadi dimulai dari melakukann proses pelaporan insiden, pencatatan insiden hingga penanganan insiden pada aplikasi dan infrastruktur TI.
4. Service desk dikelola oleh beberapa staff TI dan beberapa admin yang telah diberikan jobdesk sesuai dengan pembagian aplikasi dan infrastruktur yang ada pada perusahaan.
5. Semua system yang terdapaat pada aplikasi web sudah terintegrasi.

6. Jaringan yang digunakan local dan bisa juga digunakan jaringan luar.
7. Semua departemen memiliki system di dalam aplikasi service desk.
8. Jika terjadi insiden seperti pemadaman listrik maka systemnya dilakukan secara manual menggunakan kertas, yang kemudian akan diinputkan ke dalam application web service desk jika jaringan sudah bisa digunakan.

Untuk hasil wawancara telah dilakukan secara lengkap terlampir pada **LAMPIRAN B.**

5.2. Gambaran Umum Unit TSI

Unit Teknologi Sistem Informasi merupakan unit yang ada pada PDAM Surya Sembada Kota Surabaya. Pada umumnya fungsi dasar dan tujuan dari unit TSI adalah menjalakan siklus pengembangan teknologi informasi.

Tabel 5. 1 Tugas Pokok dan Fungsi Bagian Pengembang TI

Informasi Dasar	Uraian
Bagian	Teknologi Sistem Informasi
Seksi	Pembagian TI
Fungsi Dasar	Menjalankan proses bisnis pada Teknologi Sistem Informasi dengan proses koordinasi perencanaan, pelaksanaan, evaluasi, tindak lanjut, dan laporan hasil kerja.
Tugas Pokok	Melakukan pengawasan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan;
	Melakukan pengawasan pembuatan standarisasi software, aplikasi dan infrastruktur yang akan diimplementasikan di perusahaan

	Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan
	Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi
	Melakukan pengawasan kepastian perusahaan menggunakan perangkat lunak yang legal
	Melakukan pengawasan kegiatan *helpdesk support.*
	Menerima pengaduan IT menggunakan aplikasi helpdesk
	Sosialisasi teknologi yang sudah diperbarui
Tugas Umum	Menyusun dan menyampaikan laporan kinerja kepada supervisor pengembangan TI
	Melaksanakan tugas lain yang diberikan supervisor pengembangan TI

Tabel 5. 2 Tugas Pokok dan Fungsi Bagian Sistem Informasi

Informasi Dasar	Uraian
Bagian	Teknologi Sistem Informasi
Seksi	Sistem Informasi
Fungsi Dasar	Menjalankan proses bisnis pada Teknologi Sistem Informasi dengan proses koordinasi perencanaan,pelaksanaan,evaluasi,tindak lanjut, dan laporan hasil kerja.
Tugas Pokok	Melakukan pengawasan pemeliharaan dan perbaikan aplikasi sistem informasi
	Melakukan pengawasan kegiatan penambahan-penambahan fitur aplikasi eksisting
	Melakukan pengawasan kegiatan analisa dan desain terhadap pengembangan aplikasi eksisting

	Melakukan pengawasan kegiatan evaluasi terhadap aplikasi-aplikasi secara reguler dan mengusulkan perbaikan aplikasi
	Melakukan pengawasan kegiatan *backup* seluruh aplikasi dan *source code* secara reguler
	Melaksanakan pembuatan aplikasi baru sesuai surat keputusan direksi
	Melakukan pengawasan kegiatan perbaikan data pada *database*.
	Menambahkan fitur pada aplikasi sesuai permintaan
Tugas Umum	Menyusun dan menyampaikan laporan kinerja kepada supervisor Sistem Informasi
	Melaksanakan tugas lain yang diberikan supervisor Sistem Informasi

Tabel 5. 3 Tugas Pokok dan Fungsi Bagian Infrastruktur

Informasi Dasar	Uraian
Bagian	Teknologi Sistem Informasi
Seksi	Infrastruktur
Fungsi Dasar	Menjalankan siklus infrastruktur pada Teknologi Sistem Informasi dengan proses koordinasi perencanaan,pelaksanaan,evaluasi,tindak lanjut, dan laporan hasil kerja.
Tugas Pokok	Melaksanakan instalasi hardware dan software operating system client dan printer client
	Menyelesaikan permasalahan yang terjadi pada hardware,software, dan jaringan LAN
	Menyiapkan computer dan printer backup
	Pengecekan status update antivius server dan client harian
	Pengecekan suhu ruangan server harian dan kondisi space server untuk client serta server active directory harian
	Support helpdesk untuk client

	Pengecekan status access control network dan availability jaringan wireless
	Monitoring LAN
	Memonitorin penggunaan bandwith
	Memonitoring keamanan jaringan dan ancaman hacker dan sejenisnya dengan melakukan konfigurasi dan monitoring firewall
	Pengecekan IP dynamic server dan client
	Pengawaasan terhadap maintenance link wireless
Tugas Umum	Menyusun dan menyampaikan laporan kinerja kepada supervisor Infrastruktur
	Melaksanakan tugas lain yang diberikan supervisor Infrastruktur

Unit ini menangani beberapa system dan aplikasi operasional yang dijalankan oleh PDAM seperti aplikasi *Customer Service, Call Center, Aplikasi loket* untuk pembayaran tagihan air, Android pengecekan No.Rekening dan tagihan, sebagian *Website* untuk simulasi rekening, Aplikasi Hubungan Langganan dan masih banyk lagi. Unit ini selalu siap menangani segala gangguan pada system di PDAM yang terkait langsung dengan teknologi system informasi.

5.3. Gambaran Umum Pengelolaan Insiden Unit TSI

Tugas pokok Unit Teknologi Sistem Informasi adalah untuk melakukan pengelolaan insiden yang baik. Dimana dalam pengelolaan insiden merupakan hal yang akan berhubungan langsung dengan user pada perusahaan. Pengelolaan insiden yang baik harus bisa menangani setiap insiden dengan cepat dan tepat maka Unit TSI harus selalu siap untuk menangani setiap insiden yang muncul kapan saja dan harus ada pelaporan insiden hingga membuat dokumentasi terhdap pihak terkait seperti *user/requester* dan pihak manajemen. Berdasarkan dokumen scenario helpdesk yang dimiliki oleh Unit TSI, untuk menjalankan helpdesk terdapat tiga bagian yang pertama adalah *User* membuat pengaduan dan bisa diselesaikan langsung oleh helpdesk, kedua adalah *User* membuat pengaduan, *Helpdesk*

tidak dapat menyelesaikan sehingga diteruskan ke bagian Teknisi *Software* atau *Hardware* dan ketiga adalah *User* membuat pengaduan, *Helpdesk* atau teknisi Software atau *Hardware* tidak dapat menyelesaikan sehingga diteruskan ke rekanan.

Proses pelaporan insiden yang ada di PDAM Surya Sembada menggunakan tiga saluran untuk penanganan insiden, diantaranya adalah melalui telfon, form pelaporan *offline* dan *aplikasi service desk.* Masing-masing saluran pelaporan memiliki 2 admin yang bertugas untuk menginputkan laporan insiden ke dalam web *application service desk* dan file pencatatan insiden dalam file excel. Dimana untuk setiap tanggung jawab akan bertugas menangani indisen yang terjadi. Setelah dilakukan pencatatan, insiden yang telah masuk ke system akan dilakukan verifikasi oleh admin dan teknisi terkait penyelesaian yang dilakukan pada insiden tersebut apakah dapat dikerjakan atau tidak, jika tidak maka akan langsung diinformasikan kepada *requester,* namun jika indisen yang telah dilaporkan dapat ditangani akan langsung diberikan ke pihak teknisi atau penanggung jawab yang bertugas sesuai dengan *job desk* yang sudah diberikan tanggung jawab. Jika insiden sudah berhasil ditangani dan diselesaikan, maka admin akan mengubah status insiden menjadi close, krena hal ini akan dapat memudahkan *requester* untuk melakukan control pada insiden yang telah dilaporkan pada pihak PDAM Surya Sembada.

5.4. Proses Manajemen Insiden Berdasarkan Standard

Pengelolaan insiden merupakan sebuah aktivitas yang harus diperhatikan oleh sebuah perusahaan. Mengingat insiden merupakan suatu kejadian yang tidak direncanakan yang biasanya sering terjadi pada layanan TI sehingga memberikan penurunan kualitas pemberian layanan TI. Manajemen insiden dibutuhkan untuk memperbaiki layanan yang diberikan pada pelanggan secara cepat dan memungkinkan dapat meminimalisir dampak terhadap proses bisnis yang ada di perusahaan. Berdasarkan

standard yang digunakan dalam penelitian ini berikut akan dijelaskan pada tabel 5.1 proses pengelolaan insiden dalam Standard merupakan rincian dari proses pengelolaan insiden.

Tabel 5. 4 Proses Pengelolaan Insiden dalam COBIT 5

COBIT 5
DSS02.01 Mendefinisikan insiden dan skema klasifikasi permintaan layanan
DSS02.02 Mencatat,mengklasifikasikan dan memprioritaskan permintaan dan insiden
DSS02.03 Memverifikasikan, menyetujui dan memenuhi permintaan layanan
DSS02.04 Menginvestigasikan,mendiagnosis dan mengalokasikan insiden
DSS02.05 Menyelesaikan dan Memulihkan Insiden
DSS02.06 Menutup Permintaan Layanan dan Insiden
DSS02.07 Melacak status dan membuat laporan

Proses pengelolaan insiden berdasarkan COBIT 5 inilah yang nantinya akan digunakan dalam melakukan pendektan analisis berdasarkan tahapan perancangan. Proses inilah yang nantinya akan digunakan dalam melakukan pemetaan proses pengelolaan insiden, pemetaan control objective hingga proses mengemukan hasil audit dan memberikan rekomendasi.

5.5. Pendefinisian Kemungkinan dan Tingkat Dampak Risiko

Pada proses perancangan, pada bagian pendekatan analisis salah satunya dengan melakukan identifikasi terhadap kemungkinan terjadinya risiko untuk setiap *control objective* yang dihasilkan. Sebelum melakukan identifikasi kemungkinan

risiko pada setiap control objective, penelitian ini juga akan memberikan gambaran mengenai skala yang akan terjadi pada setiap proses pengelolaan insiden yang ada pada service desk Unit TSI. Kemungkinan risiko ini dihasilkan melalui tahapan wawancara pada SPV Manajer Unit TSI. Penulis menentukan rentang skala risiko yang menunjukan presepsi responden terhadap pernyataan yang diberikan. Rentang skala likert kuisisoner yang dipetakan dengan peringkat dampak keunggulan kompetitif ditunjukan pada **Error! Reference source not found.**.

Tabel 5. 5 Tingkat Dampak Risiko [6]

Peringkat dampak	Keunggulan Kompetitif	
	Penurunan Kepuasan Pengguna	**Keterangan**
1	I ≤ 1	*VeryLow* Kegagalan menyebabkan penurunan yang sangat tidak signifikan (sangat rendah) terhdap kepuasan pengguna layanan
2	1 < I ≤ 1,5	*Low* Kegagalan menyebabkan penurunan yang tidak signifikan (rendah) terhdap kepuasan pengguna layanan
3	1,5< I ≤ 2	*Moderate* kegagalan menyebabkan penurunan yang cukup signifikan terhdap kepuasan pengguna layanan

4	$2 < I \leq 2,5$	*High* Kegagalan menyebabkan penurunan yang signif-ikan terhadap kepuasan pengguna layanan
5	$2,5 \leq I$	*Very High* Kegagalan menyebabkan penurunan yang sangat signifikan (sangat tinggi) terhdap kepuasan pengguna layanan

Pada Tabel 5.6 dibawah adalah daftar risiko berdasarkan hasil observasi pada PDAM Surya Sembada Kota Surabaya. Dimana masih adanya risiko yang tidak sesuai deng COBIT 5 best prac-tice

Tabel 5. 6 Daftar Risiko Pengelolaan Insiden Unit TSI

No.	Indikator Risiko	Uraian Peristiwa Risiko	Sebab Risiko	Level Risiko			Peringkat dampak
				L	K	LxK	
1	Data center PDAM terletak pada dalam gedung Kantor Pusat, Termasuk penggunan fasilitas yang ada pada gedung seperti pasokan listrik (yanh menggunakan support dari PLN. Dengan semakin terkomputerisasinya berbagai kegiatan dalam layanan perusahaan maka diperlukannya data center yang selalu terjaga keaktifannya, salah satunya dengan memperhatikan pasokan listrik	Risiko tidak mendapat Suplai Listrik	- Pasokan listrik utama dari PLN Padam - Kerusakan pada komponen listrik (MCB gedung) untuk ruang server	3	3	9	3 Medium
2	Pelayanan Online payment juga adanya website sebagai media komunikasi perusahaan, maka jaringan komputer PDAM haus selalu online dan dalam beberapa detailnya dapat diakses oleh masyarakat dan pihak perbankan, yang rentan terhadap gangguan	Resiko gangguan dan serangan terhadap komputer , server dan jaringan	- Penggunaan Flashdisk dan akses internet yang terinfeksi virus - Usaha peretass untuk merusak website	4	3	12	4 High

No.	Indikator Risiko	Uraian Peristiwa Risiko	Sebab Risiko	Level Risiko			Peringkat dampak
				L	K	LxK	
	dan serangan dari pihak ketiga. selain itu pertukaran ddata di internal perusahaan melalui media media penyimpan yang ada juga rentan terhadap penularan virus computer		dengan tujuan menggagalkan operasional atau menurunkan citra perusahaan				
3	Perangkat keras dapat selalu dimanfaatkan secara optimal dalam operasi perusahaan selama masih berfungsi baik. Selain memiliki umur produktif usia pakai perangkat keras juga bergantung dari pemeliharaan dan faktor-faktor eksternal seperti adanya gangguan listrik	Risiko kerusakan perangkat keras	- Tegangan listrik yang tidak stabil - Mencapai masa MTBF (Mean Time Between Failure)	3	3	9	3 Medium
4	Dengan adanya komputerisasi dengan menggunakan berbagai aplikasi berbasis database pada beberapa lini pekerjaan, maka konseksivitas data pada jaringan yang ada sangat mutlak dibutuhkan	Risiko kegagalan koneksi data pada jaringan dalam kantor pusat (LAN)	- Kabel jaringan computer putus (LAN) - Kerusakan peralatan jaringan	2	2	4	2 Low

No.	Indikator Risiko	Uraian Peristiwa Risiko	Sebab Risiko	Level Risiko			Peringkat dampak
				L	K	LxK	
		serta antara kantor pusat dan cabang (WAN)	- Antenna Wireless (WAN) bergeser pointing-nya karena angina (factor alam)				
5	Bagian TSI selain mengelola jaringan komputer juga membuat aplikasi-aplikasi berbasis database yang dibutuhkan oleh unit kerja lain pada perusahaan untuk mempermudh pekerjaannya	Risiko eror dalam pembuatan aplikasi	Permintaan user terlalu -sering berubah untuk proses bisnis yang sama	3	3	9	3 Medium
6	Pembayaran tagihan air oleh pelanggan sekarang melalui online payment, baik dari ATM beberapa bank maupun melalui mitra-mitra loket pembayaran. Maka tidak boleh ada kegagalan. Dalam online payment karena akan menyebabkan kegagalan dalam penerimaan pendapatan perusahaan	Risiko kegagalan aplikasi payment gateway	- Kerusakan hardware - Kegagalan layanan DBMS (Database Management System) - Kegagalan koneksi dari sitching agent	2	5	15	5 Very High

No.	Indikator Risiko	Uraian Peristiwa Risiko	Sebab Risiko	Level Risiko			Peringkat dampak
				L	K	LxK	
7	Penggunaan aplikasi berbasis database pada beberapa area pekerjaan menyebabkan pentingnya jaminan ketersediaan atau kualitas kinerja database management system yang menunjang pekerjaan tersebut	Risiko Downtime database	- Kerusakan hardware - Kerusakan ORACLE Database berhenti	3	4	12	4 High
8	Semakin banyak area pekerjaan yang didukung oleh aplikasi berbasis databe maka akan semakin berat pula beban pada database dan perangkat pendukuungnya, sehingga perlu mendapat perhatian dalam pemeliharaannya	Risiko kinerja database lambat memberikan response	- Terdapat session pada DB yang tidak lepas otomatis saat aplikasi selesai meminta request - Disk space mencapai threshold (batas aman kemampuan)	4	4	16	5 Very High
9	Karena data center terletak pada dalam gedung kantor pusat maka	Risiko kebakaaran pada data center	- Gangguan binatang pada jalur listrik dan jalur	1	3.5	3.5	2 Low

No.	Indikator Risiko	Uraian Peristiwa Risiko	Sebab Risiko	Level Risiko			Peringkat dampak
				L	K	LxK	
	keberadaanya menjadi tidak independen karena bergantung pada ketersediaan fasilitas yang ada, termasuk melekatnya risiko kebakaran yang disebabkan dari ruang lain pada gedung tersebut		data (misa:tikus,serangga) - Konrsleting				
10	Karena data center terletak pada dalam gedung kantor pusat maka keberadaanya menjadi tidak independen karena bergantung pada ketersediaan fasilitas yang ada, termasuk melekatnya risiko kebocoran air hujan letak ruangan di lantai 4 langsung berhadapan dengan atap	Risiko kebocoran air hujan pada data center	Kerusakan sever dan storage pada data center	3	3,75	12,5	4 High
11	Karena data center terletak pada dalam gedung kantor pusat maka keberadaanya menjadi tidak independen karena bergantung pada	Risiko Induksi Petir	- Kerusakan pada switch data	2	2	4	2 Low

No.	Indikator Risiko	Uraian Peristiwa Risiko	Sebab Risiko	Level Risiko			Peringkat dampak
				L	K	LxK	
	ketersediaan fasilitas yang ada, termasuk melekatnya risiko Induksi petir		- Pelayananyang menggunakan aplikasi (termasuk online payment) tidak dapat beroperasi				

5.6. Pemetaan Control Objective

Pada table dibawah ini adalah hasil dari pemetaan *Control Objective* berdasarkan *Key Management Practice* yang menghasilkan proses pemetaan berdasarkan COBIT 5 dimana didalam pemetaan pada bagian ini, penulis menggunakan semua proses dan aktivitas pada COBIT 5 dengan pertimbangan perusahaan dalam menggunakan standard yang berlaku.

Pemetaan dilakukan dengan mencari hubungan antara proses ideal berdasarkan COBIT 5 domain DSS02 *Manage Service Request and Incidents* dengan control yang dibutuhkan dalam setiap prosesnya sehingga didapatkan pemetaan control objective. Tabel 5.6 Pemetaan pemetaan key management practice di bawah ini menunjuksn gambaran besar dari pemetaan control objective yang nantinya dapat digunakan dalam pembuatan hasil temuan audit.

Tabel 5. 7 Pemetaan Key Management Practice

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
P01	**DSS02.01** Mendefinisikan insiden dan skema klasifikasi permintaan layanan	Mendefinisikan insiden dan klasifikasi permintaan layanan dan kriteria untuk problem registrasi, untuk mengatur, dan menginformasikan user tentang kondisi kekinian	CO201.001	Memastikan adanya mekanisme pendefinisian insiden	Mekanisme pendefinisian telah sesuai dengan ketetapan dan ketentuan
			CO201.002	Memastikan adanya informasi untuk User atau pengguna Service Desk	Terdapat dokumen informasi pengguna Service Desk
		Mendefinisikan model insiden untuk mengetahui risiko dan memberikan solusi	CO201.003	Memastikan adanya pengelolaan insiden	Insiden yang terjadi dapat diselesaikan sesuai dengan prosedur

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
		Menentukan model permintaan layanan sesuai dengan permintaan layanan	CO201.004	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden	Menggunakan standard yang sudah ditentukan oleh PDAM
		Menentukan insiden ekskalasi dan prosedur, terutama untuk insiden besar dan insiden keamanan	CO201.005	Memastikan adanya struktur organisasi bagian TSI pada PDAM penanganan insiden	Terdapat struktur organisasi penanganan insiden
		Menetapkan insiden dan mencari sumber pengetahuan dan kegunaanya	CO202.001	Memastikan adanya mekanisme pendekatan penanganan	Terdapat mekanisme pendefinisian telah sesuai dengan ketetapan dan ketentuan

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
PO2	**DSS02.02** Mencatat,mengklasifikasikan dan memprioritaskan permintaan dan insiden	Semua log (catatan) permintaan layanan dan insiden,	CO201.003	Memastikan adanya prosedur pengelolaan insiden	Insiden yang terjadi dapat diselesaikan
			CO202.002	Memastikan adanya pencatatan insiden pada system Log	Catatan insiden pada log system pada web
			CO202.004	Memastikan adanya skema prioritas insiden berdasarkan tingkat risiko	Terdapat pendefinisian konten skema prioritas

Pemetaan akan lebih terinci terlampir pada **LAMPIRAN C**. Pemetaan Key Management Practice yang dihasilkan untuk semua proses tidak jarang memiliki kesamaan control, sehingga pada 5.8 Control Objective akan dijabarkan control-kontrol yang sudah diselesaikan.

Tabel 5. 8 Control Objective

No	ID Control Objective	Control Objective
1	CO201.001	Memastikan adanya mekanisme pendefinisian insiden. Dimana didalamnya terdapat ketentuan
2	CO201.002	Memastikan adanya informasi untuk User atau pengguna Service Desk
3	CO201.003	Memastikan adanya prosedur pengelolaan insiden.
4	CO201.004	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden.
5	CO201.005	Memastikan adanya struktur organisasi bagian TSI pada PDAM.
6	CO202.001	Memastikan adanya mekanisme pendekatan penanganan
7	CO202.002	Memastikan adanya pencatatan insiden pada System Log
8	CO202.003	Memastikan adanya mekanisme analisis tren.
9	CO202.004	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko
10	CO203.001	Memastikan adanya mekanisme persetujuan penanganan insiden
11	CO203.002	Memastikan adanya klasifikasi insiden dan permintaan layanan

No	ID Control Objective	Control Objective
12	CO205.001	Memastikan Adanya Penutupan atau Penanganan pada Insiden
13	CO207.001	Memastikan adanya pelaporan pengelolaan insiden.

5.7. Analisis Risiko

Pada proses perancangan, salah satu pendekatan analisis yang dilakukan pada penelitian ini adalah menganalisis risiko berdasarkan *best practice* COBIT 5 DSS02 untuk mencari kemungkinan risiko yang akan terjadi pada proses pengelolaan permintaan layanan dan insiden pada *service desk* Unit TSI. Dimana pada tahap analisis risiko tersebut dihasilkan tingkat risiko berdasarkan perhitungan **Kemungkinan x Dampak** maka dihasilkan hasil tingkatan risiko berdasarkan tabel perhitungan *likelihood*. Sebelum melakukan analisis risiko, dilakukan pemetaan Control Objective pada setiap proses aktivitas COBIT 5 DSS02. Kemungkinan risiko yang dihasilkan melalui tahapan wawancara dan observasi akan dijabarkan pada Tabel 5.9. Untuk hasil Analisis Risiko telah dilakukan secara lengkap terlampir pada **LAMPIRAN D**

Tabel 5. 9 Analisis Risiko Berdasarkan Aset

No	ID Risiko	Strategi	ID Control Objective	Control Objective
1	RO1	Pendefinisian insiden sesuai dengan ketentuan perusahaan	CO201.001	Memastikan adanya mekanisme pendefinisian insiden. Dimana didalamnya terdapat ketentuan
2	RO2	Melakukan pengecheckan/konfirmasi insiden yang dilakukan	CO202.002	Memastikan adanya pencatatan insiden pada System Log
3	RO3	Melalkukan monitoring server secara berkala	CO202.002	Memastikan adanya pencatatan insiden pada System Log
4	RO4	Monitoring server setiap hari untuk menghindari kegagalan back up data	CO202.004	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko
5	RO5	Pengintegrasian log system yang lebih aman	CO202.002	Memastikan adanya pencatatan insiden pada System Log

6	RO6	Mengkoordi-nasikan job-desk sesuai dengan jenis insiden	CO201.002	Memastikan adanya in-formasi un-tuk User atau pengguna Service Desk
7	RO7	Penggunaan hak akses yang lebih terin-tegrasi	CO202.004	Memastikan insiden yang ditangani sesuai dengan ting-kat pe-nanganan risiko
8	RO8	Pembuatan prosedur pengelolaan in-siden	CO201.003	Memastikan adanya prosedur pengelolaan insiden.
9	RO9	Pengecheckan sebelum menginput in-siden	CO202.002	Memastikan adanya pen-catatan in-siden pada System Log
10	RO10	Melemparkan insiden pada pihak expert	CO201.005	Memastikan adanya struktur or-ganisasi ba-gian TSI pada PDAM penanganan insiden
11	RO11	Melakukan pembekalan pada admin	CO203.001	Memastikan adanya mekanisme

		/staff untuk penanganan insiden		persetujuan penanganan insiden
12	RO12	Membatasi pemakainn user dan bandwith	CO202.001	Memastikan adanya mekanisme pendekatan penanganan
13	RO13	Monitoring rutin setiap hari kerja atas event status server dan jaringan	CO203.002	Memastikan adanya pelaporan pengelolaan insiden.
14	RO14	Monitoring usia sparepart menggunakan IT Aset Manajement	CO202.004	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko
15	RO15	Peningkatan kompetensi SDM kuaifikasi jaringan computer (jaringan eksternal)	CO202.004	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko
16	RO16	Berkoordinasi pada subdir pemeliharaan untuk melaksanakan pengecheckan berkala jalur ground gedung	CO202.004	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko

		dan jalur kabel data		
17	RO17	Melakukan testingsaat pembuatan aplikasi	CO202.001	Memastikan adanya mekanisme pendekatan penanganan
18	RO18	Menerapkan standar sesuai dengan ketentuan perusahaan	CO201.004	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden.
19	RO19	Memberikan pembekalan untuk memecahkan masalah	CO205.001	Memastikan Adanya Penutupan atau Penanganan pada Insiden
20	RO20	Pengecheckan pelaporan pengelolaan insiden setiap hari	CO207.001	Memastikan adanya pelaporan pengelolaan insiden

Tabel 5. 10 Analisis Risiko

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
RO1	Kesalahan pendefinisian insiden	Miskomunikasi, salah koordinasi sesame staff admin	Kesalahan pendefinisian insiden frekuensi terjadinya bisa ± 2x dalam sebulan	Banyak kesalaha pahaman dalam mengartikan insiden sehingga terjadi kesalahan dalam menjalankan penanganan insiden ± 2	4 Medium
RO2	Insiden tidak dicatatkan pada Web Application	Kelalaian admin	Insiden tidak dicatatkan pada web application karena insiden berkaitan langsung dengan pengguna frekuensi terjadinya bisa ± 10x dalam sebulan	Insiden yang dilaporkan tidak bisa ditangani karena tidak masuk ke dalam log system frekuensi terjadinya bisa ± 4x dalam sebulan	14 Very High

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
RO3	Risiko kinerja database lambat memberikan respone	Data overload, salah update database, database kacau	Kapasitas DB yang terbatas menyebabkan aplikasi menjadi lambat frekuensi terjadinya bisa ± 4x dalam sebulan	Beberapa aplikasi menjadi lambat frekuensi terjadinya bisa ± 14x dalam sebulan	16 Very High
RO4	Gagal melakukan backup	System backup tidak berjalan sesuai jadwal	Gagal melakukan backup pada saat pemindahan data frekuensi terjadinya bisa ± 4x dalam sebulan	Data yang ada deserver bisa saja terhapus atau data corrupt frekuensi terjadinya bisa ± 3x dalam sebulan	12 High
RO5	Bocornya log insiden	Data rahasia perusahaan bocor kepihak yang tidak bertanggung jawab	Data yang bocor disalahgunakan untuk kejahatan atau penyalahgunaan	Perusahaan mengalami kerugian atas perbuatan pihak tidak bertanggung jawab frekuensi terjadinya bisa ± 4x dalam sebulan	8 High

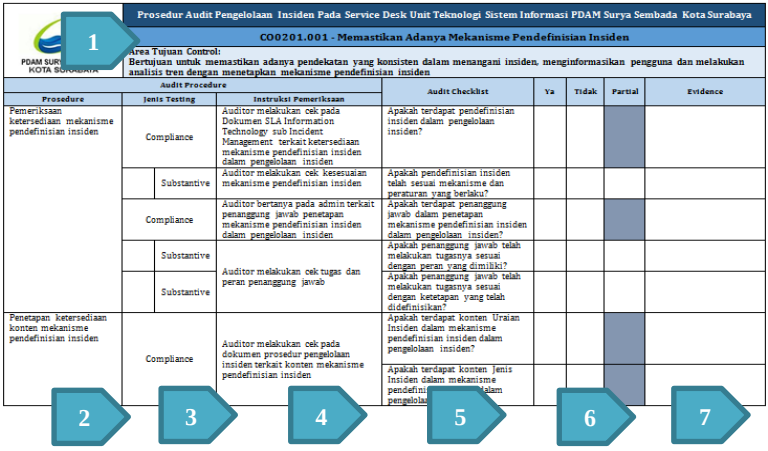
Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
			data frekuensi ter-jadinya bisa ± 2x dalam sebulan		

5.8. Perangkat Audit yang Digunakan

Pada bagian ini merupakan tahapan dalam pembuatan panduan penggunaan perangkat audit. Panduan ini dikembangkan berdasarkan panduan buku dari Kementrian Teknologi dan Informasi melalui tatanan dokumen berdasarkan tingkatannya. Pada penelitian ini ditemukan hasil temuan berdasarkan risiko. Berdasarkan perangkat audit yang sudah ada maka dihasilkan template perangkat audit seperti gambar dibawah ini yang akan menghasilkan hasil temuan untuk dijadikan hasil rekomendasi pada penelitian ini. Penulis menggunakan template perangkat audit tersebut dan memperbarui control objective berdasarkan risiko pada tahun 2017 yang telah ditemukan oleh penulis, akan dijabarkan penggunaan perangkat audit tersebut dibawah ini.

Petunjuk Pengisian Perangkat Audit

Bagian ini nantinya akan berfungsi untuk memberikan petunjuk dalam menggunakan dan bagaimana cara membaca perangkat audit yang telah disusun. Di dalan panduan ini pada bagian selanjutnya adalah penjelasan bagaimana cara membaca dan menggunakan perangkat audit yang dapat terlihat pada contoh Gambar 5.1 Template Perangkat Audit



Prosedur Audit Pengelolaan Insiden Pada Service Desk Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya

CO0201.001 - Memastikan Adanya Mekanisme Pendefinisian Insiden

Area Tujuan Control:
Bertujuan untuk memastikan adanya pendekatan yang konsisten dalam menangani insiden, menginformasikan pengguna dan melakukan analisis tren dengan menetapkan mekanisme pendefinisian insiden

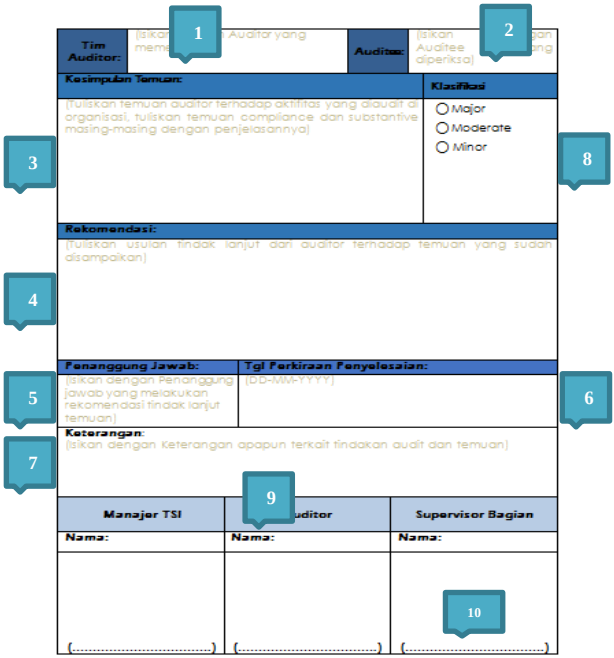
Audit Procedure			Audit Checklist	Ya	Tidak	Partial	Evidence
Prosedur	Jenis Testing	Instruksi Pemeriksaan					
Pemeriksaan ketersediaan mekanisme pendefinisian insiden	Compliance	Auditor melakukan cek pada Dokumen SLA Information Technology sub Incident Management terkait ketersediaan mekanisme pendefinisian insiden dalam pengelolaan insiden	Apakah terdapat pendefinisian insiden dalam pengelolaan insiden?				
	Substantive	Auditor melakukan cek kesesuaian mekanisme pendefinisian insiden	Apakah pendefinisian insiden telah sesuai mekanisme dan peraturan yang berlaku?				
	Compliance	Auditor bertanya pada admin terkait penanggung jawab penetapan mekanisme pendefinisian insiden dalam pengelolaan insiden	Apakah terdapat penanggung jawab dalam penetapan mekanisme pendefinisian insiden dalam pengelolaan insiden?				
	Substantive	Auditor melakukan cek tugas dan peran penanggung jawab	Apakah penanggung jawab telah melakukan tugasnya sesuai dengan peran yang dimiliki?				
	Substantive		Apakah penanggung jawab telah melakukan tugasnya sesuai dengan ketetapan yang telah didefinisikan?				
Penetapan ketersediaan konten mekanisme pendefinisian insiden	Compliance	Auditor melakukan cek pada dokumen prosedur pengelolaan insiden terkait konten mekanisme pendefinisian insiden	Apakah terdapat konten Uraian Insiden dalam mekanisme pendefinisian insiden dalam pengelolaan insiden?				
			Apakah terdapat konten Jenis Insiden dalam mekanisme pendefini... dalam pengelola...				

Gambar 5.1. Template Perangkat Audit

Dalam menggunakan perangkat audit, auditor harus memperhatikan dan memastikan bahwa perangkat yang digunakan adalah benar. Sehingga langkah awal yang dapat dilakukan adalah memastikan dengan membaca dan mengerti Area Tujuan Control yang selanjutnya akan dilanjutkan dengan langkah berikutnya.

Petunjuk Pengisian Template Temuan Audit

Setelah melakukan proses audit, langkah yang harus dilakukan adalah dengan menuliskan langkah rekomendasi terhadap temuan-temuan yang dihasilkan. Terdapat beberapa bagian penting pada template tersebut yang harus diperhatikan oleh auditor internal dalam menuliskan temuan dan langkah rekomendasi. Pada panduan umum ini, telah dijelaskan beberapa langkah yang harus diperhatikan oleh auditor tentang langkah pengisian template audit report seperti contoh Gambar 5.2 Template Temuan Audit dibawah ini:



Gambar 5.2. Template Temuan Audit

Pada table dibawah ini Tabel 5.10 Petunjuk Pengisian Template Audit Report ini merupakan penjelasan atau rincian dari setiap bagian pada table Template Audit Report.

Tabel 5. 11 Petunjuk Pengisian Template Audit Report

No. Istilah	Petunjuk Pengisian
1	Diisi sesuai dengan siapa yang melakukan audit pada saat itu
2	Diisi sesuai dengan siapa saja yang menjadi auditee pada saat itu
3	Diisi sesuai dengan semua temuan apapun yang dihasilkan berdasarkan bukti yang ada
4	Diisi sesuai dengan daftar perbaikan yang harus dilakukan berdasarkan temuan yang dihasilkan
5	Diisi sesuai dengan nama penanggung jawab yang bertugas dalam melakukan perbaikan
6	Diisi dengan tanggal perkiraan penyelesaian perbaikan yang akan dilakukan
7	Diisi dengan semua keterangan-keterangan lain yang dibutuhkan selama proses audit dan perbaikan berlangsung
8	Diisi dengan nama dan tanda tangan oleh Manajer Unit TSI
	Diisi dengan nama dan tanda tangan Auditor
	Diisi dengan nama dan tanda tangan Supervisor Bagian dimana proses audit dilakukan
9	Diisi dengan tanda tangan setiap nama yang tertera dalam daftar
10	Diisi dengan memberikan tanda centang untuk mode yang dipilih

5.9. Gambaran dan Rintangan

Dalam implementasi perancangan studi kasus terdapat beberapa hambatan dan rintangan yang dilalui oleh penulis diantaranya adalah:

1. Penulis harus melakukan wawancara yang membutuhkan waktu berkali-kali untuk memperlajari dan mengetahui pengelolaan insiden pada UNIT TSI
2. Membutuhkan waktu yang lebih lama untuk memastikan jawaban yang diberikan oleh narasumber dapat dipertanggung jawabkan.
3. Merupakan hal yang cukup sulit ketika penulis ingin mendapatkan beberapa dokumen seperti dokumen scenario service desk, dokumen log insiden, dan dokumen pendukung yang akan digunakan dalam membuat perangkat audit sebagai bukti dokumen.
4. Penulis mengalami hambatan ketika membuat janji terhadap narasumber dan supervisor.
5. Penulis harus standby di PDAM untuk bertemu dengan narasumber.

BAB VI
HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan mengenai pemaparan hasil yang didapatkan dari penulisan dan pembahasan secara keseluruhan yang didapatkan dari penelitian.

6.1. Hasil Temuan Audit

Berdasarkan perancangan studi kasus, penulis akan melakukan analisa mengenai hasil temuan audit dengan melakukan checklist terhadap temuan berdasarkan *control objective* dan didalam hasil temuan audit penulis memfokuskan pada testing *Compliance*. Berikut adalah hasil perolehan contoh temuan audit menggunakan perangkat audit Gambar 6.1 dan terdapat pada buku produk hasil temuan audit manajemen insiden pada service desk Unit TSI PDAM Surya Sembada Kota Surabaya.

	Prosedur Audit Pengelolaan Insiden Pada Service Desk Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya						
	CO0201.001 - Memastikan Adanya Mekanisme Pendefinisian Insiden						
Audit Procedure			Audit Checklist	Ya	Tidak	Partial	Evidence
Prosedur	Jenis Testing	Instruksi Pemeriksaan					
Pemeriksaan ketersediaan mekanisme pendefinisian insiden	Compliance	Auditor melakukan cek pada Dokumen SLA Information Technology sub Incident Management terkait ketersediaan mekanisme pendefinisian insiden dalam pengelolaan insiden	Apakah terdapat pendefinisian insiden dalam pengelolaan insiden?	√			Mekanisme pendefinisian telah sesuai dengan ketetapan dan ketentuan
	Compliance	Auditor bertanya pada admin terkait penanggung jawab penetapan mekanisme pendefinisian insiden dalam pengelolaan insiden	Apakah terdapat penanggung jawab dalam penetapan mekanisme pendefinisian insiden dalam pengelolaan insiden?	√			Penetapan penanggung jawab telah dilakukan sesuai dengan insiden
	Compliance	Auditor melakukan cek tugas dan peran penanggung jawab	Apakah penanggung jawab telah melakukan tugasnya sesuai dengan peran yang dimiliki?	√			Penetapan penanggung jawab telah dilakukan sesuai dengan insiden
			Apakah penanggung jawab telah melakukan tugasnya sesuai dengan ketetapan yang telah didefinisikan?	√			Penetapan penanggung jawab telah dilakukan sesuai dengan insiden
Penetapan ketersediaan konten mekanisme	Compliance	Auditor melakukan cek pada dokumen prosedur pengelolaan insiden terkait	Apakah terdapat konten Uraian Insiden dalam mekanisme	√			Insiden yang terjadi dapat diselesaikan sesuai dengan prosedur

Gambar 6.1. Contoh Hasil Temuan Audit

Pada bab hasil dan pembahasan ini telah mendapatkan hasil berupa Temuan Audit yang sudah dirangkumkan pada tabel 6.1 dibawah ini, sebagaimana hasil yang didapatkan berdasarkan control objective yang sudah dipetakan dengan menggunakan key management practice.

Pada hasil analisis risiko terdapat tingkatan level klasifikasi berdasarkan level nilai RPN yang digunakan peneliti terhadulu untuk membuat perangkat audit. Maka penulis mencantumkan klasifikasi tersebut sebagai acuan dasar proses perbaikan hasil temuan pada proses *auditee*.
Setelah dilakukan pencarian hasil temuan audit maka akan dilakukan pengurutan kategori masalah berdasarkan kriteria dan dampak. Minor >120 dampak kecil dan dapat diatasi dengan prosedur sederhana, Moderate 120 ≥ 80 dampak tergolong besar, namun dapat dikelola dengan menggunakan prosedur tertentu. Major < 80 dampak besar, berpotensi pada financial cost dan terhambatnya kinerja organisasi.

Tabel 6. 1 Kriteria Dampak

Dampak		
Rating	Kriteria	Keterangan
1	Minor	Dampak kecil dan dapat dan dapat diatasi dengan prosedur sederhana
2	Moderate	Dampak tergolong besar, namun dapat dikelola dengan menggunakan prosedur tertentu
3	Major	Dampak besar, berpotensi pada *financial cost* dan terhambatnya kinerja organisasi

Tabel 6. 2 Hasil Temuan Berdasarkan CO

No.	Control Objective	Hasil Temuan	Bukti	Klas-ifi-kasi
1	Memastikan adanya mekanisme pendefinisian insiden	Tidak adanya dokumen untuk pendefinisian insiden pada Unit TSI untuk membantu staff untuk menangani insiden	Tidak ada dokumen terkait pendefinisian insiden	Minor
2	Memastikan adanya informasi untuk User atau pengguna Service Desk	Tidak adanya dokumen informasi untuk pengguna layanan secara tertulis Service Desk jika trjadi eror pada web	Tidak ada dokumen informasi untuk user, Dokumen SMM ISO 9001, hasil survey, hasil wawancara kepada Bapak Nurlillah Satria Pratama	Moderate
3	Memastikan adanya prosedur	Tidak adanya dokumen prosedur pada system	Tidak ada dokumen prosedur pengelolaan	Minor

No.	Control Objective	Hasil Temuan	Bukti	Klas-ifi-kasi
	pengelolaan insiden		insiden pada system , hasil wa-wancara, hasil ob-servasi	
4	Memastikan adanya ke-tentuan atau standard yang digunakan dalam me-nangani in-siden	Standarisasi menggunakan ISO 9001 dan KPI	Terdapat dokumen SMM ISO 9001, ter-dapat pada lampiran, hasil wa-wancara	Mi-nor
5	Memastikan adanya struktur or-ganisasi ba-gian TSI pada PDAM penanganan insiden	Struktur or-ganisasi unit TSI	Struktur Organisasi	Mi-nor

Dari hasil temuan diatas maka didapatkan tingkatan berdasar-kan penilaian control objective. Pada hasil analisis risiko lebih terperinci terdapat pada **LAMPIRAN E.** Pada tahap selanjut-nya adalah memetakan berdasarkan urutan kriteria dan dampak.

Tabel 6. 3 Hasil Temuan Berdasarkan Kriteria Dampak

No.	Hasil Temuan	Kriteria
1	Memastikan adanya pen-catatan insiden pada sys-tem log	

No.	Hasil Temuan	Kriteria
2	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko	
3	Memastikan adanya informasi untuk User atau pengguna	
4	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden	
5	Memastikan adanya mekanisme persetujuan penanganan insiden	
6	Memastikan Adanya Penutupan atau Penanganan pada Insiden	
7	Memastikan adanya pelaporan pengelolaan insiden	
8	Memastikan adanya mekanisme pendefinisian insiden	
9	Memastikan adanya prosedur pengelolaan insiden	
10	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden	
11	Memastikan adanya struktur organisasi bagian TSI pada PDAM penanganan insiden	

No.	Hasil Temuan	Kriteria
12	Memastikan adanya mekanisme analisis tren	
13	Memastikan adanya klasifikasi insiden dan permintaan layanan	

6.2. Rekomendasi Hasil Perbaikan

Rekomendasi hasil perbaikan didasarkan oleh hasil temuan audit didasarkan oleh Manajemen Insiden *service desk* pada Unit Teknologi Sistem Informasi. Pada dokumen ini dibahas mengenai hasil temuan untuk pihak Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya. Selain itu, rekomendasi juga didasarkan pada COBIT 5 DSS02 *Manage Service Request dan Incident*. Untuk penjelasan rekomendasi hasil perbaikan berdasarkan hasil temuan audit akan dijabarkan pada Table 6.2.

Tabel 6. 4 Hasil Rekomendasi Perbaikan

No.	Hasil Temuan	Hasil Rekomendasi
1	Secara keseluruhan semua kriteria pada prosedur telah terdefinisi pada beberapa bukti yang telah tertulis pada kolom evidence	Seharusnya perlu ada petunjuk dan prosedur khusus bagi para requester dan staff lain untuk melakukan pengelolaan insiden
2	Tidak adanya dokumen informasi untuk pengguna layanan secara tertulis jka terjadi error pada system web	Perlu adanya dokumen informasi penggunaan layanan untuk pengguna secara tertulis ketika layanan melalui web tidak berfungsi
3	Tidak adanya dokumen prosedur pada system	Seharusnya ada dokumen prosedur terlampir pada system agar memudahkan

No.	Hasil Temuan	Hasil Rekomendasi
		pengguna dalam melaporkan insiden
4	Standarisai menggunakan ISO 9001 dan KPI	Seharusnya ada pembaruan standarisasi yang digunakan untuk terkait manajmen insiden
5	Struktur organisasi Unit TSI penanganan insiden	Seharusnya keterangan struktur organisasi dipublikasikan agar memudahkan seseorang dalam mencari informasi terkait PDAM atau Unit TSI

Pada hasil penelitian ini ditemukan hasil temuan dan menghasilkan rekomendasi hasil temuan dari evaluasi perangkat audit berdasarkan COBIT 5 *DSS02 Manage request and Incident* yang sudah dipetakan berdasarkan KMP. Dan akan dijelaskan lebih terperinci pada **LAMPIRAN F**.

Pada pencarian hasil temuan juga didapatkan penemuan bukti pendukung berupa dokumen dan beberapa contoh tampilan web application system untuk membantu bukti atau evidence yang terdapat pada hasil perangkat audit dan akan lebih terperinci pada **LAMPIRAN G.**

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini akan dijelaskan kesimpulan atas hasil dari penelitian tugas akhir ini serta saran kedepannya untuk penelitian selanjutnya.

7.1. Kesimpulan

Kesimpulan yang dapat diambil dari Tugas Akhir ini adalah mengaudit unit *Service Desk* pada divisi Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya.

1. Perangkat penilaian yang digunakan mengalami pembaruan dan berisi informasi tambahan. Berikut rinciannya:
    a. Perangkat penilaian temuan audit yang didapatkan dari penelitian terdahulu mengalami perubahan dengan menghapus kolom substantive. Hal ini sekaligus mengubah arah penelitian menjadi evaluasi diri dengan tujuan aga PDAM Surabaya kushusnya divisi Teknologi Sistem Informasi mendapatkan hasil penilaian yang sudah disesuaikan dengan standar COBIT 5 dan diberi hasil temuan sekaligus diberi rekomendasi pencapaian. Selain itu penuulis menambahkan pada kolom evidence tiap control objective kaena pada penelitian sebelumnya hanya membuat perangkatnya saja.
    b. Tidak semua produk kinerja di COBIT 5: Manage Request and Incident mendukung kinerja atribut, sehingga ada beberapa penyesuaian yang sudah dimiliki oleh PDAM Surya Sembada Kota Surabaya.

2. Berdasarkan pada rangkuman tabel hasil analisis risiko terdapat beberapa tingkat risiko yang sudah disesuaikan dengan tingkat risiko pada likelihood dengan indicator **Kemungkinan X Dampak**

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Gambar 7.1. Likelihood

Didapatkan hasil terdapat 20 risiko yang sudah dipetakan dari hasil pemetaan Control Objective Maka didapatkan hasil seperti tabel dibawah ini

Tabel 7. 1 Tingkat Risiko

RO2		**RO15**	
RO3		**RO17**	
RO11		**RO18**	
RO12		**RO1**	
RO19		**RO6**	
RO4		**RO10**	
RO5		**RO14**	
RO8		**RO7**	
RO9		**RO16**	
RO13		**RO20**	

Dari hasil yang didapatkan pada tabel *Control Objective* tersebut RO2, RO3, RO11, RO12, dan RO19 menempati tingkat risiko tertinggi yaitu ***Very High***. Pada level ***High*** RO4, RO5, RO8, RO9, RO13, RO15, RO17, RO18. Pada level ***Medium*** RO1, RO6, RO10, RO14**.**Sedangkan pada level ***Low*** RO7, RO16 dan RO20**.** Berdasarkan tingkat risiko yang harus diberikan rekomendasi adalah level diatas 12. Namun jika risiko yang tidak terlalu risk bisa diberikan rekomendasi

3. Berdasarkan dari Control Objective yang telah dipetakan dan mencakup beberapa risiko yang telah didapatkan maka pada perangkat audit mendapatkan Hasil temuan dan Rekomendasi yang terlampir pada **LAMPIRAN E** dan **LAMPIRAN F** dimana penulis mendapatkan 13 hasil temuan audit yang kemudian diberikan rekomendasinya.
4. Dari hasil temuan audit pada studi kasus PDAM maka ditemukan kriteria range berdasarkan kriteria

Tabel 7. 2 Hasil Kriteria Dampak

No.	Hasil Temuan	Kriteria
1	Memastikan adanya pencatatan insiden pada system log	
2	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko	
3	Memastikan adanya informasi untuk User atau pengguna	
4	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden	
5	Memastikan adanya mekanisme persetujuan penanganan insiden	
6	Memastikan Adanya Penutupan atau Penanganan pada Insiden	
7	Memastikan adanya pelaporan pengelolaan insiden	

No.	Hasil Temuan	Kriteria
8	Memastikan adanya mekanisme pendefinisian insiden	
9	Memastikan adanya prosedur pengelolaan insiden	
10	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden	
11	Memastikan adanya struktur organisasi bagian TSI pada PDAM	
12	Memastikan adanya mekanisme analisis tren	
13	Memastikan adanya klasifikasi insiden dan permintaan layanan	

Berdasarkan hasil dan kesimpulan diatas, saran yang dapat diberikan untuk penelitian Tugas Akhir ini untuk pengembangan penelitian lebih lanjut diantaranya ketika ingin mengadakan evaluasi yang serupa untuk lebih memperhatikan perangkat penilaian yang hendak digunakan agar ketika melakukan penelitian tidak perlu membuat perangkat dan tidak memodifikasi lagi. Bila demikian lebih baik membuat perangkat sendiri dan agar lebih valid hasilnya. Selain itu penelitian ini perlu adanya pencerdasan terlebih dahulu untuk para interviewer, ketika kebanyakan dari yang diwawancara terkadang tidak dimengerti sehingga penulis perlu waktu untuk menyampaikan maksud dari pertanyaan dan pernyataan yang diberikan.

DAFTAR PUSTAKA

[1] K. Deasy, "Peranan Audit Internal Dalam Menunjang Efektivitas Pengendalian Internal Piutang (Studi Kasus pada PDAM Kabupaten Bandung)," Universitas Kristen Maranatha, Bandung, 2008.

[2] P. D. A. M. S. S. K. Surabaya, "www.pdamsby.go.id/," [Online]. Available: www.pdamsby.go.id/.

[3] C. 5. E. P. ISACA, ISACA, Amerika, 2012.

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

[5] D. F. d. Y. G. Sucahyo., Audit Sistem Informasi/Teknologi Informasi Dengan Kerangka Kerja Cobit Untuk Evaluasi Manajemen Teknologi Informasi di Universitas XYZ.

[6] A. h. H. M. A. Sarah Putri Ramadhani, Pembuatan Perangkat Audit Berbasis Risiko Berdasarkan COBIT 5 dan Service Desk Standard Pada Service Desk, Surabaya: ITS, (2017).

[7] H. T. H. Ahmad Faiz Zavier, JSIKA Vol 3 2014 Audit Pengelolaan layanan Teknologi Informasi Berdasarkan ITIL Pada IT Marketing & Trading Operation Region V Surabaya., Surabaya: JSIKA, 2014.

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

[9] ". A. Accountancy Auditing TYBCom, "www.mu.ac.id/myweb_test/study TYBCom Accountancy Auditing-II.pdf," [Online].

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

[11] I. 1. (. ISO, Guidelines for Auditing Management., NEW DELHI, 2012.

[12] ICANIG, "www.icanig.org/document/aa.pdf.," (2011). [Online].

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

[14] A. Halim, "Auditing," *Dasar-Dasar Audit Laporan Keuangan UPP STIM YKPN*, 2015..

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

[16] I. F. 27005:2008., ISO/IEC, Information technology -- Security techniques-Information security risk management, 2008.

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

[18] K. K. M. R. A. Amri, "http://blogs.itb.ac.id/. [Accessed 26 April 2016]," Institut Teknologi Bandung, 15 November 2015. [Online].

[19] ". C.-E. I. F. d. I. R. M. -. P. a. G. C. I. C. Kusuma, "[Online]. Available: http://crmsindonesia.org/knowledge/crms-articles/perbandingan-coso-erm-integrate," 11 April 2014. [Online].

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

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

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

[23] C. B. Meyer, "A Case Study Methodology," 17 May 2011., pp. p. 330, .

BIODATA PENULIS

Penulis Tugas Akhir ini lahir di Surabaya Jawa Timur pada tanggan 4 April 1996 dengan nama lengkap Adhiska Putri Maharani. Penulis dengan sapaan akrab Adhiska atau Putri ini merupakan anak ketiga dari tiga bersaudara dari Papa yang bernama Ir. Sutanto Djoko Saputro dan Mama yang bernama Mistriana. Sudah 22 tahun mentetap bersama keluarga di Surabaya. Pendidikan tingkat Sekolah Dasar dihabiskan penulis di SDN Kelampis Ngasem 1/246 Surabaya dan lulus pada tahun 2008. Di jenjang menengah pertama penulis melanjutkan studi di SMP Negeri 30 Surabaya dan mendapatkan ijazah kelulusan pada tahun 2011. Kemudian melanjutkan sekolah menengah atas penulis melanjutkan studi di SMA TTRIMURTI Surabaya. Setelah menamatkan pendidikan menengah atas pada tahun 2014 penulis melanjutkan menuntut ilmu di Institut Teknologi Sepuluh Nopember Departemen Sistem Informasi Fakultas Teknologi Informasi hingga sekarang. Selama perkuliahan, penulis aktif sebagai panitia kegiatan baik tingkat jurusan maupun fakultas dengan menjadi panitia Information System Expo (ISE) ,FTIf Journey dan masih banyak.

Di Departemen Sistem Informasi, penulis mengambil bidang minat Manajemen Sistem Informasi. Untuk mengetahui mengetahui lebih jelas terkait dengan penelitihan ini, penulis dapat dihubungi melalui email adhiskaputri25@gmail.com.

LAMPIRAN A: Interview Protocol

INTERVIEW 1

Tujuan Interview

Mengetahui proses bisnis yang terkait IT dan kondisi kekinian Pengelolaan Manajemen Insiden pada Unit TSI PDAM Surya Sembada Kota Surabaya.

Tanggal : 25 Mei 2018
Waktu : -
Lokasi : PDAM Surya Sembada Kota Surabaya
Narasumber : Nurlillah Satria Pratama
Jabatan : Supervisor TSI

No	Pertanyaan
1	Bagaimana proses umum penerapan teknologi informasi pada PDAM ?
2	Bagaimana proses umum penerapan teknologi informasi pada bagian teknologi sistem informasi, keuangan dan pelayanan ?
3	Bagaimanakah struktur organisasi bagian TSI pada PDAM Surya Sembada Kota Surabaya ?
4	Pada bagian TSI terdapat berapa sub fungsi/divisi ? dan apa tugas masing-masing divisi?
5	Apakah setiap insiden yang ada telah didefiinisikan/ djabarkan penjelasan?
6	Apakah ada pihak diluar Unit TSI yang terkait dengan pengelolaan TI? Bagaimana perannya? (Vendor -> layanannya apa)
7	Apakah terdapat SOP / prosedur tertulis jika terjadi gangguan ?
8	Apakah organisasi telah menerapkan standar keamanan untuk melindungi aset Teknologi Informasi?

A-2

INTERVIEW 2

Tujuan Interview

Dilakukan untuk mengetahui identifikasi risiko, dilakukan untuk menggali informasi terkait yang ada di Unit TSI

Tanggal : 25 Mei 2018
Waktu : -
Lokasi : PDAM Surya Sembada Kota Surabaya
Narasumber : Nurlillah Satria Pratama
Jabatan : Supervisor TSI

No	Pertanyaan
1	System / aplikasi / layanan apa saja yang ditangani oleh divisi Unit TSI?
2	Apa dampak yang dirasakan oleh PDAM/Divisi Unit TSI jika sitem tidak berjalan karena mengaami gangguan ?
3	Bagaimanakah struktur organisasi bagian Unit TSI pada PDAM Surya Sembada Kota Surabaya ?
4	Apakah teknologi informasi sudah sangat membantu kinerja layanan?
5	Apakah setiap insiden yang ada telah didefiinisikan/ djabarkan penjelasan?
6	Apakah layanan yang diberikan oleh PDAM sudah sesuai dengan visi dan misi?
7	Apa saja insiden yang sering terjadi pada layanan-layanan tersebut? Dan bagaimana penanganannya?
8	Siapa yang biasanya menangani insiden tersebut?
9	Apakah ada prosedur khusus penaganan insiden?
10	Apakah ada langkah lebih lanjut mengenai penanganan insiden seperti maintenance untuk langkah perbaikan dan pencegahan?

INTERVIEW 3
Tujuan Interview

Dilakukan untuk mengetahui kondisi eksisteing service desk dalam implementasi manajemen insiden

Tanggal : 25 Mei 2018
Waktu : -
Lokasi : PDAM Surya Sembada Kota Surabaya
Narasumber : Nurlillah Satria Pratama
Jabatan : Supervisor TSI

Fase 1 Informasi Kondisi Eksisting Service Desk	
Obyektif 1 : Mendapatkan informasi mengenai kondisi eksisting service desk dalam implementasi manajemen insiden	
No	**Pertanyaan**
1	Seperti apa bentuk service desk yang ada di PDAM?
2	Apa saja yang ditangani oleh Service desk ? (Hardware/Software/jarigan/ketiganya ?)
3	Siapa yang mengelola service desk? Siapa saja yang menggunakannya? Siapa yang bertanggung jawab?
4	Bagaimana alur atau proses yang ada pada service desk?
5	Apakah ada standarisasi khusus dalam melakukan manajemen insiden?
6	Apakah dilakukan prioritas terhdap insiden?
7	Apakah dampak yang dialami oleh service desk ketika insiden tidak bisa diatasi?
8	Berapa lama untuk menangani log insiden? Apakah semua insiden dicatat?
9	Apa saja masalah yang terjadi pada service desk?

Fase 2: Kondisi Pengelolaan manajemen Insiden pada Unit TSI

Obyektif 1 : Mendapatkan informasi mengenai kondisi eksisting service desk dalam implementasi manajemen insiden	
1	Adakah permasalahan yang pernah terjadi terkait proses pengelolaan insiden?
2	Apa saja komponen-komponen teknologi informasi (hardware, software, data, network, people, prosedur) yang berkaitan dengan pengelolaan manajemen insiden (web application service desk)
3	Asset TI yang termasuk dalam aspek kritis?
4	Aplikasi atau system informasi apa saja yang dikembangkan oleh TSI?

Obyektif 2: Mendapatkan informasi mengenai identifikasi ancaman terhadap asset teknologi dan system informasi	
1	Gangguan apa yang pernah terjadi pada asset teknologi dan system informasi? (gangguan: bencana alam, error, virus, malware, bug, human error, jaringan terputus, server down)
2	Bencana alam apa saja yang mungkin dapat terjadi dan mengancam aset teknologi dan sistem informasi di fungsional bisnis kritis organisasi ?
3	Gangguan apa yang sering terjadi ?
4	Gangguan apa saja yang berdampak besar ?
5	Apakah pernah terjadi gangguan akibat perbuatan manusia ? (misalnya hacking,pencurian data, penyalahgunaan hak akses)
6	Gangguan apa saja yang pernah terjadi pada asset teknologi dan system informasi? (gangguan: bencana alam, error, virus, malware, bug, human error, jaringan terputus, server down)

LAMPIRAN B: Hasil Wawancara

HASIL INTERVIEW 1

Hasil Wawancara 1

No.	Pertanyaan	Jawaban
1.	Bagaimana proses umum penerapan teknologi informasi pada PDAM ?	Secara umum Teknologi informasi sudah diterapkan di PDAM
2.	Bagaimana proses umum penerapan teknologi informasi pada bagian teknologi sistem informasi, keuangan dan pelayanan ?	Penerapannya di seluruh bagian / departemen . dan sudah di integrasi
3.	Bagaimanakah struktur organisasi bagian TSI pada PDAM Surya Sembada Kota Surabaya ?	Struktur TSI terdiri dari 1 manager dengan 3 supervisor
4.	Pada bagian TSI terdapat berapa sub fungsi/divisi ? dan apa tugas masing-masing divisi?	Bagian TSI terdapat 3 sub fungsi **Infrastruktur :** Melakukan pengawasan instalasi, perawatan dan perbaikan komputer, printer dan perlengkapannya; Melakukan pengawasan instalasi, perawatan dan perbaikan jaringan komputer lokal dan jaringan komputer antar kantor; Melakukan pengawasan instalasi, perawatan dan perbaikan server fisikal serta

		virtual beserta *Storage System*-nya Melakukan pengawasan proses pemindahan backup data ke media eksternal dan *Dissaster Recovery Centre (DRC)*; Melakukan pengawasan keamanan operasional server, komputer dan jaringan komputer dari ancaman virus serta *hacker*; Melakukan pengawasan penyediaan layanan sistem email. **Pengembangan:** Melakukan pengawasan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan; Melakukan pengawasan pembuatan standarisasi software, aplikasi dan infrastruktur yang akan diimplementasikan di perusahaan; Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan; Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi;

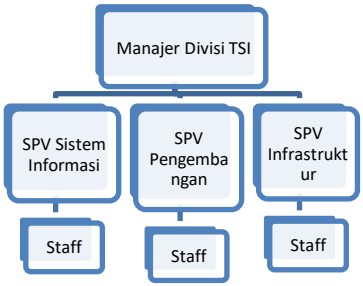
		Melakukan pengawasan kepastian perusahaan menggunakan perangkat lunak yang legal; Melakukan pengawasan kegiatan *helpdesk support*. **Sistem informasi:** Melakukan pengawasan pemeliharaan dan perbaikan aplikasi sistem informasi; Melakukan pengawasan kegiatan analisa dan desain terhadap pengembangan aplikasi eksisting; Melakukan pengawasan kegiatan penambahan-penambahan fitur aplikasi eksisting; Melakukan pengawasan kegiatan evaluasi terhadap aplikasi-aplikasi secara reguler dan mengusulkan perbaikan aplikasi; Melakukan pengawasan kegiatan *backup* seluruh aplikasi dan *source code* secara reguler; Melakukan pengawasan kegiatan perbaikan data pada *database*. (terdapat pada tabel tugas pokok)
5.	Apakah setiap insiden yang ada telah didefi-inisikan/ djabarkan pen-jelasan?	Ya, semua insiden di-masukan ke dalam dokumen SLA, tapi secara garis besar

		insiden yang dilakukan berdasarkan aplikasi yang ada pada perusahaan.
6	Apakah ada pihak diluar TSI yang terkait dengan pengelolaan TI? Bagaimana perannya? (Vendor -> layanannya apa)	PDAM berkerjasama dengan pihak ke 3 terkait dengan pengelolaan kerusakan hardware selain itu dengan switcher terkait dengan pembayaran online dimana pihak switcher sebagai penjembatan ke customer, kerjasama dengan ISP
7	Apakah terdapat SOP / prosedur tertulis jika terjadi gangguan ?	Belum ada
8	Apakah organisasi telah menerapkan standar keamanan untuk melindungi aset TI?	Belum ada

HASIL INTERVIEW 2

Hasil Interview 2

No.	Pertanyaan	Jawaban
1.	System / aplikasi / layanan apa saja yang ditangani oleh divisi TSI?	Ada sangat banyak, tapi kalau yang berhubungan langsungn dengan pelanggan ada beberapa yang sangat penting diantaranya adalah: - Aplikasi Customer Service - Call Centre -Aplikasi loket pembayaran -Android Pengecekan No. rekening dan tagihan

		-Sebagian Website untuk Simulasi Rekening -Aplikasi Hubungan Langganan (Tutupan)
2.	Apa dampak yang dirasakan oleh PDAM/Divisi TSI jika sitem tidak berjalan karena mengaami gangguan ?	Semua gangguan yang terjadi akan kami pertimbangkan sesuai risiko yang diajukan. Keluhan dan gangguan mengenai jasa yang kami berikan sangat berpengaruh karena pelanggan inginnya semua gangguan harus cepat diselesaikan. Sehingga untuk menghindari risiko itu terjadi divisi TSI harus selalu piket setiap hari.Lain lagi kalau untuk aplikasi loket, biasanya yang tejadi adalah antrian pelanggan di loket akan semakin memanjang namun hal yang dapat dilakukan hanya restart sistem, tidak ada penangnan lebih lanjut.
3.	Bagaimanakah struktur organisasi bagian TSI pada PDAM Surya Sembada Kota Surabaya ?	

4	Apakah teknologi informasi sudah sangat membantu kinerja layanan?	Iya sangat membantu, kalau dulu kan pengingat tagihan harus melalui door to door, tapi sekarang sudah dapat dicek melalui situs denga mengetikkan nomor rekening pelanggan. Selain itu saat ini sudah dipermudah dengan reminder melalui mobile. Hal ini lebih berpengaruh pada bagian infrastruktur pada divisi TSI karena saat ini pembayaran tidak hanya melalui loket tapi bisa melalui bank, mobile, dan internet
5	Apakah setiap insiden yang ada telah didefiinisikan/ djabarkan penjelasan?	Ya, pendefinisian insiden tercatat dalam dokumen SLA, tetapi secara garis besar setiap insiden didefinisikan berdasarkan aplikasi yang ada pada perusahaan
6	Apakah layanan yang diberikan oleh PDAM sudah sesuai dengan visi dan misi?	Menurut saya khusunya kalau untuk divisi TSI sudah, kalau mengingat poin yang disampaikan pada misi PDAM poin nomor 2 yaitu ‘memberi pelayanan prima bagi pelanggan dan berkelanjutan bagi pemangku kepentingan’

7	Apa saja insiden yang sering terjadi pada layanan-layanan tersebut? Dan bagaimana penanganannya?	Yang paling sering terjadi adalah masalah loading lambat pada aplikasi disebabkan karena server lambat, database penuh, aplikasi tidak mendukung banyaknya data yang diinputkan oleh user. Untuk penangnannya biasanya hanya dengan melakukan restart server, mengubah database, restart sistem atau komputer.
8	Siapa yang biasanya menangani insiden tersebut?	Biasanya alurnya user melapor pada bagian Sistem Informasi, dari bagian SI ini melanjutkan pelaporan pada bagian pengembangan. Nantinya ketika permasalahan pada aplikasi telah diselesaikan bagian Pengembangan, bagian Pengembangan melaporkan kembali pada bagian SI untuk diberitahukan pada user, namun ketika ada terjadi permasalahan teknis, bagian SI langsung melaporkan pada bagian infrastruktur.
9	Apakah ada prosedur khusus penaganan insiden?	Tidak ada, semua penanganan hanya didasarkan pada pengalaman dan by request saja

10	Apakah ada langkah lebih lanjut mengenai penanganan insiden seperti maintenance untuk langkah perbaikan dan pencegahan?	Maintenance biasanya dilakukan oleh divisi TSI bagian Sistem Informasi. tapi jika berkala waktu proses maintenancenya tidak ada. Maintenance hanya dilakukan by request dan jika ada keluhan dan laporan saja dari user selebihnya tidak ada

INTERVIEW 3
Hasil Interview 3

Fase 1 Informasi Kondisi Eksisting Service Desk		
Obyektif 1 : Mendapatkan informasi mengenai kondisi eksisting service desk dalam implementasi manajemen insiden		
No.	**Pertanyaan**	**Jawaban**
1.	Seperti apa bentuk service desk yang ada di PDAM?	Berbentuk aplikasi web yang didapatkan secara gratis dari pelatihan manage engine Service operation ITIL
2.	Apa saja yang ditangani oleh Service desk ? (Hardware / Software / jarigan / ketiganya?)	Masalah request dan problem yang berkaitan dengan TI. Ya semuanya diatasi termasuk infrastruktur TI dan aplikasi yang digunakan di PDAM. Service desk ini juga dilengkapi dengan fitur detect asset dimana dapat mengetahui di dalam satu perangkat komputer menggunakan aplikasi apa saja.
3.	Siapa yang mengelola service desk? Siapa saja yang menggunakannya? Siapa yang bertanggung jawab?	Yang mengelola adalah beberapa admin dari unit TSI, namun tidak ada bagian khusus seperti hepdesk dikarenakan tidak adanya sumber daya. Yang menggunakan adalah semua bagian PDAM yang nantinya akan memberikan request pada

		bagian unit TSI. Yang bertanggung jawab ada;ah setiap supervisor setiap bagian dalam unit TSI yaitu bagian system informasi, infrastruktur, dan bagian penegmbangan.
4.	Bagaimana alur atau proses yang ada pada service desk?	- User membuat request - membuka service desk - assign ke technician - membuka request - closing service desk untuk dilaporkan pada bagian TSI melakukan penanganan - melakukan pelaporan bahwa penanganan telah selesai dilakukan.
5.	Apakah ada standarisasi khusus dalam melakukan manajemen insiden?	Menggunakan acuan ISO 9001 dan KPI
6	Apakah dilakukan prioritas terhdap insiden?	Tergantung kapan request yang masuk dalam log sesuai urutan maka diselesaikan terlebih dahulu. Tapi permintaan tergantung, jika pihak atas yang request maka diselesaikan dulu.
7	Apakah dampak yang dialami oleh service desk ketika insiden tidak bisa diatasi?	Akan ada notifikasi overdue untuk insiden yang disesuaikan dengan KPI. Penanganan insiden disesuaikan dengan pencapaian KPI seperti penambahan fitur atau perbaikan fitur dibutuhkan waktu sedikit lama (3-5 hari batas overdue)
8	Berapa lama untuk menangani log insiden? Apakah	Tergantung masalah apa yang ditangani, semua insiden dicatat karena jika tidak ada pencatatan pada

	semua insiden di-catat?	service desk insiden tidaka kan di-tangani.
9	Apa saja masalah yang terjadi pada service desk?	Belum pernah ada masalah karena service desk yang digunakan masih standard. Bai-sanya masalah hanya terjadi saat penanganan insiden atau request yang datang

Fase 2: Kondisi Pengelolaan manajemen Insiden pada Unit TSI		
Obyektif 1 : Mendapatkan informasi Kondisi Pengelolaan manajemen Insiden pada Unit TSI PDAM Surya Sembada Kota Surabaya		
No.	**Pertanyaan**	**Jawaban**
1.	Adakah permasalahan yang pernah terjadi terkait proses pengel-olaan insiden?	- tidak adanya peran seorang helpdesk yang menangani langsung insiden yang dilaporkan - terlambat melakukan pen-catatan dikarenakan admin sibuk - saat menangani insiden ketika tidak paham cara menanganinya bertanya se-hingga butuh waktu lama - ada server yang ditangani pemkot Surabaya sehingga ketika trouble harus menghubungi pihak lain - terdapat knowledge base untuk penanganan tapi ke-banyakan tidak digunakan dikarenakan penanganan

		hanya berdasarkan pengalaman
2.	Apa saja komponen-komponen teknologi informasi (hardware, software, data, network, people, prosedur) yang berkaitan dengan pengelolaan manajemen insiden.	- Software : billing, asapta, SKA, aplikasi penagihan rekening swasta, pemerintah dan kas, aplikasi kas on line, layanan pembayaran online,website, email, Sistem Informasi Pelayanan - Jaringan : switch, router,access point - Hardware : PC, server, laptop, storage, printer - Data : database, - Aset pendukung :antivirus, firewall, genset, ups,GIS - Orang : 25 tim TSI
3.	Asset TI yang termasuk dalam aspek kritis?	Server, storage, database, data, software
4	Aplikasi atau system informasi apa saja yang dikembangkan oleh TSI?	Pendaftaran pasang baru,perencanaan pasang baru, pengambilan material di gudang, pengaduan, tindak lanjut pengaduan, pembayaran ,penerbitan rekening, workflow,sms broadcast, penertiban pelanggan,
Obyektif 2 : Mendapatkan informasi mengenai identifikasi ancaman terhadap asset teknologi dan system informasi		
No	**Pertanyaan**	**Jawaban**
1.	Gangguan apa yang pernah terjadi pada asset teknologi dan system informasi? (gangguan: bencana alam, error, vi-	- Jaringan : Jaringan terputus,switch mati, network control module mengalami trouble

	rus, malware, bug, human error, jaringan terputus, server down)	- Hardware : kerusakan hardware, server down, storage corrupt, - Software : error software, bug, kesalahan setting, salah coding - Database : lambat, Data berubah / salah update
2.	Bencana alam apa saja yang mungkin dapat terjadi dan mengancam aset teknologi dan sistem informasi di fungsional bisnis kritis organisasi ?	Gempa bumi, hujan, banjir, petir dan kilat, kebakaran, badai
3	Gangguan apa yang sering terjadi ?	Troubleshoot
4	Gangguan apa saja yang berdampak besar ?	Server down
5	Apakah pernah terjadi gangguan akibat perbuatan manusia ? (misalnya hacking,pencurian data, penyalah gunaan hak akses)	Tidak pernah

LAMPIRAN C: Pemetaan Key Management Practice

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
P01	**DSS02.01** Mendefinisikan insiden dan skema klasifikasi permintaan layanan	Mendefinisikan insiden dan klasifikasi permintaan layanan dan kriteria untuk problem registrasi, untuk mengatur, dan menginformasikan user tentang kondisi kekinian	CO201.001	Memastikan adanya mekanisme pendefinisian insiden	-
			CO201.002	Memastikan adanya informasi untuk User atau pengguna Service Desk	Terdapat dokumen informasi pengguna Service Desk

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
		Mendefinisikan model insiden untuk mengetahui risiko dan memberikan solusi	CO201.003	Memastikan adanya pengelolaan insiden	Terdapat dokumen pengelolaan insiden
		Menentukan model permintaan layanan sesuai dengan permintaan layanan	CO201.004	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden	Terdapat dokumen standard yang sudah ditentukan oleh PDAM
		Menentukan insiden ekskalasi dan prosedur, terutama untuk insiden besar dan insiden keamanan	CO201.005	Memastikan adanya struktur organisasi bagian TSI pada PDAM penanganan insiden	Terdapat dokumen struktur organisasi penanganan insiden
		Menetapkan insiden dan mencari sumber pengetahuan dan kegunaanya	CO202.001	Memastikan adanya	Terdapat mekanisme

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
				mekanisme pendekatan penanganan	pendefinisian telah sesuai dengan ketetapan dan ketentuan
PO2	**DSS02.02** Mencatat,mengklasifikasikan dan memprioritaskan permintaan dan insiden	Semua log (catatan) permintaan layanan dan insiden,	CO201.003 CO202.002 CO202.004	Memastikan adanya prosedur pengelolaan insiden Memastikan adanya pencatatan insiden pada system Log Memastikan adanya skema prioritas insiden	Terdapat dokumen prosedur pengelolaan insiden Terdapat catatan insiden pada log system pada web Terdapat pendefinisian

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
				berdasarkan tingkat risiko	konten skema prioritas
		Untuk menganalisa kondisi kekinian dan mengidentifikasi permintaan layanan berdasarkan tipe dan kategori	CO202.003	Memastikan adanya mekanisme analisis tren	Terdapat penanggung jawab yang melayani insiden
		Memprioritaskan permintaan layanan dan insiden berbasis definisi SLA	CO202.004	Memastikan adanya skema prioritas insiden berdasarkan tingkat risiko	Terdapat pendefinisian konten skema prioritas
PO3	**DSS02.03** Memverifikasikan, menyetujui dan memenuhi	Verifikasi hak untuk permintaan layanan menggunakan, jika memungkinkan, aliran	CO202.001	Memastikan adanya mekanisme pendekatan penanganan	Terdapat status notifikasi pada web application

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
	permintaan layanan	proses yang telah ditentukan dan perubahan standar			
		Memperoleh persetujuan keuangan dan fungsional atau menandatangani, jika diperlukan, atau persetujuan yang telah ditetapkan untuk menyetujui perubahan standar	CO202.001	Memastikan adanya mekanisme pendekatan penanganan	Terdapat dokumen penanganan terkait melakukan persetujuan sesuai dengan ketetapan

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
		Mendefinisikan dan mendeskripsikan gejala yang relevan untuk menetapkan penyebab kemungkinan terjadinya insiden	CO203.003 CO203.004	Memastikan adanya prosedur pengelolaan insiden Memastikan adanya klasifikasi insiden dan permintaan layanan	Penetapan penanggung jawab telah dilakukan sesuai dengan prosedur Terdapat klasifikasi koten insiden
PO4	**DSS02.04** Menginvestigasikan mendiagnosis dan mengalokasikan insiden	Mengidentifikasi dan menggambarkan gejala yang relevan untuk membangun yang paling kemungkinan penyebab, peristiwa. eference tersedia shaering sumber daya iincluding	CO202.001	Memastikan adanya mekanisme pendekatan penanganan	Terdapat dokumen penanganan terkait melakukan persetujuan sesuai dengan ketetapan

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
		dikenal kesalahan dan masalah) untuk mengidentifikasi kemungkinan penyelesaian insiden (sementara workarounds dan/atau solusi permanen)			
		Jika kesalahan yang dikenal atau masalah terkait tidak sudah ada dan jika insiden memenuhi target pada kriteria untuk masalah pendaftaran,log masalah baru	CO202.003	Memastikan adanya mekanisme analisis tren	Terdapat penanggung jawab yang melayani insiden
		Menetapkan insiden fungsi spesialisjika diperlukan keahlian yang lebih dalam dan	CO201.003	Memastikan adanya prosedur pengelolaan insiden	Terdapat dokumen prosedur pengelolaan insiden

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
		mengakhiri level manajemen yang sesuai dimana dan jika diperlukan.			
PO5	**DSS02.05** Menyelesaikan dan memulihkan insiden	Memilih dan menerapkan penyelesaian insiden yang sesuai	CO201.003	Memastikan adanya prosedur pengelolaan insiden	Terdapat dokumen prosedur pengelolaan insiden
		Mencatat solusi yang digunakan dalam menyelesaikan insiden/ masalah	CO205.001	Memastikan Adanya Penutupan atau Penanganan pada Insiden	Terdapat dokumen Penetapan penanggung jawab telah dilakukan sesuai dengan prosedur
		Melaksanakan aksi pemulihan jika dibutuhkan	CO202.004	Memastikan insiden yang ditangani sesuai dengan tingkat	Terdapat pendefinisian konten skema prioritas

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
				penanganan risiko	
		Mendokumentasikan penyelesaian insiden dan menilai jika penyelesaian dapat digunakan untuk sumber pengetahuan kedepannya	CO202.002	Memastikan adanya pencatatan insiden pada system Log	Terdapat catatan insiden pada log system pada web
PO6	**DSS02.06** Menutup permintaan layanan dan insiden	Melakukan verifikasi kepuasan permintaan layanan dan penyelesaian insiden terhadap pengguna yang terlibat	CO202.002	Memastikan adanya pencatatan insiden pada system Log	Terdapat catatan insiden pada log system pada web
		Menutup permintaan layanan dan insiden	CO203.002	Memastikan adanya klasifikasi insiden dan permintaan layanan	Terdapat dokumen SMM ISO 9001

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
PO7	**DSS02.07** Melacak status dan membuat Laporan	Memantau dan menelusuri peningkatan insiden, penyelesaian, dan prosedur permintaan pengelolaan untuk menuju penyelesaian masalah	CO203.002	Memastikan adanya klasifikasi insiden dan permintaan layanan	Terdapat dokumen SMM ISO 9001
		Melakukan identifikasi stakeholders dari informasi dan kebutuhan data atau laporan serta mengidentifikasi frekuensi dan perantara laporan	CO207.001	Memastikan adanya pelaporan pengelolaan insiden	Terdapat Penetapan penanggung jawab telah dilakukan sesuai dengan prosedur
		Menganalisis insiden dan permintaan layanan berdasarkan kategori dan tipe untuk menetap-	CO202.02	Memastikan adanya pencatatan insiden pada system Log	Terdapat catatan insiden pada log system pada web

ID Process	Key Management Practice	Activity	ID Control Objective	Control Objective	Evidence (Bukti)
		kan trend dan mengidentifikasi pola dari masalah yang berulang, pelanggaran SLA atau ketidakefisiensian. Menggunakan informasi sebagai input dalam perencanaan peningkatan berlanjut.	CO202.004 CO201.003	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko Memastikan adanya prosedur pengelolaan insiden	Terdapat pendefinisian konten skema prioritas Terdapat dokumen prosedur pengelolaan insiden
		Membuat dan mendistribusikan laporan secara tepat waktu atau menyediakan akses data secara online	CO207.001	Memastikan adanya pelaporan pengelolaan insiden	Penetapan penanggung jawab telah dilakukan sesuai dengan prosedur

LAMPIRAN D: Analisis Risiko

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
RO1	Kesalahan pendefinisian insiden	Miskomunikasi, salah koordinasi sesame staff admin	Kesalahan pendefinisian insiden frekuensi terjadinya bisa ± 2x dalam sebulan	Banyak kesalaha pahaman dalam mengartikan insiden sehingga terjadi kesalahan dalam menjalankan penanganan insiden ± 2	4 Medium
RO2	Insiden tidak dicatatkan pada Web Application	Kelalaian admin	Insiden tidak dicatatkan pada web application karena insiden berkaitan langsung dengan pengguna frekuensi	Insiden yang dilaporkan tidak bisa ditangani karena tidak masuk ke dalam log system frekuensi terjadinya bisa ± 4x dalam sebulan	14 Very High

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
			terjadinya bisa ± 10x dalam sebulan		
RO3	Risiko kinerja database lambat memberikan respone	Data overload, salah update database, database kacau	Kapasitas DB yang terbatas menyebabkan aplikasi menjadi lambat frekuensi terjadinya bisa ± 4x dalam sebulan	Beberapa aplikasi menjadi lambat frekuensi terjadinya bisa ± 14x dalam sebulan	16 Very High
RO4	Gagal melakukan backup	System backup tidak berjalan sesuai jadwal	Gagal melakukan backup pada saat pemindahan data frekuensi terjadinya bisa ± 4x dalam sebulan	Data yang ada deserver bisa saja terhapus atau data corrupt frekuensi terjadinya bisa ± 3x dalam sebulan	12 High
RO5	Bocornya log insiden	Data rahasia perusahaan bocor kepihak yang tidak	Data yang bocor disalahgunakan untuk kejahatan atau penyalahgunaan	Perusahaan mengalami kerugian atas perbuatan pihak tidak bertanggung	8 High

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
		bertanggung jawab	data frekuensi terjadinya bisa ± 2x dalam sebulan	jawab frekuensi terjadinya bisa ± 4x dalam sebulan	
RO6	Kesalahan koordinasi job-desk	Staff tidak memahami insiden yang dilaporkan oleh user	Staff tidak menguasai penanganan insiden secara keseluruhan frekuensi terjadinya bisa ± 2x dalam sebulan	Insiden yang ditangani masih dipending karena harus berdiskusi dengan staff lain frekuensi terjadinya bisa ± 2x dalam sebulan	4 Med
RO7	Penyalahgunaan hak akses system secara sengaja	Staff admin tidak bisa login kedalam web application	Staff admin lupa password sehingga menggunakan akun staff admin lain frekuensi terjadinya bisa ± 1x dalam sebulan	Memperlambat kinerja staff admin frekuensi terjadinya bisa ± 2x dalam sebulan	2 Low
RO8	Tidak adanya prosedur	Tidak adanya prosedur	Insiden yang ditangani tidak sesuai dengan prosedur	Penanganan insiden tidak sesuai dengan masalah	12 High

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
	pengelolaan insiden	pengelolaan insiden	yang seharusnya frekuensi terjadinya bisa ± 4x dalam sebulan	yang terjadi frekuensi terjadinya bisa ± 3x dalam sebulan	
RO9	Kesalahan dalam melakukan pencatatan insiden	Kelalaian staff dalam mencatat insiden pada log system	Insiden tidak bisa ditangani dan menimbulkan masalah yang seharusnya tidak terjadi frekuensi terjadinya bisa ± 5x dalam sebulan	Perusahan mengalami penumpukan insiden yang tidak terselesaikan karena tidak ada pencatatan frekuensi terjadinya bisa ± 2x dalam sebulan	10 High
RO10	Insiden tidak ditangani	Insiden yang dilaporkan tidak bisa ditangani	Karena insiden yang ditangani terlalu sulit dan banyak kemungkinan akan overdue frekuensi terjadinya	Insiden tidak mendapatkan solusi frekuensi terjadinya bisa ± 2x dalam sebulan	8 Med

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
			bisa ± 4x dalam sebulan		
RO11	Admin/ staff tidak menguasai penanganan insiden	Admin tidak memahami insiden yang ditangani	Admin tidak berpengalaman dalam menangani insiden tersebut frekuensi terjadinya bisa ± 7x dalam sebulan	Insiden yang ditangani mengalami overdue atau dilemparkan ke staff yang lain frekuensi terjadinya bisa ± 2x dalam sebulan	14 Very High
RO12	Pemakaian bandwith internet yang tidak sesuai dengan kegunaan	Karyawan menggunakan internet untuk akses web selain pekerjaan	Akses internet pada jam kerja menjadi lambat frekuensi terjadinya bisa ± 10x dalam sebulan	Internet menjadi lambat frekuensi terjadinya bisa ± 2x dalam sebulan	20 Very High
RO13	Gangguan dan serangan terhadap komputer , server dan jaringan	Penggunan flashdisk yang terkena virus dan hacker	Virus menyebabkan kerusakan pada software dan usaha peretas dalam menggagalkan	Computer server dan jaringan terganggu dan gagal memberikan layanan serta usaha peretas menampilkan informasi yang salah	12 High

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
			operasional frekuensi terjadinya bisa ± 4x dalam sebulan	frekuensi terjadinya bisa ± 3x dalam sebulan	
RO14	Risiko kerusakan perangkat keras	Kerusakan PC ,server dan perangkat keras lainnya	Komponen yang rusak frekuensi terjadinya bisa ± 2x dalam setahun	Mengganti kerusakan dengan yang baru atau menservice frekuensi terjadinya bisa ± 2x dalam setahun	4 Med
RO15	Risiko kegagalan koneksi data pada jaringan dalam kantor pusat (LAN) serta antara kantor pusat dan cabang (WAN)	Kabel jaringan komputer putus	Koneksi data gagal dan aplikasi bisnis perusahaan tidak dapat dijalankan oleh user frekuensi terjadinya bisa ± 5x dalam sebulan	Operasional perusahaan tidak berjalan dengan baik frekuensi terjadinya bisa ± 2x dalam sebulan	10 High

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
RO16	Risiko Induksi Petir	Kabel data dan jalur ground gedung terlalu dekat	Kerusakan pada switch data dan operasional terganggu frekuensi terjadinya bisa ± 1x dalam sebulan	Pelayanan pengalami gangguan frekuensi terjadinya bisa ± 2x dalam sebulan	2 Low
RO17	Risiko eror dalam pembuatan aplikasi	Permintaan user terlalu sering berubah untuk perbaikan proses bisnis yang	Terjadi error saat penggunaan aplikasi frekuensi terjadinya bisa ± 5x dalam sebulan	Aplikasi tidak bisa berjalan dengan normal frekuensi terjadinya bisa ± 2x dalam sebulan	10 High
RO18	Organisasi belum menerapkan standar keamanan untuk melindungi asset TI	Organisasi belum menentukan standar yang akan digunakan	Aset TI mengalami kerusakan atau kehillangan karena tidak ada standar keamanan yang diterapkan frekuensi	Perusahaan mengalami kerugian financial dan asset TI frekuensi terjadinya bisa ± 4x dalam setahun	12 High

Risiko	Nama Risiko	Penyebab Risiko	Analisis Risiko		Tingkat Risiko
			Kemungkinan	Dampak	
		untuk melindungi asset TI	terjadinya bisa ±3 x dalam setahun		
RO19	Troubleshoot	Salah menyelesaikan masalah	Kesalahan dalam memecahkan permasalahan insiden yang terjadi frekuensi terjadinya bisa ± 7x dalam sebulan	Insiden yang diselesaikan tidak sesuai dengan permintaan requester frekuensi terjadinya bisa ± 2x dalam sebulan	14 Very High
RO20	Pelaporaan pengelolaan insiden	Pelaporan pengelolaan tidak dilakukan	Kesalahan dalam pengelolaan laporan insiden frekuensi yang terjadi bisa 1x dalam sebulan	Laporan pengelolaan insiden tidak disetujui oleh manajer TSI untuk ditindak lanjuti frekuensi terjadinya 2x dalam sebulan	2 Low

LAMPIRAN E: Hasil Temuan

No.	Control Objective	Hasil Temuan	Bukti	Klasifikasi
1	Memastikan adanya mekanisme pendefinisian insiden	Tidak adanya dokumen untuk pendefinisian insiden pada Unit TSI untuk membantu staff untuk menangani insiden	Tidak ada dokumen terkait pendefinisian insiden	Minor
2	Memastikan adanya informasi untuk User atau pengguna Service Desk	Tidak adanya dokumen informasi untuk pengguna layanan secara tertulis/hardcopy pada Unit TSI jika terjadi error pada web	Terdapat dokumen infratruktur secara softcopy, tidak ada didalam Dokumen SMM ISO 9001, hasil survey, hasil	Moderate

			wawancara kepada Bapak Nurlillah Satria Pratama	
3	Memastikan adanya prosedur pengelolaan insiden	Tidak adanya dokumen prosedur pada system	Tidak ada dokumen prosedur pengelolaan insiden pada system , hasil wawancara, hasil observasi	Minor
4	Memastikan adanya ketentuan atau standard yang digunakan dalam menangani insiden	Standarisasi menggunakan ISO 9001 dan KPI	Terdapat dokumen SMM ISO 9001, terdapat pada lampiran, hasil wawancara	Minor
5	Memastikan adanya struktur organisasi bagian TSI pada PDAM penanganan insiden	Struktur organisasi unit TSI tidak di publikasikan	Dokumen SOP Pengelolaan penanganan Insiden. Dokumen SMM ISO 9001	Minor

6	Memastikan adanya mekanisme pendekatan penanganan	Semua penanganan insiden dilakukan sesuai dengan prosedur penanganan insiden	Dokumen SMM ISO 9001	Moderate
7	Memastikan adanya pencatatan insiden pada system log Insiden	-Tidak adanya pengidentifikasian konten *kategorisasi/klasifikasi insiden* pada log Insiden -Tidak adanya pengidentifikasian konten *Incident Impact* pada log Insiden -Terdapat pengidentifikasian konten *prioritisasi insiden* pada log	Dokumen SMM ISO 9001, Aplikasi Service Desk System Log Insiden, dokumen backup data, wawancara	Major

		Insiden namun tidak digunakan		
8	Memastikan adanya mekanisme analisis tren	Adanya kondisi kekinian terkait insiden	Hasil wawamcara lampiran	Minor
9	Memastikan insiden yang ditangani sesuai dengan tingkat penanganan risiko	- Terdapat status tingkat risiko berdasarkan prioritas pada catatan system log namun tidak digunakan - Tidak ada panduan dalam tingkat skema prioritas	Hasil Observasi, dokumen SMM ISO 9001, web application Terdapat pada lampiran	Major

10	Memastikan adanya mekanisme persetujuan pe-nanganan insiden	Terdapat beberapa data yang tidak terisi namun sudah disetujui	Lembar pengesahan yang sudah ditanda tangani namun tidak ada report insiden (melihat langsung lembar pengesahan)	Moderate
11	Memastikan adanya klasifikasi insiden dan permintaan layanan	Dokumen SMM ISO 9001	Dokumen ISO 9001	Minor
12	Memastikan Adanya Penutupan atau Pe-nanganan pada Insiden	Masih adanya perulan-gan insiden yang pernah terjadi	Terdapat status pe-nutupan insiden pada Log System, dokumen SMM ISO 9001	Moderate

13	Memastikan adanya pelaporan pengel-olaan insiden	Tidak bisa mengakses web application dari luar	Jaringan local (wawancara langsung)	Moderate

LAMPIRAN F: Hasil Rekomendasi

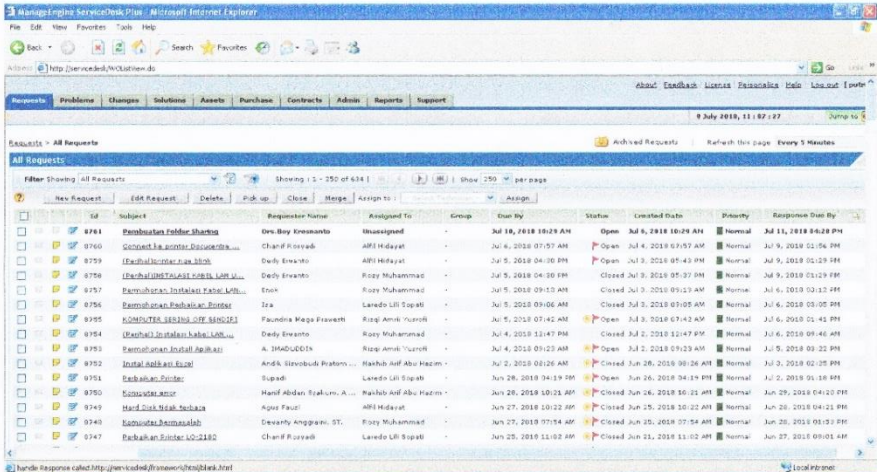
No.	Control Objective	Hasil Temuan	Hasil Rekomendasi
1	CO201.001	Tidak adanya dokumen untuk pendefinisian insiden pada Unit TSI untuk membantu staff untuk menangani insiden	Seharusnya perlu ada petunjuk dan prosedur khusus bagi para requester dan staff lain untuk melakukan pengelolaan insiden
2	CO201.002	Tidak adanya dokumen informasi untuk pengguna layanan secara tertulis hardcopy pada unit TSI	Perlu adanya dokumen informasi penggunaan layanan untuk pengguna secara tertulis ketika layanan melalui web tidak berfungsi
3	CO201.003	Tidak adanya dokumen prosedur pada system	Seharusnya ada dokumen prosedur terlampir pada system agar memudahkan pengguna dalam melaporkan insiden

4	CO201.004	Standarisai menggunakan ISO 9001 dan KPI	Seharusnya ada pembaruan standarisasi yang digunakan untuk terkait manajmen insiden
5	CO201.005	Struktur organisasi Unit TSI	Seharusnya keterangan struktur organisasi dipublikasikan agar memudahkan seseorang dalam mencari informasi terkait PDAM atau Unit TSI
6	CO202.001	Semua penanganan insiden dilakukan sesuai dengan prosedur penanganan insiden	Prosedur penaganan harus selalu diupdate untuk prosedur penanganan insiden
7	CO202.002	-Tidak adanya pengidentifikasian konten *kategorisasi/klasifikasi insiden* pada log Insiden -Tidak adanya pengidentifikasian konten *Incident Impact* pada log Insiden - Ada pengidentifikasian konten *prioritisasi insiden* pada log Insiden namun tidak digunakan	- Seharusnya pada konten log system terdapat kategori insiden berdasarkan prioritas - Seharusnya ada konten untuk incident impact pada log system untuk memudahkan pihak TSI - Seharusnya status prioritas digunakan agar memudahkan penanganan insiden

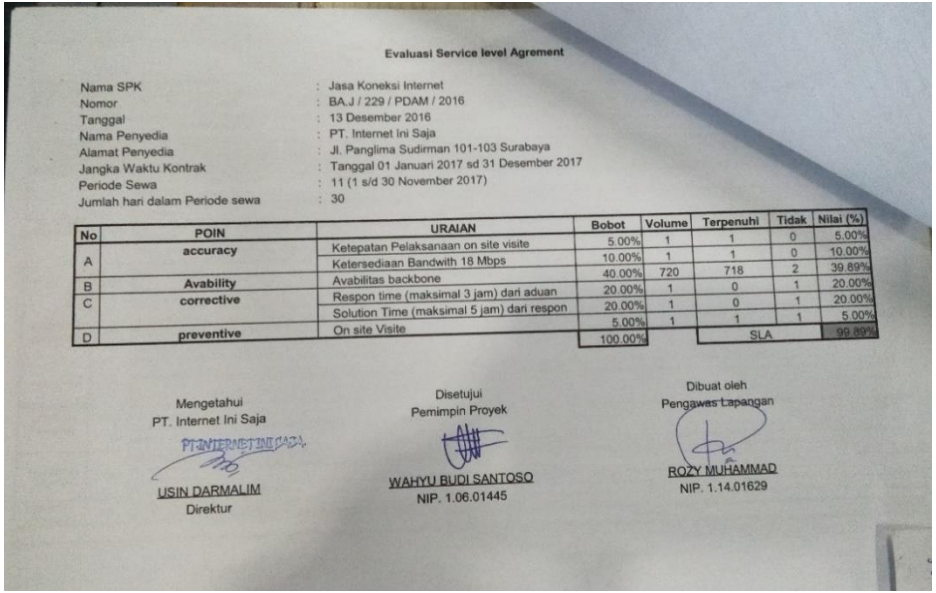
8	CO202.003	Adanya mekanisme analisis tren	Harus adanya dokumen terkait kondisi analisis tren yang selalu terupdate
9	CO202.004	- Terdapat status tingkat risiko berdasarkan prioritas pada catatan system log namun tidak digunakan - Tidak ada panduan dalam tingkat skema prioritas	- Seharusnya dalam system log digunakan status tingkat prioritas dalam masalah menangani insiden agar memudahkan insiden yang ditangani cepat terselesaikan

			- Seharusnya terdapat panduan penangaanan tingkat skema prioritas
10	CO203.001	Terdapat beberapa daya yang tidak terisi namun sudah disetujui	Pengechekan kembali persetujuan penanganan insiden yang dilakukan pada system log
11	CO203.002	Tidak mendapatkan dokumen klasifikasi	Pemberian bukti dokumen klasifikasi pada permintaan layyanan
12	CO205.001	Masih adanya perulangan insiden yang pernah terjadi	Perbaikan system dan maintenance setiap hari agar tidak meinmbulkan insiden yang selalu berulang
13	CO207.001	Tidak bisa mengakses web application dari luar	Seharusnya pelaporan yang dilakukan diluar perusahaan masih bisa melakukan atau masih bisa diakses

LAMPIRAN G: Bukti Temuan Audit



Gambar G. 1 Web Application Service Desk Catatan Log Insiden



Evaluasi Service level Agrement

Nama SPK	: Jasa Koneksi Internet
Nomor	: BA.J / 229 / PDAM / 2016
Tanggal	: 13 Desember 2016
Nama Penyedia	: PT. Internet Ini Saja
Alamat Penyedia	: Jl. Panglima Sudirman 101-103 Surabaya
Jangka Waktu Kontrak	: Tanggal 01 Januari 2017 sd 31 Desember 2017
Periode Sewa	: 11 (1 s/d 30 November 2017)
Jumlah hari dalam Periode sewa	: 30

No	POIN	URAIAN	Bobot	Volume	Terpenuhi	Tidak	Nilai (%)
A	accuracy	Ketepatan Pelaksanaan on site visite	5.00%	1	1	0	5.00%
		Ketersediaan Bandwith 18 Mbps	10.00%	1	1	0	10.00%
B	Avability	Avabilitas backbone	40.00%	720	718	2	39.89%
C	corrective	Respon time (maksimal 3 jam) dari aduan	20.00%	1	0	1	20.00%
		Solution Time (maksimal 5 jam) dari respon	20.00%	1	0	1	20.00%
D	preventive	On site Visite	5.00%	1	1	1	5.00%
			100.00%		SLA		99.89%

Mengetahui
PT. Internet Ini Saja

USIN DARMALIM
Direktur

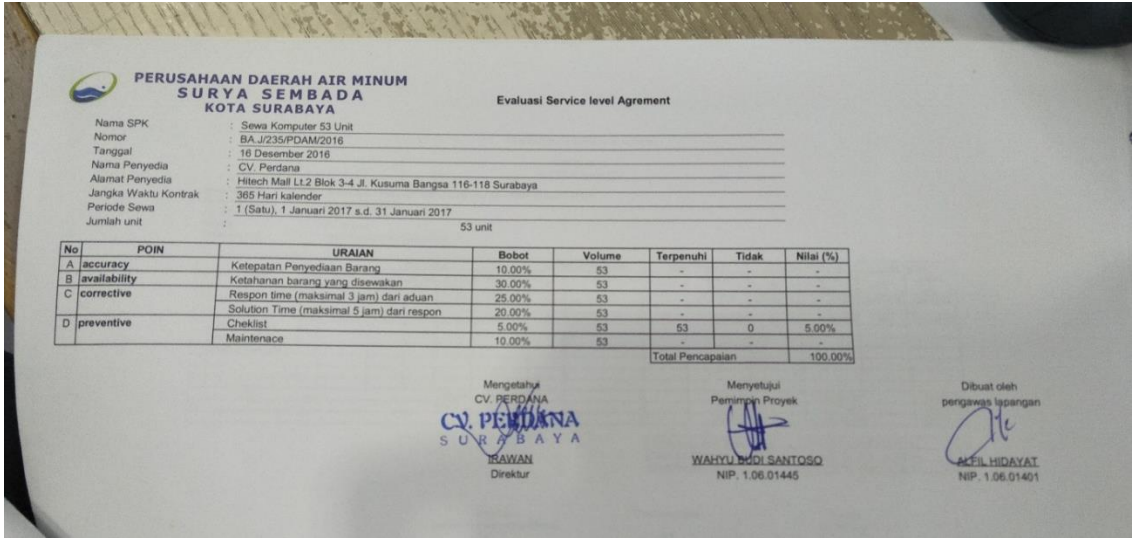
Disetujui
Pemimpin Proyek

WAHYU BUDI SANTOSO
NIP. 1.06.01445

Dibuat oleh
Pengawas Lapangan

ROZY MUHAMMAD
NIP. 1.14.01629

Gambar G. 2 Bukti Dokumen SLA



PERUSAHAAN DAERAH AIR MINUM
SURYA SEMBADA
KOTA SURABAYA

Evaluasi Service level Agrement

Nama SPK	:	Sewa Komputer 53 Unit
Nomor	:	BA.J/235/PDAM/2016
Tanggal	:	16 Desember 2016
Nama Penyedia	:	CV. Perdana
Alamat Penyedia	:	Hitech Mall Lt.2 Blok 3-4 Jl. Kusuma Bangsa 116-118 Surabaya
Jangka Waktu Kontrak	:	365 Hari kalender
Periode Sewa	:	1 (Satu), 1 Januari 2017 s.d. 31 Januari 2017
Jumlah unit	:	53 unit

No	POIN	URAIAN	Bobot	Volume	Terpenuhi	Tidak	Nilai (%)
A	**accuracy**	Ketepatan Penyediaan Barang	10.00%	53	-	-	-
B	**availability**	Ketahanan barang yang disewakan	30.00%	53	-	-	-
C	**corrective**	Respon time (maksimal 3 jam) dari aduan	25.00%	53	-	-	-
		Solution Time (maksimal 5 jam) dari respon	20.00%	53	-	-	-
D	**preventive**	Cheklist	5.00%	53	53	0	5.00%
		Maintenace	10.00%	53	-	-	-
					Total Pencapaian		100.00%

Mengetahui
CV. PERDANA
CV. PERDANA SURABAYA
IRAWAN
Direktur

Menyetujui
Pemimpin Proyek
WAHYU BUDI SANTOSO
NIP. 1.06.01445

Dibuat oleh
pengawas lapangan
AKFIL HIDAYAT
NIP. 1.06.01401

Gambar G. 3 Bukti Dokumen SLA

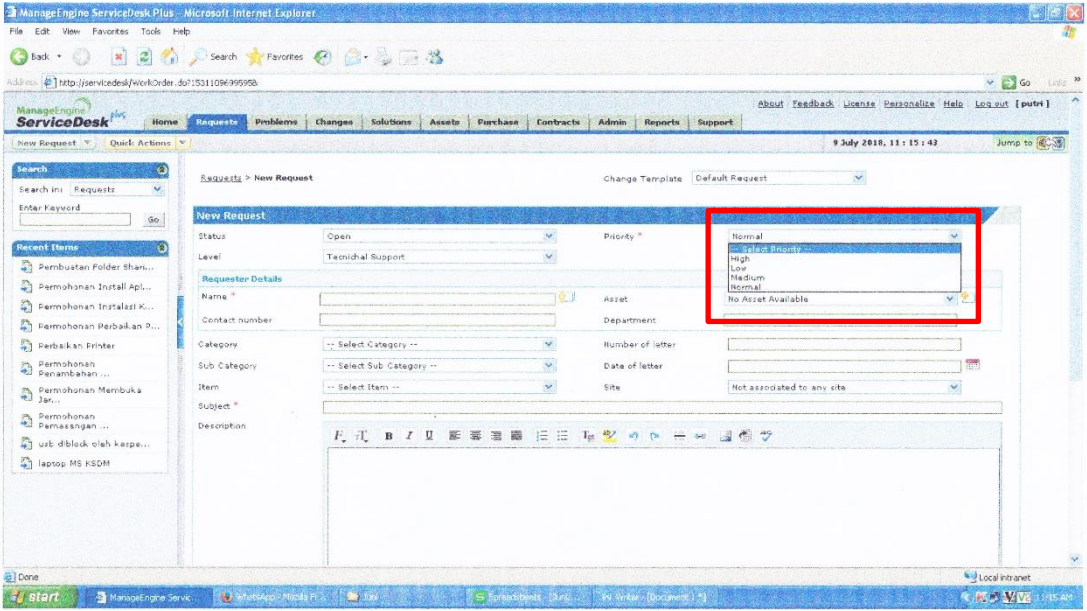
Penanggung Jawab

Resolution	Technician
Bersihkan Memori RAM	Alfil Hidayat
Komputer sudah terdaftar grub USB Flasdisk,	Alfil Hidayat
Mouse sewa, koordinasi dengan pihak ke2	Alfil Hidayat
setting IP internet	Rozy Muhammad
penggantian mainboard	Rozy Muhammad
ganti hardisk	Alfil Hidayat
ganti mainboard	Nakhib Arif Abu Hazim
install excell	Nakhib Arif Abu Hazim

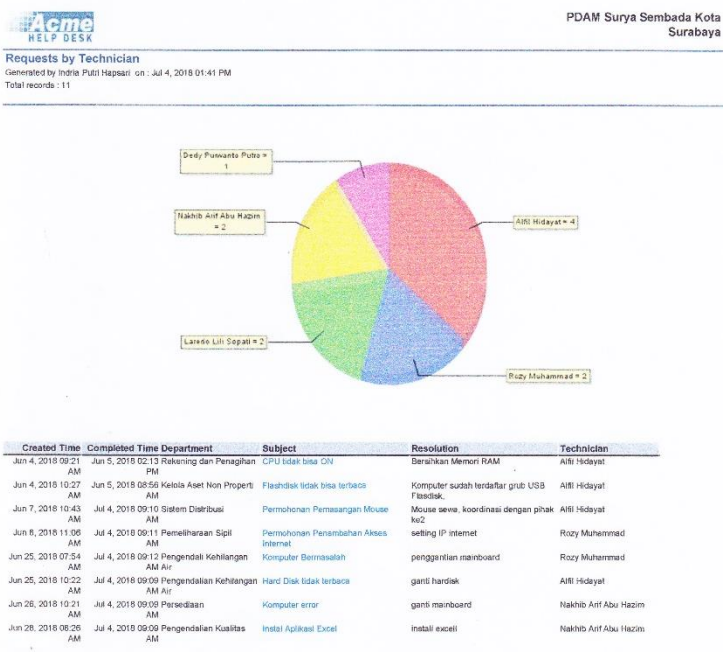
Gambar G. 4 Penanggung Jawab Insiden

Created Time	Completed Time	Department	Subject
Jun 4, 2018 09:21 AM	Jun 5, 2018 02:13 PM	Rekening dan Penagihan	CPU tidak bisa ON
Jun 4, 2018 10:27 AM	Jun 5, 2018 08:56 AM	Kelola Aset Non Properti	Flashdisk tidak bisa terbaca
Jun 7, 2018 10:43 AM	Jul 4, 2018 09:10 AM	Sistem Distribusi	Permohonan Pemasangan Mouse
Jun 8, 2018 11:06 AM	Jul 4, 2018 09:11 AM	Pemeliharaan Sipil	Permohonan Penambahan Akses Internet
Jun 25, 2018 07:54 AM	Jul 4, 2018 09:12 AM	Pengendali Kehilangan Air	Komputer Bermasalah
Jun 25, 2018 10:22 AM	Jul 4, 2018 09:09 AM	Pengendalian Kehilangan Air	Hard Disk tidak terbaca
Jun 26, 2018 10:21 AM	Jul 4, 2018 09:09 AM	Persediaan	Komputer error
Jun 28, 2018 08:26 AM	Jul 4, 2018 09:09 AM	Pengendalian Kualitas	Instal Aplikasi Excel

Gambar G. 5 Penutupan Pelaporan Insiden

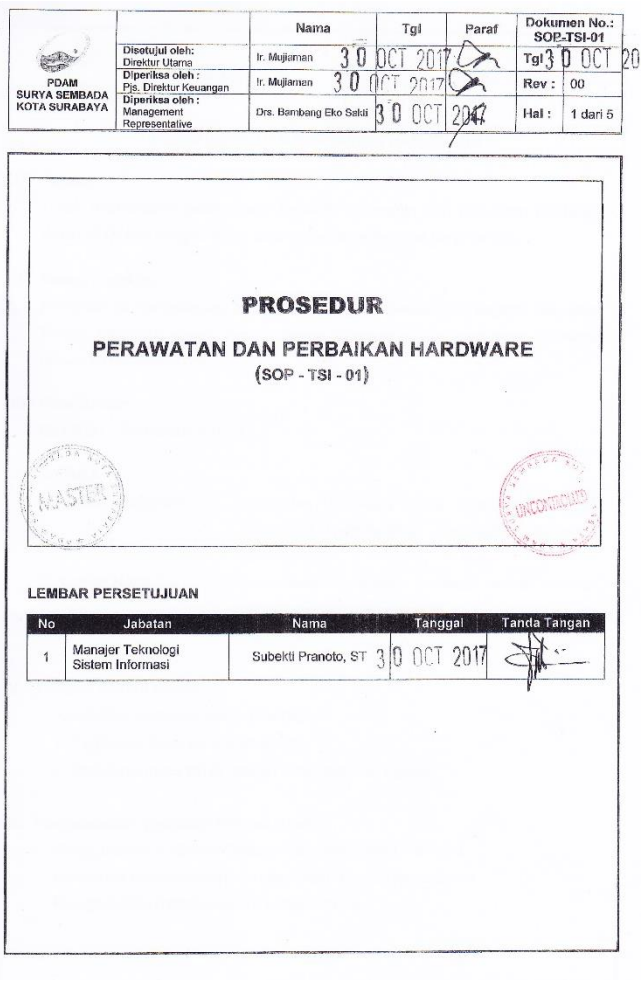


Gambar G. 6 Tingkat Prioritas Pada System Log



Gambar G. 7 Penutupan Penanganan Insiden

Dokumen SOP SMM ISO 9001



PDAM SURYA SEMBADA KOTA SURABAYA		Nama	Tgl	Paraf	Dokumen No.: SOP-TSI-01	
	Disetujui oleh: Direktur Utama	Ir. Mujiaman	30 OCT 2017		Tgl	30 OCT 20
	Diperiksa oleh : Pjs. Direktur Keuangan	Ir. Mujiaman	30 OCT 2017		Rev :	00
	Diperiksa oleh : Management Representative	Drs. Bambang Eko Saldi	30 OCT 2017		Hal :	1 dari 5

PROSEDUR

PERAWATAN DAN PERBAIKAN HARDWARE

(SOP - TSI - 01)

MASTER

UNCONTROLLED

LEMBAR PERSETUJUAN

No	Jabatan	Nama	Tanggal	Tanda Tangan
1	Manajer Teknologi Sistem Informasi	Subekti Pranoto, ST	30 OCT 2017	

Gambar G. 8 Prosedur Perawatan dan Perbaikan Hardware

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 01	Hal : 2 dari 5
			Tgl :
			Rev : 00

PERAWATAN DAN PERBAIKAN HARDWARE

I. Tujuan

Untuk memastikan pelaksanaan kegiatan perawatan dan perbaikan hardware dapat dilakukan dengan benar sesuai dengan ketentuan yang berlaku.

II. Ruang Lingkup

Prosedur ini menjelaskan tugas dan tanggung jawab dari Bagian Teknologi Sistem Informasi dalam melaksanakan perawatan dan perbaikan hardware sesuai proses flowchart.

III. Persyaratan

ISO 9001 : 2015 klausul 7.1.3

IV. Definisi

Perawatan Hardware	:	perawatan hardware yang dilakukan dengan melakukan pembersihan perangkat hardware secara rutin
Perbaikan Hardware	:	pelaksanaan perbaikan hardware sesuai dengan permintaan dari bagian terkait
Spv	:	Supervisor

V. Potensi Resiko Bisnis

- Kerusakan perangkat keras (hardware)
  - Tegangan listrik yang tidak stabil
  - Mencapai masa MTBF (Mean Time Between Failure)

VI. Pengendalian Terhadap Potensi Resiko

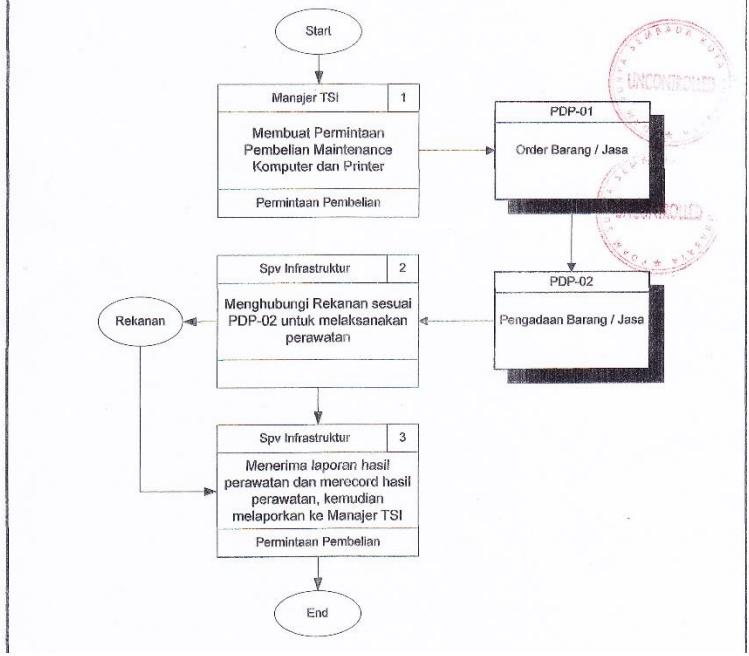
- Menggunakan automatic Voltage Regulator (AVR) dan UPS
- Monitoring usia sparepart menggunakan IT asset manajemen
- Menggunakan metode sewa perangkat keras

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen :	Hal :	3 dari 5
		SOP- TSI - 01	Tgl :	30 OCT 201
			Rev :	00

PERAWATAN DAN PERBAIKAN HARDWARE

VII. Alur Proses

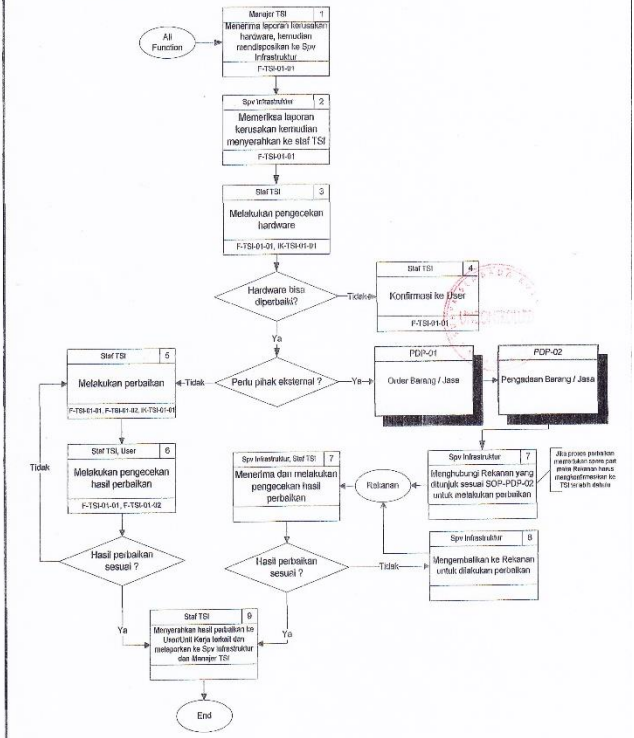
Perawatan Hardware



PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 01	Hal : 4 dari 5
			Tgl : 30 Juni 201
			Rev : 00

PERAWATAN DAN PERBAIKAN HARDWARE

Perbaikan Hardware



PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 01	Hal : 5 dari 5
			Tgl : 30 Oct 2017
			Rev : 00

PERAWATAN DAN PERBAIKAN HARDWARE

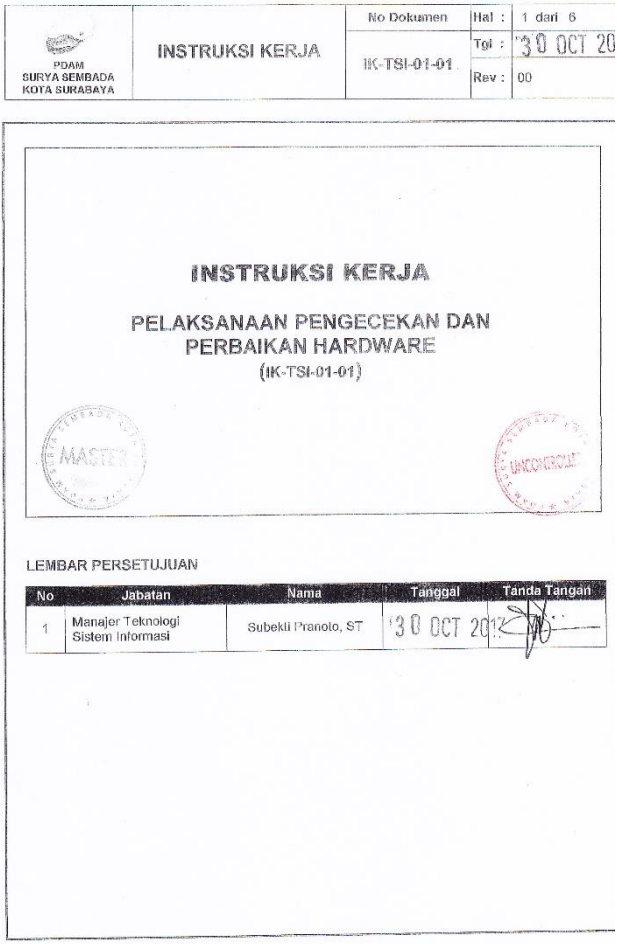
Keterangan :

VIII. Dokumen Pendukung :

No.	Nomor Dokumen	Judul Dokumen
1	F-TSI-01-01	Form Permohonan Hardware
2	F-TSI-01-02	Form Quick Response

IX. Catatan Perubahan :

No.	No. Revisi	Perubahan	Tanggal Efektif



PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen	Hal :	1 dari 6
		IK-TSI-01-01	Tgl :	30 OCT 20
			Rev :	00

INSTRUKSI KERJA

PELAKSANAAN PENGECEKAN DAN PERBAIKAN HARDWARE
(IK-TSI-01-01)

MASTER

UNCONTROLLED

LEMBAR PERSETUJUAN

No	Jabatan	Nama	Tanggal	Tanda Tangan
1	Manajer Teknologi Sistem Informasi	Subekti Pranoto, ST	30 OCT 201	

Gambar G. 9 Dokumen SOP SMM ISO 9001 Instruksi Kerja

PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen : IK-TSI- 01-01	Hal : 2 dari 6
			Tgl : 30 OCT 2017
			Rev : 00

PELAKSANAAN PENGECEKAN DAN PERBAIKAN HARDWARE

I. Tujuan

Instruksi kerja ini dibuat sebagai pedoman dalam melaksanakan kegiatan pengecekan dan perbaikan hardware.

II. Ruang Lingkup

Instruksi kerja ini menjelaskan tugas dan tanggung jawab dari Bagian Teknologi Sistem Informasi dalam melaksanakan pengecekan dan perbaikan hardware.

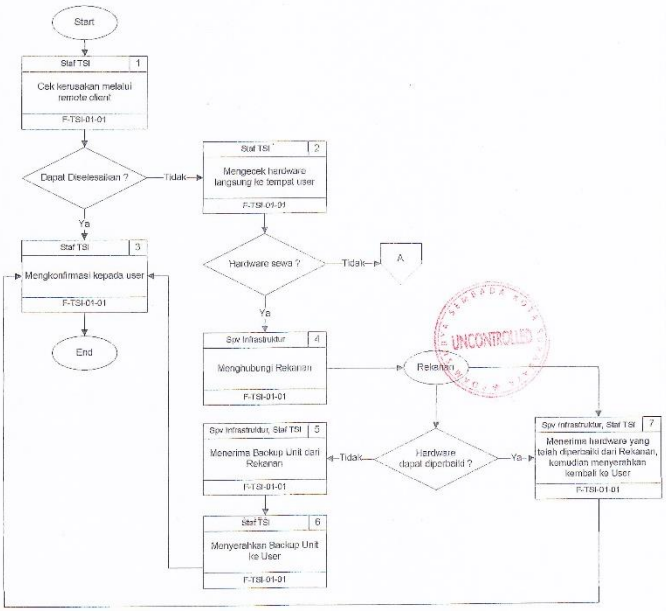
III. Definisi

Perbaikan Hardware	:	pelaksanaan perbaikan hardware sesuai dengan permintaan dari bagian terkait
Spv	:	Supervisor

PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen : IK-TSI- 01-01	Hal : 3 dari 6
			Tgl : 30 OCT 2017
			Rev : 00

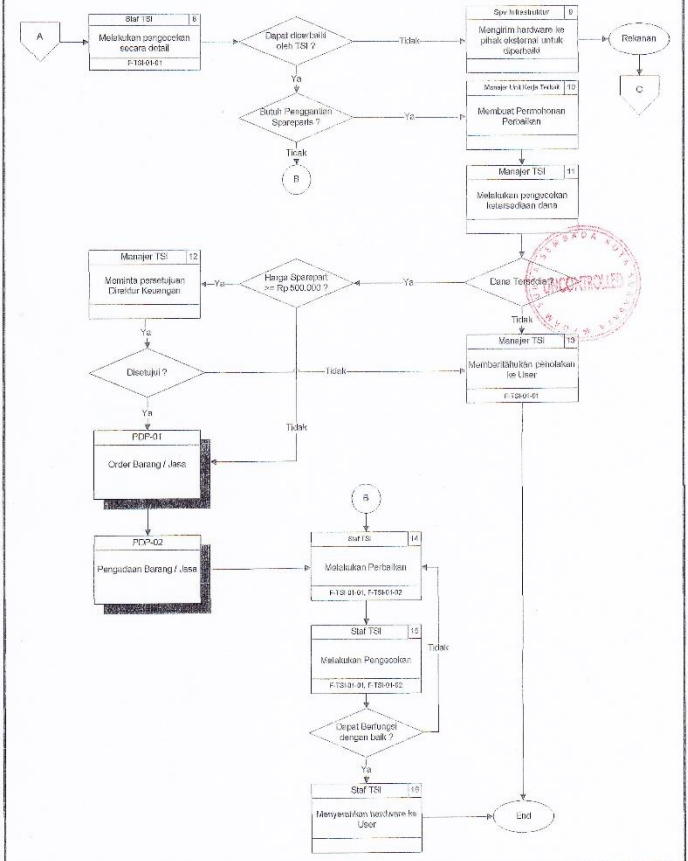
PELAKSANAAN PENGECEKAN DAN PERBAIKAN HARDWARE

IV. Alur Proses



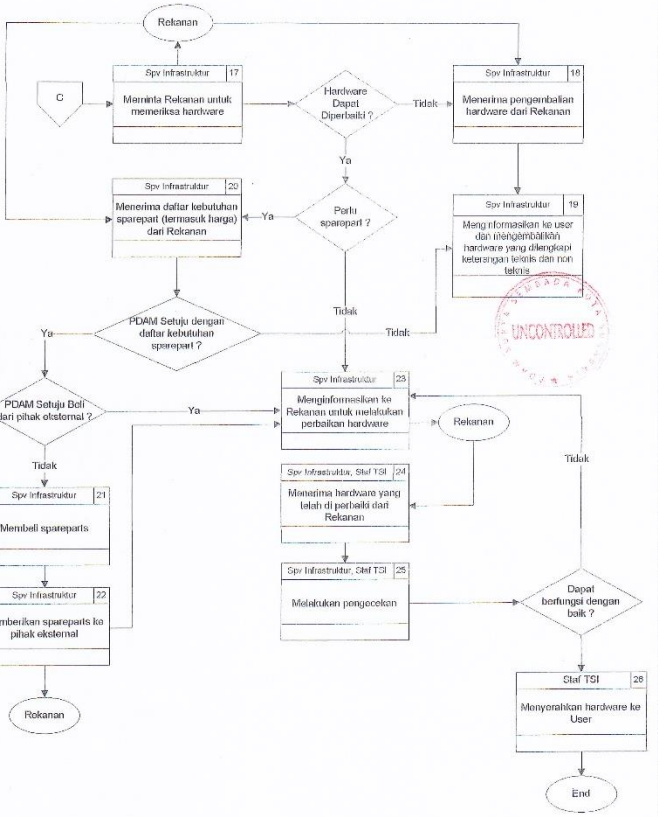
PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen : IK-TSI- 01-01	Hal : 4 dari 6
			Tgt : 30 OCT 2017
			Rev : 00

PELAKSANAAN PENGECEKAN DAN PERBAIKAN HARDWARE



PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen : IK-TSI- 01-01	Hal : 5 dari 6	Tgl : 30 OCT 2017	Rev : 00

PELAKSANAAN PENGECEKAN DAN PERBAIKAN HARDWARE



PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen : IK-TSI- 01-01	Hal : 6 dari 6	Tgl : 30 OCT 201	Rev : 00

PELAKSANAAN PENGECEKAN DAN PERBAIKAN HARDWARE

V. Keterangan :

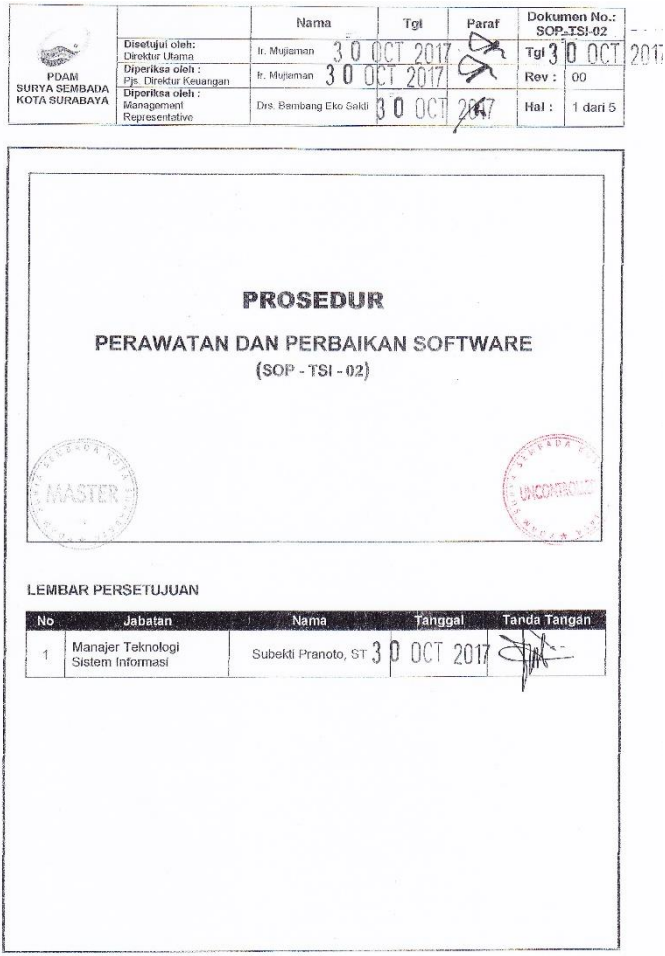
-

VI. Dokumen Pendukung :

No.	Nomor Dokumen	Judul Dokumen
1	F-TSI-01-01	Form Permohonan Hardware
2	F-TSI-01-02	Form Quick Response

VII. Catatan Perubahan :

No.	No. Revisi	Perubahan	Tanggal Efektif



PDAM SURYA SEMBADA KOTA SURABAYA		Nama	Tgl	Paraf	Dokumen No.: SOP-TSI-02	
	Disetujui oleh: Direktur Utama	Ir. Mujiaman	30 OCT 2017		Tgl	30 OCT 2017
	Diperiksa oleh : Pjs. Direktur Keuangan	Ir. Mujiaman	30 OCT 2017		Rev :	00
	Diperiksa oleh : Management Representative	Drs. Bambang Eko Sakti	30 OCT 2017		Hal :	1 dari 5

PROSEDUR

PERAWATAN DAN PERBAIKAN SOFTWARE

(SOP - TSI - 02)

MASTER

UNCONTROLLED

LEMBAR PERSETUJUAN

No	Jabatan	Nama	Tanggal	Tanda Tangan
1	Manajer Teknologi Sistem Informasi	Subekti Pranoto, ST	30 OCT 2017	

Gambar G. 10 Prosedur Perawatan dan Perbaikan Software

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 02	Hal : 2 dari 5
			Tgl : 30 OCT 2017
			Rev : 00

PERAWATAN DAN PERBAIKAN SOFTWARE

I. Tujuan

Untuk memastikan pelaksanaan kegiatan perawatan dan perbaikan software dapat dilakukan dengan benar sesuai dengan ketentuan yang berlaku.

II. Ruang Lingkup

Prosedur ini menjelaskan tugas dan tanggung jawab dari Bagian Teknologi Sistem Informasi dalam melaksanakan perawatan dan perbaikan software sesuai proses flowchart.

III. Persyaratan

ISO 9001 : 2015 klausul 7.1.3

IV. Definisi

Perawatan Software	:	perawatan software dilakukan dengan melakukan update software tertentu (antivirus dan sebagainya) secara otomatis dan rutin
Perbaikan Software		pelaksanaan perbaikan software sesuai dengan permintaan dari bagian terkait
Spv		Supervisor

V. Potensi Resiko Bisnis

- Gangguan dan serangan terhadap komputer, server dan jaringannya
  - Penggunaan flasdisk dan akses internet yang terinfeksi virus

VI. Pengendalian Terhadap Potensi Resiko

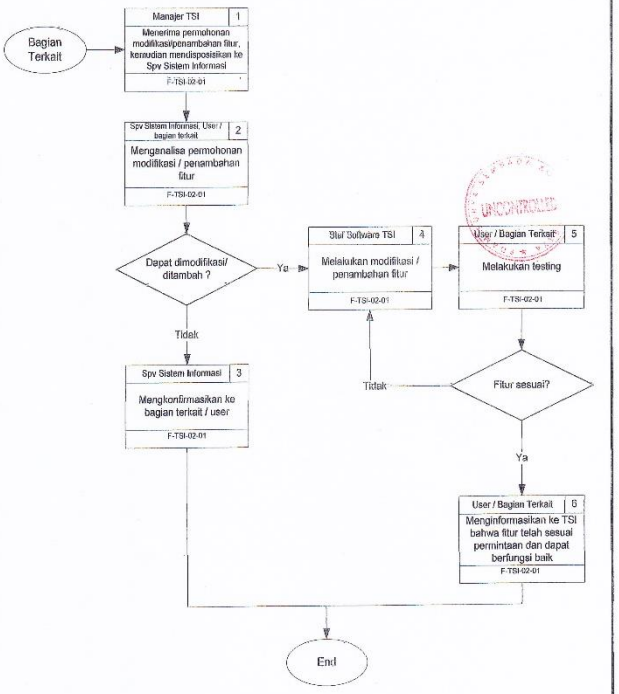
- Menggunakan antivirus dan firewall untuk semua computer dan server

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 02	Hal : 4 dari 5
			Tgl : 30 OCT 2017
			Rev : 00

PERAWATAN DAN PERBAIKAN SOFTWARE

PERBAIKAN SOFTWARE

Modifikasi / Penambahan Fitur



PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 02	Hal : 5 dari 5
			Tgl : 30 OCT 2017
			Rev : 00

PERAWATAN DAN PERBAIKAN SOFTWARE

Keterangan :

-

VIII. Dokumen Pendukung :

No.	Nomor Dokumen	Judul Dokumen
1	F-TSI-02-01	Form Permohonan Software

UNCONTROLLED

IX. Catatan Perubahan :

No.	No. Revisi	Perubahan	Tanggal Efektif

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 03	Hal : 2 dari 4	Tgl : 3 0 OKT 2017	Rev : 00

BACK UP DATA

I. Tujuan

Untuk memastikan bahwa setiap data penting yang diperlukan telah di back up sehingga apabila terjadi kehilangan data tersebut perusahaan masih memiliki arsipnya.

II. Ruang Lingkup

Prosedur ini menjelaskan tugas dan tanggung jawab dari Bagian Teknologi Sistem Informasi dalam melaksanakan back up data sesuai proses flowchart.

III. Persyaratan

ISO 9001 : 2015 klausul 7.5.2, 7.5.3, 7.1.3

UNCONTROLLED

IV. Definisi

Back up data : proses penyimpanan / pengarsipan database pada server TSI

Spv : Supervisor

V. Potensi Resiko Bisnis

- Downtime database
  - Kerusakan hardware
  - Service pada ORACLE database terhenti

VI. Pengendalian Terhadap Potensi Resiko

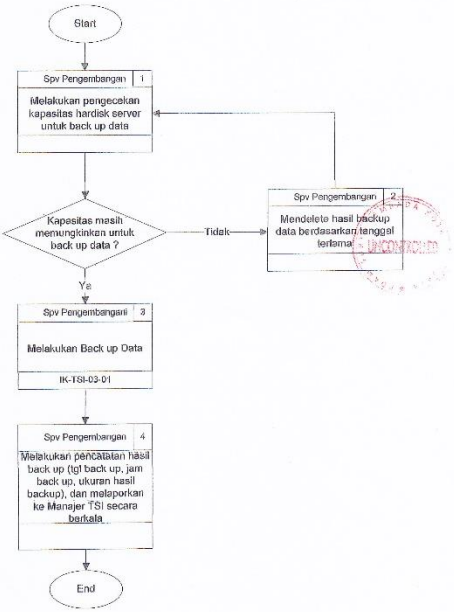
- Maintenance rutin dan monioring usia sparepart menggunakan IT Asset Management
- Monitoring status service pada ORACLE DB secara realtime
- Peremajaan hardware secara berkala

Gambar G. 11 Posedur Backup Data

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 03	Hal : 3 dari 4
			Tgl : 3 0 JAN 201
			Rev : 00

BACK UP DATA

VII. Alur Proses



PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 03	Hal : 4 dari 4	
			Tgl : 30 OCT 2017	
			Rev : 00	

BACK UP DATA

Keterangan :

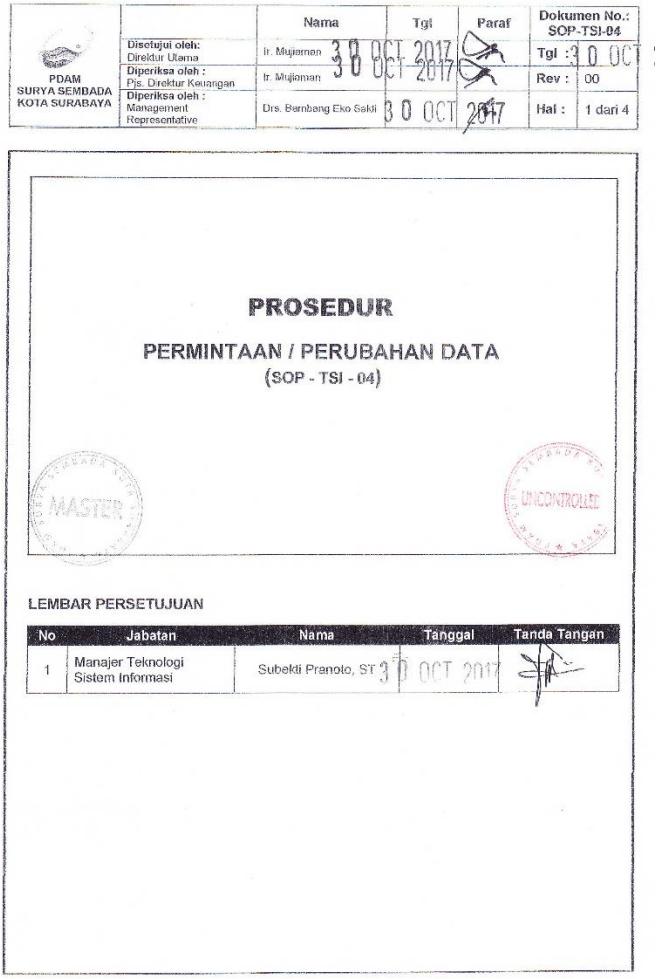
-

VIII. Dokumen Pendukung :

No.	Nomor Dokumen	Judul Dokumen
1	IK-TSI-03-01	Instruksi Kerja Pelaksanaan Back Up Data

IX. Catatan Perubahan :

No.	No. Revisi	Perubahan	Tanggal Efektif



PDAM SURYA SEMBADA KOTA SURABAYA		Nama	Tgl	Paraf	Dokumen No.: SOP-TSI-04	
	Disetujui oleh: Direktur Utama	Ir. Mujiaman	30 OCT 2017		Tgl : 30 OCT	
	Diperiksa oleh : Pjs. Direktur Keuangan	Ir. Mujiaman	30 OCT 2017		Rev :	00
	Diperiksa oleh : Management Representative	Drs. Bambang Eko Sakti	30 OCT 2017		Hal :	1 dari 4

PROSEDUR

PERMINTAAN / PERUBAHAN DATA

(SOP - TSI - 04)

MASTER

UNCONTROLLED

LEMBAR PERSETUJUAN

No	Jabatan	Nama	Tanggal	Tanda Tangan
1	Manajer Teknologi Sistem Informasi	Subekti Pranoto, ST	30 OCT 2017	

Gambar G. 12 Prosedur Permintaan/Perubahan Data

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 04	Hal : 2 dari 4
			Tgl : 30 OCT 2017
			Rev : 00

PERMINTAAN / PERUBAHAN DATA

I. Tujuan

Untuk memastikan bahwa kegiatan permintaan / perubahan data yang dilakukan sesuai dengan ketentuan yang berlaku.

II. Ruang Lingkup

Prosedur ini menjelaskan tugas dan tanggung jawab dari Bagian Teknologi Sistem Informasi dalam melaksanakan permintaan/perubahan data sesuai proses flowchart.

III. Persyaratan

ISO 9001 : 2015 klausul 7.5.2, 7.5.3

IV. Definisi

Spv	: Supervisor
TSI	: Teknologi Sistem Informasi
SLA	: Service Level Agreement

V. Potensi Resiko Bisnis

- Memperlambat proses operasional (slow down) yang terkait dengan database

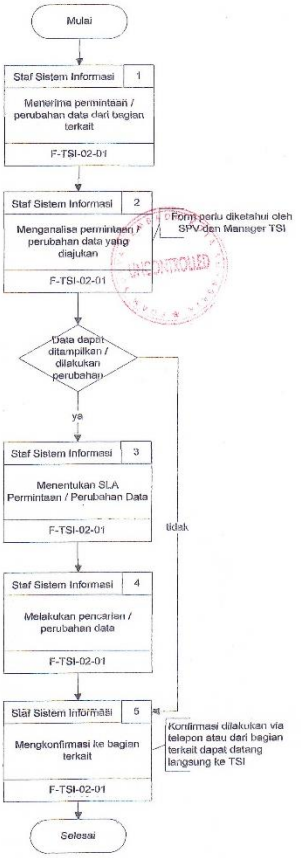
VI. Pengendalian Terhadap Potensi Resiko

- Pelaksanaan pencarian data dilaksanakan setelah jam kerja, terutama untuk data-data yang berkapasitas besar (lebih dari 300 ribu records) dan beban pencarian data di database yang besar.

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen :	Hal :	3 dari 4
		SOP- TSI - 04	Tgl :	30 OCT 20
			Rev :	00

PERMINTAAN / PERUBAHAN DATA

VII. Alur Proses



PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 04	Hal : 4 dari 4	
			Tgl : 30 OCT 201	
			Rev : 00	

PERMINTAAN / PERUBAHAN DATA

Keterangan :

-

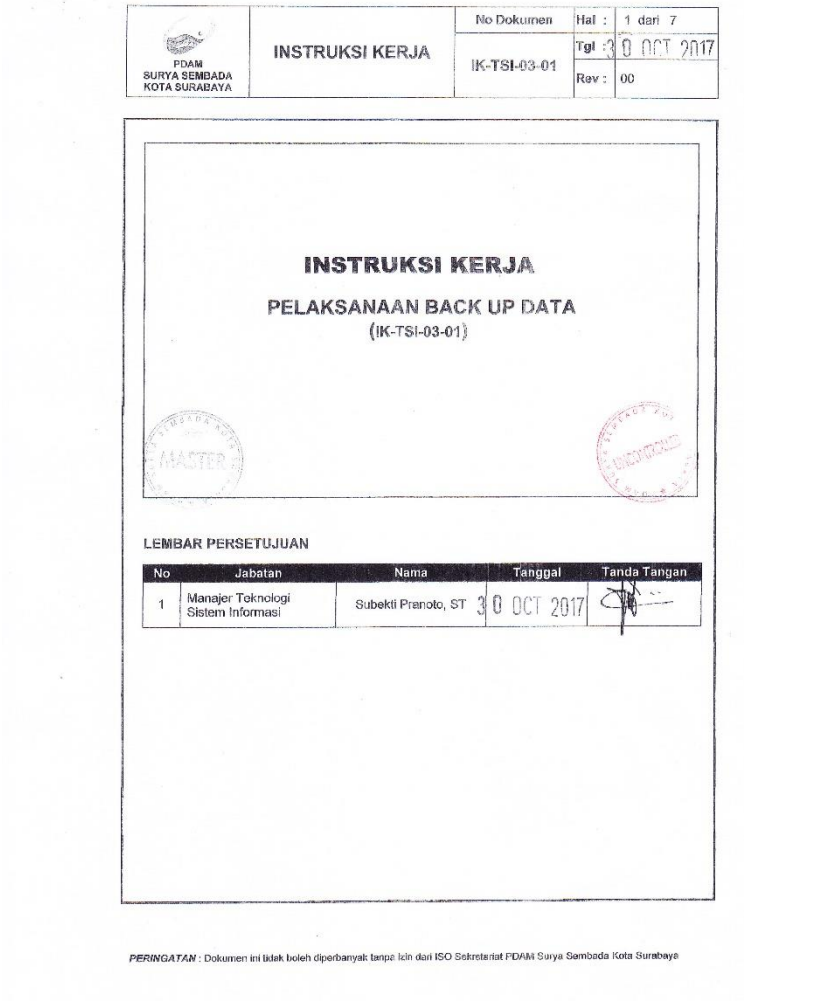
VIII. Dokumen Pendukung :

No.	Nomor Dokumen	Judul Dokumen
1.	F-TSI-02-01	Form Permohonan Software

UNCONTROLLED

IX. Catatan Perubahan :

No.	No. Revisi	Perubahan	Tanggal Efektif



PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen	Hal :	1 dari 7
		IK-TSI-03-01	Tgl :	30 OCT 2017
			Rev :	00

INSTRUKSI KERJA

PELAKSANAAN BACK UP DATA

(IK-TSI-03-01)

MASTER

TERKENDALI

LEMBAR PERSETUJUAN

No	Jabatan	Nama	Tanggal	Tanda Tangan
1	Manajer Teknologi Sistem Informasi	Subekti Pranoto, ST	30 OCT 2017	

Gambar G. 13 Instruksi Kerja Pelaksanaan Back Up Data

PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen :	Hal :	2 dari 7
		IK-TSI- 03-01	Tgl :	31 OCT 201
			Rev :	01

PELAKSANAAN BACK UP DATA

I. Tujuan

Instruksi kerja ini dibuat sebagai pedoman dalam melaksanakan kegiatan back up data.

II. Ruang Lingkup

Instruksi kerja ini menjelaskan tugas dan tanggung jawab dari Bagian Teknologi Sistem Informasi dalam melaksanakan back up data.

III. Definisi

Back up data : proses penyimpanan / pengarsipan data pada server TSI

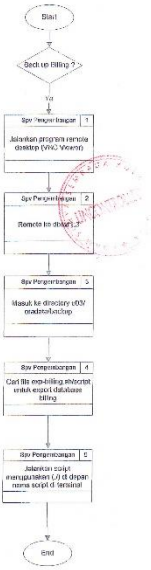
Spv : Supervisor

PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen : IK-TSI- 03-01	Hal : 3 dari 7
			Tgl : 3 0 Oct 201
			Rev : 01

PELAKSANAAN BACK UP DATA

IV. Alur Proses

BACK UP BILLING



PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen :	Hal :	4 dari 7
		IK-TSI- 03-01	Tgl :	[illegible]
			Rev :	01

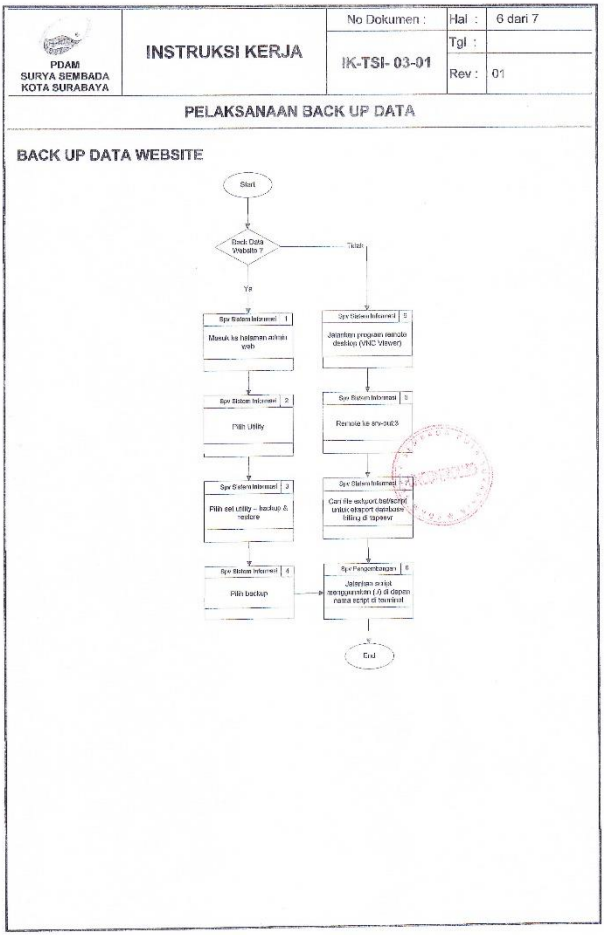
PELAKSANAAN BACK UP DATA

BACK UP AXAPTA

PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen :	Hal :	5 dari 7
		IK-TSI- 03-01	Tgl :	30 OKT 2017
			Rev :	01

PELAKSANAAN BACK UP DATA

BACK UP SKA



Gambar G. 14 Instruksi Kerja Back Up Data

PDAM SURYA SEMBADA KOTA SURABAYA	INSTRUKSI KERJA	No Dokumen : IK-TSI- 03-01	Hal : 7 dari 7	Tgl : 30 OCT 2018	Rev : 01

PELAKSANAAN BACK UP DATA

Keterangan :

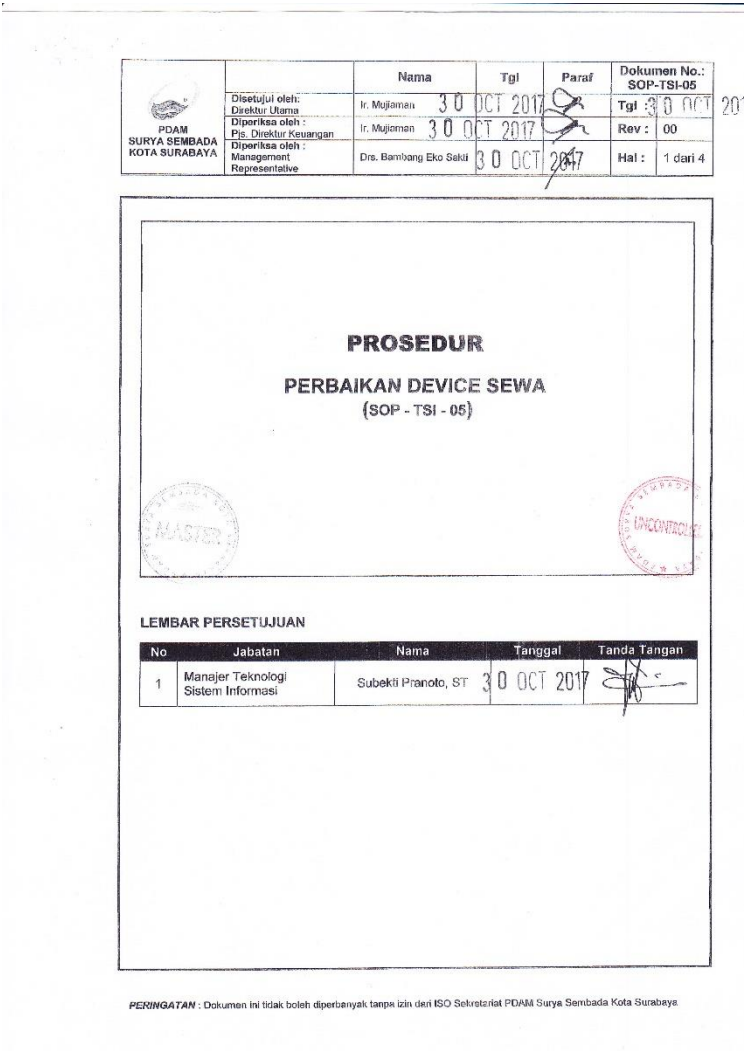
-

VI. Dokumen Pendukung :

No.	Nomor Dokumen	Judul Dokumen

VII. Catatan Perubahan :

No.	No. Revisi	Perubahan	Tanggal Efektif



PDAM SURYA SEMBADA KOTA SURABAYA		Nama	Tgl	Paraf	Dokumen No.: SOP-TSI-05	
	Disetujui oleh: Direktur Utama	Ir. Mujiaman	30 OCT 2017		Tgl :	30 OCT 20
	Diperiksa oleh : Pjs. Direktur Keuangan	Ir. Mujiaman	30 OCT 2017		Rev :	00
	Diperiksa oleh : Management Representative	Drs. Bambang Eko Sakti	30 OCT 2017		Hal :	1 dari 4

PROSEDUR

PERBAIKAN DEVICE SEWA

(SOP - TSI - 05)

MASTER

UNCONTROLLED

LEMBAR PERSETUJUAN

No	Jabatan	Nama	Tanggal	Tanda Tangan
1	Manajer Teknologi Sistem Informasi	Subekti Pranoto, ST	30 OCT 2017	

PERINGATAN : Dokumen ini tidak boleh diperbanyak tanpa izin dari ISO Sekretariat PDAM Surya Sembada Kota Surabaya

Gambar G. 15 Prosedur Perbaikan Device Sewa

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 05	Hal : 2 dari 4
			Tgl : 30 DEC 2017
			Rev : 00

PERBAIKAN DEVICE SEWA

I. Tujuan

Untuk memastikan bahwa kegiatan perbaikan device sewa yang dilakukan sesuai dengan ketentuan yang berlaku.

II. Ruang Lingkup

Prosedur ini menjelaskan tugas dan tanggung jawab dari Bagian Teknologi Sistem Informasi dalam melaksanakan perbaikan device sewa sesuai proses flowchart.

III. Persyaratan

ISO 9001 : 2015 klausul 7.1.3, 7.5.2, 7.5.3

IV. Definisi

Spv	: Supervisor
SPK	: Surat Perintah Kerja
SLA	: Service Level Agreement
TSI	: Teknologi Sistem Informasi

V. Potensi Resiko Bisnis

- Terlambat dalam melakukan perbaikan

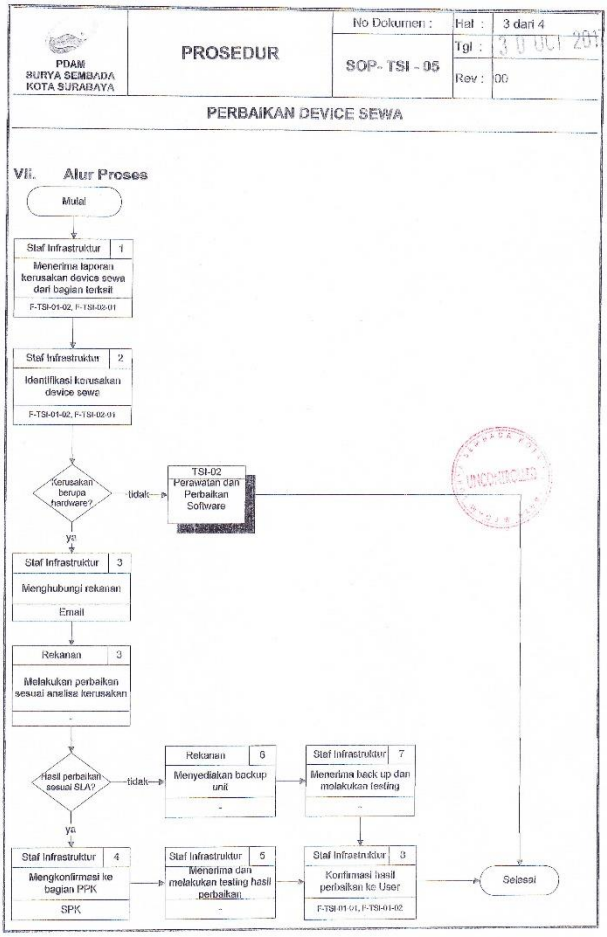
VI. Pengendalian Terhadap Potensi Resiko

- Pengendalian pada response dan solution time
- Penyediaan backup unit

PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 05	Hal : 3 dari 4
		Tgl : 30 OCT 201	
		Rev : 00	

PERBAIKAN DEVICE SEWA

VII. Alur Proses



PDAM SURYA SEMBADA KOTA SURABAYA	PROSEDUR	No Dokumen : SOP- TSI - 05	Hal : 4 dari 4
			Tgl : 30 OCT 2017
			Rev : 00

PERBAIKAN DEVICE SEWA

Keterangan :

VIII. Dokumen Pendukung :

No.	Nomor Dokumen	Judul Dokumen
1.	F-TSI-01-01	Form Permohonan Hardware
2.	F-TSI-01-02	Quick Response Form
3.	F-TSI-02-01	Form Permohonan Software
		Form korektif eksternal

IX. Catatan Perubahan :

No.	No. Revisi	Perubahan	Tanggal Efektif