TUGAS AKHIR – KS 141501

IMPLEMENTASI METODOLOGI PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (STUDI KASUS : PDAM SURYA SEMBADA KOTA SURABAYA)

METHODOLOGY IMPLEMENTATION IN DEVELOPING BUSINESS CONTINUITY PLAN DOCUMENT (CASE STUDY : PDAM SURYA SEMBADA KOTA SURABAYA*)*

CINDY ALICIA SAHARA
NRP 05211440000172

Dosen Pembimbing :
Dr. Apol Pribadi S., S.T., M.T.

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

TUGAS AKHIR – KS 141501

IMPLEMENTASI METODOLOGI PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (STUDI KASUS : PDAM SURYA SEMBADA KOTA SURABAYA)

CINDY ALICIA SAHARA
NRP 05211440000172

Dosen Pembimbing :
Dr. Apol Pribadi S., S.T., M.T.

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

FINAL PROJECT – KS 141501

METHODOLOGY IMPLEMENTATION IN DEVELOPING BUSINESS CONTINUITY PLAN DOCUMENT (CASE STUDY : PDAM SURYA SEMBADA KOTA SURABAYA*)*

CINDY ALICIA SAHARA
NRP 05211440000172

SUPERVISOR:
Dr. Apol Pribadi S., S.T., M.T.

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

LEMBAR PENGESAHAN

IMPLEMENTASI METODOLOGI PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (STUDI KASUS : 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:

CINDY ALICIA SAHARA
NRP. 05211440000172

Surabaya, Juli 2018

KEPALA
DEPARTEMEN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

IMPLEMENTASI METODOLOGI PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (STUDI KASUS : 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 :

CINDY ALICIA SAHARA
NRP. 05211440000172

Disetujui Tim Penguji : Tanggal Ujian : 3 Juli 2018
Periode Wisuda : September 2018

Dr. Apol Pribadi S., S.T., M.T. **(Pembimbing I)**

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

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

IMPLEMENTASI METODOLOGI PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (STUDI KASUS : PDAM SURYA SEMBADA KOTA SURABAYA)

Nama Mahasiswa : Cindy Alicia Sahara
NRP : 05211440000172
Jurusan : Sistem Informasi FTIK-ITS
Pembimbing 1 : Dr. Apol Pribadi S., S.T., M.T.

ABSTRAK

Penelitian ini membahas mengenai pembuatan dokumen Perencanaan Keberlangsungan Bisnis (Business Continuity Plan) pada PDAM Surya Sembada Kota Surabaya. PDAM Surya Sembada Kota Surabaya merupakan Badan Usaha Milik Daerah yang bergerak dalam usaha distribusi air bersih bagi masyarakat umum Surabaya. Sebagai suatu BUMD yang mengimplementasikan TI dalam setiap proses bisnisnya, PDAM Surya Sembada Kota Surabaya belum menerapkan BCP atau prosedur tertulis yang memberikan panduan dalam memberikan respon saat terjadi gangguan. Business Continuity Plan (BCP) sendiri adalah prosedur yang digunakan untuk membuat dan memvalidasi rencana untuk mempertahankan operasi bisnis secara terus menerus sebelum,selama dan setelah bencana atau peristiwa yang mengganggu. Penelitian ini memiliki tujuan untuk mengimplementasikan metodologi Business Continuity Plan yang diusulkan oleh mahasiswa S2 Departemen Sistem Informasi ITS, Yusrida Muflihah dengan mengempiriskan metode Business Continuity Plan tersebut pada PDAM Surya Sembada Kota Surabaya untuk menunjukkan bahwa metode tersebut dapat diimplementasikan pada perusahaan apapun menyesuaikan dengan kondisi dan tipe perusahaan.

Metode yang akan digunakan pada penelitian ini adalah kerangka kerja berbasis risiko yang dibuat oleh mahasiswa S2 Departemen Sistem Informasi ITS, Yusrida Muflihah. Metode ini menjelaskan secara komprehensif mengenai panduan dalam membuat rencana keberlangsungan bisnis yang berisikan elemen teknis dan manajerial dari BCP yang mengadopsi dari COBIT 5 Domain: Manage Continuity, ITIL-Service Design IT Service Continuity Management dan standar-standar lainnya serta juga mengadopsi siklus PDCA (Plan-Do-Check-Act) dari ISO 22301:2012. Data diperoleh melalui analisis dokumen, observasi, dan wawancara dengan pihak manajemen untuk mendapatkan pengetahuan mengenai risiko apa saja yang mungkin dihadapi, proses bisnis mana yang kritis untuk keberlangsungan organisasi, dan strategi apa yang dapat diimplementasikan untuk menjamin keberlangsungan bisnis. Dokumen BCP dihasilkan dengan meninjau hasil penilaian risiko dan penilain dampak bisnis yang disesuaikan dengan hasil formulasi kerangka kerja BCP.

Hasil dari penelitian ini diharapkan dapat menunjukkan bahwa metode pembuatan BCP ini sesuai untuk diimplementasikan pada studi kasus dan dapat menjadi referensi untuk penelitian selanjutnya terkait BCP serta dapat memberikan panduan bagi perusahaan terkait pembuatan BCP yang sesuai dengan kebutuhan perusahaan.

Kata kunci: Risiko Teknologi Informasi, Analisis Dampak Bisnis, Perencanaan Keberlangsungan Binis, Metode BCP

METHODOLOGY IMPLEMENTATION IN DEVELOPING BUSINESS CONTINUITY PLAN DOCUMENT (CASE STUDY : PDAM SURYA SEMBADA KOTA SURABAYA)

Student Name : Cindy Alicia Sahara
NRP : 05211440000172
Department : Sistem Informasi FTIK-ITS
Supervisor 1 : Dr. Apol Pribadi S., S.T., M.T.

ABSTRACT

This research discusses the making of Business Continuity Plan document at PDAM Surya Sembada Kota Surabaya. PDAM Surya Sembada Surabaya is a Goverment Regional Owned Enterprise which is engaged in the distribution of clean water for the general public of Surabaya. As a BUMD that implements IT in every business process, PDAM Surya Sembada Kota Surabaya has not implemented BCP or written procedures that provide guidance in giving response when disaster occurs. The Business Continuity Plan (BCP) itself is a procedure used to create and validate plans to maintain continuous business operations before, during and after disasters events. This research aims to implement the Business Continuity Plan methodology proposed by S2 student of Information System Department of ITS, Yusrida Muflihah by implementing Business Continuity Plan method to PDAM Surya Sembada Kota Surabaya to show that the method can be implemented in any company adjust to condition and type.

The method to be used in this research is a BCP risk-based framework created by S2 students of Information Systems Department of ITS, Yusrida Muflihah. This method explains comprehensively the guidelines in creating a business continuity plan that contains the technical and managerial elements of BCP adopting from COBIT 5 Domain: Manage

Continuity, ITIL-Service Design IT Service Continuity Management and other standards as well as adopting the PDCA cycle (Plan -Do-Check-Act) of ISO 22301: 2012. The data is obtained through observation, questionnaire and interviews to gain knowledge about what risks may be faced, which business processes are critical for the sustainability of the organization, and what strategies can be implemented to ensure business continuity. BCP documents are generated by reviewing the results of risk assessment and business impact assessment tailored to the results of the BCP framework formulation.

The results of this study are expected to show that the method of making BCP is suitable to be implemented in case study and can be a reference for further research related to BCP and can provide guidance for companies related to the manufacture of BCP in accordance with the needs of the company.

Keywords: Risks of Information Technology, BIA (Business Impact Analysis), BCP (Business Continuity Plan), BCP Method

KATA PENGANTAR

Puji dan syukur penulis tuturkan ke hadirat Allah SWT, Tuhan Semesta Alam yang telah memberikan kekuatan dan hidayah-Nya kepada penulis sehingga penulis mendapatkan kelancaran dalam menyelesaikan tugas akhir dengan judul:

IMPLEMENTASI METODOLOGI PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (STUDI KASUS : PDAM SURYA SEMBADA KOTA.

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

- Orang tua (mami dan papi), adik-adik, nenek dan seluruh keluarga penulis yang senantiasa mendoakan, memberi dukungan dan kasih sayang yang tiada henti untuk menyelesaikan tugas akhir ini.
- Dosen pembimbing, Bapak Dr. Apol Pribadi S., S.T., M.T. yang dengan sabar membimbing penulis untuk menyelesaikan tugas akhir ini.
- Bapak Ir. Aris Tjahyanto. M.Kom., selaku Ketua Jurusan Sistem Informasi ITS, yang telah menyediakan fasilitas terbaik untuk kebutuhan penelitian mahasiswa.
- Ibu Anisah Herdiyanti, S.Kom., M.Sc., dan Ibu Eko Wahyu Tyas D, S.Kom, MBA. ebagai dosen penguji peneliti, terima kasih atas kritikan dan masukan yang bersifat membangun untuk peningkatan kualitas penelitian ini.
- Ibu Wiwik selaku dosen wali, terima kasih untuk arahan dan bimbingan serta motivasi untuk penulis selama menjalani masa kuliah.
- Bapak Nurlilah Satria Pratama selaku pihak dari bagian TSI PDAM Surya Sembada Kota Suraaya yang telah bersedia untuk menjadi narasumber untuk kebutuhan penelitian.

- Bapak Hermono, selaku laboran laboratorium Manajemen Sistem Informasi, terimakasih atas segala bantuan dalam proses administrasi tugas akhir.
- Baasith Akbar, yang selalu ada dan memberikan dukungan dan motivasi dari awal sampai dengan pengerjaan tugas akhir ini.
- Teman diskusi seperjuangan dan partner dalam mengerjakan tugas akhir ini (Rachel dan anak bimbingan pak Apol lainnya).
- Teman-teman seperjuangan Markitdon (Dhira, Rara, Rachel, Nita, Septy, Patty, Dp, Nody, Roy, Risha, Ninda, Fia, Opor, Tania dan Yunis) yang telah memberikan semangat dalam menyelesaikan penelitian ini.
- Teman-teman seperjuangan dari lab MSI, Kabinet HMSI Kolaborasi dan Osiris terima kasih telah menjadi partner pengembangan diri yang luar biasa dan selalu memberikan semangat positif untuk menyelesaikan tugas akhir ini tepat waktu.

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

Surabaya, Juli 2018

Penulis

DAFTAR ISI

.....iii
ABSTRAK v
ABSTRACT vii
KATA PENGANTAR ix
DAFTAR ISI xi
DAFTAR TABEL xv
DAFTAR GAMBAR xix
BAB I PENDAHULUAN 1
1.1. Latar Belakang Masalah 1
1.2. Perumusan Masalah 4
1.3. Batasan Masalah 5
1.4. Tujuan Penelitian 5
1.5. Manfaat Penelitian 6
1.6. Relevansi 7
BAB II TINJAUAN PUSTAKA 9
2.1. Penelitian Sebelumnya 9
2.2. Dasar Teori 12
2.2.1. Risiko 12
2.2.2. *Business Impact Analysis* (BIA) 23
2.2.3. *Business Continuity Plan* (BCP) 28
2.2.1. Keterbatasan Standar BCP (Business Continuity Plan) 29
2.2.2. Metodologi BCP yang dibuat oleh Mahasiswa S2 : Yusrida 31
2.2.3. Pengujian BCP 39
BAB III METODOLOGI PENELITIAN 41
3.1. Persiapan 42
3.1.1. Identifikasi Masalah 42
3.1.2. Studi literatur 43
3.2. Pengumpulan Data 43
3.3. Fase Perencanaan 44

3.3.1. Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis 44
3.4. Fase Implementasi 45
3.4.1. Identifikasi dan Analisis Risiko 45
3.4.2. Analisis Dampak Bisnis 46
3.4.3. Penyusunan Strategi Keberlangsungan Bisnis 46
3.4.4. Penentuan Rencana Pemulihan Bencana 47
3.4.5. Pembuatan Dokumen Pelatihan Karyawan 47
3.5. Fase Pemantauan dan Review 48
3.6. Fase Pemeliharaan dan Peningkatan 48
3.7. Verifikasi dan Validasi 49
3.8. Dokumentasi BCP dan Penarikan Kesimpulan 49
BAB IV PERANCANGAN 51
4.1. Fungsional Bisnis yang Terlibat dalam Penelitian 51
4.2. Proses Bisnis yang Terlibat dalam Penelitian 52
4.3. Persiapan Pengumpulan Data dan Informasi 53
4.3.1. Wawancara 53
4.3.2. Kuesioner 60
4.4. Pengolahan Data dan Informasi 61
4.4.1. Elemen Dokumen 62
4.4.2. Analisis Risiko 62
4.4.3. Analisis Dampak Bisnis 63
4.5. Penyusunan Strategi Keberlangsungan Bisnis 68
4.6. Perancangan Evaluasi 69
4.7. Rencana Validasi 73
BAB V IMPLEMENTASI 75
5.1. Hasil Pengumpulan Data dan Informasi 75
5.1.1. Hasil Wawancara 75
5.1.2. Hasil Kuesioner 76
5.1.3. Hasil Validasi 77
5.1.4. Hambatan Pengumpulan Data 77
BAB VI HASIL DAN PEMBAHASAN 79
6.1. Profil Perusahaan 79
6.2. Implementasi Metodologi Business Continuity Plan di PDAM Surya Sembada Kota Surabaya 79
6.2.1. Fase 1 – Perencanaan 80

6.2.2. Fase 2 – Implementasi 95
6.2.3. Fase 3 – Pemantauan dan Review 161
6.2.4. Fase 4 – Pemeliharaan dan Peningkatan 165
6.3. Hasil Evaluasi Metode Yusrida 166
BAB VII KESIMPULAN DAN SARAN..... 181
7.1. Kesimpulan..... 181
7.2. Saran 183
DAFTAR PUSTAKA 185
BIODATA PENULIS 189
LAMPIRAN A 191
LAMPIRAN B 195
LAMPIRAN C 203
LAMPIRAN D 207
LAMPIRAN E 211
LAMPIRAN F..... 215
LAMPIRAN G 231
LAMPIRAN H 235
LAMPIRAN I 237
LAMPIRAN J 239
LAMPIRAN K 241

Halaman ini sengaja dikosongkan

DAFTAR TABEL

Tabel 2.1 Penelitian Sebelumnya 9
Tabel 2.2 Penentuan Nilai Dampak 20
Tabel 2.3 Penentuan Nilai Kemungkinan 21
Tabel 2.4 Penentuan Nilai Deteksi 22
Tabel 2.5 Skala nilai RPN 23
Tabel 2.6 Keterbatasan Standar *Business Continuity Plan* 29
Tabel 4.1 Ruang Lingkup 52
Tabel 4.2 Ketentuan Wawancara 54
Tabel 4.3 Jumlah dan Tujuan Wawancara 55
Tabel 4.4 Profil Narasumber 56
Tabel 4.5 *Interview Protocol* 56
Tabel 4.6 Tujuan Kuesioner 60
Tabel 4.7 Format Kuesioner 61
Tabel 4.8 Kriteria Kerugian Finansial 64
Tabel 4.9 Kriteria Kerugian Reputasi 65
Tabel 4.10 Kriteria Kerugian operasional 66
Tabel 4.11 Kriteria Tingkat Kritis Proses Bisnis 66
Tabel 4.12 Jenis Waktu Pemulihan 68
Tabel 4.13 Justifikasi Status 70
Tabel 4.14 Format Tabel Evaluasi 70
Tabel 4.15 Rencana Validasi 74
Tabel 0.1 Hasil Wawancara 75
Tabel 0.2 Hasil Kuesioner 76
Tabel 6.1 Kebutuhan BCP PDAM Surya Sembada Kota Surabaya 81
Tabel 6.2 Ruang Lingkup Fungsional dan Proses Bisnis 82
Tabel 6.3 Perangkat Keras yang dibutuhkan 87
Tabel 6.4 Perangkat Penunjang BCP 88
Tabel 6.5 Strategi Saat Terjadi Gangguan 92
Tabel 6.6 Daftar Alat Komunikasi Darurat 94
Tabel 6.7 Identifikasi Risiko dengan OCTAVE 95
Tabel 6.8 Daftar Aset Kritis 96
Tabel 6.9 Kebutuhan Keamanan Aset Kritis 97

Tabel 6.10 Daftar Ancaman TI 101
Tabel 6.11 Praktik Keamanan Aset Kritis 103
Tabel 6.12 Kelemahan Aset Kritis 106
Tabel 6.13 Komponen Utama Aset TI 106
Tabel 6.14 Ancaman Pada Aset Kritis 108
Tabel 6.15 Daftar Risiko dari Analisis Risiko Menggunakan OCTAVE 110
Tabel 6.16 Hasil Penilaian Risiko dengan Menggunakan FMEA 114
Tabel 6.17 Daftar Proses Bisnis dan Layanan TI 120
Tabel 6.18 Kriteria Severity Level Dampak Finansial, Reputasi dan Operasional 122
Tabel 6.19 Hasil Kuesioner Analisis Dampak Gangguan 123
Tabel 6.20 Kriteria Tingkat Kritis Proses Bisnis 125
Tabel 6.21 Hasil Prioritasi Proses Bisnis 126
Tabel 6.22 Hasil Prioritasi Layana TI 129
Tabel 6.23 Hasil Penentuan Waktu Pemulihan 130
Tabel 6.24 Strategi Preventif 134
Tabel 6.25 Mitigasi Risiko *ServerDown* 137
Tabel 6.26 Mitigasi Risiko *Network Trouble* 139
Tabel 6.27 Mitigasi Risiko Data Tidak Dapat diakses 141
Tabel 6.28 Mitigasi Risiko *Human Error* / Pelanggaran 144
Tabel 6.29 Strategi Saat Gangguan 145
Tabel 6.30 Strategi Pemulihan 147
Tabel 6.31 Strategi Korektif 151
Tabel 6.32 Daftar Aset TI 152
Tabel 6.33 daftar vendor dari PDAM Surya Sembada Kota Surabaya 154
Tabel 6.34 Bentuk Kontrol 156
Tabel 6.35 Modul Pelatihan BCP 159
Tabel 6.36 Skenario Pengujian *Server Down* 162
Tabel 6.37 Skenario Pengujian *Network Trouble* 163
Tabel 6.38 Hasil Evaluasi 171
Tabel A.1 Hasil Wawancara Kondisi Kekinian terkait TI 191
Tabel B.1 Hasil Wawancara Analisis Risiko 195
Tabel C.1 Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian Keuangan 203

Tabel D.1 Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian Pelayanan 207
Tabel E.1 Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian TSI 211
Tabel F.1 Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian TSI 215
Tabel G.1 Formulir Pengecekan Internal Rencana Keberlangsungan Bisnis 231
Tabel H.1 Formulir Peninjauan Manajemen..... 235

Halaman ini sengaja dikosongkan

DAFTAR GAMBAR

Gambar 2.1 Keterkaitan antara penilaian risiko dengan BIA dan komponen BCMS (Sumber : [13]) 15
Gambar 2.2 Tahapan Metode *Octave* 16
Gambar 2.3 Tahapan FMEA (Sumber : [19]) 18
Gambar 2.4 Keterkaitan BIA (Sumber: [21]) 25
Gambar 2.5 Kerangka Kerja BCP Yusrida 33
Gambar 2.6 Fase Perencanaan Metode BCP Yusrida 34
Gambar 2.7 Fase Implementasi Metode BCP Yusrida 35
Gambar 2.8 Fase Pemantauan dan Review Metodo BCP Yusrida 37
Gambar 2.9 Fase Pemeliharaan dan Peningkatan Metode BCP Yusrida 38
Gambar 3.1 Bagan Metodologi 42
Gambar 6.1 Struktur Komite BCP PDAM Surya Sembada Kota Surabaya 83
Gambar 6.2 Alur Komunikasi Gangguan Ringan 90
Gambar 6.3 Alur Komunikasi Gangguan Besar 91
Gambar 6.4 Fase 1-Perencanaan Metode BCP Yusrida 167
Gambar 6.5 Fase 2-Implementasi Metode BCP Yusrida 168
Gambar 6.6 Fase 3-Pemantauan dan Review Metode BCP Yusrida 169
Gambar 6.7 Fase 4- Pemeliharaan dan Peningkatan Metode BCP Yusrida 170

Halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

Pada bagian ini akan dijelaskan latar belakang, perumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas akhir, relevansi terhadap pengerjaan tugas akhir, dan target luaran tugas akhir. Berdasarkan uraian pada bab ini, diharapkan didapatkan gambaran umum mengenai permasalahan dan pemecahan masalah pada tugas akhir dapat dipahami.

1.1. Latar Belakang Masalah

PDAM Surya Sembada Kota Surabaya yang berbasis di Surabaya Jawa Timur merupakan satu-satunya Badan Usaha Milik Daerah peninggalan jaman Belanda, yang yang bergerak dalam usaha distribusi air bersih bagi masyarakat umum Surabaya [1]. Pada Tahun 2016 tercatat PDAM Surabaya telah memiliki 547.819 pelanggan, yang meliputi 502.124 pelanggan perumahan, 38.089 pelanggan komersial, 404 pelanggan industri, 3.794 pelanggan sosial umum, 1.239 pelanggan pemerintah, 2.163 pelanggan sosial khusus, dan 6 pelanggan pelabuhan [2]. Berdasarkan laporan keuangan terbaru dari perusahaan, PDAM Surabaya berhasil menjaga profitabilitas di tahun 2011 yaitu dengan membukukan total laba bersih sebesar Rp 149.280.000.000. Untuk dapat selalu memenuhi kebutuhan masyarakat dan menjaga profitabilitas maka perusahaan didukung oleh teknologi informasi. Pada PDAM Surya Sembada Kota Surabaya teknologi informasi memiliki peranan yang penting karena digunakan hampir pada seluruh proses bisnis. Maka sedapat mungkin penggunaan TI harus dipastikan selalu berjalan dengan lancar agar proses bisnis terkait TI tetap berjalan normal.

Pada saat perusahaan mulai mengimplementasikan TI, maka pada saat itu suatu perusahaan akan memiliki berbagai macam risiko yang timbul dari ancaman dan gangguan. Risiko dapat muncul dari sesuatu yang biasa hingga yang luar biasa-mulai dari api atau banjir kecil di ruang server hingga bencana besar seperti gempa bumi atau badai besar [3]. Potensi penyebab

adanya gangguan bisnis tidak hanya dari segi eksternal saja seperti bencana alam, melainkan internal termasuk *human error* dan gangguan utilitas. Gangguan-gangguan tersebut jika tidak ditangani dengan benar maka akan sangat berdampak pada keberlangsungan bisnis perusahaan. Oleh karena itu perusahaan harus memiliki penganan risiko yaitu dengan manajemen risiko. Manajemen risiko dapat membantu perusahaan untuk meminimalisir terjadinya dampak akibat risiko tersebut dan untuk dapat tetap menjalankan proses bisnisnya dalam segala kondisi. Untuk dapat memiliki manajemen risiko yang baik, maka suatu organisasi perlu memiliki perencanaan keberlangsungan bisnis atau yang biasa disebut dengan *Business Continuity Plan* (BCP). Menurut (Snedaker, 2014) terlepas dari seberapa sederhana atau kompleks TI di lingkungan perusahaan, perusahaan memerlukan adanya rencana terhadap gangguan yang menimpa bisnis [3].

BCP merupakan hal yang *essential* dalam penerapan TI pada perusahaan, namun jarang menjadi prioritas karena penerapannya membutuhkan komitmen dan *effort* yang sungguh-sungguh sedangkan manfaatnya *intangible* atau dapat dikatakan dapat terasa hanya ketika gangguan datang. Akan tetapi menurut penelitian Cummings, Haag & McCubbrey pada tahun 2005 terhadap perusahaan yang mengalami kehilangan data skala besar tanpa memiliki BCP didapatkan data sebagai berikut: 43% dari perusahaan ini tidak pernah dibuka lagi, 51% dari perusahaan tersebut ditutup dalam jangka waktu 2 tahun lamanya dan hanya 6% dari perusahaan dari perusahaan tersebut yang dapat bertahan dalam jangka waktu yang lama. Hal tersebut menunjukkan bahwa kemungkinan suatu perusahaan untuk tetap dapat menjaga keberlangsungan bisnisnya tanpa adanya perencanaan BCP yang baik adalah kecil. Dimana perencanaan terhadap keberlangsungan bisnis adalah sesuatu hal yang bersifat kritikal untuk suatu perusahaan yang menerapkan TI.

Menurut Snedaker, setiap perusahaan berbeda dan memiliki keunikan tersendiri, maka dari itu implementasi *Business Continuity Plan* akan berbeda juga tergantung dari kebutuhan yang dimiliki oleh perusahaan [3]. Menurut John Lindstrom, perencanaan keberlangsungan bisnis harus diadaptasi secara khusus agar sesuai dengan sasaran organisasi [4]. Selain itu, kerangka BCP dapat terus berkembang sesuai dengan kebutuhan perusahaan. Sehingga perbaikan dari BCP disesuaikan dengan peningkatan dan perkembangan kebutuhan perusahaan.

BCP sendiri dalam implementasinya pada kasus nyata sering menjadi tidak optimal. Hal terebut terjadi karena masih terdapat keterbatasan dari beberapa standar terkini mengenai BCP. Beberapa standard tersebut adalah ISO 22301:2012, COBIT 5 Domain: *Manage Continuity* dan ITIL-IT *Service Continuity Management*. Masing-masing memiliki kelebihan dan kekurangan yang kemudian memunculkan suatu usulan metodologi oleh mahasiswa S2 Departemen Sistem Informasi ITS, Yusrida Muflihah. Formulasi dari metode BCP tersebut dihasilkan dari komparasi terhadap standard-standar terkini dan menggabungkan prinsip-prinsip BCP dengan elemen BCP. Dimana metode yang diusulkan merupakan panduan mengenai BCP secara umum dan komprehensif yang mencakup elemen teknis dan manajerial. Fokus dari metodologi ini yaitu manajemen resiko serta fungsi bisnis yang menerapkan teknologi informasi. Metodologi ini mengikuti siklus PDCA pada ISO dimana terdiri dari 4 fase yaitu Plan, Do, Check, Action. Metode tersebut bersifat general dimana dapat diimplementasikan pada segala jenis perusahaan terlepas dari ukuran, aktivitas atau sektornya.

Sebagai suatu BUMD yang memiliki peran besar dalam penyediaan air bersih setiap saat untuk masyarakat kota Surabaya, PDAM Surya Sembada Kota Surabaya belum menerapkan BCP ataupun prosedur tertulis yang memberikan panduan dalam memberikan respon saat terjadi gangguan. Padahal kemungkinan untuk terjadinya gangguan, ancaman

bahkan bencana dapat terjadi kapan saja. Ketidaksiapan dalam menangani risiko dari gangguan yang terjadi dapat berpotensi untuk merugikan perusahaan baik dari segi finansial maupun operasional. Oleh sebab itu diharapakan dengan dibuatnya BCP maka kerugian tersebut dapat terminimalisir dan bahkan terhindarkan. Hal tersebut didukung dengan pernyataan bahwa pembuatan Business Continuity Plan ini merupakan upaya untuk mencegah gangguan terhadap aktivitas bisnis normal [5].

Penelitian ini memiliki tujuan untuk mengimplementasikan metodologi *Business Continuity Plan* yang diusulkan oleh mahasiswa S2 Departemen Sistem Informasi ITS, Yusrida Muflihah dengan mengempiriskan metode *Business Continuity Plan* tersebut pada PDAM Surya Sembada Kota Surabaya untuk menunjukkan bahwa metode tersebut dapat diimplementasikan pada perusahaan berbeda,yang pada studi kasus ini adalah PDAM Surya Sembada Kota Surabaya. Dalam melakukan penelitian ini, penulis berupaya mengikuti alur metodologi untuk diimplementasikan pada PDAM Surya Sembada Kota Suabaya.

1.2. Perumusan Masalah

Berdasarkan uraian latar belakang yang sudah dijelaskan, maka didapatkan perumusan masalah sebagai berikut:

1. Apa hasil penilaian risiko teknologi informasi pada PDAM Surya Sembada Kota Surabaya?
2. Bagaimana hasil implementasi dari merode pembuatan dokumen Business Continuity Plan yang sesuai dengan kebutuhan pengelolaan keberlangsungan bisnis PDAM Surya Sembada Kota Surabaya?
3. Apakah semua tahapan pada metode yang dibuat oleh mahasiswa S2 Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember yaitu Yusrida Muflihah dapat diimplementasi di PDAM Surya Sembada Kota Surabaya?

1.3. Batasan Masalah

Berdasarkan perumusan masalah yang sudah dijelaskan, maka batasan masalah untuk tugas akhir ini adalah sebagai berikut:

1. Penelitian ini dilakukan pada salah tiga fungsional bisnis di PDAM Surya Sembada Kota Surabaya yaitu bagian keuangan, pelayanan dan teknologi sistem informasi.
2. Metode yang digunakan untuk penelitian adalah wawancara dan observasi dengan menggunakan referensi model yang telah dibuat dalam penelitian mahasiswa S2 Sistem Informasi ITS yaitu metodologi yang memberi panduan mengenai BCP secara umum dan komprehensif yang mencakup elemen teknis dan manajerial.
3. Proses pengerjaan BCP berfokus kepada analisa risiko teknologi informasi serta analisis dampak risiko terhadap fungsi bisnis perusahaan yang bernilai tinggi.
4. Risiko yang di analisis pada penelitian ini hanya risiko yang berkaitan dengan teknologi informasi
5. Tahapan pengujian BCP hanya sampai kepada pembuatan skenario pengujian.
6. Tahapan pelatihan karyawan dan peninjauan keberlangsungan bisnis hanya berupa pembuatan formulir kuesioner.

1.4. Tujuan Penelitian

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

1. Mengetahui penilaian risiko terkait teknologi informasi terhadap fungsi bisnis di PDAM Surya Sembada Kota Surabaya.
2. Mengetahui penilaian terhadap dampak bisnis dari adanya gangguan yang memungkinkan dimiliki oleh PDAM Surya Sembada Kota Surabaya.
3. Menghasilkan dokumen Business Continuity Plan yang sesuai dengan keadaan PDAM Surya Sembada Kota Surabaya.

4. Mengetahui apakah setiap tahapan metodologi pembuatan BCP yang dibuat oleh Yusrida dapat diimplementasikan pada PDAM Surya Sembada Kota Surabaya.

1.5. Manfaat Penelitian

Dari pengerjaan tugas akhir ini, adapun manfaat yang dapat diberikan antara lain:

Bagi Akademis:

1. Panduan/standardisasi yang digunakan dalam penelitian ini dapat digunakan sebagai referensi bagi perusahaan yang akan membangun *business continuity plan.*
2. Penelitian ini dapat dijadikan sebagai bahan evaluasi dan masukan atau kritik terhadap hasil metode pembuatan dokumen perencanaan keberlangsungan bisnis yang dibuat oleh yusrida agar bisa dilakukan peningkatan serta memberikan referensi dalam melakukan kegiatan sejenis.

Bagi Organisasi

1. Dokumen *Business Continuity Plan* yang sesuai dengan kebutuhan bisnis PDAM Surya Sembada Kota Surabaya diharapkan dapat digunakan PDAM sebagai referensi dalam meningkatkan performa PDAM.
2. Perusahaan dapat memiliki rancangan kerja Business Continuity Plan berbasis risiko dan dampak bisnis.
3. Perusahaan mengetahui penilaian risiko yang memiliki keterkaitan dengan teknologi informasi.
4. Perusahaan dapat mengetahui faktor kritis dari analisa dampak bisnis.
5. Perusahaan mendapatkan acuan kerangka kerja Business Continuity Plan (BCP) yang dapat memfasilitasi perusahaan untuk menyesuaikan dokumen BCP dengan keadaan perusahaan.

1.6. Relevansi

Topik yang diangkat dalam penelitian tugas akhir adalah peramalan yang memiliki relevansi dengan mata kuliah yang dipelajari sebelumnya yaitu Teknik Peramalan dan berkaitan dengan Lab Rekayasa Data dan Inteligensi Bisnis. Topik yang diangkat pada penelitian ini yaitu mengenai Implementasi Metode Pembuatan Dokumen Perencanaan Keberlangsungan Bisnis (Studi Kasus Pdam Surya Sembada Kota Surabaya) . Dalam lingkup penelitian laboratorium manajemen sistem informasi, penelitian ini mempunyai relevansi erat dengan mata kuliah pilihan yaitu Perencanaan Keberlangsungan Bisnis (PKB), Manajemen Risiko Teknologi Informasi (MRTI), dan Manajemen Layanan Teknologi Informasi (MLTI). Sehingga dapat dikatakan bahwa penelitian ini telah mempunyai relevansi sesuai dengan *roadmap* laboratorium Manajemen Sistem Informasi pada Jurusan Sistem Informasi.

Halaman ini sengaja dikosongkan

BAB II
TINJAUAN PUSTAKA

Pada bagian ini akan dijelaskan studi literatur yang akan digunakan sebagai objek penelitian serta teori-teori yang mendukung dilakukannya pembuatan Perencanaan Keberlangsungan Bisnis seperti tentang manajemen risiko, analisa dampak bisnis serta teori-teori lainnya yang digunakan selama penelitian ini.

2.1. Penelitian Sebelumnya

Pada bab ini akan menjelaskan mengenai penelitian sebelumnya dan dasar teori yang dijadikan acuan atau landasan dalam pengerjaan tugas akhir ini. Penelitian-penelitian yang akan dibahas merupakan beberapa penelitian mengenai *Business Continuity Plan.* Dengan memperhatikan penelitian-penelitian tersebut dapat diketahui bagaimana analisis dan teori-teori yang telah dilakukan dalam penelitian sebelumnya terkait dengan penelitian ini. Berikut ini adalah penelitian terdahulu yang terkait dengan *Business Continuity Plan* yang dapat di lihat pada tabel

Tabel 2.1 Penelitian Sebelumnya

Penelitian 1	
Judul Paper	*BUSINESS CONTINUITY PLAN* : Sebuah Usulan Metodologi, Empiris PT PLN (Persero) Distribusi Jawa Timur
Peneliti; Tahun	Yusrida Muflihah, 2017
Deskripsi Umum Penelitian	Penelitian ini melakukan komparasi standart terkait *business continuity*, kemudian memformulasikan metodologi *Business Continuity Plan* dengan cara menggabungkan prinsip-prinsip *business continuity* yang ada pada standar terkini (ISO 22301:2012, COBIT 5*: Domain Manage Continuity* dan jurnal-jurnal yang lain) dengan elemen *business continuity plan* dan hasil penelitian

	terdahulu. Hasil dari penelitian yaitu (1) elemen utama BCP terdiri dari penentuan kebutuhan pengelolaan keberlangsungan bisnis, peninjauan kelangsungan bisnis, analisis risiko, analisis dampak bisnis, strategi kelangsungan bisnis, rencana pemulihan gangguan, pelatihan karyawan, pengujian BCP dan (2) hasil formulasi metodologi *business continuity plan* yang menjelaskan secara teknis mengenai panduan dalam membuat rencana keberlangsungan bisnis sebagai langkah mengelola keberlangsungan bisnis. Hasil formulasi tersebut diimplementasikan pada PT.PLN Distribusi Jawa Timur.
Keterkaitan Penelitian	Hasil penelitian yang berupa formulasi metodologi BCP secara umum dan komprehensif yang mencakup elemen teknis dan manajerial menjadi landasan dalam merancang dan mengimplementasikan BCP di PDAM Surya Sembada Kota Surabaya.
Penelitian 2	
Judul Paper	Perancangan Business Continuity Plan Berbasis Risiko Pada Sub Direktorat Pengembangan Sistem Informasi, Direktorat Pengembangan Teknologi Dan Sistem Informasi.
Penulis; Tahun	Caesar Fajriansah, 2017
Deskripsi Umum Penelitian	Penelitian ini membahas mengenai penyusunan kerangka Perencanaan Keberlangsungan Bisnis (*Business Continuity Plan*) dengan menggunakan pendekatan berbasis risiko pada Direktorat Pengembangan Teknologi dan Sistem Informasi yang merupakan suatu organisasi yang bergerak dibidang pengembangan dan

	pusat layanan sistem informasi di ITS. Formulasi kerangka kerja BCP dilakukan dengan melihat kebutuhan dan keinginan organisasi mengenai keberlangsungan bisnis dan menyeseuaikannya dengan standar kerangka kerja BCP yang digunakan sebagai acuan, yaitu ISO 22301:2012. Hasil dari penelitian ini yaitu rancangan dokumen BCP dengan meninjau hasil penilaian risiko dan penilaian dampak bisnis yang disesuaikan dengan kebutuhan dan kondisi organisasi tersebut
Keterkaitan Penelitian	Penelitian ini merupakan suatu bahan referensi pembuatan kerangka kerja *business continuity plan* (BCP) berbasis risiko dan bagaimana menbuat suatu BCP yang benar sesuai dengan kebutuhan dan tujuan suatu organisasi khususnya pada departemen TI.
Penelitian 3	
Judul Paper	Perancangan *Business Continuity Plan (BCP)* : Studi Kasus PT ABC
Penulis; Tahun	Prabowo Priyo Ardhiatno, 2013
Deskripsi Umum Penelitian	Penelitian ini membahas mengenai peracangan BCP pada studi kasus PT. ABC. Pengembangan BCP pada penelitian ini dilakukan dengan menggunakan kerangka kerja generik dari BS 25999. Langkah-langkah pengembangan yang dilakukan mulai dari *Risk Assesment, Business Impact Analysis* sampai dengan pengembangan BCP/DRP. Hasil dari penelitian ini adalah dokumen BCP berdasarkan BS 25999 yang memuat tujuan dan ruang lingkup, peran dan tanggung jawab, detail contact, action plan dan form. Dari penelitian ini dapat disimpulkan bahwa kunci untuk mendapatkan

	sebuah BCP yang sesuai dengan kebutuhan PT. ABC (maupun organisasi lainnya) adalah dengan melakukan proses pemahaman organisasi secara benar, melakukannya dengan runtut dan sesuai dengan batasan ruang lingkup yang sudah disepakati sebelumnya.
Keterkaitan Penelitian	Penelitian ini merupakan suatu bahan referensi pembuatan kerangka kerja business continuity planning (BCP) berbasis risiko dan bagaimana menbuat suatu BCP yang benar sesuai dengan kebutuhan dan tujuan suatu organisasi.

2.2. Dasar Teori

2.2.1. Risiko

Risiko berkaitan erat dengan kondisi ketidakpastian dimana risiko muncul karena ada kondisi ketidakpastian [6]. Menurut A.Abas Salim, risiko adalah ketidakpastian yang mungkin menghasilkan peristiwa kerugian [7]. Definisi Risiko menurut NIST SP 800-30, adalah kemungkinan (*likelihood*) suatu sumber ancaman(*threat-source*) menyerang kerentanan(*vulnerability*) yang bersifat potensial yang dimiliki oleh organisasi sehingga menimbulkan dampak(impact) yang merugikan organisasi itu sendiri[8]. Menurut Spremic, risiko dapat didefinisikan sebagai kemungkinan terjadinya suatu ancaman yang disertai kerentanan potensial dan memiliki dampak berupa kejadian yang merugikan organisasi [9].

2.2.1.1. Risiko Teknologi Informasi

Risiko TI adalah risiko apapun yang berkaitan dengan komponen-komponen TI sebagai akibat dari penerapan TI di perusahaan. Risiko TI diukur dengan melihat kemungkinan terjadinya suatu kejadian dan konsekuensinya [10]. Risiko TI memiliki makna yang lebih luas, dimana tidak hanya mencakup

dampak negatif dari operasi dan pemberian layanan yang dapat menyebabkan kerusakan atau berkurangnya nilai suatu organisasi, namun juga hilangnya peluang mendapatkan manfaat dari penggunaan TI yaitu untuk meningkatkan bisnis [11]. Untuk dapat mendapatkan manfaat dan nilai dari penggunaan TI maka perlu mengurangi ancaman atau kerentanan sehingga dapat meminimalisir risiko. Hal tersebut dapat dilakukan dengan manajemen risiko yang baik. Hughes berpendapat mengenai penerapan teknologi informasi yang menimbulkan resiko kehilangan informasi perusahaan dan upaya apa yang dapat dilakukan untuk melakukan pemulihan. Upaya tersebut diantaranya:

1 Keamanan

Perubahan informasi perusahaan oleh pihak yang tidak bertanggung jawab. Misalnya pencurian informasi atau kebocoran internal

2 Ketersediaan

Resiko yang berupa ketidaktersediaannya informasi saat dibutuhkan oleh perusahaan

3 Daya Pulih

Sebuah bentuk resiko saat sistem tidak dapat dipulihkan dalam jangka waktu yang lama sehingga mengganggu proses bisnis perusahaan.

4 Performa

Permintaan akan informasi yang meningkat dalam satuan waktu sehingga mengganggu performa

5 Daya Skala

Peningkatan kebutuhan yang pesat mengakibatkan arsitektur IT yang tersedia tidak lagi relevan

6 Ketaatan

Pelanggaran penggunaan IT dari apa yang sudah ditetapkan oleh pihak pengatur

2.2.1.2. Manajemen Risiko Teknologi Informasi

Manajemen risiko bertujuan untuk memberikan pandangan terkait kemungkinan yang bisa terjadi sehingga perusahaan dapat menyusun langkah mitigasi dan evaluasi terkait dengan risiko. Tujuan manajemen risiko adalah untuk memastikan bahwa ketidakpastian tidak membuat proyek menyimpang dari tujuan [12]. Sedangkan menurut NIST, dengan adanya manajemen risiko TI dapat membantu organisasi untuk mengelola risiko-risiko terkait TI dengan lebih baik. Manajemen risiko mencakup tiga proses, yaitu [8]:

1. Risk Assesment

Risk assesment adalah proses untuk mengidentifikasi dan mencari dampak risiko sehingga disepakati kontrol mitigasi yang sesuai.

2. Risk Mitigation

Risk mitigation dalah proses untuk mengimplementasikan kontrol yang tepat dalam mengurangi risiko yang sudah diidentifikasi sebelumnya di proses risk assessment.

3. Risk Evaluation and Assesment

Risk Evaluation and Assesment adalah proses evaluasi hasil penerapan mitigasi risiko yang sudah dilakukan dan melakukan evaluasi tindak lanjut dengan memberikan panduan agar manajemen risiko berjalan dengan baik.

Salah satu tahapan yang dilakukan dalam manajemen risiko pada penelitian ini adalah adalah penilaian risiko atau *risk assessment*. Peniliaian risiko melibatkan penilaian kemungkinan terjadinya risiko (*likelihood*) dan dampak risiko yang mengancam kegiatan organisasi serta mempersiapkan rencana respon untuk risiko yang berdampak kritis bagi

perusahaan. Menurut S. Ali Torabi, penilaian risiko memiliki hubungan dengan analisis dampak bisnis (*business impact analysis*) dan komponen BCMS [13].

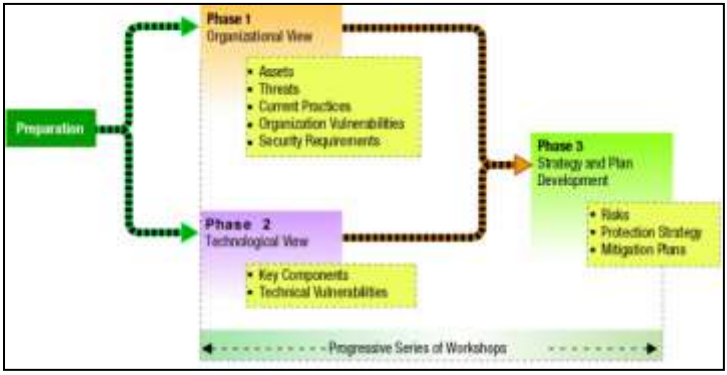
Gambar 2.1 Keterkaitan antara penilaian risiko dengan BIA dan komponen BCMS (Sumber : [13])

Penilaian risiko dan BIA memiliki keterkaitan dimana hasil dari keduanya digunakan untuk mengembangkan BCP yang sesuai untuk mengatasi risiko yang telah teridentifikasi. BIA dan RA merupakan elemen dasar dari setiap program perencanaan keberlangsungan bisnis yang efektif [14]. Kombinasi antara manajamen risiko dan BCP menjadikan perencanaan pertahanan yang seharusnya diterapkan oleh organisasi-organisasi dalam menghadapi ketidakpastian pada dewasa ini. Kombinasi tersebut akan mengurangi ketidakpastian dan mendorong operasi proses bisnis yang lebih stabil pada organisasi [15].

2.2.1.3. OCTAVE

Metode OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) merupakan strategi pengamanan berdasarkan teknik perencanaan dan risiko. OCTAVE merupakan salah satu teknik dan metode yang digunakan untuk strategi dan perencanaan risiko keamanan informasi. OCTAVE merupakan suatu proses untuk mengidentifikasi pengetahuan beberapa pihak mengenai praktek yang terjadi dari segi proses keamanan organisasi serta melihat kondisi praktek keamanan yang telah berjalan di organisasi[16].OCTAVE merupakan

metodologi berbasis proses untuk mengidentifikasi, memprioritisasi dan mengelola risiko keamanan informasi. Metode OCTAVE dibagi menjadi 8 proses : 4 proses terdapat di fase 1, 2 proses terdapat di fase 2 dan 2 proses lainnya terdapat di fase 3. Berikut merupakan tahapan dari metode OCTAVE[16].



Gambar 2.2 Tahapan Metode *Octave*

1. *Tahap Persiapan*

   Dalam tahapan ini kegiatan persiapan yang harus dilakukan adalah penyusunan jadwal, membentuk tim analisis, meminta dukungan dan menyiapkan logistic.

2. *Fase 1 : Membangun Aset Berbasis Profil Ancaman*

   Fase ini merupakan fase dari evaluasi dari pandangan organisasi (organizational view). Tim analisis akan menentukan apa saja aset yang penting untuk suatu organisasi dan apa saja yang dilakukan untuk menjaga aset tersebut. Setelah itu akan diidentifikasi masing-masing ancaman untuk tiap aset kritis sehingga menghasilkan profil ancaman untuk aset. Proses - proses yang ada pada fase 1 adalah sebagai berikut.

   - Proses 1 : Mengidentifikasi pengetahuan dari senior manajemen

- Proses 2 : Mengidentifikasi pengetahuan mengenai area operasional
- Proses 3 : Mengidentifikasi pengetahuan dari staf
- Proses 4 : Membuat profil ancaman

3. *Fase 2 : Mengidentifikasi Kerentanan Infrastruktur*

   Fase ini merupakan fase yang melihat dari pandangan teknologi (technological view). Pada fase ini akan dilakukan evaluasi terhadap infrastruktur. Pada fase ini terdapat pemeriksaan jalur akses jaringan, identifikasi masing masing kelas dari komponen TI yang berkaitan dengan aset kritis. Luaran dari tahapan ini adalah berupa komponen penting dalam aset kritis dan kelemahan infrastruktur TI yang ada saat ini. Proses - proses yang ada pada fase 2 adalah sebagai berikut.

   - Proses 5 : Mengidentikasi komponen utama
   - Proses 6 : Mengevaluasi komponen yang dipilih

4. *Fase 3 : Mengembangkan Strategi Keamanan dan Perencanaan*

   Pada fase ini akan diidentifikasi risiko dari aset kritis organisasi dan menentukan apa langkah yang harus dilakukan. Keluaran dari tahapan ini adalah strategi perlindungan untuk organisasi dan perencanaan mitigas terhadap risiko pada aset kritis. Proses - proses yang ada pada fase 3 adalah sebagai berikut.

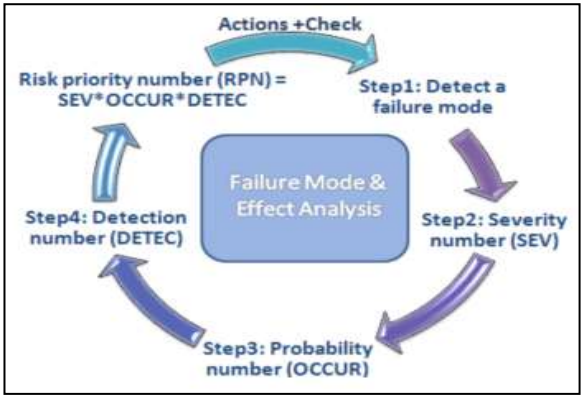
   - Proses 8 : Menjalankan analisis risiko
   - Proses 9 : Mengembangkan strategi perlindungan

2.2.1.4. Metode Failure Mode and Effect Analysis (FMEA)

Metode *Failure and Effects Analysis (FMEA)* merupakan pendekatan secara sistematis untuk mengidentifikasi peluang terjadinya kegagalan dalam sistem, proses, serta produk maupun servis serta mengurangi peluang terjadinya kegagalan. *Failure Mode* berfokus pada langkah ataupun penggunaan mode yang memungkinkan terjadinya kegagalan, sedangkan Effects Analysis berfokus pada evaluasi yang membahas konsekuensi yang akan diterima dari kegagalan tersebut. Tujuan dari *FMEA* adalah untuk menghindari terjadi kegagalan. *FMEA* mengidentifikasi tiga hal, yaitu [17]:

1. Penyebab kegagalan dari sistem, desain produk, serta proses selama siklus hidupnya,
2. Efek dari kegagalan,
3. Tingkat kekritisan efek dari suatu kegagalan.

Proses yang dilakukan dalam penerapan *FMEA* adalah mengukur potensi terjadinya kegagalan tersebut melalui tiga komponen. Tahapan dari *FMEA* digambarkan pada gambar berikut :



Gambar 2.3 Tahapan FMEA (Sumber : [19])

Alur yang tersebut menunjukkan tahapan yang dilakukan dalam melakukan identifikasi dari potensi kegagalan sistem atau proses, yaitu adalah:

1. Mengidentifikasi komponen komponen dan fungsi yang terkait
2. Mengidentifikasi mode kegagalan (*failure modes*)
3. Mengidentifikasi dampak dari mode kegagalan (*failure mode*)
4. Menentukan nilai keparahan (*severity*) dari kegagalan
5. Mengidentifikasi penyebab dari kegagalan
6. Menentukan nilai frekuensi sering terjadinya (*occurence*) kegagalan
7. Mengidentifikasi kontrol yang diperlukan
8. Menentukan nilai keefektifan kontrol yang sedang berjalan (*detection*)
9. Melakukan kalkulasi nilai RPN (*risk priority number*)
10. Menentukan tindakan untuk mengurangi kegagalan

Penilaian risiko dengan menggunakan FMEA dilakukan dengan menentukan nilai *severity*, *occurance*, dan *detection*. Berikut penjelasan dari ketiganya.

- **Penentuan Nilai Dampak (Severity = S)**

Pengukuran nilai dampak akan dilihat seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek aspek penting dalam organisasi. Terdapat tiga aspek yang akan dijabarkan yaitu aspek jadwal, aspek biaya dan aspek teknis. Berikut merupakan penjelasan dari kriteria nilai dampak [18]:

Tabel 2.2 Penentuan Nilai Dampak

Dampak	Dampak dari Efek	Ranking
Akibat Berbahaya	Melukai Pelanggan atau Karyawan	10
Akibat Serius	Aktivitas yang illegal	9
Akibat Ekstrim	Mengubah Produk atau Jasa menjadi tidak layak digunakan	8
Akibat Major	Menyebabkan ketidakpuasan pelanggan secara ekstrim	7
Akibat Signifikan	Menghasilkan kerusakan parsial secara moderat	6
Akibat Moderat	Menyebabkan penurunan kinerja dan mengakibatkan keluhan	5
Akibat Minor	Menyebabkan sedikit kerugian	4
Akibat Ringan	Menyebabkan gangguan kecil yang dapat diatas tanpa kehilangan sesuatu	3
Akibat Sangat Ringan	Tanpa disadari: terjadi gangguan kecil pada kinerja	2
Tidak Ada Akibat	Tanpa disadari dan tidak mempengaruhi kinerja	1

- **Penentuan Nilai Kemungkinan (Occurence = O)**

Nilai kemungkinan atau *occurence* merupakaan pengukuran terhadap tingkat frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat menghasilkan kegagalan. Berikut merupakan pejelasan dari kriteria kemungkinan :

Tabel 2.3 Penentuan Nilai Kemungkinan

Kemungkinan Kegagalan	Kemungkinan	Ranking
Very High: Kegagalan hampir/tidak dapat dihindari	Lebih dari satu kali tiap harinya	10
Very High: Kegagalan selalu terjadi	Satu kali setiap 3-4 hari	9
High: Kegagalan terjadi berulang kali	Satu kali dalam seminggu	8
High: Kegagalan sering terjadi	Satu kali dalam sebulan	7
Moderatly High : Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan	6
Moderate : Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan	5
Moderate Low : Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relative kecil	Satu kali dalam 1-3 tahun	3
Very Low: Kegagalan terjadi relative kecil dan sangat jarang	Satu kali dalam 3 - 6 tahun	2
Remote: Kegagalan tidak pernah terjadi	Satu kali dalam 6 - 50 tahun	1

- **Penentuan Nilai Deteksi atau cause (Detection = D)**

Detection atau deteksi merupakan suatu pengukuran terhadap tingkat efektiftas dalam mendeteksi terjadinya suatu risiko. Nilai deteksi ini akan mencerminkan kemampuan dari organinsasi untuk dapat mendeteksi risiko dan melakukan kontrol terhadap gangguan tersebut. Berikut merupakan penjelasan dari kriteria nilai deteksi.

Tabel 2.4 Penentuan Nilai Deteksi

Deteksi	Kriteria Deteksi	Ranking
Hampir tidak mungkin	Tidak ada metode deteksi	10
Sangat Kecil	Metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi	9
Kecil	Metode deteksi tidak terbukti untuk mendeteksi tepat waktu	8
Sangat Rendah	Metode deteksi tidak andal dalam mendeteksi tepat waktu	7
Rendah	Metode deteksi memiliki tingkat efektifitas yang rendah	6
Sedang	Metode deteksi memiliki tingkat efektifitas yang rata-rata	5
Cukup Tinggi	Metode deteksi memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan	4
Tinggi	Metode deteksi memiliki kemungkinan tinggi untuk dapat mendeteksi kegagalan	3
Sangat Tinggi	Metode deteksi sangat efektif untuk dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	2
Hampir Pasti	Metode deteksi hampir pasti dapat mendeteksi	1

	dengan waktu yang cukup untuk melaksanakan rencana kontingensi	

Nilai *severity*, *occurance* dan *detection* akan dikalkulasikan dengan menggunakan rumus sebagai berikut [19]:

RPN = Severity * Occurence * Detection

Sehingga menghasilkan nilai RPN atau *risk priority number*. Skala Nilai RPN yang didapat dari perhitungan akan menghasilkan level resiko tertentu. Berikut merupakan skala penentuan level risiko berdasarkan nilai RPN.

Tabel 2.5 Skala nilai RPN

Level Risiko	Skala Nilai RPN
Very High	> 200
High	< 200
Medium	< 120
Low	< 80
Very Low	< 20

Level risiko digunakan untuk menilai risiko mana yang memiliki nilai paling tinggi dan untuk prioritisasi risiko. Untuk risiko yang memiliki nilai tinggi, maka akan dilakukan strategi mitigasi untuk menjaga keberlangsungan operasional bisnis saat gangguan tersebut terjadi.

2.2.2. *Business Impact Analysis* (BIA)

Menurut NIST SP800-34, *Business Impact Analysis* (BIA) adalah mengidentifikasikan dan memprioritaskan faktor-faktor kritis dalam proses bisnis organisasi [20]. BIA membantu dalam mengidentifikasi dan memprioritaskan komponen sistem informasi yang kritis untuk menunjang proses bisnis dan misi organisasi. *Business Impact Analysis* (BIA) merupakan dokumen yang mengidentifikasi proses bisnis kritikal, perkiraan dampak bencana terhadap unit bisnis, dan kebutuhan

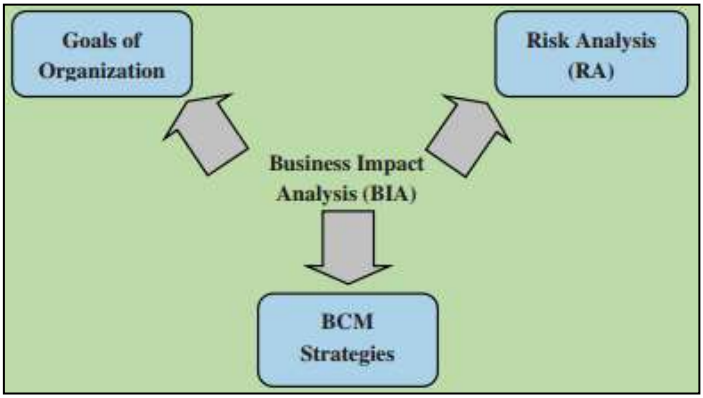
sumber daya yang diperlukan dalam pemulihan. Dimana dampak yang ada dapat secara finansial (kuantitatif) atau operasional (kualitatif, seperti ketidakmampuan untuk merespon komplain dari pelanggan). Menurut S.A. Torabi, *business impact analysis* (BIA) merupakan langkah awal dalam proses perencanaan BCP [21]. *Business Impact Analysis* meliputi tiga hal yaitu identifikasi fungsi bisnis yang penting dalam organisasi, menentukan dampak bisnis dari terhentinya fungsi bisnis serta memastikan implikasi biaya [22].

Menurut *National Institute of Standards and Technology* (NIST) BIA adalah salah satu aktivitas yang bertujuan untuk menkorelasikan sistem dengan proses bisnis maupun layanan yang tersedia dan dari informasi tersebut di dapat karakterisasi dari konsekuensi yang ada pada setiap gangguan [20]. *Business Impact Analysis* digunakan dalam melakukan identifikasi proses bisnis dan sumber daya yang mendukung proses yang sangat penting bagi perusahaan [23].

Business Impact Analysis (BIA) memiliki 3 tujuan utama antara lain:

1. **Prioritas kritis.**
   Dimana setiap proses unit bisnis yang kritis harus diidentifikasi, dibuat prioritasnya, dan dampak dari kejadian bencana harus dievaluasi. Lebih jelasnya, proses bisnis yang tidak terikat waktu akan diterapkan memiliki tingkat prioritas yang lebih rendah untuk dipulihkan dari pada proses bisnis yang terikat dengan waktu.
2. **Perkiraan Downtime.**
   Perkiraan Business Impact Analysis (BIA) digunakan untuk membantu memperkirakan Maximum Tolerable Downtime (MTD) atau maksimal lamanya waktu downtime yang dapat ditolerir dan dipraktekan oleh perusahaan.
3. **Kebutuhan Sumberdaya.**
   Kebutuhan sumber daya untuk proses yang vital juga bisa diidenfikisai pada Business Impact Analysis (BIA), proses yang sangat tergantung pada waktu akan lebih diutamakan untuk mendapatkan alokasi sumber daya.

Business Impact Analysis (BIA) memiliki keterkaitan dengan tiga hal yaitu tujuan organisasi, analisis risiko dan strategi BCM seperti yang digambarkan pada **Gambar 4** [21]**.**



Gambar 2.4 Keterkaitan BIA (Sumber: [21]**)**

Keterkaitan antara BIA dengan analisis risiko dikarenakan hasil dari keduanya digunakan untuk mengembangkan rencana keberlangsungan bisnis yang sesuai. Keterkaitan BIA dengan tujuan organisasi ditunjukkan dengan proses BIA yang tepat harus mempertimbangkan tujuan organisasi dan tidak bertentangan dengan tujuan tersebut. Sedangkan, keterkaitan BIA dengan strategi BCM adalah strategi BCM menjaga kelangsungan fungsi utama organisasi berdasarkan dengan hasil dari BIA, oleh karena itu validitas rencana keberlangsungan bisnis tergantung pada hasil BIA.

2.2.2.1. Impact Criticality

Impact critcality bertujuan untuk mengklasifikasikan fungsi-fungsi kritis yang ada di dalam sebuah organisasi, sehingga dapat memprioritaskan mana yang penting, mana yang kurang penting sehingga dapat diabaikan atau ditunda pemlihannya. Susan Snedaker membagi sistem peringkat untuk melakukan

assesment kekritisan proses/fungsi menjadi 4 kategori sebagai berikut [3]:

- **Kategori 1 : Fungsi Kritis – *Mission Critical***

Adalah bisnis proses dan fungsi yang memberikan dampak paling besar kepada operasi perusahaan dan potensi untuk pemulihan. Atau dapat dikatakan proses apa yang harus ada dalam perusahaan untuk melakukan fungsinya. Hal yang dapat dilakukan untuk memfokuskan responden mengenai fungsi-fungsi yang mission critical adalah misalnya dengan menanyakan tiga sampai lima hal apa saja yang akan mereka lakukan ketika sebuah bencana reda.

- **Kategori 2 : Funsgi Esensial - *Vital***

Fungsi berada diantara mission critical dengan important. Menurut Snedaker, tidak semua organisasi membutuhkan kategori ini, salah satu ciri organisasi tidak membutuhkan kategori ini adalah ketika organisasi tidak dapat membedakan antara mission critical dengan vital.

- **Kategori 3 : Fungsi yang dibutuhkan – *Important***

Ketidakadaan fungsi dan proses bisnis yang penting tidak akan menghentikan bisnis dari beroperasi di waktu dekat, namun fungsi-fungsi dan bisnis proses tersebut biasanya memiliki dampak jangka panjang ketika tidak berfungsi. Fungsi dan bisnis proses yang masuk ke kategori ini biasanya memiliki dampak finansial dan legal serta berdampak pada lintas unit fungsional dan lintas sistem bisnis. Contoh fungsi yang termasuk kedalam kategori ini adalah email, database, akses internet dan perangkat lunak bisnis yang digunakan untuk menjalankan fungsi-fungsi pendukung.

- **Kategori 4: Fungsi yang diinginkan – *Minor***

Fungsi dan bisnis proses minor biasanya tidak akan dibutuhkan dalam jangka waktu dekat dan tidak dibutuhkan selama operasi bisnis perusahaan belum berjalan sebagaimana mestinya jika terdapat gangguan.

2.2.2.2. Kebutuhan Waktu Pemulihan

Kebutuhan waktu pemulihan berhubungan erat dengan impact criticality. Makin penting suatu aktivitas atau fungsi biasanya akan semakin kecil pula waktu pemulihannya. Berikut ini merupakan beberapa istilah yang sering digunakan dalam mendefinisikan kebutuhan waktu pemulihan:

- ***Maximum Tolerable Downtime* (MTD)**

MTD pada beberapa literatur disebut juga sebagai maximum tolerable period of distrupment (MTPD) sesuai namanya adalah besar waktu maksimum sebuah bisnis dapat menoleransi ketidakadaan sebuah fungsi bisnis. Semakin kritis fungsi bisnis biasanya akan memiliki MTD yang semakin kecil. Secara definisi MTD adalah penggabungan dari RTO dengan WRT atau bisa dituliskan sebagai [24] :

MTD = RTO + WRT

- ***Recovery Time Objective* (RTO)**

adalah maksimum waktu yang diperbolehkan untuk sebuah proses tidak beroperasi karena kejadian darurat. RTO adalah waktu yang digunakan untuk memulihkan layanan. Situasi untuk menandai mulai dan selesainya durasi RTO harus disepakati terlebih dahulu. RTO biasanya didefinisikan dalam satuan waktu jam. Secara definisi RTO harus lebih kecil dari MTD.

- ***Work Recovery Time* (WRT)**

adalah langkah-langkah tambahan yang perlu dilakukan supaya bisnis dapat berjalan kembali setelah sistem (perangkat lunak, perangkat keras, dan konfigurasi) dikembalian (restore).

- ***Recovery Point Objective* (RPO)**

adalah maksimum durasi waktu yang diperbolehkan data aplikasinya hilang akibat tidak ter-cover oleh jadwal backup yang ditentukan. RPO didefinisikan dalam satuan waktu jam.

Sebagai contoh jika sebuah perusahaan melakukan backup secara realtime maka dapat disimpulkan toleransi kehilangan data di perusahaan tersebut hampir tidak ada. Sementara itu jika sebuah perusahaan melakukan backup setiap satu minggu sekali maka toleransi kehilangan data perusahaan tersebut maksimal adalah satu minggu.

2.2.3. *Business Continuity Plan* (BCP)

Menurut NIST SP800-34, BCP merupakan dokumen yang memuat instruksi ataupun prosedur mengenai bagaimana organisasi menjamin proses bisnis sesaat dan setelah terjadi gangguan [20]. Menurut Snedaker, Business Continuity Plan adalah metodologi yang dapat digunakan untuk membuat dan memvalidasi sebuah rencana keberlangsungan bisnis sebelum, saat terjadinya dan setelah sebuah bencana terjadi [3]. Business Continuity Plan menurut PP no.82 ayat 17 tahun, adalah suatu rangkaian proses yang dilakukan untuk memastikan terus berlangsungnya kegiatan dalam kondisi mendapatkan gangguan atau bencana [25]. Menurut ISO 22301:2012, *business continuity plan* (BCP) didefinisikan sebagai dokumen berisi prosedur yang bertujuan untuk menjadi panduan perusahaan dalam merespon, melindungi, melanjutkan dan mengembalikan (*respond*, *recover*, *resume*, *restore)* proses bisnis perusahaan ke level yang telah didefinisikan sebelumnya setelah terjadi gangguan.

BCP merupakan suatu proses berkelanjutan dalam melakukan identifikasi terhadap bencana dan kerentanan dari organisasi, kemungkinan terjadinya bencana, potensi konsekuensi terhadap tujuan dan keberhasilan strategi, keefektifan kontrol yang berlaku dan strategi untuk meningkatkan kinerja dan efisiensi[26]. BCP merupakan suatu metodologi yang digunakan untuk membuat dan memvalidasi rencana untuk mempertahankan operasi bisnis secara terus menerus, sebelum, selama dan setelah bencana dan insiden yang mengganggu [3]. *Business Continuity Plan* berhubungan dengan mengidentifikasi, memperoleh, mengembangkan, mendokumentasikan serta menguji sumber daya dan prosedur

sehingga proses bisnis kritis suatu organisasi dapat terjaga saat terjadi bencana atau insiden apapun[27].

2.2.1. Keterbatasan Standar BCP (Business Continuity Plan)

Berikut ini adalah hasil komparasi dari standart terkini terkait *Business Continuity Management* untuk melihat keterbatasan dari masing-masing standar yang ada[28]:

Tabel 2.6 Keterbatasan Standar *Business Continuity Plan*

Standart Terkini	Tujuan	Ruang Lingkup	Keterbatasan
ISO 22301:2012	Menjaga bisnis dari potensi gangguan yang dapat terjadi	Pengelolaan sistem keberlangsungan bisnis.	ISO 22301:2012 hanya menjelaskan mengenai prinsip-prinsip dari pengelolaan keberlangsungan bisnis.
COBIT 5 (Domain: *Manage Continuity*)	Melanjutkan kegiatan bisnis kritis dan menjaga ketersediaan informasi pada level yang dapat diterima oleh perusahaan jika terjadi gangguan yang signifikan.	Membuat dan memelihara perencanaan yang memungkinkan bisnis dan TI dalam merespon kejadian dan gangguan yang terjadi pada operasional proses bisnis yang kritis dan layanan TI serta untuk menjaga ketersediaan informasi yang dapat diterima perusahaan.	COBIT 5: DSS04 Manage Continuity belum menjelaskan secara detil mengenai bagaimana cara membuat *business continuity plan*
ITIL (*Service Design-IT*	Mendukung proses *Business Continuity Management*	Fokus pada kejadian yang dianggap bisnis cukup signifikan	➢ *IT Service Continuity Management* lebih berfokus

Standart Terkini	Tujuan	Ruang Lingkup	Keterbatasan
Service Continuity Management)	dengan memastikan bahwa fasilitas teknis dan layanan TI yang diperlukan (termasuk sistem komputer, jaringan, aplikasi, repositori data, telekomunikasi, lingkungan, dukungan teknis dan *service desk*) dapat dilanjutkan kembali sesuai dengan waktu yang dibutuhkan, disepakati dan rentang waktu bisnis.	untuk dianggap sebagai bencana serta kebutuhan teknis dan layanan TI yang spesifik	pada risiko, langkah pencegahan bencana dan pemulihan setelah bencana. ➢ *IT Service Continuity Management* yang pada prosesnya menghasilkan *IT Continuity Plan* lebih fokus kepada risiko yang dihadapi oleh layanan TI, langkah-langkah menghadapi bencana dan bagaimana cara untuk memulihkan layanan TI, dimana hal tersebut merupakan fokus dari *Disaster Recovery Plan* (DRP).

Berdasarkan komparasi standart-standart terkini terkait Business Continuity Management diketahui bahwa masih terdapat keterbatasan pada masing-masing standart tersebut.

Hal tersebutlah yang mendasari dibuatnya metodologi atau kerangka kerja Business Continuity Plan oleh Yusrida. Sedangkan urgensi dari penelitian yang dilakukan oleh Yusrida didukung dengan beberapa kondisi yaitu [33]:

1. Masih kurangnya kesadaran dan pengetahuan dari perusahaan mengenai rencana keberlangsungan bisnis, apa yang dibutuhkan dalam merencanakan keberlangsungan bisnis serta bagaimana cara merencanakan keberlangsungan bisnis.
2. BCP yang dimiliki oleh perusahaan masih mengalami kekurangan dalam kelengkapan strategi kelangsungan bisnis.
3. Akibat dari alur BCP yang belum sesuai dan menyeluruh dapat terlihat dari masih terjadi perpanjangan waktu saat adanya gangguan, dikarenakan adanya kekurangan/kesenjangan dari proses BCP yang diterapkan sehingga dokumen BCP yang dimiliki belum mencukupi.

2.2.2. Metodologi BCP yang dibuat oleh Mahasiswa S2 : Yusrida

Metodologi yang dibuat oleh mahasiswa S2 Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember ini menjelaskan secara teknis mengenai panduan dalam membuat rencana keberlangsungan bisnis yang berisikan delapan elemen utama dari BCP dan mengadopsi siklus PDCA (*Plan-Do-Check-Act*) yang umum diterapkan oleh ISO. Siklus PDCA ini difungsikan untuk menjaga keintegritasan keberlangsungan bisnis dan memberikan gambaran mengenai kebutuhan yang harus disiapkan, selain itu input juga didapat dari COBIT 5 Domain: Manage Continuity yang memberikan gambaran mengenai unsur-unsur BCP dan ITIL-Service Design IT Service Continuity Management yang memberikan penjelasan mengenai hal teknis dalam salah satu komponen BCP yaitu DRP.

2.2.2.1. Siklus PDCA

Siklus ini digunakan untuk membentuk suatu proses dengan pola runtut dan sistematis pada suatu metodologi serta memetakan elemen BCP. Siklus PDCA dipilih dengan alasan [28]. Siklus PDCA dipilih untuk diterapkan dalam metodologi ini dengan alasan yaitu [28]:

1. Siklus PDCA memastikan bahwa sistem kesinambungan bisnis, dan kegiatan yang didukungnya, dapat terus ditinjau dan diperbaiki
2. PDCA sesuai untuk diterapkan pada saat mengembangkan atau membuat desain baru dari sebuah proses, produk atau layanan
3. merupakan siklus umum yang biasa diterapkan termasuk oleh ISO,
4. siklus PDCA memperkuat pentingnya kelangsungan bisnis sebagai proses berulang yang terus-menerus
5. siklus PDCA yang berulang mendorong adanya perbaikan secara terus menerus

2.2.2.2. Elemen BCP

Sedangkan elemen-elemen pada metode yusrida ditentukan berdasarkan hasil penelitian terdahulu dan standart terkait Business Continuity Plan. Elemen-elemen ini dikategorikan menjadi 2 kategori yaitu:

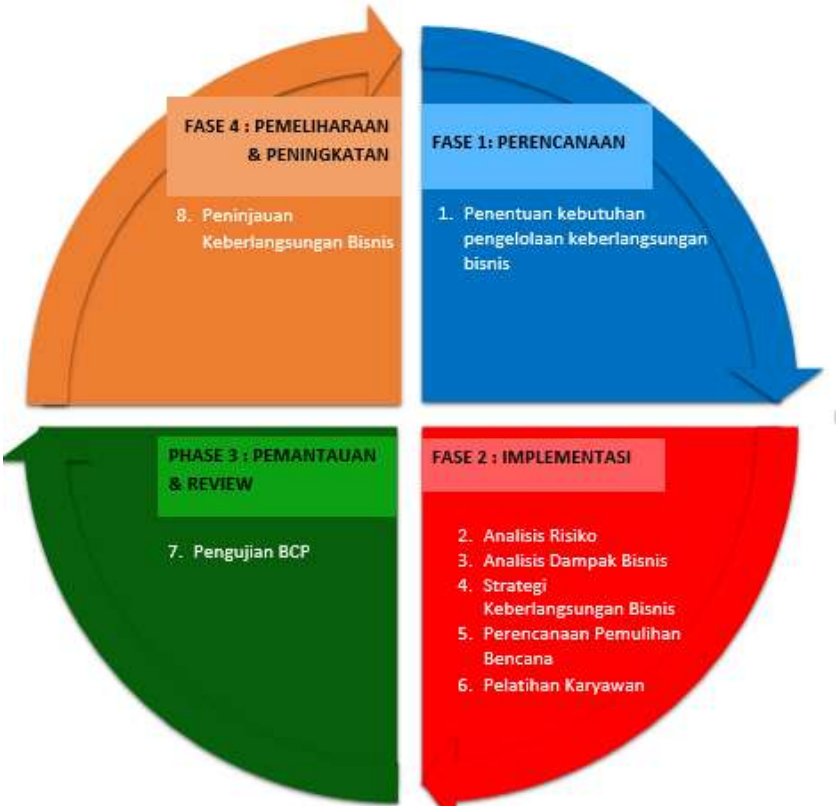
1. **elemen manajerial**

Elemen manajerial merupakan elemen yang dalam proses keberlangsungan bisnis memerlukan partisipasi dari manajemen dikarenakan adanya proses yang memerlukan adanya diskusi, kebijakan, dan pemahaman mengenai proses bisnis perusahaan. Elemen ini terdiri dari penentuan kebutuhan pengelolaan keberlangsungan bisnis, peninjauan keberlangsungan bisnis, analisis risiko dan analisis dampak bisnis.

2. **Elemen Teknis**

Elemen teknis merupakan elemen yang mengarah pada tindakan operasional dan teknis terhadap tindakan menjaga keberlangsungan bisnis sebelum, selama dan setelah adanya gangguan/bencana. Elemen teknis terdiri dari rencana pemulihan bencana, pelatihan karyawan dan pengujian BCP.

Berikut ini adalah penjelasan metode Yusrida yang memiliki 4 fase dengan lebih detil seperti yang ditunjukan pada gambar berikut :



Gambar 2.5 Kerangka Kerja BCP Yusrida

1. Perencanaan

Merupakan fase pertama dalam metodologi BCP. Pada fase ini terdapat tahapan penentuan kebutuhan pengelolaan keberlangsungan bisnis yang termasuk elemen manajerial. Fokus pada fase ini meliputi pendetilan kebutuhan awal pada lingkup manajemen terkait dengan tujuan, ruang lingkup, peran manajemen, sumber daya dan komunikasi. Berikut ini gambar tahapan pada fase ini (**Penjelasan secara detil aktifitas pada tahapan ini ditulis pada BAB III METODOLOGI PENELITIAN**):

Gambar 2.6 Fase Perencanaan Metode BCP Yusrida

Luaran dari fase perencanaan adalah berupa :

- **Poin A. Penentuan kebutuhan pengelolaan keberlangsungan bisnis**

Berisikan tujuan, ruang lingkup, peran manajemen, sumber daya dan komunikasi.

2. Implementasi

Merupakan fase kedua dalam metodologi BCP. Pada fase ini melingkupi elemen manajerial yaitu analisis risiko dan analisis dampak bisnis, serta elemen teknis yaitu strategi keberlangsungan bisnis, rencana pemulihan bencana dan pelatihan karyawan. Berikut ini gambar tahapan pada fase ini (**Penjelasan secara detil aktifitas pada tahapan ini ditulis pada BAB III METODOLOGI PENELITIAN**)

Gambar 2.7 Fase Implementasi Metode BCP Yusrida

Luaran dari fase implementasi adalah berupa :

- **Poin B : Analisis risiko**

Berisikan hasil dari identifikasi kemungkinan terjadinya risiko, penilaian risiko dan dampak dari risiko.

- **Poin C : Analisis dampak bisnis**

Berisikan hasil dari identifikasi dan prioritisasi fungsi bisnis beserta dengan aset, penentuan jangka waktu toleransi gangguan, dan identifikasi dampak dari adanya gangguan.

- **Poin D : Penyusunan strategi keberlangsungan bisnis**

Berisikan penentuan pertanggungjawaban atas dampak gangguan yang mengganggu proses bisnis dan pengembangan prosedur pengelolaan kerusakan atau gangguan.

- **Poin E: Perencanaan pemulihan gangguan**

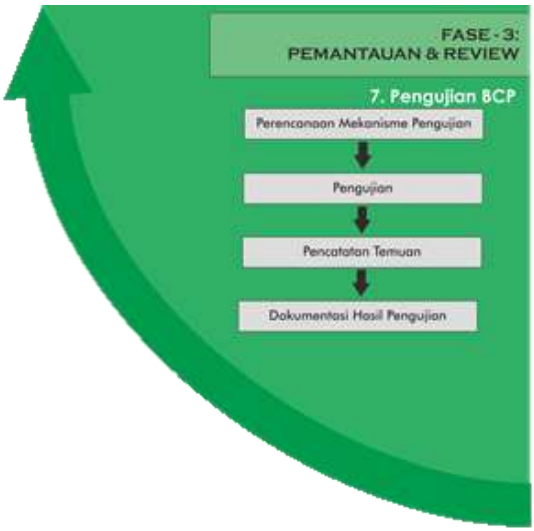
Berisikan rencana penanganan insiden, prosedur saat gangguan beserta detil mengenai pihak yang bersangkutan dan pemulihan gangguan.

- **Poin F : Pelatihan karyawan**

Berisikan mekanisme penyampaian pelatihan, pelaksanaan pelatihan yang terdiri dari latihan dan ujian, dan pemantauan kompetensi berdasarkan hasil latihan dan ujian.

3. Pemantauan dan Review

Merupakan fase ketiga dalam metodologi BCP. Pada fase ini terdapat tahapan pengujian BCP yang termasuk dalam elemen teknis, dimana fokus dari pengujian BCP yaitu pada pembuatan alur pengujian, pengujian, dan perbaikan berdasarkan hasil pengujian yang dilakukan. Berikut ini gambar tahapan pada fase ini (**Penjelasan secara detil aktifitas pada tahapan ini ditulis pada BAB III METODOLOGI PENELITIAN**)



Gambar 2.8 Fase Pemantauan dan Review Metodo BCP Yusrida

Luaran dari fase pemantauan dan review adalah berupa :

- **Poin G: Pengujian BCP**

Berisikan alur pengujian, pengujian dan perbaikan berdasarkan hasil pengujian yang dilakukan.

4. Pemeliharaan dan Peningkatan

Merupakan fase keempat dan terakhir dalam metodologi BCP. Pada fase ini terdapat tahapan peninjauan keberlangsungan bisnis yang termasuk dalam elemen manajerial. Tahapan peninjauan keberlangsungan bisnis berfokus pada peninjauan keberlangsungan bisnis yang dilihat dari kemampuan dan keefektifan keberlangsungan bisnis yang ditetapkan dalam rencana keberlangsungan bisnis serta memberikan feedback dari ketidaksesuaian keberlangsungan bisnis yang digunakan untuk memperbaiki dan meningkatkan kinerja keberlangsungan bisnis. Berikut ini gambar tahapan pada fase ini (**Penjelasan**

secara detil aktifitas pada tahapan ini ditulis pada BAB III METODOLOGI PENELITIAN

Gambar 2.9 Fase Pemeliharaan dan Peningkatan Metode BCP Yusrida

Luaran dari fase pemeliharaan dan peningkatan adalah berupa :

- **Poin H: Peninjauan kelangsungan bisnis**

  Berisikan peninjauan keberlangsungan bisnis yang dilihat dari kemampuan dan keefektifan keberlangsungan bisnis yang ditetapkan dalam rencana keberlangsungan bisnis serta memberikan feedback dari ketidaksesuaian keberlangsungan bisnis yang digunakan untuk memperbaiki dan meningkatkan kinerja keberlangsungan bisnis.

2.2.3. Pengujian BCP

Pengujian terhadap strategi BCP yang telah dibuat penting untuk dilakukan agar dapat mengetahui kefektifan dari strategi yang telah dibuat.Terdapat beberapa tipe yang dapat dilakukan dalam pengujian BCP, diantaranya[29], [30]:

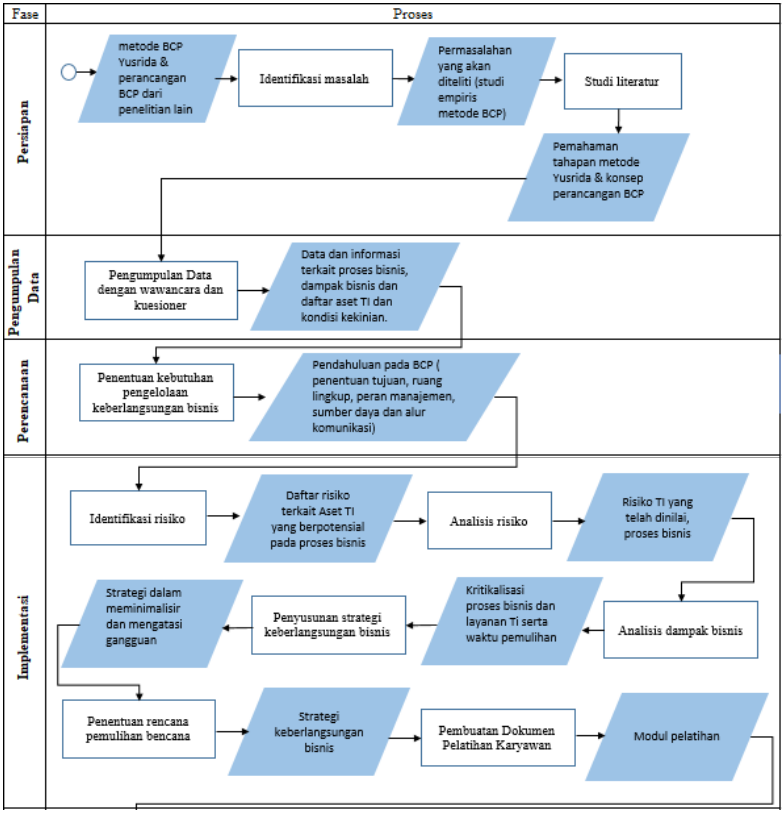
1. *Walthrough self-asessment,* merupakan diskusi yang dilakukan selama proses pembuatan rencana. Pengujian ini tidak menilai efektivitas dari kegiatan respon dan pemulihan.
2. *Checklist testing,* pengujian ini digunakan untuk menentukan ketersediaan cadangan dalam organisasi, seperti tempat penyimpanan cadangan dan manual operasi. Dalam pengujian ini, dilakukan peninjauan ulang rencana dan identifikasi bagian yang harus selalu diperbarui dan selalu tersedia.
3. *Non-business interruption testing,* merupakan pengujian dimana akan dilakukan simulasi terjadinya bencana dengan menggunakan pengujian prosedur yang telah dibuat. Simulasi yang dilakukan tidak harus mencakup seluruh prosedur. Simulasi ini dapat membantu organisasi dalam melakukan identifikasi kebutuhan untuk pengembangan BCP.
4. *Supervised walkthrough,* merupakan pengujian yang difasilitasi dengan adanya skenario untuk menguji rencana keberlangsungan bisnis. Skenario yang digunakan adalah mock skenario (skenario tiruan) yang memungkinkan staf mendiskusikan mengenai tindakan, tanggung jawab dan keputusan yang akan diambil saat mengaktifkan rencana.
5. *Process or plan simulation,* merupakan rencana kegiatan pengujian yang dilakukan di lingkungan "real life" dan akan disimulasikan sesuai dengan skenario. Pengujian ini membutuhkan banyak sumber daya dan akan menyebabkan gangguan pada bisnis inti selama berhari-hari.
6. *Full end-to-end simulation* atau *Business Interuption Tetsing,* merupakan uji skala penuh pada lingkungan "real

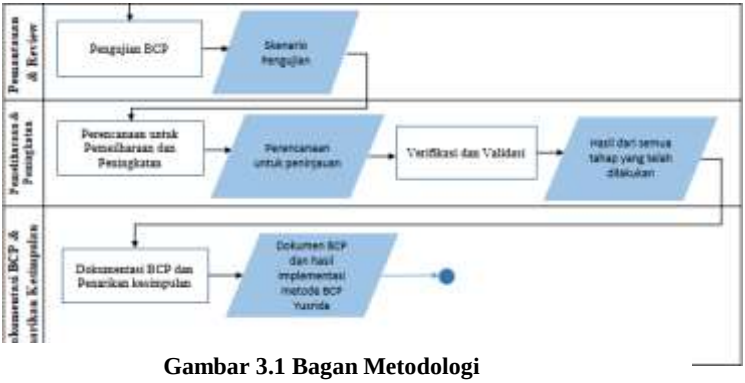
7. life" yang disimulasikan atau aktivitas rencan selama peristiwa gangguan aktual. Pengujian ini menggunakan skenario yang memungkinkan peserta untuk melakukan respon dan pemulihan sepenuhnya untuk area bisnis tertentu atau keseluruhan organisasi. Jenis pengujian ini paling sulit dan membutuhkan biaya besar untuk dilakukan karena harus menutup kegiatan bisnis atau sumber daya.

Pada penelitian ini tidak semua pengujian dilakukan, melihat kondisi terhadap objek penelitian.

BAB III
METODOLOGI PENELITIAN

Pada bagian ini akan dijelaskan metodologi penelitian yang akan digunakan untuk sebagai panduan sistematis agar pengerjaan tugas akhir terarah dan berjalan sesuai rencana. Berikut ini merupakan metodologi yang digunakan penulis:





Gambar 3.1 Bagan Metodologi

Berikut merupakan penjelasan dari setiap tahapan yang ada pada metodologi yang digunakan, yaitu:

3.1. Persiapan

Fase persiapan merupakan langah awal dalam pengerjaan tugas akhir. Peneliti melakukan persiapan dengan dua kegiatan yaitu identifikasi masalah dan studi literatur.

3.1.1. Identifikasi Masalah

Pada kegiatan ini peneliti berusaha mengidentifikasi masalah dari penelitian sebelumnya, yang pada kasus ini yaitu penelitian yang dilakukan oleh mahasiswa S2 Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Yusrida Muflihah. Pada penelitian tersebut peneliti mendapati bahwa metode yang yusrida buat hanya memiliki satu studi empiris sehingga perlu adanya studi empiris lain untuk mengetahui apakah metode Yusrida dapat diimplementasikan berdasarkan kesesuaian BCP yang dibuat dengan suatu kondisi pada studi kasus. Sehingga topik pada penelitian ini adalah mengimplementasikan formulasi metode yang dibuat oleh Yusrida dalam pembuatan BCP pada PDAM Surya Sembada

Kota Surabaya. Output dari aktifitas ini adalah pemahaman mengenai permasalahan yang akan dibahas.

3.1.2. Studi literatur

Setelah melakukan identifikasi permasalahan, kemudian dilakukan studi literatur untuk menemukan solusi dan memperdalam pemahaman akan topik yang akan diteliti. Studi literatur besumber dari penelitian sebelumnya, buku, *best practice* BCP dan metode yang dibuat oleh yusrida. Hasil dari kegiatan ini berupa pemahaman peneliti mengenai konsep penyusunan BCP dan formulasi metodologi yang dibuat oleh Yusrida.

3.2. Pengumpulan Data

Pada penelitian ini menggunakan data yaitu data kualitatif dan kuantitatif. Pada tahapan pengumpulan data terdapat beberapa metode yang dilakukan, antara lain adalah wawancara dan observasi. Data yang bersifat kualitatif berupa aset SI/TI sebagai dasar untuk melakukan analisis BIA dan penilaian risiko, sedangkan data yang bersifat kuantitatif berupa analisis dampak bisnis dan penentuan waktu pemulihan yang diperoleh melalui wawancara digunakan untuk menentukan kategori pemberian level pada analisis dampak bisnis dan strategi yang dibutuhkan.
Berikut ini adalah penjelasan dari beberapa metode tahapan pengumpulan data :

1. Wawancara

Metode wawancara akan dilakukan kepada kepala bagian teknologi sistem informasi, pelayanan dan keuangan untuk menggali data dan informasi atas penelitian yang dilaksanakan.

2. Observasi

Observasi dilakukan untuk mengumpulkan data dengan studi lapangan langsung untuk menganalisis risiko. Selain itu obserbasi ini dilakukan untuk mengamati kinerja bagian

Teknologi Sistem Informasi untuk menyusun BCP yang sesuai untuk perusahaan.

3. Kuesioner

Kuesioner pada penelitian ini digunakan untuk mengumpulkan data yang bersifat kuantitatif. Kuesioner dibagikan kepada masing-masing unit bisnis yang menjadi ruang lingkup pada penelitian ini. Data yang terkumpul akan digunakan pada tahapan BIA dimana untuk menentukan tingkat kepentingan sehingga dapat menggambarkan dampak dari bencana atau gangguan terhadap bisnis perusahaan.

3.3. Fase Perencanaan

Fase ini merupakan langkah pertama untuk membuat dokumen perencanaan keberlangsungan bisnis. Pada fase ini dilakukan kegiatan penentuan kebutuhan pengelolaan keberlangsungan bisnis.

3.3.1. Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis

Kegiatan ini fokus pada pendetilan kebutuhan awal pada lingkup manajemen terkait dengan tujuan, ruang lingkup, peran manajemen, sumber daya, dan komunikasi. Hasil yang peneliti harapkan dari fase awal ini adalah rumusan masalah serta latar belakang peneltian yang dijadikan sebagai dasar dari pembuatan dokumen perencanaan keberlangsungan bisnis. Luaran dari Berikut adalah tahapan dari kegiatan ini:

1. Menentukan tujuan dari adanya perencanaan keberlangsungan bisnis pada perusahaan.
2. Menentukan ruang lingkup yang akan menjadi bagian dari perencanaan keberlangsungan bisnis. Ruang lingkup yang diambil pada penelitian ini adalah pada bagian keuangan, pelyanan dan teknologi informasi pada PDAM Surya Sembada Kota Surabaya. 3 bagian tersebut dijadikan ruang lingkup karena 3 departemen tersebut yang memiliki

dampak kerugian paling besar jika proses bisnis dan IT yang digunakan mengalami gangguan.

3. Melakukan pembentukan komite BCP, komite BCP ini yang akan bertanggungjawab mengenai perencanaan keberlangsungan bisnis perusahaan. Komite BCP dibuat dengan koordinasi antara peneliti dan pihak TSI PDAM Surabaya.
4. Menentukan pihak internal atau eksternal yang berkaitan dengan kelangsungan bisnis perusahaan
5. Menentukan sumber daya baik manusia maupun perangkat untuk dapat memastikan bahwa proses berjalan dengan lancar dan sesuai dengan perencanaan.
6. Membuat alur komunikasi saat terjadi gangguan dalam perusahaan beserta dengan kontak dari pihak yang akan dihubungi

3.4. Fase Implementasi

Pada fase implementai, terdapat beberapa kegiatan untuk menyusun dokumen perencanaan keberlangsungan bisnis.

3.4.1. Identifikasi dan Analisis Risiko

Pada kegiatan ini berfokus pada identifikasi kemungkinan risiko apa saja yang dimiliki oleh perusahaan, penilaian risiko dan dampak dari risiko. Tahapan pada kegiatan ini meliputi.

1. Melakukan pendataan risiko yang mungkin diterima oleh perusahaan berdasarkan komponen TI dengan pendekatan OCTAVE.
2. Melakukan analisis dari setiap risiko untuk mengetahui penyebab.
3. Memberikan nilai pada setiap risiko berdasarkan tingkat kemungkinan terjadi risiko, tingkat dampak dan deteksi yang dimiliki perusahaan dengan metode FMEA. Dimana langkah-langkah di dalamnya adalah :
    a) Menentukan Severity Number dan Justifikasi
    b) Menentukan Occurance Number dan Justifikas
    c) Menentukan Detection Number dan Justifikasi
    d) Menghitung Jumlah Risk Priority Number

e) Melakukan Validasi Hasil Analisis Risiko

3.4.2. Analisis Dampak Bisnis

Pada kegiatan ini berfokus pada identifikasi dan prioritasi fungsi bisnis beserta dengan aset, penentuan jangka waktu toleransi gangguan, dan identifikasi dampak dari adanya gangguan. Tahapan pada kegiatan ini meliputi:

1. Melakukan pendataan proses bisnis perusahaan beserta layanan TI yang mendukung.
2. Melakukan prioritasi dari layanan TI sesuai dengan tingkat kritis yang didapat dari observasi peneliti dan wawancara yang dilakukan dengan user terkait layanan TI tersebut.
3. Melakukan prioritasi proses bisnis perusahaan sesuai dengan tingkat kritis yang didapat berdasarkan dari impact criticality level serta koordinasi dengan pihak terkait.
4. Melakukan analisis dampak dari adanya gangguan berdasarkan aspek finansial, reputasi dan teknis yang didapat dari observasi dan wawancara dengan pihak terkait.

Menentukan waktu pemulihan pada tiap layanan TI yang didapat dari observasi dan wawancara dengan pihak TSI.

3.4.3. Penyusunan Strategi Keberlangsungan Bisnis

Pada kegiatan ini berfokus pada penentuan pertanggungjawaban atas dampak gangguan yang mengganggu proses bisnis dan pengembangan prosedur pengelolaan kerusakan atau gangguan. Tahapan pada kegiatan ini meliputi.

1. Menentukan strategi preventif atau pencegahan untuk mengurangi risiko dan dampak.
2. Menentukan strategi mengenai tindakan atau aksi yang harus dilakukan oleh tim DRP agar dapat mengatasi gangguan dan melakukan pemulihan.

3. Menentukan strategi dalam mengatasi gangguan dan mengembalikan proses bisnis agar dapat kembali berjalan dalam kondisi normal, strategi ini dilakukan oleh seluruh pihak yang terkait dalam BCP.
4. Melakukan koreksi terhadap strategi yang telah dibuat, apabila terdapat ketidaksesuaian atau kurang efektif.

3.4.4. Penentuan Rencana Pemulihan Bencana

Pada kegiatan ini berfokus pada penanganan insiden, prosedur saat bencana beserta detil mengenai pihak yang bersangkutan dan pemulihan bencana. Tahapan pada kegiatan ini meliputi:

1. Melakukan pendataan aset TI yang dimiliki perusahaan.
2. Melakukan pendataan vendor jasa atau produk yang dibutuhkan beserta dengan tanggungjawabnya.
3. Menentukan lokasi server atau aset TI yang aman terhadap bencana
4. Membuat bentuk kontrol dari bencana atau gangguan.
5. Menentukan bilamana akan dilakukan aktivasi pemulihan mulai dari deklarasi status sampai kepada de-aktivasi.
6. Membuat skenario pengujian dan melakukan simulasi pengujian.
7. Melakukan evaluasi hasil pengujian dan melakukan revisi bentuk kontrol dari rencana pemulihan bencana

3.4.5. Pembuatan Dokumen Pelatihan Karyawan

Pada tahapan ini hanya mencakup perencanaan pelatihan dan pembuatan dokumen mekanisme penyampaian pelatihan yang terdiri dari latihan dan ujian, dan pemantauan kompetensi berdasarkan hasil latihan dan ujian. Tahapan pada kegiatan ini meliputi:

1. Menentukan jenis pelatihan yang sesuai dengan kebutuhan perusahaan.
2. Menentukan mekanisme penyampaian pelatihan

3. Merancang dan memenuhi sumber daya yang diperlukan dalam melaksanakan pelatihan.

3.5. Fase Pemantauan dan Review

Pada fase pemantauan dan review, kegiatan akan fokus pada pengujian BCP. Pengujian BCP fokus pada pembuatan alur pengujian, pengujian dan perbaikan berdasarkan hasil pengujian yang dilakukan. Aktivitas pada fase ini meliputi:

1. Merencanakan mekanisme pengujian termasuk metode pengujian dan menyusun alur pengujian.
2. Melakukan pengujian sesuai dengan metode dan rencana pengujian yang telah ditentukan.
3. Melakukan pencatatan temuan selama proses pengujian berlangsung.
4. Mendokumentasikan hasil pengujian untuk dijadikan masukan atau rekomendasi dalam peninjauan keberlangsungan bisnis.

3.6. Fase Pemeliharaan dan Peningkatan

Kegiatan ini berfokus pada peninjauan keberlangsungan bisnis yang dilihat dari kemampuan dan keefektifan keberlangsungan bisnis yang ditetapkan dalam rencana keberlangsungan bisnis serta memberikan feedback dari ketidaksesuaian keberlangsungan bisnis yang digunakan untuk memperbaiki dan meningkatkan kinerja keberlangsungan bisnis. Namun pada penelitian ini hanya sebatas pada perencanaan dan pembuatan formulir untuk peninjauan keberlangsungan bisnis. Tahapan pada kegiatan ini meliputi:

1. Menentukan periode waktu peninjauan keberlangsungan bisnis.
2. Melakukan peninjauan keberlangsungan bisnis secara berkala.

3. Melakukan analisis ulang terhadap adanya dampak, risiko, dan strategi baru terkait dengan rencana keberlangsungan bisnis yang telah diterapkan.
4. Melakukan pertimbangan terhadap perubahan dari rencana keberlangsungan bisnis yang telah ditetapkan.

3.7. Verifikasi dan Validasi

Pada tahapan ini akan dilakukan proses verifikasi kepada pihak perusahaan untuk dapat memastikan data dan informasi yang didapat valid dan dapat dipertanggung jawabkan.

3.8. Dokumentasi BCP dan Penarikan Kesimpulan

Fase terakhir dalam penelitian ini yaitu pembuatan kesimpulan serta saran dan mendokumentasikan BCP ke dalam buku tugas akhir. Pada fase ini terdapat kegiatan penarikan kesimpulan dan saran dari hasil penelitian yang telah dilakukan. Kesimpulan berupa hasil dan temuan-temuan dari penerapan tiap tahapan formulasi metode pembuatan BCP yang dibuat oleh Yusrida sehingga dapat diketahui kesesuaian dan keunikan metodologi pembuatan BCP tersebut dengan organisasi terkait studi kasus penelitian ini. Kesimpulan dan saran tersebut menjadi bahan evaluasi dan perbaikan untuk penelitian selanjutnya.

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Pada bab ini akan membahas mengenai rancangan penelitian dalam tugas akhir sebagai penjelasan lanjutan dari setiap proses yang ada pada bagian metodologi. Dalam bab perancangan ini akan berisi perancangan studi kasus, penentuan data-data yang dibutuhkan, teknik pengambilan data, pengolahan data, dan analisis data. tujuan dari tahapan ini adalah untuk mengidentifikasi teknik proses, kebutuhan proses, fokus proses dan strategi pelaksanaan pada setiap fase metode Yusrida yang dilakukan.

4.1. Fungsional Bisnis yang Terlibat dalam Penelitian

Pada penelitian tugas akhir ini, fungsional bisnis yang menjadi ruang lingkup adalah bagian keuangan, pelayanan dan teknologi sistem informasi. Alasan peneliti memilih 3 fungsional tersebut adalah karena ketiga fungsional tersebut memiliki ketergantungan yang tinggi terhadap TI dalam menjalankan proses bisnisnya. Berikut adalah penjelasan dari fungsional bisnis yang terkaitt dalam pembuatan BCP di penelitian ini:

1. Bagian Keuangan

Bagian keuangan terdiri atas beberapa sub bagian. Pada pengerjaan tugas akhir ini, hanya difokuskan pada bagian penagihan dan rekening. Bagian ini merupakan bagian penting dalam perusahaan karena sebagai penerima dan pengolahan pendapatan perusahaan seperti penerimaan kas dari pelanggan yang melakukan pembayaran *online* maupun *offline.*

2. Bagian Pelayanan

Bagian PTJSR yang merupakan sub bagian dari bagian pelayanan merupakan bagian yang bertanggung jawab dalam

melakukan pemasaran, pemasangan jaringan air pada pelanggan hingga penanganan keluhan.

3. Bagian Teknologi Sistem Informasi

Bagian TSI merupakan bagian yang bertugas dalam pengelolaan dan penyediaan layanan TI untuk mendukung keseluruhan operasional proses bisnis pada perusahaan.

4.2. Proses Bisnis yang Terlibat dalam Penelitian

Dari ketiga fungsional bisnis yang terdapat pada PDAM Surya Sembada Kota Surabaya, akan dijelaskan lebih lanjut mengenai proses bisnis dari masing masing fungsional yang terkait dengan tujuan dari organisasi. proses-proses berikut ini merupakan proses bisnis yang dianggap penting bagi keberlangsungan proses bisnis organisasi. Berikut merupakan proses bisnis terkait sistem dari ketiga fungsional bisnis yang ada.

Tabel 4.1 Ruang Lingkup

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi
Keuangan (Rekening & Penagihan)	Pengawasan rekening dan penerbitan penagihan
	Penagihan rekening swasta
	Penagihan rekening pemerintah
	Penagihan rekening pendapatan lain-lain
Pelayanan	Melakukan survey terkait lokasi pemasangan pada pelanggan
	Pembuatan RAB
	Customer Installation
	Pengelolaan Laporan Keluhan Pelanggan
	Penanganan Keluhan
Teknologi Sistem Informasi	Melakukan pengawasan instalasi, perawatan dan perbaikan terhadap infrastruktur TI (Hardware dan Jaringan)

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi
	Melakukan pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)
	Disaster Recovery Center
	Penyediaan layanan email dan sistem informasi
	Melakukan evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;
	Melakukan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan
	Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi
	Melakukan pengawasan kegiatan *helpdesk support*.
	Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan

4.3. Persiapan Pengumpulan Data dan Informasi

Pada bagian ini akan menjelaskan mengenai tahapan persiapan pengumpulan data dan informasi yang nantinya akan diolah untuk dapat menjawab rumusan masalah. Terdapat beberapa teknik yang digunakan dalam mengumpulkan data dan informasi, antara lain adalah interview atau wawancara, analisis dokumen perusahaan dan observasi.

4.3.1. Wawancara

Proses wawancara akan dilakukan pada tiga fungsional bisnis yang terdapat pada PDAM Surya Sembada Kota Surabaya sesuai dengan ruang lingkup(TSI, Keuangan dan Pelayanan). Diharapkan setelah melakukan wawancara akan didapatkan informasi terkait risiko TI yang dihadapi oleh perusahaan.

Tabel 4.2 Ketentuan Wawancara

Nama Proses	**Pengumpulan Data dan Informasi**
Teknik	Interview/Wawancara Teknik wawancara akan dilakukan dengan metode tanya jawab langsung dengan narasumber. Wawancara akan dilakukan secara terstruktur, dimana peneliti telah menyiapkan pertanyaanpertanyaan yang dibutuhkan terlebih dahulu.
Objek	Kondisi kekinian organisasi, proses bisnis organisasi, aset TI, risiko , kontrol keamanan dan dampak terhadap proses bisnis kritis.
Kebutuhan Proses	- Interview protocol - Laptop - Alat tulis
Tahapan Pelaksanaan	Tahapan dalam melakukan wawancara adalah sebagai berikut: - Menetapkan tujuan dan jumlah wawancara - Menentukan narasumber - Membuat interview protocol - Memulai proses wawancara - Mendokumentasikan hasil wawancara

4.4.1.1. Jumlah dan Tujuan Wawancara

Sebelum melakukan wawancara, terlebih dahulu ditetapkan tujuan dari wawancara yang akan dilakukan. Hal ini bertujuan agar nantinya proses wawancara dan pengambilan informasi dapat sesuai dengan tujuan penelitian dan peneliti mendapatkan data dan informasi yang dibutuhkan.

Tabel 4.3 Jumlah dan Tujuan Wawancara

Wawancara Ke-	Narasumber	Tujuan Wawancara
1	Ira Nuraini	Wawancara dilakukan untuk mengetahui kondisi kekinian, proses bisnis serta informasi mengenai penerapan TI pada bagian keuangan. serta dampak terhadap proses bisnis kritis apabila terjadi gangguan.
2	Dani	Wawancara dilakukan untuk mengetahui kondisi kekinian, proses bisnis serta informasi mengenai penerapan TI pada bagian pelayanan. serta dampak terhadap proses bisnis kritis apabila terjadi gangguan.
3	Nurlillah Satria Pratama	Wawancara dilakukan untuk mengetahui kondisi kekinian, proses bisnis serta informasi mengenai penerapan TI pada bagian Teknologi Sistem Informasi. Selain itu dilakukan penggalian lebih dalam mengenai aset TI, ancaman dan risiko TI, kelemagan TI,kebutuhan keamanan, kontrol TI apa yang sudah diterapkan serta dampak terhadap proses

Wawancara Ke-	Narasumber	Tujuan Wawancara
		bisnis kritis apabila terjadi gangguan.

4.4.1.2.Profil Narasumber Wawancara

Sebelum melakukan wawancara, peneliti terlebih dahulu harus menentukan narasumber. Narasumber yang dipilih tentu saja harus sesuai dengan tujuan wawancara serta berada dalam kapasitas objek wawancara. Hal ini bertujuan agar narasumber dapat memberikan informasi yang valid dan sesuai serta relevan dengan cakupan wawancara itu sendiri. Berikut merupakan profil narasumber yang akan diwawancara dalam penelitian ini:

Tabel 4.4 Profil Narasumber

Nama	Jabatan
Ira Nuraini	Senior Staf Penerimaan dan Pendistribusian Rekening (Keuangan)
Dani	Senior Staf Pelayanan
Nurlillah Satria Pratama	Supervisor TSI

4.4.1.3. Daftar Pertanyaan Wawancara

Berikut merupakan daftar pertanyaan yang tercantum pada *interview protocol :*

Tabel 4.5 *Interview Protocol*

No	Tujuan Pertanyaan	Standar Acuan Terkait	Detail Ringkas Pertanyaan
1.	Untuk mengetahui proses bisnis yang terkait IT dan kondisi kekinian dari PDAM Surya	-	• Proses bisnis di 3 fungsional bisnis PDAM Surabaya

No	Tujuan Pertanyaan	Standar Acuan Terkait	Detail Ringkas Pertanyaan
	Sembada Kota Surabaya.		• Data struktur organisasi dan tupoksi masing-masing fungsi. • Proses umum penerapan TI di PDAM
2.	Wawancara dilakukan untuk melakukan identifikasi risiko. Hal ini dilakukan dengan menggali informasi terkait aset kritis teknologi dan sistem informasi, ancaman dan kerentanan terhadap aset TI, serta kebutuhan keamanan dan praktik kemanan TI yang telah diterapkan.	OCTAVE Fase 1 - Build AssetBased Threat Profile (Membangun aset berdasarkan ancaman profil)	• Aset TI yang digunakan dalam proses bisnis kritikal • Aset TI kritikal yang dapat memberi ancaman pada organisasi • Kebutuhan keamanan TI dari organisasi • Ancaman yang mungkin terjadi kepada aset TI Praktik keamanan TI yang telah dilakukan oleh organisasi • Kelemahan Organisasi
		OCTAVE Fase 2 -	• Komponen aset TI yang ada di orgainsasi

No	Tujuan Pertanyaan	Standar Acuan Terkait	Detail Ringkas Pertanyaan
		Identify Infrastructure Vulnerabilities	• Kelemahan teknis aset TI organisasi
			• Manajemen risiko terkait TI Kontrol keamanan yang diterapkan
3.	Untuk mengidentifikasi layanan TI, proses bisnis TI dan aktivitas TI serta tingkat prioritasnya. Selain itu bertujuan untuk dapat mengetahui toleransi waktu dan dampak yang terjadi apabila adanya gangguan pada proses bisnis.	ISO 22317 Klausa 5.3 – Prioritisasi produk dan layanan	• Layanan TI organisasi • Tingkat prioritas pada layanan TI
		ISO 22317 Klausa 5.4 – Prioritisasi Proses	• Proses bisnis yang ada pada fungsional organisasi • Prioritisasi proses bisnis
		ISO 22317 Klausa 5.5 - Prioritisasi	• Aktivitas yang terdapat pada proses bisnis • Prioritisasi terhadap aktivitas

No	Tujuan Pertanyaan	Standar Acuan Terkait	Detail Ringkas Pertanyaan
		Aktivitas	
		ISO 22317 Klausa 5.6 Analisis dan Konsolidasi	• Dampak yang terjadi akibat gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis) • Waktu yang ditoleransi organisasi terkait gangguan • Toleransi waktu dalam tahap pemulihan sistem apaila terjadi gangguan • Respon organisasi terhadap proses bisnis kritis bila

No	Tujuan Pertanyaan	Standar Acuan Terkait	Detail Ringkas Pertanyaan
			terjadi gangguan?

4.3.2. Kuesioner

Pengambilan data dengan kuesioner ini bertujuan untuk menentukan tingkat kritis sehingga dapat menggambarkan dampak dari gangguan/bencana terhadap bisnis. Kuesioner analisa dampak bisnis berupa penilaian dampak bisnis apabila terjadi gangguan yang terdiri atas dampak finansial, operasional dan reputasi. Serta hasil dari penentuan tingkat kritis akan menjadi dasar dalam penentuan waktu pemulihan.

4.4.2.1 Tujuan

Sebelum melakukan pengambilan data, terlebih dahulu ditetapkan tujuan dari dari kuesioner yang dibuat. Hal ini bertujuan agar nantinya proses pengambilan informasi dapat sesuai dengan tujuan penelitian dan peneliti mendapatkan data dan informasi yang dibutuhkan.

Tabel 4.6 Tujuan Kuesioner

Narasumber	Nurlillah Satria Pratama
Jabatan	Supervisor TSI
Tujuan	Untuk mendapatkan penilaian terkait analisa dampak bisnis setiap proses bisnis fungsional bisnis.

4.4.2.2 Format Kuesioner

Berikut ini adalah format kuesioner yang digunakan dalam pengambilan data kuantitatif. (**Untuk Dampak Operasional**

dan Dampak Reputas secara detil pada Lampiran C, D dan E)

Tabel 4.7 Format Kuesioner

1. Dampak Finansial	
Ketentuan penilaian aspek finansial 0 bila tidak berdampak pada aspek finansial 1 bila adanya penambahan biaya kurang dari 5% dari anggaran proses bisnis 2 bila adanya penambahan biaya 5-10% dari anggaran proses bisnis 3 bila adanya penambahan biaya 11-20% dari anggaran proses bisnis 4 bila adanya penambahan biaya 21-25% dari anggaran proses bisnis 5 bila adanya penambahan biaya lebih dari 25% dari anggaran proses bisnis	
Proses Bisnis terkait sistem	**Skor**
Pengawasan rekening dan penerbitan penagihan	
Penagihan rekening swasta	
Penagihan rekening pemerintah	
Penagihan rekening pendapatan lain-lain	

4.4. Pengolahan Data dan Informasi

Pengolahan data dan informasi merupakan proses yang dilakukan setelah proses pengambilan data selesai. Penelitian ini tergolong dalam penelitian kualitatif, dimana pengumpulan data dilakukan dengan wawancara, observasi, dan mempelajari dokumen perusahaan. Data yang telah terkumpul akan

diterjemahkan oleh penulis dan dan dilakukan analisis. Analisis yang akan dilakukan pada penelitian ini mencakup beberapa hal, diantaranya adalah:

4.4.1. Elemen Dokumen

Perancangaan dalam menentukan elemen dalam dokumen BCP mengacu pada elemen BCP yang telah disusun oleh Yusrida, yang terdiri atas :

1. Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis
2. Peninjauan Keberlangsungan Bisnis
3. Analisis Risiko
4. Analisis Dampak Bisnis
5. Strategi Keberlangsungan Bisnis
6. Rencana Pemulihan Bencana
7. Pelatihan Karyawan
8. Pengujian BCP

4.4.2. Analisis Risiko

Beberapa tahapan yang dilakukan untuk mengidentifikasi dan menganalisis risiko berdasarkan metode Yusrida meliputi:

1. Identifikasi Risiko

Melakukan pendataan risiko yang mungkin diterima oleh perusahaan berdasarkan komponen TI yaitu *hardware*, *software*, data, jaringan, prosedur dan manusia dengan pendekatan OCTAVE. Pendataan risiko didapat dari memetakan hasil dari wawancara, observasi dan analisis dokumen terkait kondisi kekinian organisasi, aset-aset kritis dan ancaman terhadap aset.

2. Penilaian Risiko dengan FMEA

Memberikan nilai pada setiap risiko berdasarkan tingkat kemungkinan terjadi risiko (*occurance*), tingkat dampak

(*severity*) dan deteksi (*detection*) yang dimiliki perusahaan dengan metode FMEA hingga menghasilkan nilai RPN yang selanjutnya akan diurutkan dari yang paling besar untuk menghasilkan prioritasi risiko.

4.4.3. Analisis Dampak Bisnis

Setelah melakukan identifikasi dan analisis risiko dilanjutkan dengan analisis dampak bisnis. Analisis dampak bisnis bertujuan untuk menentukan dan melakukan prioritisasi proses operasional bisnis yang paling dianggap kritis pada suatu organisasi. berikut ini adalah detil aktivitas yang ada pada metodologi BCP Yusrida :

1. Melakukan pendataan proses bisnis perusahaan beserta layanan TI yang mendukung.
   Pendataan dilakukan dengan membuat daftar proses bisnis perusahaan beserta dengan layanan TI yang mendukung proses bisnis tersebut pada bagian keuangan, pelayanan dan teknologi sistem informasi.

2. Analisis dampak dari adanya gangguan

   Melakukan analisis dampak dari adanya gangguan berdasarkan aspek finansial, reputasi dan operasional yang didapat dari observasi dan wawancara dengan pihak terkait. Analisis dampak gangguan merupakan proses penilaian dampak dari masing masing proses bisnis apabila terjadi risiko yang tidak diinginkan. Hasil dari analisis dampak gangguan akan menjadi dasar tingkar kritis pada setiap proses bisnis sehingga dapat menentukan waktu pemulihan terhadap layanan secara tepat.

Berikut ini adalah penjelasan dari ketiga aspek dampak dari adanya gangguan :

A. Penilaian dampak finansial

Penilaian dampak finansial dilakukan dengan menanyakan “sejauh mana dampak atau kerugian finansial yang diakibatkan

jika sebuah proses bisnis mengalami gangguan ?" kerugian finansial dapat berupa :

- Pinalti karena ketidakmampuan dalam memenuhi kontrak
- Kehilangan sumber dana (kepercayaan investor)
- Kehilangan kesempatan untuk mendapatkan keuntungan
- Menyewa karyawan tambahan untuk membantu penyelesaian
- Perjalanan, akomodasi, penginapan
- Upah lembur untuk kerja tambahan
- Sewa peralatan pengganti
- Biaya perbaikan kerusakan perangkat

Sedangkan untuk pengelompokan kerugian finansial didapatkan berikut ini :

Tabel 4.8 Kriteria Kerugian Finansial

Level	Kriteria
0 (none)	bila tidak berdampak pada aspek finansial
1 (low)	bila adanya penambahan biaya kurang dari 5% dari anggaran proses bisnis
2 (medium)	bila adanya penambahan biaya 5-10% dari anggaran proses bisnis
3 (medium-high)	bila adanya penambahan biaya 11-20% dari anggaran proses bisnis
4 (high)	bila adanya penambahan biaya 21-25% dari anggaran proses bisnis
5 (highest)	bila adanya penambahan biaya lebih dari 25% dari anggaran proses bisnis

B. Penilaian Dampak Reputasi

Penilaian dampak reputasi dilakukan dengan menanyakan "sejauh mana dampak atau kerugian dilihat dari sisi reputasi

perusahaan yang diakibatkan jika sebuah proses bisnis mengalami gangguan ?" kerugian reputasi dapat berupa :

- Kepuasaan pelanggan
- Kepercayaan vendor
- Citra perusahaan
- Opini negatif dari media dan masyarakat
- kehilangan pelanggan yang potensial

Sedangkan untuk pengelompokan kerugian reputasi didapatkan berikut ini :

Tabel 4.9 Kriteria Kerugian Reputasi

Level	Kriteria
0 (none)	bila tidak berdampak pada aspek reputasi
1 (low)	bila adanya penurunan yang sangat kecil dari reputasi perusahaan
2 (medium)	bila adanya penurunan yang kecil dari reputasi perusahaan
3 (medium-high)	bila adanya penurunan yang sedang dari reputasi perusahaan
4 (high)	bila adanya penurunan yang tinggi dari reputasi perusahaan
5 (highest)	bila adanya penurunan yang sangat tinggi dari reputasi perusahaan

C. Penilaian Dampak Operasional

Penilaian dampak finansial dilakukan dengan menanyakan "sejauh mana jika sebuah proses bisnis mengalami gangguan akan berdampak pada sisi operasional?" kerugian operasional dapat berupa :

- Moral karyawan
- Efisiesiensi operasional bisnis

- Efektivitas operasional bisnis

Sedangkan untuk pengelompokan kerugian reputasi (severity level) didapatkan berikut ini :

Tabel 4.10 Kriteria Kerugian operasional

Level	Kriteria
0 (none)	Bila tidak berdampak pada operasional
1 (low)	Bila adanya penurunan hasil kurang dari 5% dari target proses bisnis
2 (medium)	Bila adanya penurunan hasil 5-10% dari target proses bisnis
3 (medium-high)	Bila adanya penurunan hasil 11-20% dari target proses bisnis
4 (high)	Bila adanya penurunan hasil 21-25% dari target proses bisnis
5 (highest)	Bila adanya penurunan hasil lebih dari 25% dari target proses bisnis

3. Prioritasi Proses Bisnis Perusahaan

Prioritisasi proses bisnis dilakukan untuk dapat mengetahui tingkat kepentingan dari masing masing proses bisnis yang terkait dengan layanan TI. Prioritasi proses bisnis dilakukan sesuai dengan tingkat kritis yang didapat berdasarkan dari analisis dampak gangguan serta koordinasi dengan pihak terkait. Berikut ini merupakan tabel pungategorian tingkat kritis untuk proses bisnis dan Aktivitas TI yang dimiliki oleh perusahaan :

Tabel 4.11 Kriteria Tingkat Kritis Proses Bisnis

Tingkat Kritis	Definisi	Keterangan
Kritis	Proses bisnis dikategorikan kritis apabila proses bisnis ini memiliki dampak yang	Dampak finansial nomor 3 adalah bila adanya

	sangat besar apabila terjadi gangguan yaitu dampak finansial no 3 atau lebih serta dampak operasional dan reputasi no 4 atau lebih.	penambahan biaya 11-20% dari anggaran proses bisnis. Sedangkan Dampak operasional nomor 4 adalah Bila adanya penurunan hasil 21-25% dari target proses bisnis dan Dampak reputasi nomor 4 adalah bila adanya penurunan yang tinggi dari reputasi perusahaan.
Penting	Proses bisnis dikategorikan penting apabila proses bisnis ini memiliki dampak yang tidak terlalu besar apabila terjadi gangguan yaitu dampak finansial no 1 – 2 serta dampak operasional dan reputasi no 1 – 3.	
Minor	Proses bisnis diaktegorikan minor apabila proses bisnis ini tidak memiliki dampak atau dampaknya hampir tidak terasa saat terjadi gangguan yaitu dampak finansial, operasional serta reputasi no 0.	

4. Prioritasi dari layanan TI

Perusahaan perlu melakukan identifikasi layanan SI/TI beserta dengan melakukan prioritisasi tingkat kritis masing masing layanan. Tingkat kritisasi didapat dari observasi peneliti dan wawancara yang dilakukan dengan user terkait layanan TI tersebut serta hasil dari prioritasi proses bisnis.

5. Menentukan waktu pemulihan pada tiap layanan TI

Setelah melakukan prioritisasi maka selanjutnya akan akan dilakukan identifikasi waktu pemulihan. Pada masing masing layanan TI yang mendukung proses bisnis akan dilakukan

identifikasi waktu pemulihan apabila terjadi gangguan. Penentuan waktu pemulihan didapatkan dari hasil observasi peneliti dan wawancara dengan pihak TSI serta hasil dari analisis dampak gangguan. Analisis waktu pemulihan dibagi menjadi tiga, yaitu sebagai berikut :

Tabel 4.12 Jenis Waktu Pemulihan

Jenis waktu pemulihan	Keterangan
Maximum Tolerable Downtime (MTD)	• merupakan jumlah waktu maksimal yang dapat ditoleransi oleh perusahaan terhadap kegagalan proses bisnis
Recovery Time Objective (RTO)	• adalah jumlah waktu lumpuh maksimal untuk seluruh sumber daya sistem yang ada, sebelum terjadi dampak lain kepada sumber daya lainnya.
Recovery Point Objective (RPO)	• adalah jumlah waktu yang diperlukan setelah terjadinya gangguan, untuk memulihkan data setelah terjadinya gangguan.

4.5. Penyusunan Strategi Keberlangsungan Bisnis

Strategi BCP dikategorikan menjadi 4 jenis, yaitu strategi prevetif, strategi DRP, strategi saat terjadi gangguan dan strategi korektif. Berikut ini penjelasan secara detilnya [31]:

- Strategi Preventif

Strategi preventif adalah aksi organisasi yang dilakukan untuk mengunrangi risiko terjadinya gangguan dan juga mengurangi dampak yang terjadi akibat risiko tersebut. Strategi ini dilakukan supaya organisasi siap dalam menghadapi gangguan yang akan terjadi sehingga dapat mengatasi gangguan dalam batas toleransi yang telah ditentukan sebelumnya.

- Strategi Saat Gangguan

Strategi saat terjadi gangguan merupakan suatu tindakan atau aksi yang dilakukan organisasi untuk dapat mengatasi gangguan dan mengembalikan proses bisnis agar dapat kembali berjalan dalam kondisi normal. Berbeda dengan strategi DRP, strategi saat gangguan tidak terbatas hanya untuk tim DRP namun untuk keseluruhan komite BCP yang terkait. Fokus utama strategi ini adalah untuk dapat mengembalikan kondisi organisasi ke status normal.

- Strategi Korektif

Strategi Korektif merupakan suatu tindakan atau aksi yang dilakukan organisasi untuk dapat terus menerus memperbaiki kinerja dari perencanaan BCP. Strategi korektif dilakukan saat organisasi melihat adanya ketidaksesuaian atau kurangnya tingkat keefektifan dari perencanaan BCP yang telah disusun. Diharapkan nantinya strategi korektif ini dapat membantu organisasi untuk dapat terus menerus meningkatkan performa dari strategi BCP.

4.6. Perancangan Evaluasi

Evaluasi yang dilakukan bertujuan untuk melihat apakah setiap aktivitas pada fase metode Yusrida dapat diimplementasi pada objek studi kasus. Selain itu juga untuk menemukan ketidaksesuaian dan temuan berdasarkan objek penelitian yang pada tugas akhir ini adalah pada PDAM Surya Sembada Kota Surabaya.

Evaluasi ini dilakukan dengan menggunakan peran perangkat evaluasi berupa checklist untuk setiap tahapan pada metode Yusrida. Checklist akan menunjukkan apakah setiap aktivitas dapat dilakukan tanpa adanya perubahan atau dapat dilakukan dengan perubahan ataupun tidak dapat diimplementasi sama sekali. Berikut ini adalah format perangkat evaluasi :

Tabel 4.13 Justifikasi Status

Nomor	Keterangan
1	Dapat diimplementasi tanpa perubahan
2	Dapat diimplementasi dengan perubahan
3	Tidak dapat diimplementasi

Tabel 4.14 Format Tabel Evaluasi

Tahap	Aktivitas	1	2	3	Justifikasi
Fase 1. Perencanaan					
Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis	Penentuan Tujuan				
	Penentuan Ruang Lingkup				
	Pembentukan Komite				
	Penentuan Tanggung Jawab				
	Penentuan Pihak Terkait				
	Penentuan Sumberdaya				
	Pembuatan Alur Komunikasi				

Tahap	Aktivitas	1	2	3	Justifikasi
Fase 2. Implementasi					
Analisis Risiko	Pendataan Kemungkinan Risiko				
	Analisis Risiko				
	Penilaian Risiko				
Analisis Dampak Bisnis	Pendataan Proses Bisnis dan TI				
	Prioritisasi Layanan TI				
	Prioritisasi Proses Bisnis				
	Analisis Dampak Gangguan				
	Penentuan Waktu Pemulihan				
Strategi keberlangsungan Bisnis	Penentuan Strategi Preventif				
	Penentuan Strategi Saat Gangguan				
	Penentuan Strategi Pemulihan				
	Koreksi Terhadap Strategi				

Tahap	Aktivitas	1	2	3	Justifikasi
Rencana Pemulihan Bencana	Pendataan Aset Teknologi informasi				
	Pendataan Vendor				
	Penentuan Lokasi Server dan Aset TI				
	Pembuatan Kontrol				
	Permintaan Aktivasi dan Deaktivasi				
	Skenario Pengujian				
	Evaluasi Bentuk Kontrol				
Pelatihan Karyawan	Penentuan Jenis Pelatihan				
	Mekanisme Penyampaian Pelatihan				
	Rencana Kebutuhan Pelatihan				
	Pelaksanaan pelatihan				
Fase 3. Pemantauan dan Review					
Pengujian BCP	Rencana Mekanism				

Tahap	Aktivitas	1	2	3	Justifikasi
	e Pengujian				
	Pengujian				
	Pencatatan Temuan				
	Dokumentasi Hasil Pengujian				
Fase 4. Pemeliharaan dan Peningkatan					
Peninjauan Keberlangsungan bisnis	Penentuan Periode Waktu Peninjauan				
	Peninjauan Secara Berkala				
	Pengkajian Ulang Terhadap rencana				
	Pertimbangan Terhadap Perubahan				

4.7. Rencana Validasi

Validasi bertujuan untuk memastikan bahwa hasil dari analisa risiko dan dampak bisnis telah sesuai dengan kondisi perusahaan. Serta untuk mengonfirmasi apakah dokumen BCP yang dibuat telah sesuai dengan kebutuhan PDAM Surya Sembada Kota Surabaya. Validasi dilakukan dengan mengonsultasikan dan menunjukkan dokumen BCP yang telah dibuat kepada pihak manajemen yang diwakilkan oleh TSI. Jika dokumen BCP yang dibuat dianggap telah valid maka akan diminta persetujuan pada surat konfirmasi yang akan dibuat. Berikut ini merupakan tabel yang berisi rencana validasi yang akan diajukan:

Tabel 4.15 Rencana Validasi

No	Hal	Deskripsi
1.	Validasi kesesuaian analisa risiko PDAM Surya Sembada Kota Surabaya.	Validasi ini bertujuan untuk memastikan bahwa analisis dan penilaian risiko yang dibuat telah sesuai dengan kondisi organisasi, yaitu PDAM Surya Sembada Kota Surabaya.
2.	Validasi kesesuaian analisa dampak bisnis	Validasi ini bertujuan untuk memastikan bahwa analisis dampak bisnis yang dibuat telah sesuai dengan kondisi organisasi, yaitu PDAM Surya Sembada Kota Surabaya.
3.	Validasi dokumen akhir BCP PDAM Surya Sembada Kota Surabaya.	Validasi ini bertujuan untuk memastikan bahwa dokumen BCP yang dibuat oleh peneliti telah sesuai dengan keadaan dan kebutuhan dari PDAM Surya Sembada Kota Surabaya.

BAB V
IMPLEMENTASI

Bab ini menjelaskan hasil dari perancangan dan proses pelaksanaan dari penelitan. Selain itu, akan dijabarkan pula mengenai hasil pengumpulan data dan informasi serta hambatan dan rintangan dalam pelaksanaan penelitian.

5.1. Hasil Pengumpulan Data dan Informasi

Proses pengumpulan data dan informasi dilakukan dengan tiga metode, yaitu dengan melakukan wawancara, analisis dokumen dan kuesioner.

5.1.1. Hasil Wawancara

Pengumpulan data menggunakan metode wawancara dilakukan kepada beberapa pihak terkait di PDAM Surya Sembada Kota Surabaya. Berikut merupakan keterangan dari pelaksanaan tahap pengumpulan data dan informasi dengan menggunakan metode wawancara:

Tabel 0.1 Hasil Wawancara

Wawancara Ke- 1	
Narasumber	Nurlillah Satria Pratama
Jabatan	Supervisor TSI
Tanggal	26 April 2018
Topik	Kondisi kekinian organisasi, proses bisnis organisasi, aset TI, risiko ,kebutuhan dan kontrol keamanan,gangguan yang pernah dan berpotensi untuk terjadi serta dampak gangguan terhadap proses bisnis kritis.
Hasil	Lampiran A, B, C, D dan E
Wawancara Ke- 2	
Narasumber	Ira Nuraini
Jabatan	Senior Staf Penerimaan dan Pendistribusian Rekening (Keuangan)
Tanggal	26 April 2018

Topik	Proses bisnis pada bagian penagihan dan rekening (Keuangan), risiko, gangguan yang pernah dan berpotensi untuk terjadi serta dampak gangguan terhadap proses bisnis kritis.
Hasil	Lampiran C
Wawancara Ke- 3	
Narasumber	Dani
Jabatan	Senior Staf Pelayanan
Tanggal	26 April 2018
Topik	Proses bisnis pada bagian pelayanan, risiko, gangguan yang pernah dan berpotensi untuk terjadi serta dampak gangguan terhadap proses bisnis kritis.
Hasil	Lampiran D

5.1.2. Hasil Kuesioner

Pengumpulan data menggunakan metode kuesioner dilakukan kepada perwakilan bagian TSI di PDAM Surya Sembada Kota Surabaya. Berikut merupakan keterangan dari pelaksanaan tahap pengumpulan data dan informasi dengan menggunakan metode Kuesioner:

Tabel 0.2 Hasil Kuesioner

Wawancara Ke- 1	
Narasumber	Nurlillah Satria Pratama
Jabatan	Supervisor TSI
Tanggal	26 April 2018
Topik	Penilaian dampak bisnis dari segi operasional, finansial dan reputasi pada proses bisnis bagian pelayanan, keuangan dan TSI.
Hasil	**Lampiran C, D dan E**

5.1.3. Hasil Validasi

Validasi dilakukan untuk memastikan bahwa hasil analisa risiko dan analisa dampak bisnis yang dilakukan sudah benar dan sesuai dengan kondisi perusahaan. Validasi juga dilakukan sebagai konfirmasi apakah dokumen BCP yang dikerjakan oleh peneliti telah sesuai dengan kebutuhan dari PDAM Surya Sembada Kota Surabaya. Proses validasi dilakukan dengan mengajukan surat konfirmasi pada perwakilan TSI.

Hasil validasi telah memastikan bahwa analisis risiko, analisis dampak bisnis dan dokumen BCP yang dibuat telah sesuai dengan kondisi perusahaan. Untuk hasil validasi dapat dilihat pada **lampiran J, K dan L**.

5.1.4. Hambatan Pengumpulan Data

Pada bagian ini akan dijelaskan mengenai hambatan serta rintangan dalam pengerjaan penelitian, beberapa hambatan dan rintangan tersebut antara lain:

- Perizinan untuk melakukan wawancara dan memberikan kuesioner pada objek studi kasus yang memerlukan waktu yang lama dikarenakan proses birokrasi
- Analisis dampak bisnis memerlukan waktu yang lama dikarenakan narasumber kesulitan dalam melakukan estimasi

Walaupun terdapat kesulitan dan hambatan dalam pengerjaan tugas akhir, namun pihak Teknologi Sistem Informasi pada PDAM Surya Sembada Surabaya sangat berperan besar dalam penyelesaian penelitian ini. Hal tersebut dikarenakan pihak TSI yang sangat kooperatif dan bersedia meluangkan waktu untuk melakukan pengambilan data, asistensi dan konsultasi serta validasi.

Halaman ini sengaja dikosongkan

BAB VI
HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan mengenai hasil dan pembahasan terkait dengan permasalahan yang diangkat dalam penelitian ini yaitu implementasi metodologi Business Continuity Plan di PDAM Surya Sembada Kota Surabaya. Selain itu, bab ini juga akan menyampaikan berbagai temuan yang didapatkan selama melakukan penelitian.

6.1. Profil Perusahaan

PDAM Surya Sembada Kota Surabaya adalah salah satu unit usaha milik daerah yang bergerak dalam usaha distribusi air bersih bagi masyarakat umum di Surabaya, Pasuruan, Sidoarjo dan Gresik. Perusahaan ini berdiri sejak tahun 1976 dan dimiliki oleh pemerintah kota Surabaya. Disahkan dengan Surat Keputusan Gubernur Kepala Daerah Tingkat I Jawa Timur, tanggal 06 Nopember 1976 No. II/155/76 dan diundangkan dalam Lembaran Daerah Kotamadya Daerah Tingkat II Surabaya tahun 1976 seri C pada tanggal 23 Nopember 1976 No. 4/C[1].

6.2. Implementasi Metodologi Business Continuity Plan di PDAM Surya Sembada Kota Surabaya

Pada bagian ini akan menjelaskan mengenai implementasi metodologi BCP sesuai pada PDAM Surya Sembada Kota Surabaya dengan metode yang telah diformulasikan oleh Yusrida. Implementasi dari metodologi BCP merupakan bentuk validasi empiris yang dilakukan dalam penelitian ini. Dalam melakukan implementasi, keseluruhan dari tahapan yang ada pada metodologi akan diterapkan dan akan menghasilkan luaran berupa dokumen Business Continuity Plan PDAM Surya Sembada Kota Surabaya.

6.2.1. Fase 1 – Perencanaan

Pada fase perencanaan yang mencakup tahapan penentuan kebutuhan pengelolaan keberlangsungan bisnis, perusahaan diharuskan untuk menentukan kebutuhan di awal terkait menjaga bisnis agar tetap sustain ketika terjadi gangguan atau interupsi. Pada fase ini, perusahaan menentukan beberapa hal diantaranya tujuan keberlangsungan bisnis, ruang lingkup, peran manajemen beserta dengan sumber daya yang terlibat dan komunikasi selama pengelolaan keberlangsungan bisnis berlangsung. Berikut ini hasil penentuan kebutuhan pengelolaan keberlangsungan bisnis PDAM Surya Sembada Kota Surabaya:

6.2.1.1. Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis

Pada tahapan penentuan kebutuhan pengelolaan keberlangsungan bisnis, terdapat aktivitas pembuatan tujuan keberlangsungan bisnis, penentuan ruang lingkup, peran manajamen, kebutuhan sumber daya dan alur komunikasi saat terjadi gangguan. Aktivitas pada tahap ini bertujuan untuk mendefinisikan alur dan peran serta tanggung jawab pihak manajemen untuk kemudian menjalankan strategi keberlangsungan bisnis dan perencanaan keberlangsungan bisnis yang telah dibuat jika terjadi risiko pada proses bisnis kritis.

6.2.1.1.1. Tujuan Keberlangsungan Bisnis

Sesuai dengan tahapan pada metode Yusrida,untuk menentukan tujuan keberlangsungan bisnis, perlu diketahui terlebih dahulu kebutuhan rencana keberlangsungan bisnis perusahaan. Karena setiap perusahaan memiliki karakteristik yang berbeda sehingga kebutuhan akan BCP juga berbeda. Berikut ini merupakan kebutuhan rencana keberlangsungan bisnis dari PDAM Surya Sembada Kota Surabaya yang didapatkan berdasarkan wawancara dan konfirmasi dengan perwakilan bagian TSI.

Tabel 6.1 Kebutuhan BCP PDAM Surya Sembada Kota Surabaya

KEBUTUHAN BCP PDAM Surya Sembada Kota Surabaya
BCP sesuai dengan operasional proses bisnis perusahaan
BCP sesuai dengan teknologi informasi yang sudah diimplemetasikan
BCP sesuai dengan sumber daya manusia dan teknologi informasi yang diterapkan
BCP mampu menjaga agar proses bisnis perusahaan tetap *sustain*
BCP mencakup risiko beserta dampaknya bagi proses bisnis perusahaan
BCP dapat meminimalisir dan menangani risiko dan dampak yang timbul dari teknologi informasi yang diimplementasikan perusahaan
BCP dapat dilakukan pembaharuan dari waktu ke waktu

Tujuan dari rencana keberlangsungan bisnis (BCP) PDAM Surya Sembada Kota Surabaya, adalah:

1. Memastikan bahwa proses bisnis kritis dapat tetap berlangsung selama ada interupsi berupa gangguan maupun bencana.
2. Meminimalisir dampak dari adanya risiko yang dapat mengganggung proses bisnis perusahaan.
3. Mendokumentasikan proses bisnis kritis, layanan TI kritis, dampak dari gangguan, strategi keberlangsungan, pemulihan gangguan dan hal lain terkait kelangsungan bisnis

6.2.1.1.2. Ruang Lingkup

Ruang lingkup berfungsi untuk memberikan batasan dari rencana keberlangsungan bisnis karena pada penelitian ini hanya mencakup salah tiga dari seluruh fungsional bisnis yang

ada pada PDAM. Berikut ini fungsional bisnis PDAM Surya Sembada Kota Surabaya:

Tabel 6.2 Ruang Lingkup Fungsional dan Proses Bisnis

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi
Keuangan (Rekening & Penagihan)	Pengawasan rekening dan penerbitan penagihan
	Penagihan rekening swasta
	Penagihan rekening pemerintah
	Penagihan rekening pendapatan lain-lain
Pelayanan	Melakukan survey terkait lokasi pemasangan pada pelanggan
	Pembuatan RAB
	Customer Installation
	Pengelolaan Laporan Keluhan Pelanggan
	Penanganan Keluhan
Teknologi Sistem Informasi	Melakukan pengawasan instalasi, perawatan dan perbaikan terhadap infrastruktur TI (Hardware dan Jaringan)
	Melakukan pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)
	Disaster Recovery Center
	Penyediaan layanan email dan sistem informasi
	Melakukan evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;
	Melakukan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan
	Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi
	Melakukan pengawasan kegiatan *helpdesk support*.

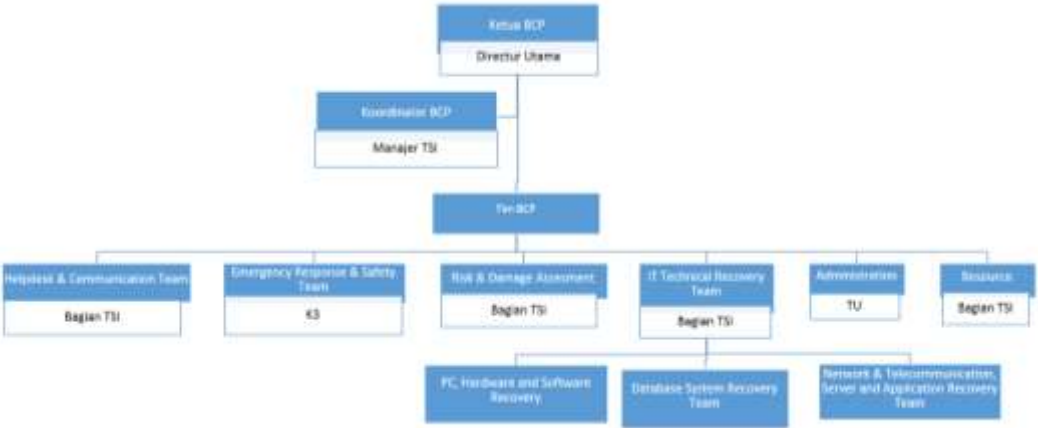
Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi
	Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan

6.2.1.1.3. Peran Manajemen dan Sumber Daya

Sesuai dengan metode Yusrida, pembentukan struktur Komite BCP dilakukan untuk dapat mengoptimalkan rencana keberlangsungan bisnis yang telah dibuat. Komite BCP ini dapat memastikan masing-masing peran dan tanggung jawab tiap bagian terhadap adanya perencanaan keberlansungan bisnis.

Peran Manajemen

Dalam melakukan pembuatan struktur komite BCP ini, peneliti melakukan konsultasi dan konfirmasi pada pihak manajemen yang diwakilkan oleh bagian Teknologi dan Sistem Informasi pada PDAM Surya Sembada Kota Surabaya. Berikut ini adalah komite BCP PDAM Surya Sembada Kota Surabaya.



Gambar 6.1 Struktur Komite BCP PDAM Surya Sembada Kota Surabaya

Berikut merupakan tugas dan tanggung jawab dari masing masing peran yang terdapat dalam komite BCP:

A. Ketua BCP

- Bertanggung jawab untuk meninjau kembali BCP setiap periode waktu tertentu
- Mengawasi berjalannya proses BCP
- Memimpin rapat/*briefing* komite BCP

B. Koordinator BCP

- Bertanggung jawab dalam pengembangan BCP
- Melaksanakan rapat koordinasi saat adanya gangguan kritis
- Melakukan pelatihan dan pengujian sesuai dengan BCP

C. Tim BCP

- Mengawasi kesesuaian pelaksanaan teknis BCP dengan perencanaan yang telah dibuat
- Memberikan arahan teknis kepada seluruh tim.

D. Helpdesk & Communication Team

- Menerima laporan/peringatan dari peronel, senior management ataupun *security* di tempat terjadinya insiden.
- Memberitahu tim BCP ketika ada gangguan untuk menjalankan rencana dan prosedur pemulihan
- Menyediakan informasi yang cepat akurat dan konsisten kepada *stakeholder* (staf, manajemen, partner bisnis eksternal, pelanggan, publik, vendor dll)

E. Emergency Response & Safety

- Melindungi nyawa, aset dan lingkungan segera setelah terjadinya bencana

- Melakukan evakuasi dan penyelamatan secara langsung (jika memang diperlukan).
- Membantu memastikan keselamatan kerja saat gangguan dan pemulihan
- Melakukan penyelamatan terhadap aset-aset kritis
- Melakukan koordinasi dengan pemadam kebakaran, kepolisian, rumah sakit dan pihak terkait

F. Risk & Damage Assesment

- Melakukan penilaian terhadap dampak gangguan dan kerugian yang didapatkan
- Melakukan penilaian dan pengontrolan terhadap risiko
- Mengklasifikasi gangguan yang terjadi berdasarkan penilaian yang telah dilakukan.
- Memperkirakan waktu pemulihan sesuai waktu pemulihan yang telah diperkirakan

G. IT Technical Recovery Team

Tim ini bertugas untuk menentukan opsi pemulihan yang terbaik untuk menyelesaikan masalah yang terjadi. Melakukan pemulihan dam restorasi infrastruktur TI yang terdiri atas :

- Network & telecommunication, server and application recovery team

Tim ini bertugas memastikan secara teknis hal-hal terkait jaringan komputer, server, telekomunikasi serta sistem operasi dan perangkat lunak pendukung layanan TI dapat berfungsi dengan baik pada lokasi alternatif ketika bencana terjadi maupun ketika proses restorasi pada lokasi utama.

- Database system recovery team

Tugas tim ini adalah melakukan restorasi terhadap database sesuai dengan backup terakhir pada masing-masing sistem

informasi yang ada baik pada lokasi alternatif ketika bencana serta pada lokasi utama ketika proses pemulihan

- PC, hardware and software recovery

Tugas tim ini adalah melakukan perbaikan dan restorasi terhadap PC, pernagkat keras beserta perangkat lunak pendukung dapat berfungsi dengan normal baik pada lokasi alternative ketika bencana maupun pada lokasi utama ketika proses pemulihan.

H. Administration

- Membuat dokumentasi terkait gangguan dan penanganannya
- Melakukan pencatatan pengeluaran

I. Resource

- Melakukan penilaian terhadap kebutuhan mendadak dari masing-masing unit bisnis
- Memastikan sumber daya dan peralatan yang dibutuhkan didapatkan tepat waktu
- Melakukan mobilisasi sumber daya, peralatan dan perlengkapan

Sumber Daya

Sumber daya diperlukan pada pelaksaan BCP untuk dapat memastikan bahwa proses berjalan dengan lancar dan sesuai dengan perencanaan. Untuk itu perusahaan perlu mengidentifikasi sumber daya perangkat dan ketersediaan infrastruktur yang dapat menunjang operasional saat terjadinya gangguan maupun bencana. Sehingga nantinya diharapkan proses BCP dapat berjalan lancar dengan ketersediaan perangkat – perangkat ini. Identifikasi sumber daya ini dilakukan dengan melakukan konsultasi pada Bagian TI serta menyesuaikan dengan strategi BCP yang dibuat. Berikut

merupakan perangkat keras kritikal yang dibutuhkan dalam melakukan perencanaan keberlangsungan bisnis.

Tabel 6.3 Perangkat Keras yang dibutuhkan

No	Sumber Daya
1	Server Cadangan
2	Genset
3	UPS
4	Alat komunikasi
5	PC Cadangan
6	Printer Cadangan
7	Laptop
8	Remote data storage
9	Tape backup
10	Unit disk/DASD
11	Telepon line
12	Modem portable
13	Kamera
14	Ruang meeting
15	Brankas
16	Cabinet
17	Peralatan Pertukangan
18	Peralatan keselamatan kerja
19	Peralatan forensik fisik
20	Ruangan dengan jaringan internet dan telekomunikasi serta fasilitas listrik

Berikut adalah dokumentasi serta perangkat penunjang yang dibutuhkan dalam perencanaan keberlangsungan bisnis teknologi informasi pada PDAM Surya Sembada Kota Surabaya.

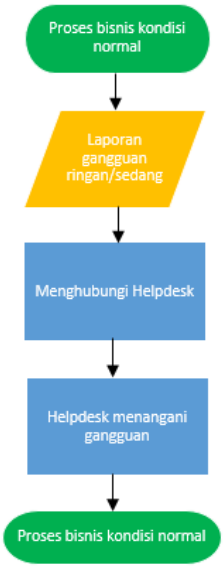
Tabel 6.4 Perangkat Penunjang BCP

No.	Daftar Perangkat
1.	Dokumen Daftar Aset TI
2.	Portofolio Aplikasi
3.	Dokumentasi Pengembangan dan Pengujian Aplikasi
4.	Checklist laporan kondisi aset TI
5.	Kebijakan Keamanan Fisik Infrastruktur TI
6.	Prosedur Monitoring dan Pemeliharaan Data Center
7.	Kebijakan Pengunjung Ruang Server
8.	Prosedur Monitoring dan pemeliharaan UPS/Generator set
9.	Prosedur Penanganan Kebakaran
10	Prosedur Backup dan Restore Data
11	Prosedur Pengembangan dan Pengujian Aplikasi
12	Prosedur Pengelolaan Layanan TI
13	Prosedur Penanganan Gangguan Jaringan
14	Prosedur Penanganan Gangguan Database

No.	Daftar Perangkat
15	Prosedur Penanganan Gangguan Perangkat Keras
16	Prosedur Penanganan virus dan malware
17	Prosedur Pemulihan Pasca Bencana
18	Prosedur Pengujian Rencana Keberlangsungan Bisnis
19	Prosedur Pelaporan Gangguan
20	Prosedur Penanganan gangguan dan pemulihan
21	Laporan dan Dokumentasi Penanganan Gangguan dan Pemulihan
22	Daftar kontak darurat
23	Daftar Vendor
24	Modul pelatihan BCP

6.2.1.1.4. Alur Komunikasi

Dalam rencana keberlangsungan bisnis akan ditetapkan alur komunikasi untuk dapat menjamin kelancaran proses BCP yang telah direncanakan. Alur komunikasi ini merupakan gambaran proses komunikasi yang harus dilakukan untuk masing masing peran. Selain itu diperlukan adanya pengaturan struktur pemberian perintah dan tugas antar peran.



Gambar 6.2 Alur Komunikasi Gangguan Ringan

Berikut adalah alur komunikasi saat terjadi gangguan kecil/sedang. Berikut merupakan penjelasan mengenai alur komunikasi saat ada gangguan ringan/sedang:

1. Alur ini mulai dilakukan saat terjadi gangguan yang menimpa salah satu sistem pada fungsional bisnis, namun

gangguan yang terjadi tidak mengganggu proses bisnis kritis dan tergolong ringan.

2. Dalam mengatasi gangguan tersebut, yang dapat dilakukan adalah melapor kepada layanan helpdesk kemudian layanan helpdesk akan menjalankan prosedur yang sesuai untuk menangani gangguan.

Sedangkan untuk **gangguan yang memiliki dampak kerusakan tinggi atau termasuk bencana** maka alur yang dijalankan adalah sebagai berikut :

Gambar 6.3 Alur Komunikasi Gangguan Besar

Berikut merupakan penjelasan mengenai alur komunikasi saat ada gangguan/bencana :

1. Alur dimulai ketika terjadi gangguan atau bencana pada teknologi informasi yang menyebabkan beberapa fungsional bisnis dan proses bisnis terganggu, membutuhkan waktu dalam memulihkan, perlu adanya penggantian infrastruktur.
2. Selanjutnya adalah menjalankan strategi saat terjadi gangguan yaitu alur penanganan saat terjadi gangguan berdasarkan peran dan tanggung jawab komite BCP masing-masing **(**peran dan tanggung jawab terdapat pada **bagian 6.2.1.13..Peran Manajemen)** :

Tabel 6.5 Strategi Saat Terjadi Gangguan

Menjalankan alur penanganan saat terjadi gangguan
1. Notifikasi & respon awal a. Menerima laporan/peringatan dari peronel, senior management ataupun security di tempat terjadinya insiden. b. Menghubungi pihak terkait seperti pemadam kebakaran atau vendor apabila dibutuhkan c. Melakukan evakuasi dan penyelamatan secara langsung (jika memang diperlukan). d. Menghubungi pihak terkait jika kondisi sudah sangat berbahaya seperti pemadam kebakaran, pihak kepolisian, rumah sakit dll.
2. **Identifikasi gangguan** a. Melakukan identifikasi terhadap insiden yang terjadi yaitu obyek, penyebab dan dampak pada aset TI. b. Melakukan pemeriksaan dan investiasi jika terdapat pelaku penyebab kerusakan. Invesstigasi dilakukan dengan memeriksa personel, aset terkait atau data-data hasil monitoring untuk dapat dianalisa.

c. Melakukan penilaian terhadap dampak gangguan dan kerugian yang didapatkan d. Melakukan penilaian terhadap risiko keselamatan kerja e. bisnis serta aset-aset yang mengalami kerusakan. f. Mengklasifikasi gangguan yang terjadi
3. Deklarasi gangguan a. Menentukan opsi pemulihan dan restorasi terbaik yang telah di deskripsikan pada strategi pemulihan b. Melakukan perhitungan biaya
4. Pemulihan a. Mempersiapkan pemulihan berdasarkan waktu pemulihan dan strategi yang dipilih b. Mempersiapkan kebutuhan pemulihan c. Menjalankan prosedur penanganan gangguan dan pemulihan serta melakukan perbaikan terhadap aset yang mengalami kerusakan. Jika kerusakan dianggap sangat parah maka menggunakan aset cadangan untuk dapat melanjutkan proses bisnis d. Melakukan langkah-langkah perlindungan aset TI seperti pengamanan data dengan melakukan backup, menonaktifkan sistem sementara apabila diperlukan, pengecekan data dan infrastruktur. e. Melakukan validasi dan konfirmasi bahwa aset atau sistem telah berjalan dengan normal Dibuat. **(selengkapnya pada Strategi saat gangguan)**

Setelah perbaikan dan pemulihan dilakukan, selanjutnya adalah melakukan validasi dan konfirmasi terhadap sistem agar dapat

memastikan bahwa sistem dapat benar-benar pulih dan proses bisnis dapat melanjutkan operasionalnya.

Alat komunikasi darurat merupakan suatu perangkat yang tersedia untuk dapat memastikan bahwa alur komunikasi saat terjadinya bencana dapat dilakukan dengan baik dan lancar. Untuk itu perusahaan harus mendaftar ketersediaan dari alat-alat komunikasi yang digunakan saat kondisi darurat. Berikut merupakan alat komunikasi darurat yang disediakan oleh tim komite BCP.

Tabel 6.6 Daftar Alat Komunikasi Darurat

Daftar Alat Komunikasi Darurat
1. Telepon
2. Email
3. Telepon Genggam

6.2.2. Fase 2 – Implementasi

Pada fase implementasi, perusahaan akan melakukan implementasi perencanaan untuk dapat menyusunan perencanaan keberlangsungan bisnis. Dalam fase ini ada beberapa tahapan antara lain adalah (1) analisis risiko, (2) analisis dampak bisnis, (3) penyusunan strategi keberlangsungan bisnis dan (4) pelatihan karyawan.

6.2.2.1. Analisis Risiko

Dalam melakukan tahapan analisis risiko sesuai dengan detil aktivitas yang ada pada metodologi BCP, dilakukan aktivitas identifikasi kemungkinan terjadinya risiko dan penilaian risiko. Pada implementasi BCP di PDAM Surya Sembada Kota Surabaya, identifikasi risiko menggunakan metode OCTAVE sedangkan penilaian risiko dilakukan dengan metode FMEA. Analisis risiko diperlukan untuk mengetahui risiko mana yang memiliki dampak paling tinggi sehingga jika risiko terjadi dampak yang diakibatkan pada proses bisnis yang sedang berjalan dapat dikontrol dan diminimalisir.

6.2.2.1.1. Identifikasi Risiko dengan OCTAVE

Pada analisis risiko metode OCTAVE digunakan dengan tujuan agar dapat mengidentifikasi kemungkinan risiko, kelemahan dan ancaman apa yang dapat terjadi pada aset TI yang dimiliki oleh organisasi. Identifikasi risiko dilakukan dengan mengikuti dua fase pada metode OCTAVE sebagai berikut :

Tabel 6.7 Identifikasi Risiko dengan OCTAVE

Fase	Luaran
OCTAVE Fase 1 - *Build Asset Based Threat Profile* (Membangun aset berdasarkan ancaman profil)	Daftar Aset Kritis
	Daftar Kebutuhan Keamanan Aset Kritis
	Daftar Ancaman Terhadap Aset Kritis

	Daftar Praktik Keamanan yang Dilakukan Organisasi
	Daftar Kelemahan Teknis Organisasi Terkait TI
OCTAVE Fase 2 - *Identify Infrastructure Vulnerabilities* (Mengidentifikasi Kelemahan Infrastruktur TI)	Daftar Komponen Utama
	Daftar Kerentanan Teknologi
	Daftar Risiko untuk Aset Kritis

Fase 1 dan Fase 2 diterapkan pada saat wawancara untuk menggali informasi sehingga hasil dari wawancara tersebut digunakan untuk melakukan penilaian risiko selanjutnya. Setiap tahapan memiliki *input* yang didapatkan dari hasil wawancara yang terlampir pada lampiran dan telah dilakukan verifikasi hasil risiko.

OCTAVE Fase 1 - *Build Asset Based Threat Profile*

Tabel 6.8 Daftar Aset Kritis

Daftar Aset Kritis Organisasi	
Hardware	PC dan Laptop
	Server dan Storage
	Genset
	UPS
Software	Billing
	Arsip Digital
	Geographic Information System (GIS)
Network	Switch
	Router
	Access Point
	Media transmisi (kabel jaringan)
Data	Database Pelanggan Database Keuangan
People	Staff TSI

	Pegawai Non-TI

Setelah melakukan identifikasi dari aset kritis TI, akan dilakukan identifikasi kebutuhan keamanan dari masingmasing aset. Hal ini dilakukan nantinya untuk dapat mengetahui apa saja yang dibutuhkan organisasi Berikut merupakan kebutuhan keamanan aset kritis organisasi.

Tabel 6.9 Kebutuhan Keamanan Aset Kritis

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset	Deskripsi
Hardware	PC dan Laptop	Confidentiality (kerahasiaan)	• Adanya hak akses dan otorisasi
		Integrity (Integritas)	• Adanya hak akses dan otorisasi • Adanya antivirus dan firewall • adanya antivirus
		Availability (Ketersediaan)	• adanya PC cadangan • Adanya genset untuk sumber listrik cadangan
	Server dan Storage	Confidentiality (kerahasiaan)	• Adanya perangkat kontrol akses ruang server • pembatasan pengunjung • menggunakan authentication berlapis
		Integrity (Integritas)	• Adanya antivirus dan firewall
		Availability (Ketersediaan)	• Adanya server cadangan

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset	Deskripsi
			• Adanya genset untuk sumber listrik cadangan
	Genset	Availability (Ketersediaan)	• Genset harus tersedia pada saat diperlukan.
	UPS	Availability (Ketersediaan)	• UPS harus tersedia pada saat diperlukan.
Software	Billing	Confidentiality (kerahasiaan)	• Adanya autentikasi
		Integrity (Integritas)	• Adanya perbedaan hak akses untuk setiap posisi user (Multilevel user) • Adanya autentikasi
		Availability (Ketersediaan)	Software selalu dapat diakses saat dibutuhkan.
	Arsip Digital	Confidentiality (kerahasiaan)	Adanya autentikasi
		Integrity (Integritas)	Adanya perbedaan hak akses untuk setiap posisi user (Multilevel user) Adanya autentikasi
		Availability (Ketersediaan)	Software selalu dapat diakses saat dibutuhkan.
	Geographic Information System (GIS)	Confidentiality (kerahasiaan)	Adanya autentikasi
		Integrity (Integritas)	• Adanya perbedaan hak akses untuk setiap posisi user (Multilevel user) • Terdapat validasi untuk input data dan password

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset	Deskripsi
		Availability (Ketersediaan)	Software selalu dapat diakses saat dibutuhkan.
Network	Router	Confidentiality (kerahasiaan)	• Peletakkan router pada tempat yang tidak mudah terjangkau dan diberi pelindung • Menggunakan kontrol akses dengan password • Menggunakan teknologi enkripsi
		Integrity (Integritas)	• Hanya pegawai dengan hak akses yang bisa mengkonfigurasi router. • menggunakan system filter IP address kepada remote device yang memang diberikan akses saja
		Availability (Ketersediaan)	Adanya genset untuk sumber listrik cadangan
	Switch	Confidentiality (kerahasiaan)	• Peletakkan switch pada tempat yang tidak mudah terjangkau dan diberi pelindung • Menggunakan kontrol akses dengan password Menggunakan teknologi enkripsi
		Integrity (Integritas)	• Hanya pegawai dengan hak akses yang bisa mengkonfigurasi router.

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset	Deskripsi
			menggunakan system filter IP address kepada remote device yang memang diberikan akses saja
		Availability (Ketersediaan)	Adanya genset untuk sumber listrik cadangan
	Access Point	Confidentiality (kerahasiaan)	• Peletakkan acces point pada tempat yang tidak mudah terjangkau dan diberi pelindung • Menggunakan kontrol akses dengan password • melakukan enkripsi
		Integrity (Integritas)	• Hanya pegawai dengan hak akses yang bisa mengkonfigurasi router. menggunakan system filter IP address kepada remote device yang memang diberikan akses saja
		Availability (Ketersediaan)	Adanya genset untuk sumber listrik cadangan
	Media transmisi (kabel jaringan)	Confidentiality (kerahasiaan)	Kabel diletakkan pada tempat yang tidak mudah terjangkau dan dilengkapi dengan case.
		Availability (Ketersediaan)	Kabel dilengkapi dengan case
Data	Database Pelanggan Database	Confidentiality (kerahasiaan)	Adanya autentikasi pada sistem database
		Integrity (Integritas)	• melakukan enkripsi data • menggunakan antivirus

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset	Deskripsi
	Keuangan		
		Availability (Ketersediaan)	Server harus selalu menyala agar data dapat diakses
People	Staff TSI	Confidentiality (kerahasiaan)	• pembatasan hak akses yang berbeda (multi level user) • memberikan kebijakan mengenai password user
		Integrity (Integritas)	memberikan sosialisasi mengenai social engineering
		Availability (Ketersediaan)	Terdapat kebijakan kehadiran dan kontrak
	Pegawai Non-TI	Confidentiality (kerahasiaan)	• pembatasan hak akses yang berbeda (multi level user) • memberikan kebijakan mengenai password user
		Integrity (Integritas)	memberikan sosialisasi mengenai social engineering
		Availability (Ketersediaan)	Terdapat kebijakan kehadiran dan kontrak

Setelah melakukan identifikasi kebutuhan keamanan akan dilakukan identifikasi ancaman yang dikategorikan berdasarkan lingkungan, manusia, infrastruktur dan ancaman spesifik terkait TI. Berikut merupakan daftar ancaman TI yang kemungkinan bisa terjadi pada organisasi.

Tabel 6.10 Daftar Ancaman TI

Ancaman Dari Lingkungan
Banjir
Badai / Hujan Lebat
Kilat dan Petir
Gempa Bumi

Hewan pengerat
Suhu dan kelembababn tidak stabil
Ancaman Dari Manusia
Kebakaran
Penyalahgunaan Hak Akses
Pencurian Data
Sabotase/ Hacking
Kelalaian (update, salah input)
Ketidakhadiran (keterbatasan sumber daya)
Pemadaman Listrik
Kesalahan konstruksi gedung
Kesalahan koding
Ancaman Dari Infrastruktur
Network
Kerusakan perangkat
Trouble pada sistem
Gangguan pada jaringan
Kabel LAN terputus
Sullit mendeteksi gangguan
Kesalahan konfigurasi
Hardware
Server down
Server Overheat
Kerusakan perangkat
Kesalahan konfigurasi
Storage corrupt
Software
Virus/Malware
Trouble
Data Corrupt
Kesalahan instalasi dan konfigurasi
Konsletting

Setelah mengetahui ancaman-ancaman apa saja yang dapat terjadi pada aset TI maka langkah selanjutnya adalah dengan mengidentifikasi praktik keamanan apa saja yang telah dilakukan oleh organisasi untuk mempersiapkan diri dari ancaman. Hal ini juga dapat membantu untuk penentuan nilai

deteksi pada penilaian risiko. Berikut adalah daftar praktik keamanan yang telah diterapkan oleh organisasi.

Tabel 6.11 Praktik Keamanan Aset Kritis

Jenis Aset IT	Nama Aset IT	Praktik Kemanan	Pihak yang Bertanggung Jawab
Hardware	PC dan Laptop	Memasang Antivirus Memiliki Firewall Melakukan perawatan secara rutin	Teknologi Sistem Informasi
	Server dan Storage	Kebijakan Hak Akses Ruang server (data center) memiliki sistem pengukur suhu (Presission Cooling System) Ruang server (data center) memiliki sistem pendeteksi kebakaran (Smoke Detector) Ruang server (data center) memiliki CCTV Ruang server (data center) memiliki finger print untuk sistem keamanan pada pintu masuk Menggunakan genset sebagai sumber tenaga cadangan Setiap hari melakukan backup pada data center Terdapat fire extinguisher untuk memadamkan api Dilakukan backup setiap hari	Teknologi Sistem Informasi

Jenis Aset IT	Nama Aset IT	Praktik Kemanan	Pihak yang Bertanggung Jawab
	Genset	Dilakukan pengecekan dan pemeliharaan secara rutin	Teknologi Sistem Informasi
	UPS	Membatasi orang yang masuk ke ruang data center Dilakukan pengecekan dan pemeliharaan secara rutin	Teknologi Sistem Informasi
Software	Billing	Terdapat perbedaan hak akses Pembatasan waktu akses SIM termasuk proses timeouts dan otomatis logout aplikasi mobile untuk data pelanggan tidak akan di tampilkan nama dan alamat	Teknologi Sistem Informasi
	Arsip Digital	Terdapat perbedaan hak akses Pembatasan waktu akses SIM termasuk proses timeouts dan otomatis logout aplikasi mobile untuk data pelanggan tidak akan di tampilkan nama dan alamat	Teknologi Sistem Informasi
	Geographic Information System (GIS)	Terdapat perbedaan hak akses Pembatasan waktu akses SIM termasuk proses timeouts dan otomatis logout aplikasi mobile untuk data pelanggan tidak akan di tampilkan nama dan alamat	Teknologi Sistem Informasi

Jenis Aset IT	Nama Aset IT	Praktik Kemanan	Pihak yang Bertanggung Jawab
Network	Switch	Meletakkan switch pada lokasi tersembunyi Melakukan pengecekan dan pemeliharaan rutin terhadap switch	Teknologi Sistem Informasi
	Router	Meletakkan router pada lokasi tersembunyi Melakukan pengecekan dan pemeliharaan rutin terhadap router	Teknologi Sistem Informasi
	Access Point	Meletakkan pada lokasi tersembunyi Melakukan pengecekan dan pemeliharaan rutin terhadap router	Teknologi Sistem Informasi
	Media transmisi (kabel jaringan)	Telah menerapkan manajemen kabel TIA 942 Meletakkan kabel ditempat tersembunyi Terdapat sistem monitoring	Teknologi Sistem Informasi
Data	Database Pelanggan Database Keuangan	Melakukan pembaharuan lisensi antivirus setiap tahun Melakukan database setiap hari pada akhir hari	Teknologi Sistem Informasi
People	Staff TSI	Prosedur dan kebijakan	Teknologi Sistem Informasi
	Pegawai Non-TI	Prosedur dan kebijakan	Teknologi Sistem Informasi

Selain praktik keamanan organisasi, terdapat pula beberapa kelemahan organisasi terkait keamanan teknologi informasi yang didapatkan saat wawancara. Kelemahan akan menjadi masukan untuk dapat menganalisa risiko maupun penyebab risiko yang dapat terjadi. Berikut merupakan daftar kelemahan organisasi.

Tabel 6.12 Kelemahan Aset Kritis

Kategori	Kelemahan
Hradware	*mirroring database* (cadangan) masih pada pihak ketiga
	Belum memiliki kebijakan terkait keamanan untuk ruang penempatan aset TI
Software	Tidak melakukan pengawasan pada transaction log

OCTAVE Fase 2 – *Identify Infrastructure Vulnerabilities*

Setelah melakukan fase 1 selanjutnya adalah masuk pada fase dimana dilakukan evaluasi terhadap komponen utama pada setiap aset kritis. Dari proses identifikasi komponen utama maka akan ditinjau kelemahannya. Output yang dihasilkan dari fase ini nantinya adalah tabel komponen utama dan tabel kerentanan teknologi.

Tabel 6.13 Komponen Utama Aset TI

Server dan Storage	
Server dan storage menyimpan semua data-data penting PDAM Surya Sembada Kota Surabaya.	
Komponen Utama	Sistem Operasi Aliran listrik Network Connection Genset UPS Antivirus

	Presission Cooling System Firewall
Jaringan	
Jaringan dan komponen-komponen pendukung yang ada di PDAM Surya Sembada Kota Surabaya.	
Komponen Utama	Switch Access Point Aliran Listrik Router Firewall Media Transmisi (Kabel)
Software	
Sistem informasi kritis yang dikembangkan oleh TSI dan aplikasi-aplikasi yang digunakan oleh bagian keuangan, pelayanan dan TSI.	
Komponen Utama	Server Sistem Operasi Antivirus Dokumentasi PC
Data	
Data-data yang penting seperti data pelanggan, data keuangan dan data penggunaan air.	
Komponen Utama	Sistem Database Network Connection Administrator Databbase Storage Server Aliran listrik UPS dan Genset
PC/Laptop	
PC dan laptop yang digunkan oleh PDAM Surya Sembada Kota Surabaya.	
Komponen Utama	CPU,Monitor, keyboard dan mouse Network Connection Firewall Antivirus Sistem Operasi Aliran listirk Genset dan UPS

People	
Sumber daya manusia terdiri atas tim TSI dan pegawai non TI.	
Komponen Utama	Pengetahuan dan ketrampilan

Setelah mengidentifikasi komponen utama yang terdapat pada aset kritis, selanjutnya akan dilakukan identifikasi ancaman untuk masing-masing komponen utama aset kritis. Tujuannya adalah untuk dapat melihat kerentanan pada aset kritis dengan lebih dalam. Berikut merupakan kemungkinan ancaman terhadap aset kritis organisasi.

Tabel 6.14 Ancaman Pada Aset Kritis

Nama Aset Kritis	Komponen Utama Aset Kritis	Ancaman pada Aset Utama berdasarkan Komponen
Server dan Storage	Sistem Operasi	Kegagalan sistem operasi
	Perangkat keras	Kerusakan komponen hard drive, mother board, RAM Kesalahan konfigurasi System overload (request terlalu banyak) / peak time
	Firewall	Hacker DOS Attack
	Network Connection	Jaringan mengalami trouble
	Genset dan UPS	Kerusakan UPS dan genset
	Antivirus	Virus
	Presission Cooling System	Kerusakan sistem pengatur suhu
	Aliran listrik	Fluktuasi arus listrik/Konsletting
Jaringan	Switch	Kerusakan fisik Kesalahan konfigurasi
	Access Point	Kerusakan fisik Kesalahan konfigurasi
	Aliran Listrik	Pemadaman listrik
	Router	Kerusakan fisik Kesalahan konfigurasi

Nama Aset Kritis	Komponen Utama Aset Kritis	Ancaman pada Aset Utama berdasarkan Komponen
	Firewall	Spoofing dan Sniffing
	Media Transmisi (Kabel)	Media transmisi (kabel) tergigit tikus
	antivirus	Virus dan malware
Software	Server	Server down
	Sistem Operasi	Kesalahan instalasi dan konfigurasi
	Antivirus	Virus dan malware
	Dokumentasi	Belum melakukan testing secara menyeluruh Tidak ada dokumentasi selama pengembangan software
	PC	Kesalahan instalasi dan konfigurasi Perangkat keras yang tidak kompatibel
Data	Sistem Database	Data Corrupt SQL Injection Logical error (salah query) Kegagalan sistem database Belum menerapkan manajemen tabel untuk database
	Network Connection	Gangguan pada jaringan
	Administrator Database	Social Engineering Penyalahgunaan dan pelanggaran hak akses
	Storage	Kerusakan perangkat keras (storage dan server) Kapasitas memori penuh
	Server	Gangguan pada jaringan
	UPS dan Genset	Kerusakan UPS dan Genset
	antivirus	Virus dan malware
	firewall	Hacker (pencurian dan modifikasi data)

Nama Aset Kritis	Komponen Utama Aset Kritis	Ancaman pada Aset Utama berdasarkan Komponen
PC	CPU,Monitor, keyboard dan mouse	Kerusakan komponen Usia yang sudah tua dan usang Kesalahan konfigurasi
	Firewall	Kesalahan konfigurasi
	Antivirus	Virus dan malware
	Sistem Operasi	Kesalahan konfigurasi
	Aliran listirk	Pemadaman listrik
Pegawai TSI	Pengetahuan	Kurang kompeten
Pegawai Non TSI	Pengetahuan	Kurang kompeten

Setelah melakukan identifikasi dan analisi risiko dengan menggunakan OCTAVE maka didapatkanlah daftar risiko sebagai berikut :

Tabel 6.15 Daftar Risiko dari Analisis Risiko Menggunakan OCTAVE

ID Risiko	Kategori Aset	Nama Aset	Penyebab Potensial	Risiko
1	Hardware	Server dan Storage	Kerusakan komponen utama	Server Down
2			Hacker	
3			Kesalahan konfigurasi	
4			System overload (request terlalu banyak) / peak time	
5			Gangguan jaringan	
6			Kegagalan sistem operasi	
7			Kerusakan sistem pengatur suhu	
8			Dos Attack	
9			Virus	

ID Risiko	Kategori Aset	Nama Aset	Penyebab Potensial	Risiko
10			Kerusakan UPS dan genset	
11			Bencana alam	
12			overheat	Kebakaran ruang server
13			Fluktuasi arus listrik/Konsletting	
14		PC & Laptop	Kerusakan komponen	Kerusakan PC
15			Virus dan malware	
16			Usia yang sudah tua dan usang	
17			Kesalahan konfigurasi	PC/Laptop tidak dapat beroperasi
18			Hacker	
19			Pemadaman listrik	
20	Jaringan	switch, router dan acces point	Kerusakan fisik infrastruktur jaringan (switch, router dan acces point)	Network Trouble
21		Kabel	Media transmisi (kabel) tergigit tikus	
22		switch, router dan acces point	Kesalahan konfigurasi	
23		Sistem jaringan	Virus dan malware	
24			Spoofing dan Sniffing	
25		switch, router dan acces point	Pemadaman listrik	
26	Software	GIS, Billing	Kesalahan instalasi dan konfigurasi	

ID Risiko	Kategori Aset	Nama Aset	Penyebab Potensial	Risiko
		dan		Software
27		Arsip	Virus dan malware	tidak dapat
28		Digital.	Perangkat keras yang tidak kompatibel	diakses
29			Server down	
30			Kesalahan koding	
31			Belum melakukan testing secara menyeluruh	Software tidak sesuai dengan kebutuhan
32			Tidak ada dokumentasi selama pengembangan software	
33	Data	Database	Data Corrupt	Kehilangan data
34		Pelanggan	Gangguan pada jaringan	Data tidak dapat diakses / tidak tersedia
35		Database	Virus dan malware	
36		Keuangan	Kerusakan perangkat keras (storage dan server)	
37			SQL Injection	
38			Logical error (salah query)	
39			Kegagalan sistem database	
40			Hacker (pencurian dan modifikasi data)	Data kehilangan integritas
41			Social Engineering	
42			Penyalahgunaan dan pelanggaran hak akses	
43			Kerusakan UPS dan Genset	Kegagalan Backup

ID Risiko	Kategori Aset	Nama Aset	Penyebab Potensial	Risiko
44			Belum menerapkan manajemen tabel untuk database	Database lambat untuk diakses
45			Kapasitas memori penuh	
46	SDM	TI	Kurang kompeten	Human Error / Pelanggaran
47		TI dan non TI	Tidak terdapat prosedur dan kebijakan terkait pengelolaan dan penggunaan aset	
48		TI dan non TI	Tidak adanya pengawasan / monitoring hak akses pada transaction log	

Dari hasil identifikasi risiko yang dilakukan dengan menggunakan metode OCTAVE didapatkan 48 risiko terkait teknologi informasi yaitu 3 untuk risiko terkait sumber daya manusia, 13 terkait data, 7 terkait *software*, 6 terkait jaringan, 13 terkait server dan storage serta 6 terkait PC dan laptop.

6.2.2.1.2. Penilaian Risiko

Penilaian risiko dilakukan dengan memberikan skor dampak, kemungkinan dan deteksi. Untuk setiap risiko yang muncul akan dilakukan perhitungan nilai nilai RPN (rish priority number), RPN nantinya merupakan skala untuk dapat menilai tingkat prioritas risiko. Berikut hasil penilaian risiko. Untuk justifikasi secara rinci terdapat **pada Lampiran F - Lampiran Penilaian Risiko**

Tabel 6.16 Hasil Penilaian Risiko dengan Menggunakan FMEA

Level Risiko	Risiko	Nama Aset	ID Risiko	Penyebab Kegagalan	S	O	D	RPN
Very High	Server Down	Server dan Storage	5	Gangguan jaringan	8	4	7	224
Very High	Human Error / Pelanggaran	TI dan non TI	48	Tidak adanya pengawasan / monitoring hak akses pada transaction log	7	4	8	224
Very High	Network trouble	switch, router dan acces point	20	Kerusakan infrastruktur jaringan (switch, hub,router, konektor kabel)	6	6	6	216
Very High	Data tidak dapat diakses / tidak tersedia	Database Keuangan dan database pelanggan	34	Gangguan pada jaringan	8	5	5	200
High		Billing, GIS dan Arsip Digital	29	Server down	8	6	4	192
High	Data kehilangan integritas	Database Keuangan dan database pelanggan	41	Social Engineering	6	6	5	180
High	Data kehilangan integritas	Database Keuangan dan database pelanggan	42	Penyalahgunaan dan pelanggaran hak akses	6	6	5	180
High	Network trouble	Sistem jaringan	24	Spoofing dan Sniffing	8	3	7	168
High	Software tidak dapat diakses	Billing, GIS dan Arsip Digital	30	Kesalahan koding	7	4	6	168

Level Risiko	Risiko	Nama Aset	ID Risiko	Penyebab Kegagalan	S	O	D	RPN
High	Server Down	Server dan Storage	7	Kerusakan sistem pengatur suhu	8	4	5	160
High	Kerusakan PC	PC & Laptop	14	Kerusakan komponen	6	5	5	150
High	Database lambat untuk diakses	Database Keuangan dan database pelanggan	44	Belum menerapkan manajemen tabel untuk database	5	5	6	150
High	Server Down	Server dan Storage	8	Dos Attack	8	3	6	144
High	Software tidak dapat diakses	Billing, GIS dan Arsip Digital	26	Kesalahan instalasi dan konfigurasi	4	6	6	144
High	Data tidak dapat diakses / tidak tersedia	Database Keuangan dan database pelanggan	37	SQL Injection	8	3	6	144
High	Network trouble	Sistem jaringan	23	Virus dan malware	8	4	4	128
High	Server Down	Server dan Storage	11	Bencana alam	10	2	6	120
High	Kebakaran ruang server	Server dan Storage	13	Fluktuasi arus listrik/Konsletting	10	3	4	120
High	Kerusakan PC	PC & Laptop	18	Hacker	5	4	6	120
High	Network trouble	switch, router dan acces point	22	Kesalahan konfigurasi	4	5	6	120
High	Software tidak sesuai dengan kebutuhan	Billing, GIS dan Arsip Digital	31	Belum melakukan testing secara menyeluruh	5	4	6	120

Level Risiko	Risiko	Nama Aset	ID Risiko	Penyebab Kegagalan	S	O	D	RPN
High	Software tidak sesuai dengan kebutuhan	Billing, GIS dan Arsip Digital	32	Tidak ada dokumentasi selama pengembangan software	5	4	6	120
High	Server Down	Server dan Storage	1	Kerusakan komponen utama	8	6	3	108
High	Server Down	Server dan Storage	2	Hacker	8	4	3	96
Medium	Server Down	Server dan Storage	6	Kegagalan sistem operasi	8	3	4	96
Medium	Network trouble	Kabel	21	Media transmisi (kabel) tergigit tikus	8	3	4	96
Medium	Software tidak dapat diakses	Billing, GIS dan Arsip Digital	27	Virus dan malware	6	4	4	96
Medium	Kehilangan data	Database Keuangan dan database pelanggan	33	Data Corrupt	8	4	3	96
Medium	Data tidak dapat diakses / tidak tersedia	Database Keuangan dan database pelanggan	35	Virus dan malware	8	4	3	96
Medium	Data tidak dapat diakses / tidak tersedia	Database Keuangan dan database pelanggan	36	Kerusakan perangkat keras (storage dan server)	8	4	3	96
Medium	Data tidak dapat diakses /	Database Keuangan dan	39	Kegagalan sistem database	8	4	3	96

Level Risiko	Risiko	Nama Aset	ID Risiko	Penyebab Kegagalan	S	O	D	RPN
	tidak tersedia	database pelanggan						
Medium	Server Down	Server dan Storage	10	Kerusakan UPS dan genset	6	3	5	90
Medium	Kerusakan PC	PC & Laptop	16	Usia yang sudah tua dan usang	6	3	5	90
Medium	Kerusakan PC	PC & Laptop	17	Kesalahan konfigurasi	3	5	6	90
Medium	Kebakaran ruang server	Server dan Storage	12	overheat	10	4	2	80
Medium	Human Error / Pelanggaran	Pegawai TI	46	Kurang kompeten	5	4	4	80
Medium	Server Down	Server dan Storage	3	Kesalahan konfigurasi	3	4	6	72
Medium	Data kehilangan integritas	Database Keuangan dan database pelanggan	40	Hacker (pencurian dan modifikasi data)	6	4	3	72
Low	Server Down	Server dan Storage	9	Virus	8	4	2	64
Low	Network trouble	switch, router dan acces point	25	Pemadaman listrik	3	4	5	60
Low	Database lambat untuk diakses	Database Keuangan dan database pelanggan	45	Kapasitas memori penuh	5	4	3	60
Low	Kerusakan PC	PC & Laptop	19	Pemadaman listrik	3	6	3	54
Low	Kegagalan Backup	Database Keuangan dan	43	Kerusakan UPS dan Genset	3	3	6	54

Level Risiko	Risiko	Nama Aset	ID Risiko	Penyebab Kegagalan	S	O	D	RPN
		database pelanggan						
Low	Kerusakan PC	PC & Laptop	15	Virus dan malware	6	4	2	48
Low	Server Down	Server dan Storage	4	System overload (request terlalu banyak) / peak time	5	3	3	45
Low	Software tidak dapat diakses	Billing, GIS dan Arsip Digital	28	Perangkat keras yang tidak kompatibel	5	3	3	45
Low	Data tidak dapat diakses / tidak tersedia	Database Keuangan dan database pelanggan	38	Logical error (salah query)	8	3	6	14
Low	Human Error / Pelanggaran	I dan non TI	47	Tidak terdapat prosedur dan kebijakan terkait pengelolaan dan penggunaan aset	4	6	6	14

Berdasarkan penilaian terhadap risiko yang telah dilakukan dengan metode FMEA, terdapat 4 risiko dengan level Very High yaitu server down karena gangguan pada jaringan, human error / pelanggaran karena tidak adanya pengawasan / monitoring hak akses pada transaction log, network trouble karena kerusakan fisik salah satu atau beberapa infrastruktur jaringan dan data tidak dapat diakses / tidak tersedia karena tidak adanya pengawasan hak akses pada transaction log. Serta terdapat 20 risiko dengan level high dimana risiko-risiko tersebut adalah software tidak dapat diakses, data kehilangan

integritas, network trouble, server down, kerusakan PC, kegagalan backup, data tidak dapat diakses / tidak tersedia, human error / pelanggaran, kebakaran ruang server, PC/laptop tidak dapat beroperasi dan software tidak sesuai dengan kebutuhan. Selain itu terdapat 14 risiko dengan level medium dan 10 risiko dengan level low.

Hasil penilaian risiko yang berupa risiko dengan nilai *very high* akan digunakan dalam pembuatan strategi yaitu mitigasi risiko untuk mengontrol dan meminimalisir risiko tersebut.

6.2.2.2. Analisis Dampak Bisnis

Analisis dampak bisnis bertujuan untuk menentukan prioritasi proses bisnis operasional yang paling dianggap kritis pada suatu perusahaan. Dalam melakukan analisis dampak bisnis, detil aktivitas dilakukan penyesuaian terhadap objek sehingga urutannya menjadi pendataan proses bisis perusahaan, analisa dampak gangguan, prioritasi proses bisnis, prioritasi layanan TI dan menentukan waktu pemulihan pada tiap layanan TI.

Keterkaitan antara BIA dengan analisis risiko dikarenakan hasil dari keduanya digunakan untuk mengembangkan rencana keberlangsungan bisnis yang sesuai. Hasil prioritasi dari analisis dampak gangguan digunakan untuk dapat melakukan prioritasi penanganan gangguan jika terjadi risiko pada proses bisnis tersebut. Penanganan gangguan selanjutnya akan berdasar pada alur dan strategi keberlangsungan bisnis yang telah ditentukan.

6.2.2.2.1. Pendataan proses bisnis perusahaan dan layanan TI yang mendukung

Berikut merupakan daftar proses bisnis perusahaan beserta dengan layanan TI yang mendukung proses bisnis tersebut.

Tabel 6.17 Daftar Proses Bisnis dan Layanan TI

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi	Sistem dan Layanan TI
Keuangan (Rekening & Penagihan)	Pengawasan rekening dan penerbitan penagihan	Billing (Rekening)
	Penagihan rekening swasta	Billing (PRS)
	Penagihan rekening pemerintah	Billing (PRP)
	Penagihan rekening pendapatan lain-lain	Billing (Kas)
Pelayanan	Pemasaran	Billing Informasi Pelanggan Billing MBD Billing PB Billing SMS Center Billing UPTIGA Billing Customer Service Billling Call Center Arsip Digital Aplikasi Foto Catat Meter
	Customer Installation	Billing Perencanaan
	Melakukan survey terkait lokasi pemasangan pada pelanggan	GIS (Sistem Informasi Geografis PDAM)
		Arsip Digital
		Billing Perencanaan
	Pembuatan RAB	GIS (Sistem Informasi Geografis PDAM)
		Arsip Digital
		Billing Perencanaan
	Pengelolaan Laporan Keluhan Pelanggan	Billing PTJSR Aplikasi Foto Materisasi
	Penanganan Keluhan	
Teknologi Sistem Informasi	Melakukan pengawasan instalasi, perawatan dan perbaikan terhadap	Service desk

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi	Sistem dan Layanan TI
	infrastruktur TI (Hardware dan Jaringan)	
	Melakukan pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)	-
	Disaster Recovery Center	Copy file
	Penyediaan layanan email dan sistem informasi	Email
	Melakukan evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;	-
	Melakukan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan	-
	Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi	-
	Melakukan pengawasan kegiatan *helpdesk support*.	Service desk
	Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan	-

6.2.2.2.2. Analisis Dampak Dari Adanya Gangguan

Analisis dampak gangguan merupakan proses penilaian dampak dari masing masing proses bisnis apabila terjadi risiko yang tidak diinginkan. Dampak ini dibagi menjadi tiga, dampak ditinjau dari aspek finansial, dampak ditinjau dari reputasi dan juga dampak ditinjau dari operasional. Analisis dampak

gangguan akan menjadi dasar dari prioritasi proses bisnis dan layanan TI. Berikut ini adalah tingkat keparahan kerugian jika terjadi gangguan dilihat dari finansial, reputasi dan operasional. Kriteria keparahan dampak finansial, reputasi dan operasional telah didiskusikan dan dikonfirmasikan dengan perwakilan pihak manajemen PDAM Surya Sembada Kota Surabaya yaitu Supervisor Teknologi Informasi.

Tabel 6.18 Kriteria Severity Level Dampak Finansial, Reputasi dan Operasional

Level	Dampak Finansial	Dampak Reputasi	Dampak Operasional
0 (none)	Bila tidak berdampak pada aspek finansial	Bila tidak berdampak pada aspek reputasi	Bila tidak berdampak pada operasional
1 (low)	Bila adanya penambahan biaya kurang dari 5% dari anggaran proses bisnis	Bila adanya penurunan yang sangat kecil dari reputasi perusahaan	Bila adanya penurunan hasil kurang dari 5% dari target proses bisnis
2 (medium)	Bila adanya penambahan biaya 5-10% dari anggaran proses bisnis	Bila adanya penurunan yang kecil dari reputasi perusahaan	Bila adanya penurunan hasil 5-10% dari target proses bisnis
3 (medium-high)	Bila adanya penambahan biaya 11-20% dari anggaran proses bisnis	Bila adanya penurunan yang sedang dari reputasi perusahaan	Bila adanya penurunan hasil 11-20% dari target proses bisnis
4 (high)	Bila adanya penambahan biaya 21-25% dari anggaran proses bisnis	Bila adanya penurunan yang tinggi dari reputasi perusahaan	Bila adanya penurunan hasil 21-25% dari target proses bisnis
5 (highest)	Bila adanya penambahan biaya lebih dari 25% dari anggaran proses bisnis	Bila adanya penurunan yang sangat tinggi dari reputasi perusahaan	Bila adanya penurunan hasil lebih dari 25% dari target proses bisnis

Dalam melakukan analisis dampak bisnis, dilakukan kegiatan wawancara serta kuesioner pada pengguna dan pengelola layanan TI yaitu bagian TSI dan bagian-bagian terkait. Hal tersebut guna memperoleh penilaian terhadap dampak finansial, reputasi dan operasional pada proses bisnis. **Untuk rekapitulasi kuesioner analisis dampak bisnis, dapat dilihat pada Lampiran C, D dan E.** Berikut merupakan hasil analisis dampak gangguan terhadap proses bisnis.

Tabel 6.19 Hasil Kuesioner Analisis Dampak Gangguan

Fungsional Bisnis	Proses bisnis terkait sistem	Dampak		
		Finansial	Reputasi	Operasional
Keuangan (Rekening & Penagihan)	Pengawasan rekening dan penerbitan penagihan	4	5	4
	Penagihan rekening swasta	3	4	3
	Penagihan rekening pemerintah	3	4	3
	Penagihan rekening pendapatan lain-lain	3	3	3
Pelayanan	Pemasaran	4	3	4
	Customer Installation	3	3	3
	Melakukan survey terkait lokasi pemasangan pada pelanggan	3	3	3
	Pembuatan RAB	3	3	3
	Pengelolaan Laporan Keluhan Pelanggan	2	2	2
	Penanganan Keluhan	2	2	2
Teknologi Sistem Informasi	Melakukan pengawasan instalasi, perawatan dan perbaikan terhadap	5	3	5

Fungsional Bisnis	Proses bisnis terkait sistem	Dampak		
		Finansial	Reputasi	Operasional
	infrastruktur TI (Hardware dan Jaringan)			
	Melakukan pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)	4	3	5
	Disaster Recovery Center	5	3	5
	Penyediaan layanan email dan sistem informasi	2	3	1
	Melakukan evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;	3	2	2
	Melakukan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan	3	3	3
	Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi	2	2	3
	Melakukan pengawasan kegiatan *helpdesk support*.	2	1	2
	Melakukan pengawasan pemeliharan dan pengembangan database sesuai	2	1	2

Fungsional Bisnis	Proses bisnis terkait sistem	Dampak		
		Finansial	Reputasi	Operasional
	perkembangan bisnis perusahaan			

6.2.2.2.3. Prioritisasi Proses Bisnis Perusahaan

Prioritisasi proses bisnis dilakukan untuk dapat mengetahui tingkat kepentingan dari masing masing proses bisnis yang terkait dengan layanan TI. Prioritasi didapatkan dari kuesioner analisis dampak gangguan. Berikut ini merupakan tingkat dari prioritasi proses bisnis yang didapatkan dari analisis dampak bisnis :

Tabel 6.20 Kriteria Tingkat Kritis Proses Bisnis

Tingkat Kritis	Definisi	Keterangan
Kritis	Proses bisnis dikategorikan kritis apabila proses bisnis ini memiliki dampak yang sangat besar apabila terjadi gangguan yaitu dampak finansial no 3 atau lebih serta dampak operasional dan reputasi no 4 atau lebih.	Dampak finansial nomor 3 adalah bila adanya penambahan biaya 11-20% dari anggaran proses bisnis. Sedangkan Dampak operasional nomor 4 adalah Bila adanya penurunan hasil 21-25% dari target proses bisnis dan Dampak reputasi nomor 4 adalah bila adanya penurunan yang tinggi dari reputasi perusahaan.
Penting	Proses bisnis dikategorikan penting apabila proses bisnis ini memiliki dampak yang tidak terlalu besar apabila terjadi gangguan yaitu dampak finansial no 1 – 2 serta dampak operasional dan reputasi no 1 – 3.	
Minor	Proses bisnis diaktegorikan minor apabila proses bisnis ini tidak memiliki dampak atau dampaknya hampir	

	tidak terasa saat terjadi gangguan yaitu dampak finansial, operasional serta reputasi no 0.	

Berikut merupakan prioritasi proses bisnis dan aktivitas terkait layanan TI :

Tabel 6.21 Hasil Prioritasi Proses Bisnis

Fungsional Bisnis	Proses Bisnis	Aktivitas terkait layanan TI	Kritikalitas
Keuangan	Pengawasan rekening dan penerbitan penagihan	• Menghitung kubik pemakaian air pelanggan • Upload data tagihan pelanggan ke switcher	Kritis
	Penagihan rekening swasta	Rekonsiliasi hasil tagihan(data update lunas pelanggan)	Kritis
	Penagihan rekening pemerintah	Rekonsiliasi hasil tagihan (data update lunas pelanggan)	Kritis
	Penagihan rekening pendapatan lain-lain	Menerima data dari bagian pelayanan (customer service	Penting
Pelayanan	Pemasaran	Melakukan pemasaran terhadap calon pelanggan	Kritis
	Customer Installation	Pemasangan rekening baru	Kritis
	Melakukan survey terkait lokasi pemasangan pada pelanggan	Melihat data pelanggan terkait geografis	Penting
		Mendokumentasikan jaringan pipa	
	Pembuatan RAB	Mengkalkukasi estimasi RAB	Penting

Fungsional Bisnis	Proses Bisnis	Aktivitas terkait layanan TI	Kritikalitas
		Melihat informasi calon pelanggan	
	Pengelolaan Laporan Keluhan Pelanggan	Menginputkan keluhan pelanggan	Penting
	Penanganan Keluhan	Melihat data keluhan pelanggan	Penting
Teknologi Sistem Informasi	Pengawasan instalasi, perawatan dan perbaikan terhadap infrastruktur TI (Hardware dan Jaringan)	Monitoring infrastruktur TI	Kritis
	Pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)	Monitoring dan konfiguras terkait keamanan jaringan dan infrastruktur TI	Kritis
	Disaster Recovery Center	*Copy file*	Kritis
	Penyediaan layanan email dan sistem informasi	Menyediakan layanan email dan sistem informasi	Penting
	Evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;	Melakukan monitoring dan pengembangan aplikasi	Penting
	Pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan	Melakukan pengembangan aplikasi baru	Penting
	Pengawasan *backup-restore* database utama dan pengamanan aplikasi	Melakukan backup	Penting

Fungsional Bisnis	Proses Bisnis	Aktivitas terkait layanan TI	Kritikalitas
	Pengawasan kegiatan *helpdesk support*.	Menangani keluhan dan *troubleshooting*	Penting
	Pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan	Monitoring dan pengembangan database	Penting

Berdasarkan hasil dari analisa dampak gangguan, maka prioritasi proses bisnis pada ketiga bagian pada PDAM Surya Sembada Kota Surabaya yaitu bagian Keuangan, Pelayanan dan TSI terdapat 8 proses bisnis yang dianggap kritis dari keseluruhan 19 proses bisnis dengan rincian 3 proses bisnis kritis pada fungsional bisnis keuangan yaitu pengawasan rekening dan penerbitan penagihan, penagihan rekening swasta dan penagihan rekening pemerintah. Kemudian 2 proses bisnis kritis pada fungsional bisnis pelayanan yaitu pemasaran dan customer installation serta 3 proses bisnis kritis pada fungsional bisnis TSI yaitu pengawasan instalasi, perawatan dan perbaikan terhadap infrastruktur TI (hardware dan jaringan), pengawasan keamanan terhadap infrastruktur TI (hardware dan jaringan) dan Disaster Recovery Center.

6.2.2.2.4. Prioritisasi dari layanan TI

Perusahaan perlu melakukan identifikasi layanan SI/TI beserta dengan melakukan prioritisasi tingkat kritis masing masing layanan. Tingkat dari prioritasi layanan SI/TI didapatkan dari wawancara dengan pihak TSI serta pertimbangan dari hasil prioritasi proses bisnis. Berikut merupakan prioritasi untuk masing masing layanan TI yang dimiliki oleh perusahaan.

Tabel 6.22 Hasil Prioritasi Layana TI

Sistem dan Layanan TI	Kritikalitas
Billing (Rekening)	Kritis
Billing (PRS)	Kritis
Billing (PRP)	Kritis
Billing (Kas)	Penting
Billing Informasi Pelanggan	Kritis
Billing MBD	Kritis
Billing PB	Kritis
Billing SMS Center	Kritis
Billing UPTIGA	Kritis
Billing Customer Service	Kritis
Billling Call Center	Kritis
Arsip Digital	Kritis
Aplikasi Foto Catat Meter	Kritis
GIS (Sistem Informasi Geografis PDAM)	Kritis
Billing Perencanaan	Kritis
Billing PTJSR	Penting
Aplikasi Foto Materisasi	Penting
Service desk	Penting
Copy file	Kritis
Email	Penting

Berdasarkan prioritasi layanan TI yang dilakukan terhadap 20 layanan TI yang terkait dengan proses bisnis pada bagian Keuangan, TSI dan Pelayanan, terdapat 15 layanan TI yang bersifat kritis pada PDAM Surya Sembada kota Surabaya yaitu Billing (Rekening), Billing (PRS), Billing (PRP), Billing Informasi Pelanggan, Billing MBD, Billing PB, Billing SMS Center, Billing UPTIGA, Billing Customer Service, Billling Call Center, Arsip Digital, Aplikasi Foto Catat Meter, GIS (Sistem Informasi Geografis PDAM), Billing Perencanaan dan Copy file. Sedangkan untuk 5 layanan TI sisanya dianggap penting.

6.2.2.2.5. Penentuan waktu pemulihan pada tiap layanan TI

Pada masing masing layanan TI yang mendukung proses bisnis akan dilakukan identifikasi waktu pemulihan apabila terjadi gangguan. Analisis waktu pemulihan dibagi menjadi tiga, yaitu sebagai berikut:

- *Maximum Tolerable Downtime* (MTD) merupakan jumlah waktu maksimal yang dapat ditoleransi oleh perusahaan terhadap ketidaktersediaan atau kegagalan proses bisnis, layanan dan aset atau jumlah waktu maksimal yang dimiliki oleh bagian perencanaan teknologi informasi untuk menyediakan layanan continuity system sampai sistem kembali tersedia (*available*).
- *Recovery Time Objective* (RTO) adalah jumlah waktu lumpuh maksimal untuk seluruh sumber daya sistem yang ada atau jumlah waktu yang ditentukan oleh perusahaan untuk mengembalikan (restored) proses bisnis, layanan, dan aset setelah bencana atau gangguan terjadi atau jumlah waktu yang dimiliki oleh bagian perencanaan teknologi informasi untuk menyediakan layanan continuity system sampai sistem kembali tersedia (*available*).
- *Recovery Point Objective* (RPO) adalah jumlah waktu yang diperlukan setelah terjadinya gangguan, untuk memulihkan data atau menyediakan layanan backup data setelah terjadinya gangguan. Berikut merupakan contoh hasil analisis waktu pemulihan untuk proses bisnis tertentu.

Tabel 6.23 Hasil Penentuan Waktu Pemulihan

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi	Sistem dan Layanan TI	MTD	RTO	RPO
Keuangan	Pengawasan rekening dan penerbitan penagihan	Billing (Rekening)	8 jam	<4 jam	4 jam
	Penagihan rekening swasta	Billing (PRS)	8 jam	<4 jam	4 jam
	Penagihan rekening pemerintah	Billing (PRP)	8 jam	<4 jam	4 jam

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi	Sistem dan Layanan TI	MTD	RTO	RPO
	Penagihan rekening pendapatan lain-lain	Billing (Kas)	8 jam	<4 jam	<24 jam
Pelayanan	Pemasaran	Billing Informasi Pelanggan	Kritis	8 jam	<4 jam
		Billing MBD	8 jam	<4 jam	<12 jam
		Billing PB	8 jam	<4 jam	<12 jam
		Billing SMS Center	8 jam	<4 jam	<12 jam
		Billing UPTIGA	8 jam	<4 jam	<12 jam
		Billing Customer Service	8 jam	<4 jam	<12 jam
		Billlling Call Center	8 jam	<4 jam	<12 jam
		Arsip Digital	8 jam	<4 jam	<12 jam
		Aplikasi Foto Catat Meter	8 jam	<4 jam	<12 jam
	Customer Installation	Billing Perencanaan	8 jam	<4 jam	<12 jam
	Melakukan survey terkait lokasi pemasangan pada pelanggan	GIS (Sistem Informasi Geografis PDAM)	24 jam	<12 jam	<48 jam
		Arsip Digital	24 jam	<12 jam	<48 jam
		Billing Perencanaan	24 jam	<12 jam	<48 jam
	Pembuatan RAB	GIS (Sistem Informasi Geografis PDAM)	24 jam	<12 jam	<48 jam

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi	Sistem dan Layanan TI	MTD	RTO	RPO
		Arsip Digital	24 jam	<12 jam	<48 jam
		Billing Perencanaan	24 jam	<12 jam	<48 jam
	Pengelolaan Laporan Keluhan Pelanggan	Billing PTJSR	24 jam	<12 jam	<48 jam
	Penanganan Keluhan	Aplikasi Foto Materisasi	24 jam	<12 jam	<24 jam
Teknologi Sistem Informasi	Melakukan pengawasan instalasi, perawatan dan perbaikan terhadap infrastruktur TI (Hardware dan Jaringan)	Service desk	8 jam	<4 jam	<4 jam
	Melakukan pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)	Antivirus	8 jam	<4jam	<4 jam
	Disaster Recovery Center	Copy file	<16 jam	<12 jam	<4 jam
	Penyediaan layanan email dan sistem informasi	Email	<16 jam	<12 jam	<4 jam
	Melakukan evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;	-			
	Melakukan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan	-			
	Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi	Sistem Database	24 jam	<24 jam	<24 jam

Fungsional Bisnis	Proses Bisnis Terkait Teknologi Informasi	Sistem dan Layanan TI	MTD	RTO	RPO
	Melakukan pengawasan kegiatan *helpdesk support*.	Service desk	16 jam	<12 jam	<12 jam
	Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan	-	24 jam	<12 jam	<4 jam

Berdasarkan penentuan waktu pemulihan terhadap layanan TI dan proses bisnis didapatkan bahwa semakin proses bisnis tersebut dinilai kritis maka semakin kecil pula waktu pemulihan yang diberikan. Hal tersebut dikarenakan proses bisnis kritis memiliki transaksi-transaksi yang bersifat harus terus berjalan.

6.2.2.3. Penyusunan Strategi Keberlangsungan Bisnis

Penyusunan strategi keberlangsungan bisnis dibuat berdasarkan pada hasil analisis risiko dan analisis dampak bisnis. Strategi keberlangsungan bisnis dibuat dengan tujuan untuk dapat menjaga keberlangsungan proses bisnis kritis. Sesuai dengan metodologi Yusrida, strategi yang dibuat merupakan strategi preventif, strategi pemulihan, strategi saat terjadi gangguan dan strategi korektif. Pada tahap ini ditambahkan berdasarkan inisiatif peneliti, yaitu strategi mitigasi untuk setiap risiko.

Strategi-strategi yang dibuat digunakan sebagai panduan apa yang harus dilakukan jika terjadi risiko pada suatu proses bisnis sehingga dapat mengontrol meminimalisir dampak gangguan yang diakibatkan dari risiko tersebut.

6.2.2.3.1. Strategi Preventif

Strategi preventif bertujuan agar perusahaan lebih siap untuk menghadapi gangguan yang berpotensi untuk terjadi. Berikut merupakan strategi preventif yang direkomendasikan:

Tabel 6.24 Strategi Preventif

Strategi Preventif	Deskripsi	Bentuk Kontrol
Mendokumentasikan aset TI	Pendokumentasian aset TI bertujuan untuk mengetahui aset yang dinilai oleh perusahaan memiliki nilai (*value*) yang dapat memberikan manfaat bagi perusahaannya dalam kegiatan operasional. Dokumentasi aset TI dilakukan secara keseluruhan yaitu hardware, software, data, dan aset pendukungnya. Dokumentasi aset TI dapat membantu dalam identifikasi secara cepat dari keberadaan aset dan fungsi utama dari aset tersebut.	• Intruksi kerja pendataan aset TI • Dokumen Daftar Aset TI • Portofolio Aplikasi

Pemberlakuan monitoring	Melakukan pemantauan secara berkala pada aset kritis yaitu server, data center dan kondisi network.	• Prosedur Pemeliharaan aset TI
		  ○ Intruksi Kerja Pemeliharaan aset TI
		  ○ Checklist laporan kondisi aset TI

Audit secara berkala	Audit yang berkala pada aset TI akan membantu dalam mengungkap setiap aktivitas berbahaya yang ada pada perusahaan. Selain itu untuk dapat melihat apakah penggunaan dan pengelolaan aset tersebut sudah sesuai standar yang berlaku sehingga dapat meminimalisir risiko yang berpotensi untuk terjadi.	• Prosedur Audit • Intruksi Kerja Audit • Formulir Audit • Check sheet audit

Menerapkan manajemen tabel	Manajemen tabel merupakan solusi untuk meningkatkan performa ketika *create, loading, update* dan *querying* tanpa harus menambah storage.	-
Backup	Menyediakan backup data, proses restorasi, termasuk media penyimpanan off-site yang memadai bagi pegawai sebuah organisasi	• Prosedur Backup Data ○ Intruksi Kerja Pelaksanaan Backup Data
Training	Memberikan pelatihan penanganan insiden dan gangguan pada tim BCP serta setiap perwakilan dari tiap fungsional bisnis.	• Modul Pelatihan
Mekanisme pengamanan fisik	Menyediakan mekanisme pengamanan fisik untuk menjamin ketersediaan jaringan vital dan komponen hardware, termasuk file dan print server. Selain terhadap komponen hardware, pengamanan juga perlu diterapkan terhadap user sebagaimana berdasarkan best practice dibawah ini :	• Kebijakan Keamanan Fisik Infrastruktur TI • Prosedur Keamanan Fisik Infrastruktur TI • Intruksi Kerja Pengamanan Fisik Infrastruktur TI • Check sheet Pengamanan Fisik Infrastruktur TI • Kebijakan Penggunaan yang diperbolehkan
Menurut best practice SOP Incident Handling Infrastruktur Fisik oleh Indonesia Government Computer Security Incident Response Team (Gov-CSIRT)[32]**:** Berikut merupakan rekomendasi apa saja yang harus dilakukan : **1. Mengedukasi akan kesadaran keamanan**		

Memberikan edukasi pada pengguna tentang cara melindungi informasi, apa yang harus dilakukan dan apa yang tidak harus dilakukan, siapa yang harus dihubungi pada keadaan darurat

2. Pemberlakuan Kebijakan Keamanan

Dokumen kebijakan keamanan harus memberikan informasi sesuai dengan kebutuhan bisnis, hukum dan peraturan yang relevan untuk membantu dalam penanganan insiden.

3.**Pemberlakukan kebijakan penggunaan yang diperbolehkan**

Kebijakan ini berisi tentang sesuatu yang diperbolehkan atau tidak diperbolehkan, termasuk pemanfaatan semua sumber daya organisasi. Hal ini akan membantu mencegah terhadap masuknya penyusup ke dalam fasilitas peralatan teknologi informasi.

4. Akses terhadap fisik fasilitas

Mengoptimalkan pengawasan seperti :

- pemasangan CCTV yang memiliki kemampuan terhadap cahaya rendah dan tahan terhadap suhu dan cuaca,
- pemasangan detektor bom,
- penggunaan petugas keamanan yang profesional yang memiliki kemampuan untuk menangkis, merespon, dan mengontrol serta memandu.

5. **Perangkat Kontrol Akses Fasilitas**

Merupakan perangkat kontrol akses personel terhadap aset TI, yaitu :

- menggunakan kunci untuk mengakses suatu aset seperti kunci preset (kunci pada umumnya seperti *key-in-knob*, *mortise* dan *rim lock*), kunci berbasis mekanik atau elektronik (kunci sandi yang membutuhkan pengguna untuk memasukkan sandi).
- Menggunakan *security access card*, seperti kartu berfoto (yang otentikasi dan otorisasi dilakukan dengan menunjukkan kepada penjaga), *digital-coded card* (yang terdapat *chip* atau sandi garis magnetik) yang dikombinasikan dengan card reader

- Perangkat biometrik seperti sidik jari, *retina scan, iris scan, facial scan, palm scan*, geometri tangan suara dan *handwritten signature dynamics*. Pengamanan didalam bangunan yang bertujuan untuk mendeteksi adanya ancaman secara fisik terhadap fasilitas teknologi informasi seperti detektor gerak, detektor suara dan sistem alarm.

Melakukan pengujian pada jaringan	Melakukan *vulnerable test* pada jaringan dengan menggunakan aplikasi pengujian.

6.2.2.3.2. Mitigasi Risiko

Selain strategi preventif yang bersifat umum, berikut ini akan didetailkan rencana perbaikan dan mitigasi untuk setiap risiko yang bernilai "*very high*". Mitigasi risiko dibuat berdasarkan pada risiko yang memiliki skala besar yaitu kebakaran dan risiko yang memiliki nilai RPN Very High yaitu :

1. Server Down
2. Human Error / Pelanggaran
3. Network trouble
4. Data tidak dapat diakses / tidak tersedia

Tabel 6.25 Mitigasi Risiko *ServerDown*

Risiko Server Down
Penyebab : • Gangguan jaringan • Kerusakan komponen utama • Hacker • Kesalahan konfigurasi • System overload (request terlalu banyak) / peak time • Kegagalan sistem operasi • Kerusakan sistem pengatur suhu • Dos Attack • Virus • Kerusakan UPS dan genset • Bencana alam

Mitigasi	Bentuk Kontrol
- Menyediakan server cadangan untuk mirroring - Menerapkan sistem monitoring server - Menerapkan perangkat pengamanan autentikasi pada pintu ruang server - Menambah kapasitas UPS pada ruang server	• Prosedur Penanganan Gangguan Server o Intruksi kerja penanganan gangguan server o Formulir penanganan gangguan • Prosedur Penanganan gangguan jaringan o Intruksi kerja penanganan o Formulir penanganan gangguan • Prosedur Pemeliharaan Server dan Storage o Intruksi Kerja Pemeliharaan server dan storage o Formulir pemeliharaan server dan storage • Prosedur Pemeliharaan UPS dan Genset o Intruksi Pemeliharaan UPS dan Genset • Kebijakan Pengunjung Ruang Server • Prosedur Pelaporan Gangguan o Intruksi kerja pelaporan gangguan o Formulir pelaporan gangguan • Prosedur penanganan virus dan malware o Intruksi Kerja penanganan virus dan malware

Tabel 6.26 Mitigasi Risiko *Network Trouble*

<table>
<tr><th colspan="2">Risiko Network Trouble</th></tr>
<tr><td colspan="2">Penyebab :
• Kerusakan fisik infrastruktur jaringan (switch, hub,router, konektor kabel)
• Media transmisi (kabel) tergigit tikus
• Kesalahan konfigurasi
• Virus dan malware
• Spoofing dan Sniffing
• Pemadaman listrik</td></tr>
<tr><th>Mitigasi</th><th></th></tr>
<tr><td>- Pembaharuan dokumentasi jalur LAN
- Merancang penempatan jalur backbone yang strategis
- Melakukan monitoring dan menganalisa terhadap lalu lintas data
- Melakukan filter ataupun pembatasan terhadap port-port yang tidak dibutuhkan
- Merancang tata letak perangkat yang memadai
- Membangun sistem control untuk perangkat Wireless LAN</td><td>• Prosedur Penanganan gangguan jaringan
o Intruksi kerja penanganan
o Formulir penanganan gangguan
• Prosedur Pemeliharaan jaringan
o Intruksi Kerja Pemeliharaan jaringan
o Formulir pemeliharaan jaringan
o Check sheet kondisi jaringan
• Dokumentasi topologi jaringan
• Prosedur Pelaporan Gangguan
o Intruksi kerja pelaporan gangguan
o Formulir pelaporan gangguan</td></tr>
</table>

	• Prosedur penanganan virus dan malware o Intruksi Kerja penanganan virus dan malware
Menurut best practice SOP Incident Handling Network oleh Indonesia Government Computer Security Incident Response Team (Gov-CSIRT)[33] **:** Untuk mengatasi serangan terhadap jaringan berikut ini adalah beberapa hal yang bisa dilakukan : 1. Menggunakan teknologi enkripsi dalam melakukan pengiriman data 2. Melakukan koneksi vpn 3. Sistem operasi harus dapat memberikan nomor urut yang acak ketika menjawab inisiasi koneksi dari sebuah host 4. Otentikasi host dengan digital-certificate 5. Konfigurasi firewall yang tepat	
Menurut best practice SOP Incident Handling Network oleh Indonesia Government Computer Security Incident Response Team (Gov-CSIRT)[33]**:** Berikut merupakan rekomendasi apa saja yang harus dilakukan : 1. Menetapkan prosedur dengan ISP untuk menentukan bagaimana mereka dapat membantu organisasi selama terjadinya serangan pada jaringan. 2. Mengetahui tentang SLA yang ada dan biaya-biaya apa yang mungkin timbul 3. Menetapkan informasi kontak selama 24 jam 7 hari untuk ISP dan metode alternatif untuk komunikasi 4. Menggunakan tools network packet analyzer untuk menganalisa kinjerja jaringan termasuk protokol didalamnya. 5. Menguji coba ketahanan dengan menggunakan software security 6. Melakukan dokumentasi yaitu :	

a. Membuat daftar dari alamat IP yang diprioritaskan untuk diperbolehkan melewati jaringan selama penanganan insiden
b. Menyiapkan dokumen topologi jaringan

7. Melakukan persiapan komponen keamanan jaringan antara lain,
   a. Firewall
   b. anti malware
   c. IDS/IPS
   c.VPN
8. Mencatat log file seperti protocol analyzer, sniffer, server SMTP, DHCP FTP dan WWW, router, firewall dan semua aktivitas sistem. Untuk menjadi sumber informasi jika terjadi sesuatu.
9. Melakukan pengamanan jaringan :
   a. Otentikasi dengan account locking
   b. Password aging & expiration
   c. Password Complexity Verification
   d. Menggunakan metode single sign on
   e. Enkripsi

Tabel 6.27 Mitigasi Risiko Data Tidak Dapat diakses

Risiko Data tidak dapat diakses	
Penyebab : • Gangguan pada jaringan • Virus dan malware • Kerusakan perangkat keras (storage dan server) • SQL Injection • Logical error (salah query) • Kegagalan sistem database	
Mitigasi	**Bentuk Kontrol**
Menurut best practice SOP Incident Handling Database oleh Indonesia Government	• Prosedur Backup Data

Computer Security Incident Response Team (Gov-CSIRT) [34]**:** - Memberlakukan kebijakan backup dimana mendefinisikan secara jelas mengenai jenis informasi dan kapan waktu proses backup haris dilakukan, dan bagaimana cara untuk melakukannya. - Membatasi akses ke data dan layanan - Memonitor aktivitas-aktivitas yang mencurigakan - Menonaktifkan perangkat removable - *Hash sistem file* untuk file-file yang penting - Menggunakan *Intrusion Detection System* - Memeriksa konfigurasi dan patch dar aplikasi database dan sistem operasi database server - Memastikan bahwa kode program yang digunakan telah memenuhi standar keamanan tertentu - Melakukan enkripsi - Memperbaharui metode akses - Memblokir password yang digunakan untuk mengakses database - Mengimplementasikan sistem database yang aman, handal, mudah	○ Intruksi Kerja Pelaksanaan Backup Data • Prosedur penaganan gangguan pada database ○ Intruksi kerja penanganan gangguan pada database ○ Formulir penanganan gangguan pada database • Prosedur Pelaporan Gangguan ○ Intruksi kerja pelaporan gangguan ○ Formulir pelaporan gangguan • Prosedur penanganan virus dan malware ○ Intruksi Kerja penanganan virus dan malware

diakses dan menyala 7 x 24 jam - Memperhatikan keamanan database sebagai berikut : 1. Pembatasan akses terhadap server 2. *Trusted Ip Acces* yaitu memberi respon pada alamat ip yang dikenali saja 3. Penggunaan kontrol akses tabel 4. Selalu mengupdate *patch* 5. Menerapkan aturan firewall yang ketat 6. Memblock port akses database seperti TCP dan UDP 1434 9MS SQL) dan TCP 1521-1520 (Oracle) 7. Penyaringan terhadap input data dari user 8. Membuan *stored procedure* 9. Enkripsi session -	

Tabel 6.28 Mitigasi Risiko *Human Error* / Pelanggaran

Risiko Human Error / pelanggaran	
Penyebab : • Kurang kompeten • Tidak terdapat prosedur dan kebijakan terkait pengelolaan dan penggunaan aset • Tidak adanya pengawasan / monitoring hak akses pada transaction log	
Mitigasi	**Bentuk Kontrol**
- Memberlakukan kebijakan penggunaan aset - Pemberlakukan kebijakan penggunaan yang diperbolehkan - Mengoptimalkan pengawasan - Meningkatkan keamanan dengan perangkat kontrol akses fasilitas - Memberikan pelatihan - Memberikan kesempatan untuk karyawan mengikuri pelatihan atau workshop eksternal	• Kebijakan penggunaan aset TI o Modul penggunaan aset TI • Kebijakan Penggunaan akun • Prosedur Investigasi o Intruksi kerja investigasi o Formulir investigasi • Prosedur Pelaporan Gangguan o Intruksi kerja pelaporan gangguan o Formulir pelaporan gangguan

6.2.2.3.3. Strategi Saat Gangguan

Strategi saat gangguan adalah tindakan yang dilakukan perusahaan untuk dapat menangani gangguan dan mengembalikan operasional proses bisnis agar dapat kembali bekerja normal. Strategi saat gangguan berupa alur atau

mekanisme dalam menangani pada saat terjadi gangguan hingga mengembalikan kondisi ke kondisi normal.

Tabel 6.29 Strategi Saat Gangguan

Menjalankan alur penanganan saat terjadi gangguan
1. Notifikasi & respon awal a. Menerima laporan/peringatan dari peronel, senior management ataupun security di tempat terjadinya insiden. b. Menghubungi pihak terkait seperti pemadam kebakaran atau vendor apabila dibutuhkan c. Melakukan evakuasi dan penyelamatan secara langsung (jika memang diperlukan). d. Menghubungi pihak terkait jika kondisi sudah sangat berbahaya seperti pemadam kebakaran, pihak kepolisian, rumah sakit dll.
2. **Identifikasi gangguan** a. Melakukan identifikasi terhadap insiden yang terjadi yaitu obyek, penyebab dan dampak pada aset TI. b. Melakukan pemeriksaan dan investiasi jika terdapat pelaku penyebab kerusakan. Invesstigasi dilakukan dengan memeriksa personel, aset terkait atau data-data hasil monitoring untuk dapat dianalisa. c. Melakukan penilaian terhadap dampak gangguan dan kerugian yang didapatkan d. Melakukan penilaian terhadap risiko keselamatan kerja e. Melakukan penilaian celah keamanan gedung dan dampak gangguan terhadap operasional proses bisnis serta aset-aset yang mengalami kerusakan. f. Mengklasifikasi gangguan yang terjadi untuk menentukan level kerusakan dari gangguan tersebut berdasarkan penilaian yang telah dilakukan. g. Menyiapkan laporan untuk dokumentasi
3. Deklarasi gangguan a. Setelah mengetahui penyebab terjadinya gangguan maka selanjutnya adalah menelusuri dokumen untuk mencari

pengetahuan yang berisi insiden yang pernah terjadi di masa lalu. b. Menentukan opsi pemulihan dan restorasi terbaik yang telah di deskripsikan pada strategi pemulihan c. Melakukan perhitungan biaya d. Jika gangguan yang terjadi memiliki level kerusakan yang tinggi maka dilakukan deklarasi gangguan yang berisi informasi mengenai gangguan yang terjadi, waktu terjadi, level kerusakan, strategi pemulihan yang dpilih, perkiraan waktu pemulihan dan pic
4. Pemulihan a. Mempersiapkan pemulihan berdasarkan waktu pemulihan dan strategi yang dipilih b. Mempersiapkan kebutuhan pemulihan c. Menjalankan prosedur penanganan gangguan dan pemulihan serta melakukan perbaikan terhadap aset yang mengalami kerusakan. Jika kerusakan dianggap sangat parah maka menggunakan aset cadangan untuk dapat melanjutkan proses bisnis d. Melakukan langkah-langkah perlindungan aset TI seperti pengamanan data dengan melakukan backup, menonaktifkan sistem sementara apabila diperlukan, pengecekan data dan infrastruktur. e. Jika diperlukan, memindahkan aset kritis yang sedang dipulihkan ke tempat yang lebih baik f. Memutuskan kapan sistem dapat kembali bekerja normal g. Melakukan validasi dan konfirmasi bahwa aset atau sistem telah berjalan dengan normal
5. **Dokumentasi hasil pemulihan** a. Dokumentasi bertujuan untuk menambahkan pengetahuan tentang penanganan insiden di masa depan
6. **Evaluasi**

a. Melakukan evaluasi terhadap mekanisme pemulihan dan penanganan gangguan yang telah dilakukan
b. Melakukan evaluasi terhadap prosedur yang digunakan
c. Melakukan peningkatan keamanan

6.2.2.3.4. Strategi Pemulihan

Strategi pemulihan adalah tindakan yang harus segera dilakukan untuk mengatasi gangguan maupun bencana yang saat itu terjadi. Berikut ini adalah alternatif-alternatif pemulihan yang dapat diterapkan oleh perusahaan:

Tabel 6.30 Strategi Pemulihan

Kategori Opsi Pemulihan	**Opsi Pemulihan**	**Deskripsi**
Backup Type	*Incremental*	Incremental dilakukan untuk file yang berubah atau baru dibuat sejak waktu full backup atau backup yang terakhir. Direkomendasikan untuk diterapkan pada sistem informasi yang mempunyai transaksi rutin dengan kebutuhan RPO kecil.
	Full	Dapat diterapkan pada sistem informasi yang mempunyai transaksi tidak rutin dengan kebutuhan RPO besar atau waktu yang cukup lama, untuk semua file.
	Differential	Backup dilakukan untuk file yang berubah atau baru dibuat serjak waktu full backup yang terakhir.
Metode *Backup*	*Remote Mirroring*	Data dicerminkan/mirror ke lokasi alternatif untuk menyediakan continous availability menggunakan

Kategori Opsi Pemulihan	Opsi Pemulihan	Deskripsi
		teknologi seperti trans Action router maupun fault toleran
	Wide Area High Availability Clustering	Fasilitas yang menggunakan beberapa sumber daya komputasi pada lokasi geografis yang berbeda. Tujuannya adalah untuk mendukung kelangsungan bisnis perusahaan dengan menyediakan location-independent load balancing dan failover. Clustering WAN dapat digunakan untuk hampir semua sumber daya termasuk mainframe, file server dan aplikasi perangkat lunak.
	Storage Virtualization	Mengombinasikan beberapa perangkat penyimpanan ke dalam sebuah peralatan penyimpanan logical yang dapat diatur secara tersentralisasi.
	Disk Mirroring	Sebuah teknik dimana dua buah harddisk ditulis bersamaan secara sinkron. Disk mirroring memberikan perlindungan jika terjadi kegagalan pada salah satu harddisk.
	Disk Shadowing	Teknik untuk mempertahankan satu set dari dua atau lebih disk yang identik dengan tujuan untuk meningkatkan keandalan dan ketersediaan penyimpanan sekunder dengan menyediakan beberapa jalur unruk data yang redundan.
	Application or Utility based data replication	Sebuah aplikasi yang mengirimkan data dari server pertama ke server kedua yang berada diluar kantor.

Kategori Opsi Pemulihan	Opsi Pemulihan	Deskripsi
	Electronic Vaulting	Bavkup yang dibuat secara otomatis melalui penyedia layanan vaulting elektronis.
	Remote Journaling	Transaction logs dikirim ke fasilitas pemulihan alternatif.
	Tape Backup	Backup tradisional dengan menggunakan media tape
Alternate Site Facility	*Hot site*	Backup site yang memungkinkan perusahaan untuk dapat melanjutkan operasi bisnis normal dalam waktu singkat setelah terjadinya gangguan. Pemulihan ini dapat dikonfigurasi di kantor cabang perusahaan, data center atau bahkan secara cloud. Pemulihan ini juga harus dilengkapi dengan ruangan kantor, perabotan furniture, semua perangkat keras, software, jaringan dan konektivitas internet yang diperlukan. Data secara berkala dicadangkan atau direplikasi ke hit site sehingga dapat sepenuhnya beroperasi secepat mungkin jika terjadi bencana pada lokasi asli. Hot site juga harus berlokasi jauh dari lokasi asli untuk mencegah gangguan mengenai hot site itu juga. Opsi ini adalah opsi yang membutuhkan biaya paling banyak dari pada opsi yang lain. **Hot site direkomendasikan untuk diterapkan pada aplikasi**

Kategori Opsi Pemulihan	Opsi Pemulihan	Deskripsi
		yang terkait dengan proses bisnis kritis dimana transaksi-transaksi penting berjalan.
	Warm site	Fasiltas altrnatif yang memiliki sarana yang tidak selengkap hot site. Misalnya ada jaringan, perabotan-perabotan dan perabotan. Tetapi tidak siap untuk beroperasi langsung. Waktu yang diperlukan untuk beralih dari lokasi asli yang terkena gangguan ke warm site lebih lama daripada hot site. Pemulihan akan tertunda selama pengambilan data. **Hot site direkomendasikan untuk diterapkan pada aplikasi yang terkait dengan proses bisnis kategori penting.**
	Cold site	Cold site memiliki fasilitas yang lebih sedikit dari pada warm site. Cold site akan membutuhkan waktu lebih lama dari pada warm dan hot site untuk melanjutkan operasi. Cold site meyediakan ruang kantor yang telah dilengkapi listrik, perabotan dan fasilitas teknis dasar namun memerlukan beberapa hari atau bahkan minggu untuk mempersiapkan, menginstall dan mengonfigurasi sehingga dapat dioperasikan. Cold site dinilai

Kategori Opsi Pemulihan	Opsi Pemulihan	Deskripsi
		pilihan yang lebih terjangkau dari opsi lainnya. **Hot site direkomendasikan untuk diterapkan pada aplikasi yang terkait dengan proses bisnis kategori minor.**

6.2.2.3.5. Strategi Korektif

Strategi korektif adalah suatu tindakan yang dilakukan perusahaan untuk memperbaiki dari perencanaan BCP. Strategi korektif dilakukan saat organisasi melihat adanya ketidaksesuaian atau kurangnya tingkat keefektifan dari perencanaan BCP yang telah disusun.

Tabel 6.31 Strategi Korektif

Strategi Korektif	Deskripsi
Evaluasi	Melakukan evaluasi terhadap pembagian tanggung jawab, penanganan gangguan dan mekanisme pelaksanaan pemulihan sehingga dapat dilakukan perbaikan untuk kedepannya.
Melakukan peningkatan keamanan	Meningkatkan keamanan terhadap akses ases TI sesuai dengan pelajaran yang didapatkan dari gangguan yang pernah terjadi.
Menurut best practice SOP Incident Handling Infrastruktur Fisik oleh Indonesia Government Computer Security Incident Response Team (Gov-CSIRT) Berikut merupakan rekomendasi apa saja yang harus dilakukan : 1. Memperbarui dokumenrasi Setelah berhasil menangani sebuah insiden yang harus dilakukan selanjutnya adalah memperbarui pengetahuan. Dokumentasi		

tersebut harus di review oleh tim semua pihak yang telah berperan dalam penanganan insiden. Hal ini akan membantu dalam penanganan insiden serupa di masa depan dengan mudah, efisien dan cepat.
2. Audit
Dengan melakukan audit secara berkala pada komponen aset sistem dan teknologi informasi, maka akan membantu dalam menungkap setiap aktivitas yang dilakukan pengguna pada sistem.
3. Pelatihan untuk tim penanganan insiden/ tim BCP
Bertujuan untuk membantu tim lebih memahami proses penanganan gangguan da juga agar lebih terampil dalam menanggulangi gangguan serupa di masa mendatang.
4. Memperbarui aturan penjagaan
Dilakukan dengan memperbarui aturan untuk memasuki suatu ruangan (seperti sensor biometrik)

6.2.2.4. Perencanaan Pemulihan Bencana

Perencanaan pemulihan bencana akan dijadikan sebagai pelengkap dalam menjalankan strategi perencanaan keberlangsungan bisnis dimana pada tahapan ini terdapat penentuan mengenai pihak yang bersangkutan dalam pemulihan gangguan yaitu vendor, pendefinisian aset TI yang dimiliki perusahaan, aktivasi dan deaktivasi serta bentuk kontrol. Berikut merupakan rencana pemulihan gangguan.

6.2.2.4.1. Pengelolaan Aset

Pembuatan daftar aset TI akan memudahkan komite BCP dalam melakukan evakuasi aset-aset kritis pada saat terjadi gangguan. Selain itu juga memudahkan untuk melihat *history* kondisi dari masing-masing aset. Berikut ini adalah daftar aset TI untuk memudahkan dalam pengelolaan dan perawatan aset :

Tabel 6.32 Daftar Aset TI

Komponen Teknologi Informasi	Aset Teknologi Informasi
Hardware	PC
	Server dan Storage

	Laptop
	Genset
	UPS
Software	Sistem Informasi Keuangan (Billing, AXAPTA, SKA, aplikasi penagihan rekening swasta, pemerintah dan kas, aplikasi kas on line, layanan pembayaran online)
	Sistem Informasi Pelayanan Pelanggan
	Website
	Email
	Service Desk
	Remote System
	Antivirus
	Firewall
	Geographic Information System (GIS)
Network	Switch
	Router
	Access Point
	Media transmisi (kabel jaringan)
Data	Database Pelanggan Database Keuangan Database Pegawai
People	Tim TSI
	Pegawai Non-TI

6.2.2.4.2. Pengelolaan Vendor (Pihak ketiga)

Pengelolaan vendor merupakan proses mengenai pendefinisian pihak ketiga (vendor) yang bekerjasama dengan perusahaan untuk keperluan penanganan risiko bencana serta pemulihan aset TI. Selain itu, vendor management berisikan informasi kontak pihak ketiga (vendor).

Peran dan Tanggungjawab Vendor:

1. Memahami kebutuhan yang diperlukan oleh perusahaan sehingga dapat menyediakan produk dan jasa atau segala keperluan PDAM Surya Sembada Kota Surabaya dengan baik dan tepat.
2. Memiliki ketersedian setiap saat dan dapat dihubungi ketika dalam kondisi kritis dan darurat.

3. Kecepatan respon menanggapi dan menangani keluhan pada PDAM Surya Sembada Kota Surabaya
4. Handal dan dapat dipercaya oleh perusahaan dalam menangani pemulihan dari kondisi kritis.
5. Melaksanakan apa yang sudah disepakati pada SLA sesuai dengan waktu yang telah ditentukan
6. Mengomunikasikan dan bersikap terbuka dalam memberikan solusi

Berikut ini daftar vendor dari PDAM Surya Sembada Kota Surabaya.

Tabel 6.33 daftar vendor dari PDAM Surya Sembada Kota Surabaya

No	Critical Equipment	Vendor	Telp Darurat
1.	Penyedia layanan untuk pemeliharaan printer dan PC	Vendor A	*Regulary Update*
2.	Penyedia sewa komputer dan printer	Vendor B	*Regulary Update*
3.	*Switcher* (Penyedia layanan pembayaran online)	Vendor C	*Regulary Update*
		Vendor D	*Regulary Update*
		Vendor E	*Regulary Update*
		Vendor F	*Regulary Update*
4.	Penyedia layanan untuk internet (ISP)	Vendor G	*Regulary Update*
5.	Penyedia layanan server mirroring	Vendor H	*Regulary Update*
6.	Penyedia layanan untuk pemeliharaan AC	Vendor H	*Regulary Update*

7.	Penyedia layanan untuk pemeliharaan AC	Vendor I	*Regulary Update*

6.2.2.4.3. Aktivasi dan Deaktivasi

Tahapan ini merupakan tahapan dimana dilakukan penentuan kondisi dan tindakan yang telah ditetapkan dalam sebuah perencanaan dimulai (aktif) dan dinyatakan sudah cukup untuk dinonaktifkan. Dalam hal ini, menentukan kondisi gangguan yang masih dapat diatasi hingga gangguan yang bersifat *disaster* yaitu yang membutuhkan banyak sumber daya untuk dapat memulihkan kondisi menjadi normal. Apabila gangguan hanya terjadi pada satu fungsional bisnis, tidak memiliki pengaruh pada fungsional bisnis lain, megganggu proses bisnis kritis dan memberikan dampak finansial/operasional/teknis yang tinggi, maka gangguan tersebut dapat diatasi dengan cara melaporkan gangguan yang dialami pada TSI tepatnya bagian helpdesk untuk selanjutnya dapat ditangani.

Gangguan dikatakan sebagai disaster/bencana atau gangguan skala besar apabila berada pada kondisi, sebagai berikut:

1. Gangguan yang terjadi disebabkan oleh bencana alam dan kebakaran
2. Gangguan yang terjadi mengancam keselamatan pekerja
3. Gangguan terjadi pada proses bisnis kritis dan memiliki waktu pemulihan melebihi waktu pemulihan (MTD) yang telah ditentukan.
4. Gangguan menyebabkan beberapa fungsional bisnis tidak dapat menjalankan proses bisnis kritisnya.
5. Gangguan menimbulkan kerugian finansial/biaya ekstra >20% dan kehilangan potensi pendapatan perusahaan, berdampak besar pada reputasi perusahaan dan mengganggu > 20% target operasional dari proses bisnis

Maka yang harus dilakukan adalah melakukan strategi saat terjadi gangguan dan pemulihan, dimana akan dijalankan alur

komunikasi gangguan besar yang telah ditetapkan, mencari penyebab terjadinya gangguan, melakukan penyelamatan data semampunya, memulihkan kondisi dengan melibatkan semua pihak baik internal maupun eksternal sesuai dengan tanggungjawab (bila diperlukan berhubungan dengan vendor untuk penggantian infrastruktur) dan mengkomunikasikan proses bisnis agar tetap dapat berjalan.

6.2.2.4.4. Bentuk Kontrol

Bentuk kontrol sesuai dengan metode yusrida adalah berupa prosedur terkait dalam melakukan pencegahan, deteksi sumber masalah dan pengurangan dampak. Bentuk kontrol dibuat dengan disesuaikan dengan strategi yang ada pada strategi keberlangsungan bisnis. Berikut ini adalah bentuk kontrol untuk BCP pada PDAM Surya Sembada Kota Surabaya.

Tabel 6.34 Bentuk Kontrol

No.	Bentuk Kontrol
1.	Dokumen Daftar Aset TI Intruksi kerja pendataan aset TI Portofolio Aplikasi
2.	Prosedur Pemeliharaan aset TI Intruksi Kerja Pemeliharaan aset TI Checklist laporan kondisi aset TI
3.	Prosedur Audit Intruksi Kerja Audit Formulir Audit Check sheet audit
4.	Prosedur Backup Data Intruksi Kerja Pelaksanaan Backup Data
5.	Kebijakan Keamanan Fisik Infrastruktur TI Prosedur Keamanan Fisik Infrastruktur TI Intruksi Kerja Pengamanan Fisik Infrastruktur TI Check sheet Pengamanan Fisik Infrastruktur TI Kebijakan Penggunaan yang diperbolehkan

No.	Bentuk Kontrol
6.	Prosedur Penanganan Gangguan Server Intruksi kerja penanganan gangguan server Formulir penanganan gangguan
7.	Kebijakan Pengunjung Ruang Server
8.	Prosedur Penanganan gangguan jaringan Intruksi kerja penanganan Formulir penanganan gangguan
9.	Prosedur Pemeliharaan UPS dan Genset Intruksi Pemeliharaan UPS dan Genset
10.	Prosedur Pemeliharaan Server dan Storage Intruksi Kerja Pemeliharaan server dan storage Formulir pemeliharaan server dan storage
11.	Prosedur Pelaporan Gangguan Intruksi kerja pelaporan gangguan Formulir pelaporan gangguan
12.	Prosedur penanganan virus dan malware Intruksi Kerja penanganan virus dan malware
13.	Prosedur Pemeliharaan jaringan Intruksi Kerja Pemeliharaan jaringan Formulir pemeliharaan jaringan Check sheet kondisi jaringan Dokumentasi topologi jaringan
14.	Prosedur Pelaporan Gangguan Intruksi kerja pelaporan gangguan Formulir pelaporan gangguan
15.	Prosedur penaganan gangguan pada database Intruksi kerja penanganan gangguan pada database Formulir penanganan gangguan pada database
16.	Kebijakan penggunaan aset TI Modul penggunaan aset TI
17.	Kebijakan Penggunaan akun
18.	Prosedur Investigasi Intruksi kerja investigasi Formulir investigasi

No.	Bentuk Kontrol
19.	Prosedur Pengujian Rencana Keberlangsungan Bisnis
20.	Daftar kontak darurat
21.	Daftar Vendor
22.	Modul pelatihan BCP

6.2.2.5. Pelatihan Karyawan

Perusahaan dapat menjalankan BCP dengan efektif jika pihak manajemen dan karyawan memiliki kemampuan dan kompetensi dalam menjalankan peran masing-masing pada BCP. Selain itu setiap perlu memiliki kesadaran akan BCP. Oleh karena itu maka edukasi dan pelatihan perlu diberikan.

Tahapan pelatihan dilakukan untuk dapat memberikan pengetahuan dan pemahaman kepada keseluruhan karyawan terhadap strategi perencanaan keberlangsungan bisnis maupun prosedur keberlangsungan bisnis yang berlaku. Pada metodologi Yusrida, pelatihan karyawan fokus pada proses pelatihan yang mencakup mekanisme penyampaian pelatihan, pelaksanaan pelatihan yang terdiri dari latihan dan ujian, dan pemantauan kompetensi berdasarkan hasil latihan dan ujian.

Namun pada ruang lingkup pengerjaan tugas akhir ini hanya merencanakan mekanisme penyampaian pelatihan dan membuat modul pelaatihan.

6.2.2.5.1. Mekanisme Penyampaian Pelatihan

Pelatihan yang dilakukan akan dilakukan dengan memberikan edukasi dan pelatihan mengenai persiapan dan strategi saat adanya gangguan bagi setiap karyawan, termasuk tanggungjawab dan mekanisme komunikasi penyampaian adanya gangguan dari level bawah (operasional) ke level atas.

Pelatihan ini ditujukan untuk tim BCP dan seluruh karyawan, dengan penanggung jawab dari bagian TSI PDAM Surya Sembada Kota Surabaya. Berikut ini merupakan mekanisme pelatihan :

1. **Pre pelatihan**
   - persiapan modul/materi pelatihan
   - pendataan peserta pelatihan
   - penentuan waktu dan tempat
   - persiapan peralatan pendukung,
   - pemilihan metode pelatihan
   - persiapan kebutuhan pendukung lainnya
2. **Pelaksanaan Pelatihan**
   - Penyampaian materi
   - Simulasi
3. **Paska pelatihan**
   - test
   - evaluasi

6.2.2.5.2. Modul Pelatihan

Berikut ini merupakan konten modul yang akan digunakan dalam pelatihan mengenai persiapan saat adanya gangguan.

Tabel 6.35 Modul Pelatihan BCP

GAMBARAN UMUM MODUL **Edukasi dan Pelatihan BCP PDAM Surya Sembada Kota Surabaya**	
Metode	*Lecture*, *e-learning*, *workshops*, simulasi, *walk through*
Deskripsi Pelatihan ini bertujuan untuk memberikan edukasi kepada karyawan mengenai BCP dan bagaimana agar setiap karyawan dapat ikut berperan aktif dalam menangani gangguan ataupun keadaan darurat.	
Sasaran	Perwakilan karyawan dari tiap bidang

Materi Umum
Dalam pelatihan ini akan diberikan edukasi kepada karyawan mengenai: 1. Konsep umum BCP dan mengapa perusahaan membutuhkan BCP. 2. Business Continuity Plan PDAM Surya Sembada Kota Surabaya yang berisi: - Pengetahuan mengenai risiko dan penyebab terkait komponen TI yang mendukung proses bisnis perusahaan. - Pengetahuan mengenai dampak gangguan bagi perusahaan dari segi finansial, teknis, operasional dan lainnya. - Penjelasan mengenai struktur dan peran komite BCP - Pengetahuan mengenai mekanisme pelaporan ketika ada gangguan. - Pengetahuan mengenai prosedur dan mekanisme yang harus dijalankan untuk mencegah terjadinya gangguan dan saat adanya gangguan. 3. Teori dan teknis (seperti bagaimana menjalankan backup, memastikan keamanan, dll) 4. Kemampuan akan menangani gangguan dan keadaan darurat ketika sudah tidak sempat membaca prosedur manual
Kebutuhan : - Pemateri - Materi - Ruangan - Modul - Proyektor - Konsumsi - Peralatan simulasi

Selain mengadakan pelatihan untuk karyawan internal PDAM Surya Sembada Kota Surabaya, direkomendasikan untuk

mengikutkan tim BCP atau karyawan TSI mengikuti seminar eksternal, *academic course* dan *workshop* untuk menambah wawasan terkait BCP.

6.2.3. Fase 3 – Pemantauan dan Review

Pada fase pemantauan dan review terdapat tahapan yang harus dilakukan oleh perusahaan yaitu pengujian rencana keberlangsungan bisnis yang telah disusun.
Pengujian terhadap BCP bertujuan untuk mengonfirmasi apakah BCP yang dibuat sesuai dan dipastikan bahwa karyawan yang termasuk tim BCP memamahami tanggung jawab dan apa saja yang harus dilakukan saat adanya gangguan.
Dalam tahapan pengujian BCP akan dilakukan pembuatan alur pengujian, pengujian dan perbaikan berdasarkan hasil pengujian yang dilakukan. Namun karena keterbatasan waktu yang telah dijelaskan dalam batasan penelitian tugas akhir, ruang lingkup tahapan pengujian BCP hanya sampai pembuatan skenario pengujian BCP.

6.2.3.1. Pengujian BCP

Skenario pengujian rencana keberlangsungan bisnis yang akan dibuat pada PDAM Surya Sembada Kota Surabaya adalah pengujian jenis ***Process or Plan Simulation***. Pengujian dengan jenis *process or plan simulation* merupakan rencana kegiatan pengujian yang dilakukan di lingkungan "real life" dan akan disimulasikan sesuai dengan skenario. Pembuatan skenario pengujian didasarkan pada salah dua kemungkinan risiko yang dihadapi oleh PDAM Surya Sembada Kota Surabaya yaitu *network trouble* dan *server down*. Skenario yang dibuat yaitu :

6.2.3.1.1. Skenario Pengujian *Server Down*

Pengujian terhadap salah satu risiko tertinggi yaitu *server down*. *Server down* dapat disebabkan oleh:

- Kerusakan komponen utama
- Hacker

- Kesalahan konfigurasi
- System overload (request terlalu banyak)
- Gangguan jaringan
- Kegagalan sistem operasi
- Kerusakan sistem pengatur suhu
- Dos Attack
- Virus
- Kerusakan UPS dan genset
- Bencana alam

Pengujian dilakukan dengan menggunakan metode *Process or plan simulation* yaitu dengan melakukan simulasi terjadinya gangguan pada lingkungan "real life" dan akan disimulasikan sesuai dengan skenario. Pada pengujian ini akan dilakukan DoS Attack pada jaringan hingga server mengalami down.Pengujian ini direkomendasikan untuk dilakukan pada akhir hari dimana sudah tidak terjadi transaksi-transaksi penting perusahaan.

Tabel 6.36 Skenario Pengujian *Server Down*

Skenario Pengujian *Server Down*	
Jenis Pengujian	*Process or plan simulation*
Gangguan yang terjadi	Melakukan DoS Attack yaitu TCP SYN dimana permintaan koneksi jaringan dikirimkan ke server dalam jumlah yang sangat besar. Akibatnya server dibanjiri permintaan koneksi dan menjadi lambat atau bahkan tidak dapat dicapai sama sekali
Peran	• Pelaku : sebagai pelaku yang melakukan penyerangan • Tim Komite BCP : sebagai salah satu dari tim *Network & Telecommunication, Server and Application Recovery Team* yang melakukan penanganan gangguan

Penanganan Gangguan:	Sesuai dengan alur penanganan gangguan pada strategi saat gangguan dan prosedur jaringan, hal yang perlu dilakukan adalah : 1. Identifikasi masalah 2. Menentukan opsi pemulihan dan restorasi 3. Mempersiapkan pemulihan berdasarkan waktu pemulihan dan strategi yang dipilih 4. Melakukan pemulihan 5. Meningkatkan keamanan

6.2.3.1.2. Skenario Pengujian *Network Trouble*

Pengujian terhadap salah satu risiko tertinggi *yaitu network trouble*. Network trouble dapat disebabkan oleh kerusakan fisik infrastruktur jaringan (switch, hub,router, konektor kabel), media transmisi (kabel) tergigit tikus, kesalahan konfigurasi, virus dan malware, spoofing dan Sniffing dan pemadaman listrik.

Pengujian dilakukan dengan menggunakan metode *Process or plan simulation* yaitu dengan melakukan simulasi terjadinya gangguan pada lingkungan "real life" dan akan disimulasikan sesuai dengan skenario. Pada pengujian ini akan dilakukan sniffing pada jaringan hingga didapatkan password dari user yang berada didalam traffic paket-paket data.
Pengujian ini direkomendasikan untuk dilakukan pada akhir hari dimana sudah tidak terjadi transaksi-transaksi penting perusahaan.

Tabel 6.37 Skenario Pengujian *Network Trouble*

Skenario Pengujian *Network Trouble*	
Jenis Pengujian	*Process or plan simulation*
Gangguan yang terjadi	Melakukan *packet sniffing* yaitu mencuri password dari sniffing yang dilakukan terhadap paket-paket data.

Peran	• Karyawan TSI : sebagai pelaku yang melakukan penyerangan • Tim Komite BCP : sebagai salah satu dari tim *Network & Telecommunication, Server and Application Recovery Team* yang melakukan penanganan gangguan
Penanganan Gangguan:	Sesuai dengan alur penanganan gangguan pada strategi saat gangguan dan prosedur jaringan, hal yang perlu dilakukan adalah : 1. Identifikasi masalah Melakukan identifikasi masalah dengan melakukan network discovery atau diagnosa dan melakukan pemeriksaan fisik pada infrastruktur jaringan. Network discovery dilakukan dengan melihat pada konfigurasi yaitu : - Melihat user traffic - Konfigurasi switch dan router - Network connectivity - Memeriksa traffic dan protokol yang digunakan - Network performance - Packet capture - Mengetes response time pada server 2. Jika sudah diketahui penyebabnya yang dilakukan kemudian adalah melakukan perbaikan dengan cara - menonaktifkan semua lalu lintas yang sudah jelas palsu (alamat IP yang tidak seharusnya masuk atau keluar jaringan), - melakukan penyaringan layanan pada router terluar, - menonaktifkan semua layanan dan membatasi hak akses ke dan dari semua host, - menerapkan rate limiting untuk protokol tertetu,

	- membatasi jumlah paket per detik untuk protokol tertentu mengakses suatu host - menonaktifkan jaringan

6.2.4. Fase 4 – Pemeliharaan dan Peningkatan

Sesuai dengan Metode Yusrida, fase pemeliharaan dan peningkatan merupakan tahapan dilakukannya pennjauan keberlangsungan bisnis. Hal tersebut bertujuan untuk meninjau kemampuan dan keefektifan keberlangsungan bisnis yang ditetapkan dalam BCP serta untuk mendapatkan feedback dari ketidaksesuaian BCP agar dapat memperbaiki dan meningkatkan kinerja keberlangsungan bisnis. Tahapan peninjauan kelangsungan bisnis dilakukan oleh pihak manajemen dengan tujuan untuk memastikan bahwa rencana keberlangsungan bisnis telah sesuai dengan kondisi, tujuan dan kebutuhan organisasi. Keberlangsungan bisnis direkomendasikan untuk ditinjau ulang setiap 2 tahun sekali sesuai dengan perubahan pada perusahaan.

Berikut ini adalah cakupan yang perlu ditinjau oleh pihak manajemen PDAM Surya Sembada Kota Surabaya :

1. Adanya perubahan dari internal dan eksternal yang berkaitan dengan BCP
2. Informasi terkait dengan kinerja BCP seperti adanya ketidaksesuaian yang terjadi dan langkah korektif yang telah dilakukan serta hasil audit
3. Kebutuhan untuk melakukan perubahan terhadap BCP terkait penilaian risiko dan analisis dampak bisnis
4. Pemberian level kritis terhadap proses bisnis
5. Penambahan atau perubahan perangkat BCP yaitu kebijakan maupun prosedur yang dapat meningkatkan kinerja dan keefektifan BC .
6. Pembaruan Strategi BCP dengan melihat perkembangan teknologi dan ilmu pengetahuan pada TI

7. Pengetahuan yang didapatkan dari tindakan yang dilakukan dalam penangana gangguan yang telah terjadi.
8. Implementasi BCP
9. Hasil dari pengujian BCP

6.2.4.1. Peninjauan kelangsungan bisnis

Sesuai dengan batasan masalah pengerjaan tugas akhir dan tahapan pada metode Yusrida, peninjauan kelangsungan bisnis hanya pada sampai mempersiapkan formulir yang berupa kuesioner. Formulir pada peninjauan kelangsungan bisnis adalah sebagai berikut :

6.2.4.1.1.Formulir Pengecekan Rencana Keberlangsungan Bisnis

Formulir ini digunakan untuk mengetahui telah seberapa jauh kesiapan rencana keberlangsungan bisnis dilihat dari pengelolaan BCP, kesesuaian BCP dengan perusahaan, keefektifan strategi BCP, pelatihan, pengujian dan peninjauan BCP. Formulir ini akan diisi oleh pihak manajemen sebagai masukan dalam peninjauan keberlangsungan bisnis. Namun pada pengerjaan tugas akhir ini hanya sampai membuat formulir. Berikut ini adalah formulir pengecekan rencana keberlangsungan bisnis (**formulir terdapat pada Lampiran G**)

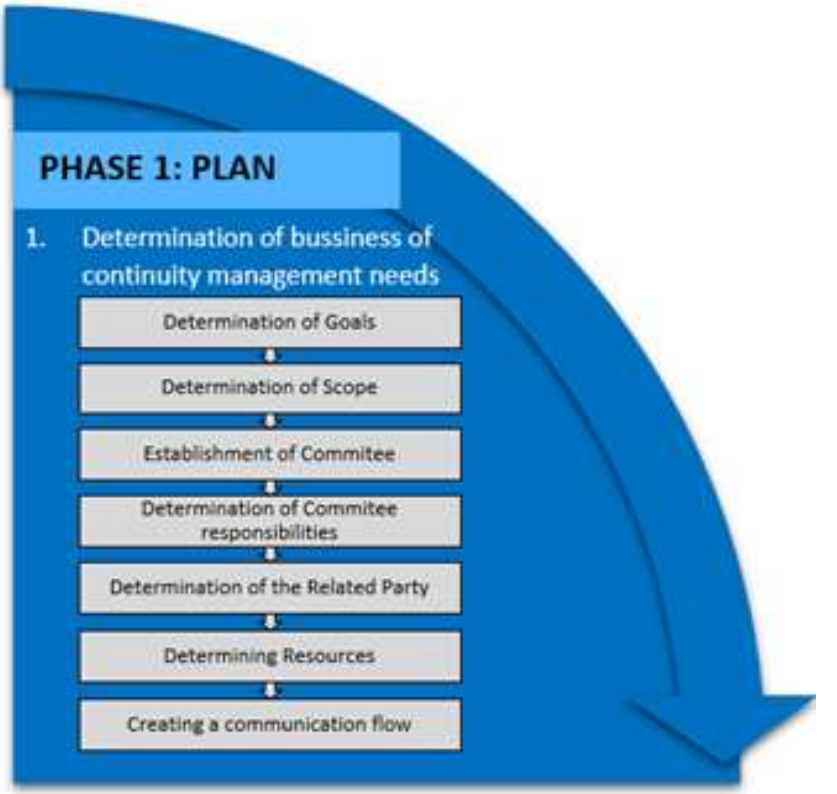
6.2.4.1.2. Formulir Peninjauan Manajemen

Formulir ini merupakan laporan hasil rapat yang telah diputuskan oleh seluruh peserta rapat. (**formulir terdapat pada Lampiran H**)

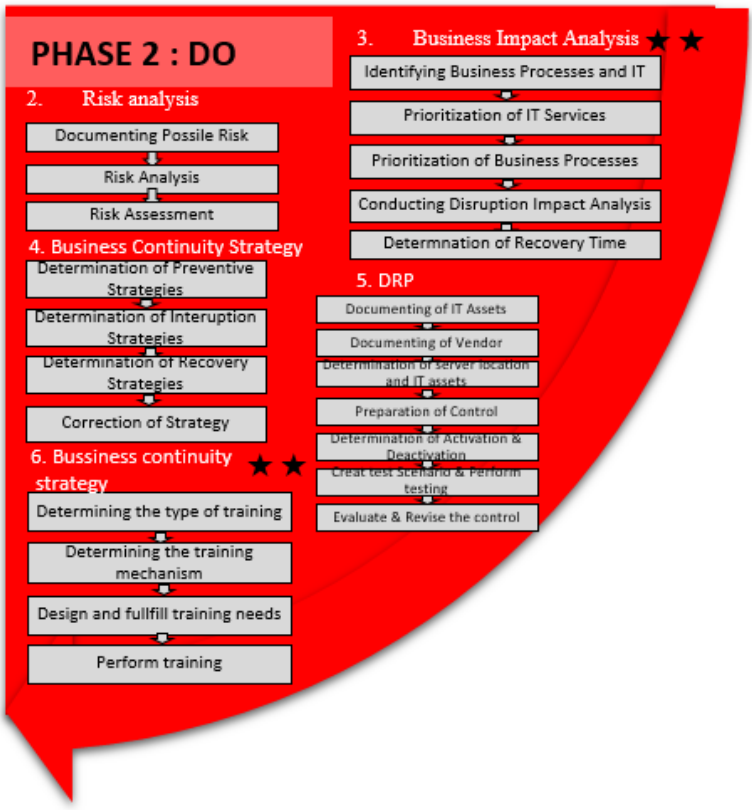
6.3. Hasil Evaluasi Metode Yusrida

Evaluasi terhadap metode BCP yang diusulkan Yusrida bertujuan untuk mengetahui apakah dapat untuk diimplementasi pada perusahaan lain. Oleh karena itu pada penelitian ini dilakukan studi empiris pada PDAM Surya Sembada Kota Surabaya dengan mengikuti panduan pada

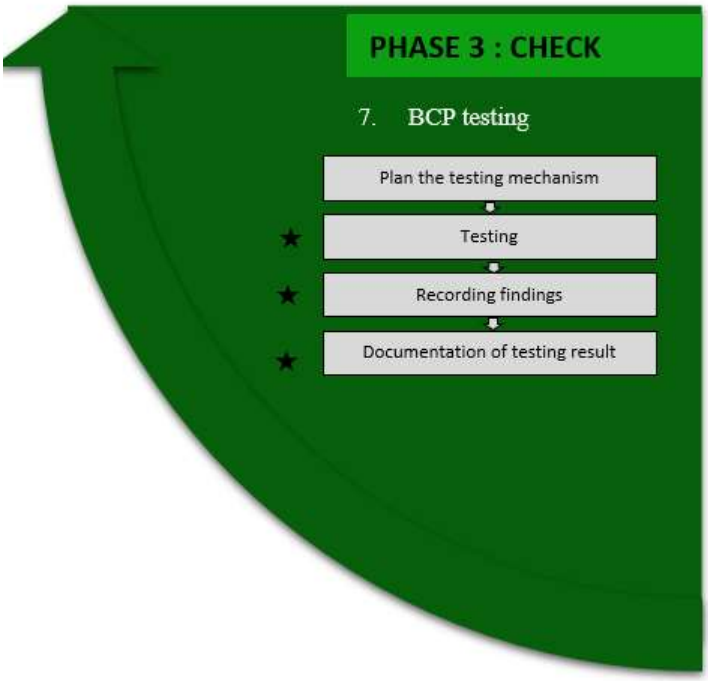
seluruh tahapan yang ada di metode Yusrida. Berikut ini adalah gambaran keseluruhan metode BCP yang diusulkan oleh Yusrida, dimana yang diberi bintang merupakan aktivitas yang tidak dapat diimplementasi dan memerlukan modifikasi (Penjelasan lebih rinci mengenai setiap tahap terdapat pada **Tabel 6.37 Hasil Evaluasi**) :



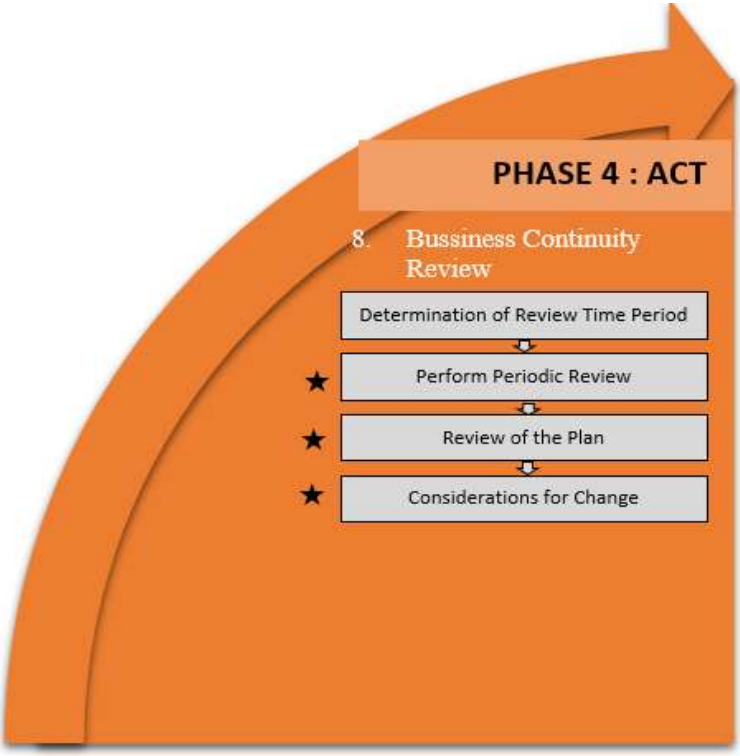
Gambar 6.4 Fase 1-Perencanaan Metode BCP Yusrida



Gambar 6.5 Fase 2-Implementasi Metode BCP Yusrida



Gambar 6.6 Fase 3-Pemantauan dan Review Metode BCP Yusrida



Gambar 6.7 Fase 4- Pemeliharaan dan Peningkatan Metode BCP Yusrida

Evaluasi dilakukan dengan melihat apakah setiap tahapan pada metode Yusrida dapat dilakukan pada studi kasus yaitu PDAM Surya Sembada Kota Surabaya dengan menggunakan checklist evaluasi. Tanda "✓" pada kolom 1 berarti aktivitas tersebut dapat dikerjakan dan dilakukan sesuai dengan metode BCP yang diusulkan oleh Yusrida, sedangkan pada kolom 2 berarti aktivitas tersebut dapat dikerjakan dan dilakukan namun terdapat modifikasi dan perubahan dan pada kolom 3 berarti aktivitas tersebut tidak dapat dilakukan. Berikut ini adalah checklist hasil evaluasi setiap aktivitas pada tahapan metode yang diusulkan oleh Yusrida.

Tabel 6.38 Hasil Evaluasi

Tahap	Aktivitas	1	2	3	Justifikasi
Fase 1. Perencanaan					
Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis	Penentuan Tujuan	✓			Dapat dilakukan sesuai dengan tahapan Yusrida yaitu menyesuaikan BCP yang akan dibuat dengan kebutuhan dan kondisi PDAM Surya Sembada Kota Surabaya. (hasil terdapat pada **bagian 6.2.1.1.1 Tujuan Keberlangsungan Bisnis**)
	Penentuan Ruang Lingkup	✓			Dapat dilakukan sesuai dengan tahapan Yusrida yaitu mengambil tiga fungsional bisnis pada PDAM Surya Sembada Kota Surabaya sebagai ruang lingkup. (hasil terdapat pada **bagian 6.2.1.1.2)**
	Pembentukan Komite	✓			• Dapat dilakukan sesuai dengan tahapan Yusrida

Tahap	Aktivitas	1	2	3	Justifikasi
					• Komite BCP dibuat dengan menyesuaikan kebutuhan keberlangsungan bisnis dan struktur organisasi perusahaan. (hasil terdapat pada **bagian 6.2.1.1.3)**
	Penentuan Tanggung Jawab	✓			• Dapat dilakukan sesuai dengan tahapan Yusrida. • Penentuan tugas dan tanggung jawab pada struktur komite BCP dibuat dengan menyesuaikan kebutuhan keberlangsungan bisnis dan struktur organisasi perusahaan (hasil terdapat pada **bagian 6.2.1.1.3)**
	Penentuan Pihak Terkait	✓			• Dapat dilakukan sesuai dengan tahapan Yusrida. • Penentuan pihak yang akan memiliki peran tanggung jawab pada komite BCP dibuat dengan menyesuaikan terhadap struktur organisasi perusahaan (hasil

Tahap	Aktivitas	1	2	3	Justifikasi
					terdapat pada **bagian 6.2.1.1.3)**
	Penentuan Sumberdaya	✓			• Dapat dilakukan sesuai dengan tahapan Yusrida. • Penentuan sumber daya apa saja yang dibutuhkan ketika terjadi gangguan dilakukan dengan menyesuaikan dengan hasil analisis risiko dan strategi BCP yang telah dibuat. (hasil terdapat pada **bagian 6.2.1.1.3)**
	Pembuatan Alur Komunikasi	✓			• Dapat dilakukan sesuai dengan tahapan Yusrida. • Alur komunikasi disesuaikan dengan strategi penanganan saat terjadi gangguan (hasil terdapat pada **bagian 6.2.1.1.4)**
Fase 2. Implementasi					
Analisis Risiko	Pendataan Kemungkinan Risiko	✓			Dapat dilakukan sesuai dengan tahapan Yusrida dengan menggunakan metode OCTAVE. (hasil terdapat pada **bagian 6.2.2.1.1)**
	Analisis Risiko	✓			Dapat dilakukan sesuai dengan tahapan Yusrida

Tahap	Aktivitas	1	2	3	Justifikasi
					(hasil terdapat pada **bagian 6.2.2.1.1)**
	Penilaian Risiko	✓			Dapat dilakukan sesuai dengan tahapan Yusrida dengan menggunakan metode FMEA. (hasil terdapat pada **bagian 6.2.2.1.2)**
Analisis Dampak Bisnis	Pendataan Proses Bisnis dan TI		✓		• Dapat dilakukan sesuai dengan tahapan Yusrida • Pendataan proses bisnis dan layanan TI yang terkait dilakukan berdasarkan dengan ruang lingkup yang telah ditentukan (hasil terdapat pada **bagian 6.2.2.2.1)**
	Prioritisasi Layanan TI		✓		Aktivitas ini dilakukan dengan melakukan perubahan. Objek studi kasus yaitu PDAM Surya Sembada Kota Surabaya belum melakukan analisa dampak bisnis dan melakukan prioritasi proses bisnis sehingga kesulitan dalam menentukan prioritasi layanan TI. Maka analisis dampak gangguan dilakukan terlebih dahulu sebagai dasar dalam penentuan prioritasi layanan TI dan proses bisnis serta
	Prioritisasi Proses Bisnis		✓		
	Analisis Dampak Gangguan		✓		

Tahap	Aktivitas	1	2	3	Justifikasi
					penentuan waktu pemulihan. Oleh karena itu urutan dalam melaksanan analisis dampak bisnis menjadi : 1. Pendataan Proses Bisnis dan TI Analisis Dampak Ganggu 2. Prioritisasi Proses Bisnisan 3. Prioritisasi Layanan TI 4. Penentuan Waktu Pemulihan (hasil terdapat pada **bagian 6.2.2.2.2, 6.2.2.2.3** dan **6.2.2.2.4)**
	Penentuan Waktu Pemulihan		✓		Dilakukan dengan melihat prioritasi proses bisnis dan layanan TI. (hasil terdapat pada **bagian 6.2.2.2.5)**
Strategi keberlangsungan Bisnis	Penentuan Strategi Preventif		✓		Dilakukan sesuai dengan tahapan Yusrida dengan mengacu kepada suatu *best practice*. Namun ditambahkan sub aktivitas yaitu penentuan mitigasi Risiko. Oleh karena itu urutan dalam penentuan strategi keberlangsungan bisnis bertambah menjadi : 1. Penentuan Strategi Preventif 2. Penentuan Mitigasi Risiko
	Penentuan Strategi Saat Gangguan		✓		
	Penentuan Strategi Pemulihan		✓		
	Koreksi Terhadap Strategi		✓		

Tahap	Aktivitas	1	2	3	Justifikasi
					3. Penentuan Strategi Saat Gangguan 4. Penentuan Strategi Pemulihan 5. Koreksi Terhadap Strategi (hasil terdapat pada **bagian 6.2.2.3)**
Rencana Pemulihan Bencana	Pendataan Aset Teknologi informasi	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.2.4.1)**
	Pendataan Vendor	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.2.4.2)**
	Pembuatan Kontrol		✓		Bentuk kontrol dibuat dengan disatukan pada strategi mitigasi risiko.
	Permintaan Aktivasi dan Deaktivasi	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.2.4.3)**
	Skenario Pengujian	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.3.1)**
	Evaluasi Bentuk Kontrol			✓	Tidak dilakukan karena perusahaan memutuskan untuk tidak melakukan.
Pelatihan Karyawan	Penentuan Jenis Pelatihan	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.2.5.2)**
	Mekanisme Penyampaian Pelatihan	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.2.5.1)**

Tahap	Aktivitas	1	2	3	Justifikasi
	Rencana Kebutuhan Pelatihan	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.2.5.3)**
	Pelaksanaan pelatihan			✓	Tidak dilakukan karena perusahaan memutuskan untuk tidak melakukan.
Fase 3. Pemantuan dan Review					
Pengujian BCP	Rencana Mekanisme Pengujian	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.3.1)**
	Pengujian			✓	Tidak dilakukan karena perusahaan memutuskan untuk tidak melakukan.
	Pencatatan Temuan			✓	Tidak dilakukan karena perusahaan memutuskan untuk tidak melakukan.
	Dokumentasi Hasil Pengujian			✓	Tidak dilakukan karena perusahaan memutuskan untuk tidak melakukan.
Fase 4. Pemeliharaan dan Peningkatan					
Peninjauan Keberlangsungan bisnis	Penentuan Periode Waktu Peninjauan	✓			Dapat dilakukan sesuai dengan tahapan Yusrida. (hasil terdapat pada **bagian 6.2.4)**
	Peninjauan Secara Berkala			✓	Tidak dilakukan karena perusahaan memutuskan untuk tidak melakukan. Namun telah dibuat perangkat peninjauan yaitu formulir peninjauan keberlangsungan bisnis dan formulir peninjauan manajemen. (hasil terdapat pada **bagian 6.2.4)**
	Pengkajian Ulang Terhadap rencana			✓	
	Pertimbangan Terhadap Perubahan			✓	

Dari keseluruhan aktivitas pada tiap tahapan metode Yusrida yaitu yang pertama pada **fase 1-Perencanaan** dimana terdapat 7 sub-aktivitas dan keseluruhan aktivitas tersebut dapat diimplementasi tanpa adanya modifikasi pada metode BCP.

Kemudian pada **fase-2 Implementasi dimana** terdapat 5 aktivitas, terdapat aktivitas yang tidak dapat diimplementasi yaitu pelaksanaan pelatihan karyawan. Hal tersebut disebabkan karena objek studi kasus yaitu PDAM Surya Sembada Kota Surabaya memutuskan untuk tidak melakukan.

Sedangkan aktivitas yang dapat dilakukan namun mengalami perubahan adalah analisis dampak bisnis dan pembuatan strategi keberlangsungan bisnis. Analisis dampak bisnis disesuaikan dengan kondisi perusahaan dimana perusahaan belum melakukan dan memiliki dasar penilaian untuk menentukan prioritasi proses bisnis dan layanan TI. Sehingga aktivitas analisa dampak gangguan yang terdiri atas dampak finansial, reputasi dan operasional digunakan sebagai dasar penentuan tingkat kritikalisasi dimana tingkat kritikalisasi atau prioritasi tersebut dapat dijadikan sebagai dasar dalam penentuan waktu pemulihan. Kemudian aktivitas penentuan strategi keberlangsungan bisnis dimana ditambahkan satu strategi baru yaitu mitigasi untuk setiap risiko yang bernilai *very high* sehingga risiko dapat terminimalisir. Serta aktivitas penentuan bentuk kontrol pada tahapan perencanaan pemulihan bencana dimana digabung pada strategi preventif dan mitigasi risiko.

Selanjutnya pada pada **fase 3-Pemantauan dan Review** dari 4 sub-aktivitas, aktivitas yang dilakukan adalah pembuatan rencana dan mekanisme pengujian sedangkan pelaksanaan tidak dapat dilakukan. Hal tersebut disebabkan karena objek studi kasus yaitu PDAM Surya Sembada Kota Surabaya memutuskan untuk tidak melakukan.

Yang terakhir yaitu **fase 4- pemeliharaan dan peningkatan,** dari 4 sub-aktivitas hanya aktivitas penentuan dan perencanaan peninjauan yang dapat dilakukan. Sedangkan aktivitas

pelaksanaan peninjauan tidak dapat dilakukan Hal tersebut disebabkan karena objek studi kasus yaitu PDAM Surya Sembada Kota Surabaya memutuskan untuk tidak melakukan. Sedangkan untuk aktivitas-aktivitas lainnya dapat dilakukan sesuai dengan metode BCP yang dibuat oleh Yusrida tanpa adanya perubahan yang berarti.

Dari hasil evaluasi didapatkan bahwa metode BCP yang dibuat oleh Yusrida masih memerlukan perbaikan dan penambahan pedoman. Dimana pedoman yang dimaksud adalah dalam melakukan aktivitas analisis risiko dan analisis dampak gangguan pada fase 2-Implementasi. Serta disarankan untuk tetap menjalankan seluruh aktivitas pada tahapan metodologi BCP Yusrida karena seluruh aktivitas tersebut dibutuhkan dalam pembuatan suatu BCP. Namun diantara keseluruhan aktivitas, aktivitas harus dilakukan dengan penyesuaian terhadap kondisi dan kebutuhan perusahaan. Penyesuain juga dapat berupa konten dan urutan aktivitas.

Halaman ini sengaja dikosongkan

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini dibahas mengenai kesimpulan dari seluruh proses yang telah dilakukan dan saran yang dapat diambil untuk pengembangan yang lebih baik.

7.1. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan dapat ditarik kesimpulan mengenai implementasi metodologi pembuatan dokumen perencanaan keberlangsungan bisnis pada PDAM Surya Sembada Kota Surabaya yaitu:

1. Penelitian ini menghasilkan analisis dan penilaian risiko untuk teknologi informasi pada PDAM Surya Sembada Kota Surabaya dengan menggunakan metode OCTAVE dan FMEA. Hasil dari analisis dan penilaian risiko adalah sebagai berikut:

   - Dari hasil identifikasi risiko yang dilakukan dengan menggunakan metode OCTAVE didapatkan 48 risiko terkait teknologi informasi yaitu 19 risiko untuk kategori perangkat keras, 6 risiko untuk kategori jaringan, 7 risiko untuk kategori perangkat lunak, 13 risiko untuk kategori data dan 3 risik untuk kategori sumber daya manusia.
   - Terdapat 4 risiko dengan level Very High yaitu server down, human error / pelanggaran , network trouble dan data tidak dapat diakses / tidak tersedia.

   - Terdapat 20 risiko dengan level high dan 14 risiko dengan level medium dan 10 risiko dengan level low.

2. Penelitian ini menghasilkan analisis dampak bisnis untuk PDAM Surya Sembada Kota Surabaya. Hasil dari analisis dampak bisnis adalah sebagai berikut:

   - Urutan analisis dampak bisnis yang dilakukan adalah pendataan proses bisnis perusahaan, kemudian analisis dampak dari adanya gangguan berdasarkan segi finansial, reputasi dan operasional, prioritasi proses bisnis, prioritasi layanan TI dan penentuan waktu pemulihan.
   - Berdasarkan hasil dari analisa dampak gangguan dan pengkategorian tingkat kritis yang dibuat oleh peneliti serta konfirmasi dengan perwakilan pihak TSI PDAM Surya Sembada Kota Surabaya terdapat 8 proses bisnis yang dianggap kritis dengan rincian 3 proses bisnis kritis pada fungsional bisnis keuangan. Kemudian 2 proses bisnis kritis pada fungsional bisnis pelayanan erta 3 proses bisnis kritis pada fungsional bisnis TSI.
   - Terdapat 15 layanan TI yang bersifat kritis dan 5 layanan TI yang bersifat penting pada PDAM Surya Sembada kota Surabaya terkait bagian Keuangan, bagian Pelayanan dan bagian TSI.
   - Terdapat identifikasi nilai MTD, RTO dan RPO yang didapatkan dari tingkat kritis masing-masing proses bisnis. Semakin kritis proses bisnis tersebut maka waktu pemulihan yang direkomendasikan adalah semakin kecil.

3. Implementasi metodologi *Business Continuity Plan* yang dilakukan di PDAM Surya Sembada Kota Surabaya menghasilkan sebuah dokumen perencanaan keberlangsngan bisnis yang sesuai dengan kebutuhan perusahaan. Dokumen BCP ini terdiri atas elemen-elemen utama sebagai berikut :

a. Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis
b. Peninjauan Keberlangsungan Bisnis
c. Analisis Risiko
d. Analisis Dampak Bisnis
e. Strategi Keberlangsungan Bisnis
f. Rencana Pemulihan Bencana
g. Pelatihan Karyawan
h. Pengujian BCP

4. Dari keseluruhan aktivitas pada tiap tahapan metode Yusrida terdapat beberapa aktivitas yang tidak dapat diimplementasi yaitu pelatihan karyawan, pengujian BCP dan peninjauan keberlangsungan bisnis. Sedangkan untuk aktivitas yang dapat dilakukan namun mengalami perubahan adalah aktivitas penentuan strategi keberlangsungan bisnis dan untuk aktivitas-aktivitas lainnya dapat dilakukan sesuai dengan metode BCP yang dibuat oleh Yusrida tanpa adanya perubahan yang berarti. Dari hasil evaluasi didapatkan bahwa metode BCP yang dibuat oleh Yusrida masih memerlukan perbaikan dan penambahan pedoman. Serta disarankan untuk tetap menjalankan seluruh aktivitas pada tahapan metodologi BCP Yusrida karena seluruh aktivitas tersebut dibutuhkan dalam pembuatan suatu BCP. Namun diantara keseluruhan aktivitas, beberapa harus dilakukan dengan penyesuaian terhadap kondisi dan kebutuhan perusahaan.

7.2. Saran

Berdasarkan hasil penelitian tugas akhir ini, maka saran yang dapat diberikan untuk pengembangan penelitian selanjutnya antara lain:

1. Penelitian ini memiliki keterbatasan yaitu ruang lingkup penelitian hanya pada 3 fungsional bisnis dimana suatu BCP idealnya adalah untuk keseluruhan perusahaan. Hal

tersebut dikarenanakan keterbatasan perizinan birokrasi. Oleh karena itu diharapkan untuk penelitian selanjutnya dapat mengembangkan BCP secara menyeluruh pada PDAM Surya Sembada Kota Surabaya.

2. Diharapkan pada penelitian selanjutnya dapat melanjutkan hingga tahap pembuatan prosedur, pengujian dan peninjauan keberlangsungan bisnis sehingga dokumen BCP benar-benar dapat diimplementasikan secara keseluruhan untuk menjaga keberlangsungan bisnis di PDAM Surya Sembada Kota Surabaya.

3. Dalam melakukan analisis dampak bisnis tepatnya analisa dampak gangguan, terdapat kesulitan dalam melakukan perhitungan estimasi kerugian dampak finansial, reputasi dan operasional dikarenakan pada metode Yusrida belum terdapat panduan secara jelas untuk perhitungan tersebut. Oleh karena itu perlu ada penelitian lanjutan yang membahas dasar perhitungan dalam melakukan analisa dampak bisnis.

4. Kedepannya perlu adanya beberapa penelitian lain dengan studi empiris metode BCP pada studi kasus lain sehingga dapat dapat dilakukan analisis mengenai keunikan dari BCP dan perbedaan implementasi sebagai masukan dalam perbaikan dan penyempurnaan metode BCP.

DAFTAR PUSTAKA

[1] PDAM Surya Sembada Kota Surabaya, "Sejarah & Status PDAM Surya Sembada Kota Surabaya." [Online]. Available: http://www.pdam-sby.go.id/page.php?get=sejarah_status_pdam&bhs=1. [Accessed: 03-Jan-2018].

[2] PDAM Surya Sembada Kota Surabaya, "Jumlah Pelanggan Tahunan." [Online]. Available: http://www.pdam-sby.go.id/page.php?get=jumlah_pelanggan_tahunan&bhs=1. [Accessed: 03-Jan-2018].

[3] S. Snedaker and C. Rima, *Business Continuity and Disaster Recovery Planning for IT Professionals*, vol. XXXIII, no. 2. 2014.

[4] S. S. J. Lindstrom, "Business Continuity Planning Methodology. Disaster Prevention and Management:," *An Int. J.*, pp. 243–255, 2010.

[5] U. Solehudin, "Business Continuity and Disaster Recovery Plan," 2005.

[6] M. M. Hanafi, "Risiko, Proses Manajemen Risiko, dan Enterprise Risk Management," pp. 1–40, 2014.

[7] H. A. Salim, *Asuransi Dan Manajemen Risiko*. Jakarta: Raja Grafindo Persada, 2007.

[8] N. S. Publication, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology,"

vol. 30, no. July, 2002.

[9] M. Spremic and M. Popovic, “Emerging issues in IT governance: implementing the corporate IT risks management model,” *WSEAS Trans. Syst.*, vol. 7, no. 3, 2008.

[10] ISO/IEC 27005 and ISO, “ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management,” *International Organization for Standardization, ISO*. pp. 1–64, 2011.

[11] ISACA, “T he R isk IT F ramework,” 2009.

[12] M. Crouchy, D. Galai, and R. Mark, *THE RISK ESSENTIALS OF MANAGEMENT*. New York: McGraw-Hill Education, 2014.

[13] S. A. Torabi, R. Giahi, and N. Sahebjamnia, “An enhanced risk assessment framework for business continuity management systems,” *Saf. Sci.*, vol. 89, pp. 201–218, 2016.

[14] J. Rupert, “The Relationship Between the Business Impact Analysis and Risk Assessment,” 2013. [Online]. Available: http://perspectives.avalution.com/2013/the-relationship-between-the-business-impact-analysis-and-risk-assessment/. [Accessed: 12-Jan-2018].

[15] A. Berman, “Risk Management and Business Continuity: Improving Business Resiliency.” [Online]. Available: http://www.riskmanagementmonitor.com/risk-management-and-business-continuity-improving-business-resiliency/. [Accessed: 12-Jan-2018].

[16] C. Alberts and A. Dorofee, “Introduction to the

OCTAVE Approach," *... , PA, Carnegie Mellon ...*, no. August, pp. 1–37, 2003.

[17] Dyadem Engineering Corporation, *Guidelines for Failure Mode and Effects Analysis for Automotive , Aerospace and General Manufacturing Industries*. 2003.

[18] D. H. Stamatis, *Failure Mode and Effect Analysis FMEA from Theory to Execution Second Edition*. Milwaukee: ASQ, 2003.

[19] Dyadem Engineering Corporation, *Guidelines for Failure Mode and Effects Analysis For Automotive, Aerospace and General Manufacturing Industries*. Ontario Canada: DYADEM Press, 2003.

[20] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, "Contingency Planning Guide for Federal Information Systems.," *NIST Spec. Publ. 800-34 Rev. 1*, no. May, p. 150, 2010.

[21] S. A. Torabi, H. Rezaei Soufi, and N. Sahebjamnia, "A new framework for business impact analysis in business continuity management (with a case study)," *Saf. Sci.*, vol. 68, pp. 309–323, 2014.

[22] M. Devargas, "Survival is not compulsory: an introduction to business continuity planning," *Comput. Secuirty*, vol. 18, pp. 35–46, 1999.

[23] BSI, "Business Continuity Management for SMEs using the Cloud," *Fed. Off. Inf. Secur.*, p. 45, 2013.

[24] P. P. Ardhiatno, "Perancangan business ...., Prabowo Priyo Ardhiatno, Fasilkom UI, 2013," 2013.

[25] Government of Indonesia, “PP No. 82/2012 Penyelenggaraan Sistem dan Transaksi Elektronik,” pp. 1–54, 2012.

[26] C. McAndrew, “Business Continuity Framework,” *Griffith Univ.*, no. 07, pp. 1–24, 2013.

[27] P. Ranjan, P. Kumar, and K. Abhishek, “Business Continuity Planning in Indian Perspective,” *J. Adv. Comput. Res. An Int. J.*, vol. 1, no. 1, 2012.

[28] Y. Muflihah, “BUSINESS CONTINUITY PLAN : SEBUAH USULAN METODOLOGI, EMPIRIS PT PLN (Persero) DISTRIBUSI JAWA TIMUR.” 2017.

[29] Queensland Government, “Testing Business Continuity Plans,” Queensland.

[30] T. Bronack, “Overview of How to Test a Business Continuity Plan,” 2012.

[31] S. L. Putri, “Perancangan Business Continuity Plan Untuk Teknologi Informasi Pada Studi Kasus STIE Perbanas,” Institut Teknologi Sepuluh Nopember, 2015.

[32] D. K. Informasi, “Incident Handling Infrastruktur Fisik Indonesia Government Computer Security Incident Response Team (Gov-CSIRT).”

[33] D. K. Informasi, “Incident Handling Network Indonesia Government Computer Security Incident Response Team (Gov-CSIRT).”

[34] D. K. Informasi, “Incident Handling Database Indonesia Government Computer Security Incident Response Team (Gov-CSIRT).

BIODATA PENULIS

Penulis bernama lengkap Cindy Alicia Sahara lahir di Kediri Jawa Timur pada tanggal 20 Maret 1996. Penulis merupakan anak pertama dari tiga bersaudara. Penulis telah menempuh pendidikan formal di SDI Al-fath Pare, SMP Negeri 2 Pare dan SMA Negeri 2 Pare. Setelah lulus dari sekolah menengah, penulis meneruskan pendidikan di Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya dan terdaftar dengan NRP 5210100172. Di Jurusan Sistem Informasi penulis mengambil bidang studi Manajemen Sistem Informasi (MSI). Selama masa perkuliahan, penulis aktif di BEM ITS pada BSO ITS Education Care Center dan organisasi HMSI menjadi staff departemen Kewirausahaan dan Sekretaris Umum HMSI Kolaborasi. Dan aktif di kepanitiaan/*volunteer* di program kerja HMSI, ISE dan BEM ITS. Dan di akhir masa perkuliahan, penulis memilih topik Tugas Akhir pada bidang minat lab MSI (Manajemen Sistem Informasi). Apabila terdapat pertanyaan mengenai Tugas Akhir ini, penulis dapat dihubungi melalui e-mail cindyaliciasahara@gmail.com

Halaman ini sengaja dikosongkan

LAMPIRAN A

Lampiran Hasil Wawancara Kondisi Kekinian

Tabel A.1 Hasil Wawancara Kondisi Kekinian terkait TI

Narasumber	Nurlillah Satria Pratama
Jabatan	Supervisor TSI
Tanggal	26 April 2018
Lokasi	PDAM Surya Sembada Kota Surabaya
Tujuan	Untuk mengetahui proses bisnis yang terkait TI dan kondisi kekinian dari PDAM Surya Sembada Kota Surabaya.

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
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;

No.	Pertanyaan	Jawaban
		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**

No.	Pertanyaan	Jawaban
		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*.
5.	Apakah ada pihak diluar TSI yang terkait dengan pengelolaan TI? Bagaimana perannya? (Vendor -> layanannya apa)	PDAM berkerjasama dengan pihak luar terkait dengan pengelolaan kerusakan printer,sewa komputer dan sewa printer selain itu dengan switcher terkait dengan pembayaran online dimana pihak switcher sebagai penjembatan ke customer, kerjasama dengan ISP

Halaman ini sengaja dikosongkan

LAMPIRAN B

Lampiran Hasil Wawancara l Analisis Risiko

Tabel B.1 Hasil Wawancara Analisis Risiko

Narasumber	Nurlillah Satria Pratama
Jabatan	Supervisor TSI
Tanggal	26 April 2018
Lokasi	PDAM Surya Sembada Kota Surabaya
Tujuan	Wawancara dilakukan untuk melakukan identifikasi risiko. Hal ini dilakukan dengan menggali informasi terkait aset kritis teknologi dan sistem informasi, ancaman dan kerentanan terhadap aset TI, serta kebutuhan keamanan dan praktik kemanan TI yang telah diterapkan.

Fase 1 Membangun aset berdasarkan ancaman profil		
Obyektif 1 : Mendapatkan informasi mengenai aset kritis teknologi dan sistem informasi yang telah digunakan organisasi		
No.	Pertanyaan	Jawaban
1.	Apa sajakah fungsional organisasi pada PDAM yang menggunakan teknologi dan sistem informasi?	Seluruh fungsi organisasi menggunakan teknologi dan sistem informasi
2.	Apa saja aset TI yang dimiliki oleh PDAM ? (contoh : data, software,hardware,jaringan, people)	- 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.	Manakah aset TI yang termasuk kritis ?	Server, storage, database, data, software
4.	Komponen utama setiap aset TI ?	-
5.	Aplikasi atau sistem 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 aset teknologi dan sistem informasi		
No.	Pertanyaan	Jawaban
1.	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
2.	Gangguan apa saja yang pernah terjadi pada aset teknologi dan sistem informasi ? (gangguan : bencana alam, erorr, virus, malware, bug,human error, jaringan terputus, server down)	- Jaringan : Jaringan terputus,switch mati, network control module mengalami trouble - Hardware : kerusakan hardware, server down, storage corrupt, - Software : error software, bug, kesalahan setting, salah coding - Database : lambat, Data berubah / salah update -
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

Obyektif 3: Mendapatkan informasi mengenai praktik keamanan terkini yang telah dilakukan oleh organisasi dan kebutuhan keamanan TI organisasi

No.	Pertanyaan	Jawaban
1.	Apa usaha yang telah dilakukan organisasi dalam menghadapi ancaman yang ada?	- Renewal Antivirus setiap tahun - Melakukan pembelian software VEEM untuk solusi backup virtual machine (VM) - Sedang proses pembelian server baru - Proses pemindahan ruang server dari lantai 4 ke lantai 3
2.	Adakah solusi/strategi backup saat ini?	Saat ini backup dilakukan setiap hari
3.	Berapa kali melakukan backup data pada area fungsional bisnis kritis ? (jangka waktu)	- Database : 1 kali dalam 1 hari pada akhir hari - Server : setiap hari - Menggunakan aplikasi VM
4.	Berapa kali organisasi melakukan maintenance terhadap aset TI yang mendukung fungsional bisnis kritis organisasi ?	Untuk database setiap saat ketika perlu dilakukan penambahan index Sedangkan untuk perangkat keras (PC) hanya berupa pembersihan.
5.	Apakah terdapat mekanisme proteksi keamanan aset teknologi dan informasi pada fungsional bisnis kritis organisasi ?	aplikasi mobile untuk data pelanggan tidak akan di tampilkan nama dan alamat
6.	Apakah organisasi telah menerapkan standar keamanan untuk melindungi aset TI?	Belum

7.	Keamanan di PC menggunakan apa ? (antivirus)	Antivirus Kaspersky
8.	Apakah setiap user memiliki hak akses yang berbeda?	Untuk masuk ke aplikasi memiliki hak akses yang berbeda
9.	Apakah terdapat kebijakan terkait keamanan akun user ? (misal mengganti password secara periodik)	Ada, tetapi tidak dijalankan
10.	Apakah terdapat kebijakan mengenai keamanan terkait jaringan ?	Ada tetapi tidak menerapkan manajemen kabel
Obyektif 4: Mengidentifikasi kelemahan organisasi		
No.	Pertanyaan	Jawaban
1.	Apakah terdapat SOP / prosedur tertulis terkait keamanan teknologi dan sistem informasi ?	Belum ada
2.	Apakah terdapat SOP / prosedur tertulis jika terjadi gangguan ?	Belum ada
3.	Apakah terdapat permasalahan organisasi apabila terjadi gangguan pada aset teknologi dan informasi?	-Jika terjadi gangguan otomatis layanan terhadap pelanggan terganggu - pendapatan tertunda - pelayanan terhadap pelanggan terhenti
4.	Apa saja kelemahan teknis untuk aset TI yang ada pada organisasi?	- Belum terdapat prosedur tertulis jika terjadi gangguan pada proses bisnis - Tidak adanya maintenaince secara rutin untuk aset TI - Belum menerapkan standar keamanan yang memadai

Fase 2 Identifikasi Kelemahan Infrastruktur		
Obyektif 1 : Mengidentifikasikan komponen aset teknologi dan informasi yang diterapkan		
No.	Pertanyaan	Jawaban
1.	Apakah seluruh sistem yang digunakan memiliki kebutuhan infrastruktur yang sama?	Setiap sistem memiliki kebutuhan infrastruktur yang tidak sama namun kebutuhan dasarnya sama.
2.	Apa sajakah komponen yang digunakan pada aset kritis organisasi? (jaringan : kabel, switch, router.	- Server :
3.	Apa saja kerentanan dari masing-masing komponen TI dari organisasi? (hardware,software,network,people, data)	- Kinerja database lambat karena kinerja processor, IO, dan memori menurun - Gangguan atau kerusakan dikarenakan putusnya kabel - Karyawannya sedikit sehingga jika berhalangan hadir akan kekurangan resource - PC tidak dapat berfungsi karena mengalami kerusakan - Genset hanya melingkupi data center - Server down - Sabotase pada database - Network modul control mengalami trouble - Pemasangan kabel yang tidak menerapkan cable management - Belum memiliki server cadangan - Tidak ada aktivitas pengecekan penggunaan hak akses

Obyektif 2 : **Mengidentifikasikan kelemahan aset teknologi informasi yang diterapkan pada fungsional kritis organisasi**		
No.	Pertanyaan	Jawaban
1.	Kelemahan teknis apa saja yang terdapat pada organisasi terkait dengan teknologi informasi?	Aplikasi yang di gunakan menggunakan teknologi client server
2.	Apakah ruang penempatan aset TI telah dibuat sesuai dengan standar dan rancangan yang dapat menghindari dari ancaman seperti bencana alam (kebakaran, gempa, dl) serta dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Kalau mengikuti standar atau tidaknya belum. Tetapi ruang server (data center) sudah dilengkapi dengan smoke detector, presission cooling system data center, CCTV, finger print untuk akses masuk, buku tamu bagi siapa saja yang diberi hak untuk berkunjung dan sistem untuk memonitoring server bawaan dari server itu sendiri.
3.	Apakah terdapat proses pemeriksaan pada tiap aset yang digunakan untuk mengidentifikasi kemungkinan adanya celah kelemahan?	Tidak kecuali untuk server
Obyektif 3		
1.	Apa saja layanan TI yang ada pada organisasi dan bagaimana tingkat prioritas untuk masing masing layanan ?	Yang paling kritis adalah plikasi yang digunakan pada bagian keuangan (Sistem Informasi Keuangan)
2.	Apa saja aktivitas/proses bisnis yang berlangsung pada proses bisnis kritis yang dimiliki organisasi? Bagaimana prioritisasi aktivitas tersebut?	Yang paling kritis adalah proses bisnis yang ada pada bagian keuana yaitu penerbitan rekening dan pembayaran.
3.	Apakah dampak yang terjadi pada layanan bila terjadi gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis)	Kalau untuk finansial tidak pernah membuat estimasi tetapi pasti ada untuk dampak operasional dan reputasi.
4.	Apabila terjadi gangguan bagaimana waktu yang ditoleransi	Belum mendefinisikan

	organisasi terkait gannggguan tersebut ?	
5.	Apakah organisasi memiliki toleransi waktu dalam tahap pemulihan sistem apabila terjadi gangguan?	Belum mendefinisikan, seselesainya waktu proses perbaikan
6.	Apa yang dilakukan organisasi terhadap proses bisnis kritis bila terjadi gangguan ?	User segera menghubungi bagian TSI, kemudian langsung menangani gangguan tersebut.
7.	Sumber daya apa saja yang anda butuhkan untuk dapat meresume pekerjaan anda disaat terjadinya bencana ?	- Komputer cadangan - Printer cadangan - Server cadangan -

Halaman ini sengaja dikosongkan

LAMPIRAN C

Lampiran Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian Keuangan

Tabel C.1 Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian Keuangan

Narasumber	Ira Nuraini
Jabatan	Senior Staf Penerimaan dan Pendistribusian Rekening (Keuangan)
Tanggal	26 April 2018
Lokasi	PDAM Surya Sembada Kota Surabaya
Tujuan	Wawancara dilakukan untuk melakukan identifikasi

Obyektif 1 : Untuk mengidentifikasi layanan TI, proses bisnis TI dan aktivitas TI serta tingkat prioritasnya. Selain itu bertujuan untuk dapat mengetahui toleransi waktu dan dampak yang terjadi apabila adanya gangguan pada proses bisnis.		
No.	Pertanyaan	Jawaban
1.	Deskripsikan aktivitas/ proses bisnis apa saja yang ada di bagian Keuangan ?	• Pengawasan rekening dan penerbitan penagihan • Penagihan rekening swasta • Penagihan rekening pemerintah Penagihan rekening pendapatan lain-lain
2.	Apa saja layanan TI yang digunakan ? Apa saja aktivitas TI terkait proses bisnis tersebut ? (aplikasi) & Aplikasi apa yang digunakan pada bagian (per subbagian)?	• Billing • (Rekening) • Billing (PRS) • Billing (PRP) • Billing (Kas) • SKA • Axapta

3.	Risiko/gangguan apa saja yang pernah dan mungkin terjadi ? (TT dan Non TI)	Server down sehingga pembayaran tertunda
4.	Apakah organisasi sudah memperhitungkan kegagalan proses bisnis bila terjadi ganguan ?	belum

Dampak gangguan dibagi menjadi tiga dampak ditinjau dari aspek finansial, dampak ditinjau dari reputasi dan juga dampak ditinjau dari target teknis.

Narasumber	Nurlillah Satria Pratama
Jabatan	Supervisor TSI
Tanggal	Juni 2018
Lokasi	PDAM Surya Sembada Kota Surabaya

1. Dampak Finansial

Ketentuan penilaian aspek finansial
0 bila tidak berdampak pada aspek finansial
1 bila adanya penambahan biaya kurang dari 5% dari anggaran proses bisnis
2 bila adanya penambahan biaya 5-10% dari anggaran proses bisnis
3 bila adanya penambahan biaya 11-20% dari anggaran proses bisnis
4 bila adanya penambahan biaya 21-25% dari anggaran proses bisnis
5 bila adanya penambahan biaya lebih dari 25% dari anggaran proses bisnis

Proses Bisnis terkait sistem	**Skor**
Pengawasan rekening dan penerbitan penagihan	4
Penagihan rekening swasta	3
Penagihan rekening pemerintah	3
Penagihan rekening pendapatan lain-lain	3

2. Dampak Reputasi

Kententuan penilaian aspek reputasi

0 bila tidak berdampak pada aspek reputasi
1 bila adanya penurunan yang sangat kecil dari reputasi perusahaan
2 bila adanya penurunan yang kecil dari reputasi perusahaan
3 bila adanya penurunan yang sedang dari reputasi perusahaan
4 bila adanya penurunan yang tinggi dari reputasi perusahaan
5 bila adanya penurunan yang sangat tinggi dari reputasi perusahaan

Proses Bisnis terkait sistem	Skor
Pengawasan rekening dan penerbitan penagihan	5
Penagihan rekening swasta	4
Penagihan rekening pemerintah	4
Penagihan rekening pendapatan lain-lain	3

3. Dampak Operasional

Kententuan penilaian aspek operasional
0 bila tidak berdampak pada aspek operasional
1 bila adanya penurunan hasil kurang dari 5% dari target proses bisnis
2 bila adanya penurunan hasil 5-10% dari target proses bisnis
3 bila adanya penurunan hasil 11-20% dari target proses bisnis
4 bila adanya penurunan hasil 21-25% dari target proses bisnis
5 bila adanya penurunan hasil lebih dari 25% dari target proses bisnis

Proses Bisnis terkait sistem	Skor
Pengawasan rekening dan penerbitan penagihan	4
Penagihan rekening swasta	3
Penagihan rekening pemerintah	3
Penagihan rekening pendapatan lain-lain	3

Halaman ini sengaja dikosongkan

LAMPIRAN D

Lampiran Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian Pelayanan

Tabel D.1 Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian Pelayanan

Narasumber	Dani
Jabatan	Senior Staf Pelayanan
Tanggal	Juni 2018
Lokasi	PDAM Surya Sembada Kota Surabaya
Tujuan	Wawancara dilakukan untuk melakukan identifikasi

Obyektif 1 : Untuk mengidentifikasi layanan TI, proses bisnis TI dan aktivitas TI serta tingkat prioritasnya. Selain itu bertujuan untuk dapat mengetahui toleransi waktu dan dampak yang terjadi apabila adanya gangguan pada proses bisnis.		
No.	Pertanyaan	Jawaban
1.	Deskripsikan aktivitas/ proses bisnis apa saja yang ada di bagian Keuangan ?	- Pemasaran Billing Informasi Pelanggan - Customer Installation - Melakukan survey terkait lokasi pemasangan pada pelanggan - Pembuatan RAB - Pengelolaan Laporan Keluhan Pelanggan - Penanganan Keluhan
2.	Apa saja layanan TI yang digunakan ? Apa saja aktivitas TI terkait proses bisnis tersebut ? (aplikasi) & Aplikasi apa yang digunakan pada bagian (per subbagian)?	- Billing MBD - Billing PB - Billing SMS Center - Billing UPTIGA - Billing Customer Service - Billling Call Center - Arsip Digital - Aplikasi Foto Catat Meter

		- GIS (Sistem Informasi Geografis PDAM) - Arsip Digital - Billing Perencanaan - Billing PTJSR - Aplikasi Foto Materisasi
3.	Risiko/gangguan apa saja yang pernah dan mungkin terjadi ? (TT dan Non TI)	- Koneksi jaringan down - Hacking website
4.	Apakah organisasi sudah memperhitungkan kegagalan proses bisnis bila terjadi ganguan ?	belum

Dampak gangguan dibagi menjadi tiga dampak ditinjau dari aspek finansial, dampak ditinjau dari reputasi dan juga dampak ditinjau dari target teknis.

Narasumber	Nurlillah Satria Pratama
Jabatan	Supervisor TSI
Tanggal	Juni 2018
Lokasi	PDAM Surya Sembada Kota Surabaya

1. Dampak Finansial

Ketentuan penilaian aspek finansial
0 bila tidak berdampak pada aspek finansial
1 bila adanya penambahan biaya kurang dari 5% dari anggaran proses bisnis
2 bila adanya penambahan biaya 5-10% dari anggaran proses bisnis
3 bila adanya penambahan biaya 11-20% dari anggaran proses bisnis
4 bila adanya penambahan biaya 21-25% dari anggaran proses bisnis
5 bila adanya penambahan biaya lebih dari 25% dari anggaran proses bisnis

Proses Bisnis terkait sistem	**Skor**
Pemasaran	4

Customer Installation	3
Melakukan survey terkait lokasi pemasangan pada pelanggan	3
Pembuatan RAB	3
Pengelolaan Laporan Keluhan Pelanggan	2
Penanganan Keluhan	2

2. Dampak Reputasi

Kententuan penilaian aspek reputasi

0 bila tidak berdampak pada aspek reputasi
1 bila adanya penurunan yang sangat kecil dari reputasi perusahaan
2 bila adanya penurunan yang kecil dari reputasi perusahaan
3 bila adanya penurunan yang sedang dari reputasi perusahaan
4 bila adanya penurunan yang tinggi dari reputasi perusahaan
5 bila adanya penurunan yang sangat tinggi dari reputasi perusahaan

Proses Bisnis terkait sistem	**Skor**
Pemasaran	3
Customer Installation	3
Melakukan survey terkait lokasi pemasangan pada pelanggan	3
Pembuatan RAB	3
Pengelolaan Laporan Keluhan Pelanggan	2
Penanganan Keluhan	2

3. Dampak Operasional

Kententuan penilaian aspek operasional
0 bila tidak berdampak pada aspek operasional
1 bila adanya penurunan hasil kurang dari 5% dari target proses bisnis
2 bila adanya penurunan hasil 5-10% dari target proses bisnis
3 bila adanya penurunan hasil 11-20% dari target proses bisnis

4 bila adanya penurunan hasil 21-25% dari target proses bisnis 5 bila adanya penurunan hasil lebih dari 25% dari target proses bisnis

Proses Bisnis terkait sistem	**Skor**
Pemasaran	4
Customer Installation	3
Melakukan survey terkait lokasi pemasangan pada pelanggan	3
Pembuatan RAB	3
Pengelolaan Laporan Keluhan Pelanggan	2
Penanganan Keluhan	2

LAMPIRAN E

Lampiran Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian TSI

Tabel E.1 Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian TSI

Narasumber	Nurlillah Satria Pratama
Jabatan	Supervisor TSI
Tanggal	Juni 2018
Lokasi	PDAM Surya Sembada Kota Surabaya
Tujuan	Untuk mengidentifikasi layanan TI, proses bisnis TI dan aktivitas TI serta tingkat prioritasnya. Selain itu bertujuan untuk dapat mengetahui toleransi waktu dan dampak yang terjadi apabila adanya gangguan pada proses bisnis. Dampak gangguan dibagi menjadi tiga dampak ditinjau dari aspek finansial, dampak ditinjau dari reputasi dan juga dampak ditinjau dari target teknis.

1. Dampak Finansial	
Ketentuan penilaian aspek finansial 0 bila tidak berdampak pada aspek finansial 1 bila adanya penambahan biaya kurang dari 5% dari anggaran proses bisnis 2 bila adanya penambahan biaya 5-10% dari anggaran proses bisnis 3 bila adanya penambahan biaya 11-20% dari anggaran proses bisnis 4 bila adanya penambahan biaya 21-25% dari anggaran proses bisnis 5 bila adanya penambahan biaya lebih dari 25% dari anggaran proses bisnis	
Proses Bisnis terkait sistem	**Skor**
Melakukan pengawasan instalasi, perawatan dan perbaikan terhadap infrastruktur TI (Hardware dan Jaringan)	5

Melakukan pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)	4
Disaster Recovery Center	5
Penyediaan layanan email dan sistem informasi	2
Melakukan evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;	3
Melakukan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan	3
Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi	2
Melakukan pengawasan kegiatan *helpdesk support*.	2
Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan	2

2. Dampak Reputasi

Kententuan penilaian aspek reputasi

0 bila tidak berdampak pada aspek reputasi
1 bila adanya penurunan yang sangat kecil dari reputasi perusahaan
2 bila adanya penurunan yang kecil dari reputasi perusahaan
3 bila adanya penurunan yang sedang dari reputasi perusahaan
4 bila adanya penurunan yang tinggi dari reputasi perusahaan
5 bila adanya penurunan yang sangat tinggi dari reputasi perusahaan

Proses Bisnis terkait sistem	**Skor**
Melakukan pengawasan instalasi, perawatan dan perbaikan terhadap infrastruktur TI (Hardware dan Jaringan)	3
Melakukan pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)	3

Disaster Recovery Center	3
Penyediaan layanan email dan sistem informasi	3
Melakukan evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;	2
Melakukan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan	3
Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi	2
Melakukan pengawasan kegiatan *helpdesk support*.	1
Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan	1

3. Dampak Operasional	
Kententuan penilaian aspek operasional 0 bila tidak berdampak pada aspek operasional 1 bila adanya penurunan hasil kurang dari 5% dari target proses bisnis 2 bila adanya penurunan hasil 5-10% dari target proses bisnis 3 bila adanya penurunan hasil 11-20% dari target proses bisnis 4 bila adanya penurunan hasil 21-25% dari target proses bisnis 5 bila adanya penurunan hasil lebih dari 25% dari target proses bisnis	
Proses Bisnis terkait sistem	**Skor**
Melakukan pengawasan instalasi, perawatan dan perbaikan terhadap infrastruktur TI (Hardware dan Jaringan)	2
Melakukan pengawasan keamanan terhadap infrastruktur TI (Hardware dan Jaringan)	5
Disaster Recovery Center	5
Penyediaan layanan email dan sistem informasi	5
Melakukan evaluasi, pemeliharaan dan perbaikan aplikasi sistem informasi;	1

Melakukan pengembangan aplikasi baru sesuai perkembangan bisnis perusahaan	2
Melakukan pengawasan *backup-restore* database utama dan pengamanan aplikasi	3
Melakukan pengawasan kegiatan *helpdesk support*.	3
Melakukan pengawasan pemeliharan dan pengembangan database sesuai perkembangan bisnis perusahaan	2

LAMPIRAN F

Lampiran Penilaian Risiko

Tabel F.1 Hasil Wawancara dan Kuesioner Analisa Dampak Bisnis Bagian TSI

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
1	Hardware	Server dan Storage	Kerusakan komponen utama	Server Down	8	Jika terjadi akan berdampak pada hampir seluruh kegiatan operasional PDAM sehingga pemberian layanan terhadap pelanggan terhambat.	6	Kerusakan komponen hardware pernah terjadi sesekali waktu.	3	Sudah melakukan monitoring terhadap server secara rutin	108
2			Hacker		8		4	tidak pernah terjadi pada PDAM namun berpotensi untuk terjadi .	3	Metode deteksi dan kontrol berupa penggunaan firewall dan antivirus.	96
3			Kesalahan konfigurasi	Server Down	3	Jika terjadi dampak yang diakibatkan tidak terlalu fatal.	4	Kesalahan konfigurasi pernah terjadi pada instalasi layanan TI di PDAM namun tidak sering.	6	Metode deteksi memiliki efektifitas yang rendah	72

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
4			System overload (request terlalu banyak) / peak time	Server Down	5	Jika terjadi maka akan megakibatkan server tidak dapat beroperasi pada saat-saat yang sangat diperlukan.	3	Tidak pernah terjadi dan berpeluang kecil untuk terjadi.	3	Server selalu dimonitoring sehingga lebih cepat terdeteksi.	45
5			Gangguan jaringan		8	Jika terjadi akan berdampak pada hampir seluruh kegiatan operasional PDAM sehingga pemberian layanan terhadap pelanggan terhambat.	4	Jarang terjadi namun berpotensi untuk terjadi.	7	Metode deteksi belum efektif.	224
6			Kegagalan sistem operasi		8	Jika terjadi akan berdampak pada hampir seluruh kegiatan operasional PDAM sehingga pemberian layanan terhadap	3	Belum pernah terjadi dan tidak terlalu berpotensi tinggi untuk terjadi.	4	Sudah melakukan monitoring terhadap server secara rutin serta memang sengaja tidak dilakukan pembaharuan sistem operasi	96

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						pelanggan terhambat.				karena terkendala kompatibilitas terhadap aplikasi.	
7			Kerusakan sistem pengatur suhu		8	Kerusakan sistem pengatur suhu akan menyebabkan pernagkat keras server mengalami overheat sehingga dapat memungkinkan untuk terjadinya gangguan pada server.	4	Belum pernah terjadi namun potensi untuk terjadi relatif kecil.	5	Sudah melakukan monitoring terhadap server secara rutin namun belum secara rutin untuk ruangan dan infrastruktur keseluruhan.	160
8			Dos Attack		8	Dos Attack akan membuat server mengalami overload request sehingga memungkinkan untuk mengalami down.	3	Belum pernah terjadi namun potensi untuk terjadi relatif kecil.	6	Metode deteksi memiliki efektifitas yang rendah	144
9			Virus		8	Virus dapat menyerang sistem	4	Pernah terjadi dan berpotensi	2	Praktik deteksi dan kontrol berupa	64

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						pada server sehingga akan memungkinkan server untuk mengalami down.		untuk terjadi lagi.		penggunaan antivirus.	
10			Kerusakan UPS dan genset		6	Kerusakan UPS dan genset pada saat kondisi terjadi gangguan pada sumber utama listrik akan menyebabkan server tidak dapat beroperasi.	3	Belum pernah terjadi namun berpotensi untuk terjadi	5	Sudah terdapat monitoring dan maintenance yang dilakukan secara rutin yaitu setiap minggu dan setiap bulann.	90
11			Bencana alam		10	Selain mempengaruhi kegiatan operasional juga berpotensi untuk melukai karyawan.	2	Daerah Surabaya berpotensi rendah untuk terjadinya bencana alam	6	Belum terdapat metode preventif atau strategi alternatif untuk menganggulangi jika terjadi bencana.	120
12			overheat	Kebakaran ruang server	10	Kebakaran pada ruang server dapat membahayakan	4	Belum pernah terjadi namun potensi untuk	2	Sudah terdapat sistem pengatur suhu ruangan dan sistem pendeteksi	80

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						keselamatan karyawan.		terjadi relatif kecil.		kebakaran pada ruang server.	
13			Fluktuasi arus listrik/Konsletting		10		3	Berlum pernah terjadi dan potensi untuk terjadi sangat kecil karena sudah terdapat genset dan UPS yang dialokasikan untuk data center	4	Tidak terdapat praktik deteksi khusus jika terjadi konsletting namun sudah melakukan antisipasi dengan adanya sistem pendeteksi asap/ kebakaran serta sudah terdapat genset dan UPS	120
14		PC & Laptop	Kerusakan komponen	Kerusakan PC	6	PC yang rusak akan menghambat kegiatan operasional PDAM namun PDAM memiliki cadangan PC.	5	Kerusakan komponen hardware pernah terjadi sesekali waktu.	5	Karena tidak melakukan perawatan dan pemeliharaan secara rutin namun secara rutin melakukan pembersihan.	150
15			Virus dan malware				4	Belum pernah terjadi namun potensi untuk	2	Memiliki antivirirus yang cukup baik	48

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
								terjadi relatif kecil.			
16			Usia yang sudah tua dan usang				3	Kerusakan PC karena usia berpotensi untuk terjadi namun PDAM memiliki PC cadangan.	5	Melakukan monitoring setiap bulan dan perawatan setiap 6 bulan.	90
17			Kesalahan konfigurasi	PC/Laptop tidak dapat beroperasi	3	Terdapat PC cadangan	5	Kegagalan konfigurasi pernah terjadi pada saat waktu tertentu.	6	Tidak memiliki metode deteksi khusus terkait untuk mengantisi pasi kesalahan konfigurasi	90
18			Hacker		5	PC yang rusak akan menghambat kegiatan operasional PDAM namun PDAM memiliki cadangan PC.	4	Belum pernah terjadi namun berpotensi untuk terjadi.	6	Metode deteksi dan kontrol berupa penggunaan firewall dan antivirus.	120
19			Pemadaman listrik		3		6	Berpotensi untuk terjadi beberapa kali.	3	Sudah terdapat genset gedung.	54

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
20	Jaringan	switch, router dan acces point	Kerusakan infrastruktur jaringan (switch, hub,router, konektor kabel)	Network trouble	6	Kerusakan salah satu komponen saja dapat menyebabkan jaringan terganggu dan akan menghambat pengaksesan data serta penggunaan layanan TI.	6	Kerusakan komponen hardware pernah terjadi sesekali waktu dan berpotensi untuk terjadi lagi.	6	Sudah melakukan monitoring selama 12 jam.	216
21		Kabel	Media transmisi (kabel) tergigit tikus		8	Jaringan yang mengalami down akan mempengaruhi ketersediaan layanan sehingga berdampak pada keberlangsungan bisnis PDAM.	3	Kabel tergigit tikus belum pernah terjadi karena kabel sudah dilapisi dengan case khusus	4	kabel sudah dilapisi dengan case khusus	96
22		switch, router dan acces point	Kesalahan konfigurasi	Network trouble	4	Jika terjadi dampak yang diakibatkan tidak terlalu fatal.	5	Kegagalan konfigurasi pernah terjadi pada saat waktu tertentu.	6	Metode deteksi memiliki efektifitas yang rendah	120

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
23		Sistem jaringan	Virus dan malware		8	Jaringan yang mengalami down akan mempengaruhi ketersediaan layanan sehingga berdampak pada keberlangsungan bisnis PDAM.	4	Belum pernah terjadi namun potensi untuk terjadi relatif kecil karena PDAM setiap tahun selalu memperbarui antivirus.	4	Metode deteksi berupa penggunaan antivirus dan firewall.	128
24			Spoofing dan Sniffing		8	Spoofing dan sniffing menjadikan kecepatan koneksi berkurang secara drastis.	3	Belum pernah terjadi namun potensi untuk terjadi relatif kecil	7	Belum terdapat mekanisme deteksi	168
25		switch, router dan acces point	Pemadaman listrik	Network trouble	3	PDAM sudah memiliki genset gedung sehingga trouble hanya akan terjadi dalam waktu yang tidak lama.	4	Berpotensi untuk terjadi beberapa kali	5	PDAM sudah memiliki genset gedung.	60

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
				Network trouble							
26	Software	Billing, GIS dan Arsip Digital	Kesalahan instalasi dan konfigurasi	Software tidak dapat diakses	4	Kesalahan konfigurasi akan memungkinkan gangguan pada pengaksesan aplikasi.	6	Kesalahan konfigurasi dan instalasi terkait software pernah terjadi beberapa kali.	6	Metode deteksi memiliki efektifitas yang rendah.	144
27			Virus dan malware		6	Virus dan malware memungkinkan untuk terjadinya kerusakan software.	4	Belum pernah terjadi namun potensi untuk terjadi relatif kecil karena PDAM setiap tahun selalu memperbarui antivirus.	4	Metode deteksi berupa penggunaan firewall dan antivirus.	96
28			Perangkat keras yang tidak kompatibel		5	Mengakibatkan perpanjangan waktu pengembangan aplikasi sehingga	3	Belum pernah terjadi namun memiliki potensi yang kecil untuk terjadi.	3	Sudah melakukan pengecekan terhadap spesifikasi pernagkat keras	45

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						akan menghambat kinerja.				yang akan digunakan.	
29			Server down		8	Server down akan menyebabkan aplikasi tidak dapat diakses.	6	Pernah terjadi beberapa kali dan berpotensi untuk terjadi lagi.	4	Sudah terdapat server cadangan namun masih dari pihak ketiga.	192
30			Kesalahan koding		7	Mengakibatkan perpanjangan waktu pengembangan aplikasi serta bug sehingga akan menghambat kinerja.	4	Pernah terjadi pada sesekali waktu.	6	Belum menerapkan konsep programming dengan konsep clean code serta pengujian yang tidak selalu dilakukan.	168
31			Belum melakukan testing secara menyeluruh	Software tidak sesuai dengan kebutuhan	5	Jika sistem informasi atau software tidak sesuai dengan kebutuhan dan masih memiliki banyak bug maka akan menyebabkan	4	Belum pernah diketahui terjadi namun memiliki potensi untuk terjadi	6	Testing tidak selalu dulakukan.	120
32			Tidak ada dokumentasi selama pengembangan software						6	Belum mendokumentasikan pengembangan aplikasi dengan	120

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						penurunan kinerja pada PDAM karena menghambat penggunaan aplikasi.				rinci dan terstruktur.	
33	Data	Database Keuangan dan database pelanggan	Data Corrupt	Kehilangan data	8	Data merupakan aset yang sangat kritis bagi PDAM terutama data pelanggan, jika data tidak dapat diakses atau tidak tersedia maka proses-proses yang ada pada PDAM akan terhenti seperti perhitungan kubik air terpakai dan pembayaran.	4	Belum pernah terjadi namun memiliki potensi untuk terjadi.	3	Telah melakukan maintenance secara rutin	96
34			Gangguan pada jaringan	Data tidak dapat diakses / tidak tersedia			5	Pernah terjadi namun tidak sering.	5	telah terdapat maintenance	200
35			Virus dan malware				4	Belum pernah terjadi yang berakibat data tidak dapat diakses namun memiliki potensi untuk terjadi.	3	Metode deteksi berupa penggunaan antivirus dan firewall.	96
36			Kerusakan perangkat keras				4	Belum pernah terjadi namun memiliki	3	Sudah melakukan monitoring secara	96

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
			(storage dan server)					potensi untuk terjadi.		rutin terhadap server dan storage	
37			SQL Injection				3	Belum pernah terjadi namun memiliki potensi yang kecil untuk terjadi.	6	Belum ada mekanisme deteksi secara khusus selain penggunaan firewall.	144
38			Logical error (salah query)				3	Belum pernah terjadi namun memiliki potensi yang kecil untuk terjadi.	6	Belum menerapkan manajemen tabel basis data.	144
39			Kegagalan sistem database				4	memiliki potensi untuk terjadi.	3	Database rutin di monitoring.	96
40			Hacker (pencurian dan modifikasi data)	Data kehilangan integritas	6	Jika data kehilangan intetegritasnya maka akan menjadikan data tidak valid dan konsisten selain itu akan	4	Belum pernah terjadi namun memiliki potensi untuk terjadi.	3	Sudah mengaktifkan firewall dan antivirus	72
41			Social Engineering				6	Belum pernah diketahui jika pernah terjadi	5	PDAM sangat ketat dalam membagikan data	180

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						berdampak pada proses bisnis yang terjadi dengan pihak switcher terkait data pelanggan		atau tidak karena tidak terdapat pengawasan hak ases serta pengaksesan user pada transaction log.		yang bersifat confidental serta pernah melakukan sosialisasi terkait namun tidak ada pengawasan.	
42			Penyalahgunaan dan pelanggaran hak akses				6	Belum pernah diketahui jika pernah terjadi atau tidak karena tidak terdapat pengawasan hak ases serta pengaksesan user pada transaction log.	5	Sudah terdapat kebijakan hak akses untuk pengaksesan data namun tidak ada pengawasan setiap user pada transaction log aplikasi	180
43			Kerusakan UPS dan Genset	Kegagalan Backup	3	Kegagalan backup dapat diatasi dengan mengakses log.	3	Belum pernah terjadi namun memiliki potensi yang kecil untuk terjadi.	6	Belum melakukan monitoring secara rutin	54

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
44			Belum menerapkan manajemen tabel untuk database	Database lambat untuk diakses	5	Database yang lambat akan menyebabkan kegiatan operasional PDAM terhambat bahkan dapat mengakibatkan terhambatnya penanganan keluhan pelanggan.	5	Berpotensi untuk terjadi sesekali waktu	6	Belum terdapat mekanisme deteksi	150
45			Kapasitas memori penuh		5		4	Belum pernah terjadi namun memiliki potensi untuk terjadi.	3	Sudah melakukan monitoringsecara rutin pada sistem sotrage	60
46	SDM	Pegawai TI	Kurang kompeten	Human Error / Pelanggaran	5	Kurangnya pengetahuan dan kompetensi pada karyawan akan menyebabkan kesalahan dalam penggunaan aset TI.	4	Belum pernah terjadi namun memiliki potensi untuk terjadi.	4	terdapat pelatihan untuk karyawan secara periodik.	80
47		TI dan non TI	Tidak terdapat prosedur dan kebijakan terkait pengelolaan dan penggunaan aset		4	Tidak terdapatnya prosedur yang bersifat mengikat mengakibatkan	6	Berpotensi untuk terjadi setiap saat karena tidak ada prosedur atau	6	Belum terdapat kebijakan yang bersifat mengontrol	144

ID Risiko	Tipe Aset	Nama Aset	Penyebab Potensial	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						pengguanaan TI yang tidak benar.		kebijakan yang mengatur.			
48		TI dan non TI	Tidak adanya pengawasan / monitoring hak akses pada transaction log		7	Tidak adanya pengecekan dan pengawasan dapat mengakibatkan pihak-pihak tertentu melakukan pelanggaran dan penyalahgunaan.	4	Belum pernah terjadi namun memiliki potensi untuk terjadi.	8	Tidak adanya pengawasan / monitoring hak akses pada transaction log	224

Halaman ini sengaja dikosongkan

LAMPIRAN G

Formulir Pengecekan Internal Rencana Keberlangsungan Bisnis

Tabel G.1 Formulir Pengecekan Internal Rencana Keberlangsungan Bisnis

No	Pertanyaan	Status			Keterangan
		Ya	Dalam Progress	Tidak	
1.	Pengelolaan Umum Mengenai *Business Continuity Plan*				
1.1	Apakah masing masing peran dan tanggung jawab terhadap BCP telah sepenuhnya terdefinisi pada level manajemen?				
1.2	Apkah organisasi memiliki pihak senior yang spesifik bertanggung jawab terhadap keseluruhan BCP?				
1.3	Apakah organisasi telah mendokumentasikan BCP dengan baik?				
1.4	Apakah Proses BCP telah selaras dengan peraturan yang berlaku?				
1.5	Apakah dokumen BCP telah tersedia dan dipahami oleh keseluruhan organisasi?				
2.	Keselarasan BCP dengan perusahaan				
2.1	Apakah organisasi telah mendefinisikan sumber daya kritis yang mendukung aktivitas?				
2.2	Apakah organisasi telah mengidentifikasi proses bisnis yang memiliki ketergangungan pada TI yang ada di organisasi?				
2.3	Apakah organisasi telah mengidentifikasi risiko yang dapat terjadi dan mengancam keberlangsungan bisnis?				

No	Pertanyaan	Status			Keterangan
		Ya	Dalam Progress	Tidak	
2.4	Apakah organisasi telah melakukan prioritisasi terhadap layanan dan proses yang memiliki ketergantungan terhadap TI?				
2.5	Apakah organisasi telah menentukan toleransi waktu pemulihan terhadap gangguan dan telah disetujui oleh manajemen senior?				
2.6	Apakah organisasi telah melakukan perhitungan dampak bisnis terhadap proses bisnis apabila terjadi gangguan?				
3.	Pengelolaan strategi BCP				
3.1	Apakah organisasi telah mendokumentasikan strategi pencegahan apabila tehadap bencana atau gangguan?				
3.2	Apakah organisasi telah mendokumentasikan strategi pemulihan terjadi bencana atau gangguan?				
3.3	Apakah organisasi telah mendokumentasikan strategi korektif setelah terjadi bencana atau gangguan?				
3.4	Apakah strategi tersebut telah secara formal disetujui oleh manajemen senior?				
3.5	Apakah telah ada prosedur yang mendukung strategi – strategi BCP?				
3.6	Apakah strategi BCP telah dikomunikasikan kepada keseluruhan organisasi?				

No	Pertanyaan	Status			Keterangan
		Ya	Dalam Progress	Tidak	
3.7	Apakah prosedur terkait BCP telah dikomunikasikan kepada pegawai?				
3.8	Apakah keseluruhan risiko kritis telah dicakup pada BCP?				
3.9	Apakah BCP juga telah mencakup perencanaan komunikasi yang efektif antar bagian?				
4.	Pelatihan dan pengujian BCP				
4.1	Apakah telah dilakukan pelatihan formal terhadap tim BCP?				
4.2	Apakah terdapat pengujian BCP secara keseluruhan (full test) maupun sebagian (partial test)?				
4.3	Apakah semua aspek perencanaan telah di uji pada 1 tahun terakhir ini?				
4.4	Apakah pengujian dilakukan oleh staf yang memang terkait dengan perencanaan?				
4.5	Apakah hasil pengujian telah sepenuhnya terdokumentasi?				
5.	Pemeliharaan dan peninjauan BCP				
5.1	Apakah terdapat proses peninjauan terhadap BCP?				
5.2	Apakah terdapat proses untuk mengukur keefektifan BCP?				
5.3	Apakah terdapat proses untuk melakukan tindakan perbaikan dengan tujuan untuk meningkatkan BCP?				

Halaman ini sengaja dikosongkan

LAMPIRAN H

Formulir Peninjauan Manajemen

Tabel H.1 Formulir Peninjauan Manajemen

Masukan	Pemimpin rapat:			
	Tanggal dan waktu rapat:			
	Peserta rapat yang hadir/tidak hadir:			
	Sumber daya yang dibutuhkan:	□ Laporan hasil tinjauan sebelumnya □ Laporan hasil pengecekan □ Hasil pengujian BCP		
Analisis	**Topik diskusi**	**Keputusan/Tindakan**	**Batas Waktu**	**Penanggungjawab**
	Status dari tindakan yang ditinjau pada tinjauan manajemen sebelumnya			
	Perubahan internal dan eksternal yang berkaitan dengan BCP			

	Hasil audit BCP dan langkah korektif yang dilakukan			
	Kebutuhan untuk melakukan perubahan terhadap BCP untuk kebijakan maupun prosedur			

LAMPIRAN I

Hasil Validasi Analisis Risiko

SURAT KONFIRMASI

Kesesuaian Hasil Analisis Risiko

Dengan hormat,
Saya yang bertanda tangan dibawah ini:

Nama : Cindy Alicia Sahara
NRP : 05211440000172
Pekerjaan : Mahasiswa Departemen Sistem Informasi
Institut Teknologi Sepuluh Nopember

Dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis risiko terkait aset TI untuk PDAM Surya Sembada Kota Surabaya. Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis risiko terkait aset TI yang dibuat sesuai dengan kebutuhan dan kondisi PDAM Surya Sembada Kota Surabaya.

Atas perhatian dan kesediaan Bapak/Ibu Pimpinan, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI
Surabaya, 2 Juli 2018

Mengetahui,
Supervisor Teknologi Sistem Informasi

Nurlillah Satria Pratama

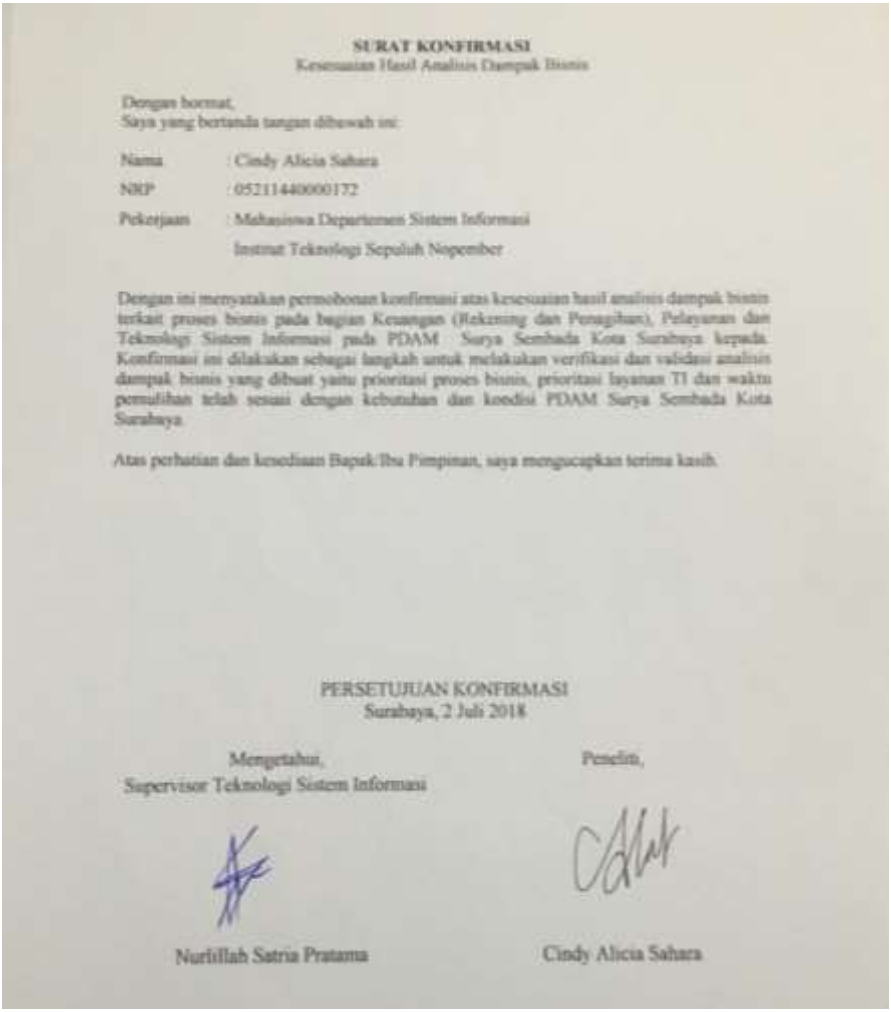
Penelisi

Cindy Alicia Sahara

Halaman ini sengaja dikosongkan

LAMPIRAN J

Hasil Validasi Analisis Dampak Bisnis



SURAT KONFIRMASI
Kesesuaian Hasil Analisis Dampak Bisnis

Dengan hormat,
Saya yang bertanda tangan dibawah ini:

Nama : Cindy Alicia Sahara
NRP : 05211440000172
Pekerjaan : Mahasiswa Departemen Sistem Informasi
Institut Teknologi Sepuluh Nopember

Dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis dampak bisnis terkait proses bisnis pada bagian Keuangan (Rekening dan Penagihan), Pelayanan dan Teknologi Sistem Informasi pada PDAM Surya Sembada Kota Surabaya kepada. Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi dan validasi analisis dampak bisnis yang dibuat yaitu prioritasi proses bisnis, prioritasi layanan TI dan waktu pemulihan telah sesuai dengan kebutuhan dan kondisi PDAM Surya Sembada Kota Surabaya.

Atas perhatian dan kesediaan Bapak/Ibu Pimpinan, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI
Surabaya, 2 Juli 2018

Mengetahui,
Supervisor Teknologi Sistem Informasi

Nurfillah Satria Pratama

Peneliti,

Cindy Alicia Sahara

Halaman ini sengaja dikosongkan

LAMPIRAN K

Hasil Validasi Dokumen BCP PDAM Surya Sembada Kota Surabaya

SURAT KONFIRMASI

DOKUMEN *BUSINESS CONTINUITY PLAN* (BCP)

PT. PDAM Surya Sembada Kota Surabaya

Dengan hormat,
Saya yang bertanda tangan dibawah ini

Nama	: Cindy Alicia Sahara
NRP	: 05211440000172
Pekerjaan	: Mahasiswa Departemen Sistem Informasi
	Institut Teknologi Sepuluh Nopember

Dengan ini menyatakan permohonan konfirmasi atas kesesuaian dokumen *business continuity plan* PDAM Surya Sembada Kota Surabaya. Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi dan validasi bahwa dokumen *business continuity plan* yang dibuat sesuai dengan kebutuhan dan kondisi PDAM Surya Sembada Kota Surabaya serta dapat diterima oleh perusahaan.

Atas perhatian dan kesediaan Bapak/Ibu Pimpinan, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI
Surabaya, 2 Juli 2018

Mengetahui,	Peneliti,
Supervisor Teknologi Sistem Informasi	
Nurfillah Satria Pratama	Cindy Alicia Sahara