TUGAS AKHIR – KS 141501

PENYUSUNAN PERENCANAAN KEBERLANGSUNGAN BISNIS PT PLN (PERSERO) APD JATENG DAN DIY DENGAN ISO 22301 DAN METODE OCTAVE

ARRANGING BUSINESS CONTINUITY PLAN FOR PT PLN (PERSERO) APD JATENG AND DIY WITH ISO 22301 AND OCTAVE METHODE

AZMI AFIFAH ZAHRA
NRP 5212 100 140

Dosen Pembimbing
Dr. APOL PRIBADI, S.T., M.T.
EKO WAHYU TYAS D, S.Kom., MBA

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

TUGAS AKHIR – KS 141501

PENYUSUNAN PERENCANAAN KEBERLANGSUNGAN BISNIS PT PLN (PERSERO) APD JATENG DAN DIY DENGAN ISO 22301 DAN METODE OCTAVE

AZMI AFIFAH ZAHRA
NRP 5212 100 140

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

Dosen Pembimbing II
Eko Wahyu Tyas D, S.Kom.,MBA

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

FINAL PROJECT – KS 141501

ARRANGING BUSINESS CONTINUITY PLAN FOR PT PLN (PERSERO) APD JATENG AND DIY WITH ISO 22301 AND OCTAVE METHOD

AZMI AFIFAH ZAHRA
NRP 5212 100 140

Academic Promotor I
Dr. Apol Pribadi, S.T. , M.T.

Academic Promotor II
Eko Wahyu Tyas D, S.Kom., MBA.

INFORMATION SYSTEM DEPARTMENT
Information Technology Faculty
Sepuluh Nopember Institute of Technology
Surabaya 2016

LEMBAR PENGESAHAN

PENYUSUNAN PERENCANAAN KEBERLANGSUNGAN BISNIS PT PLN (PERSERO) APD JATENG DAN DIY DENGAN ISO 22301 DAN METODE OCTAVE

TUGAS AKHIR

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

Oleh :

AZMI AFIFAH ZAHRA
NRP 5212 100 140

Surabaya, ... Juli 2016

KETUA
JURUSAN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

PENYUSUNAN PERENCANAAN KEBERLANGSUNGAN BISNIS PT PLN (PERSERO) APD JATENG DAN DIY DENGAN ISO 22301 DAN METODE OCTAVE

TUGAS AKHIR

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

Oleh :

AZMI AFIFAH ZAHRA
NRP 5212 100 140

Disetujui Tim Penguji :

Tanggal Ujian	:	.. Juli 2016
Periode Wisuda	:	September 2016

Dr. Apol Pribadi, S.T., M.T.	**(Pembimbing I)**
Eko Wahyu Tyas D, S.Kom., MBA	**(Pembimbing II)**
Ir. Achmad Holil Noor Ali, M.Kom.	**(Penguji I)**
Bekti Cahyo Hidayanto, S.Si, M.Kom.	**(Penguji II)**

PENYUSUNAN PERENCANAAN KEBERLANGSUNGAN BISNIS PT PLN (PERSERO) APD JATENG DAN DIY DENGAN ISO 22301 DAN METODE OCTAVE

Nama Mahasiswa	**: Azmi Afifah Zahra**
NRP	**: 5212 100 140**
Pembimbing 1	**: Dr. Apol Pribadi, S.T., M.T.**
Pembimbing 2	**: Eko Wahyu Tyas D, S.Kom., MBA**
LAB	**: Manajemen Sistem Informasi**

ABSTRAK

PT PLN (Persero) APD Jateng dan DIY merupakan perusahaan yang mengandalkan peran dari teknologi informasi dalam menjalankan proses bisnisnya. Namun peran teknologi informasi tidak terlepas pula dengan ancaman terhadap risiko TI yang dapat mengancam keberlangsungan bisnis perusahaan. Meskipun saat ini PT PLN telah menetapkan tiap unit bisnisnya untuk melakukan manajemen risiko yang tertuang dalam buku prosedur Penyusunan Profil dan Kajian Risiko, namun pelaksanaannya hanya sampai pada profil dan kajian risiko terhadap proses bisnis saja. Sedangkan untuk strategi keberlangsungan bisnis dan penanggulangan risiko terutama pada risiko TI belum terdapat standar baku dan sesuai dengan ISO.

Oleh karena itu, penelitian tugas akhir ini bertujuan untuk melakukan penyusunan untuk rencana keberlangsungan bisnis PT PLN (Persero) APD Jateng dan DIY berbasis pada risiko TI. Proses penyusunan untuk perencanaan keberlangsungan bisnis akan dibuat terlebih dahulu dengan perancangan alur kerja perencanaan keberlangsungan bisnis untul PT PLN (Persero) APD Jateng dan DIY dengan menggunakan acuan ISO 22301:2012 sebagai kerangka dasar formulasi alur kerja dan Metode OCTAVE sebagai tahap penentuan identifikasi risiko TI pada perusahaan.

Hasil akhir dari penelitian tugas akhir ini adalah berupa rekomendasi alur kerja dan strategi keberlangsungan bisnis untuk perusahaan dalam upaya menanggulangi dan menghadapi risiko TI yang mengancam keberlangsungan bisnis perusahaan. Standar praktis yang digunakan sebagai referensi strategi keberlangsungan bisnis adalah ISO 27002 dan bentuk strategi praktis yang telah diterapkan oleh perusahaan Department of Energy di United States.

Kata kunci : Perencanaan keberlangsungan bisnis (BCP) berbasis risiko, alur kerja BCP, ISO 22301:2012, Metode OCTAVE, PT PLN (Persero), PT PLN (Persero) APD Jateng dan DIY, Department of Energy United States, ISO 27002.

ARRANGING BUSINESS CONTINUITY PLAN FOR PT PLN (PERSERO) APD JATENG AND DIY WITH ISO 22301 AND OCTAVE METHOD

Student Name : **Azmi Afifah Zahra**
NRP : **5212 100 140**
Supervisor 1 : **Dr. Apol Pribadi, S.T., M.T.**
Supervisor 2 : **Eko Wahyu Tyas, S.Kom**
LAB : **Management of Information System**

ABSTRACT

PT PLN (Persero) APD Jateng and DIY is a company that rely on information technology roles to run their business process. But the roles of information technology are not apart with IT risks which could threat company's business continuity. Eventhough PT PLN (Persero) has established risk management implementation for each business units, but the reality is that risk management implementation only implemented to assses risks at company's business process. Meanwhile, the IT strategy for business continuity plan and risk mitigation has not determined yet by the company with any best practices or ISO standard.

Because of that reasons, in this thesis research would arrangge a business continuty plan for PT PLN (Persero) APD Jateng and DIY based on IT risk. The Business Continuoty Plan (BCP) arrangement process would be started to formulation process of BCP workflow which consists of ISO 22301:2012 as a base framework and OCTAVE Method as a method for IT risk identification.

The results of this research are workflow of BCP based on IT Risk and business continuity strategies recommendation as a company readiness to business continuity from IT risks. IT business continuity strategy would refers from ISO 27002 as an information security management systems and best practice of BCP from Department of Energy United States.

Keywords : Business Continuity Plan (BCP) based on Risk, workflow of BCP, ISO 22301:2012, OCTAVE Method, PT PLN (Persero), PT PLN (Persero) APD Jateng dan DIY, Department of Energy United States, ISO 27002.

DAFTAR ISI

ABSTRAK v
ABSTRACT vii
KATA PENGANTAR ix
DAFTAR ISI xi
DAFTAR GAMBAR xv
DAFTAR TABEL xv
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Tugas Akhir 4
1.5 Manfaat Tugas Akhir 5
1.6 Relevansi 5
BAB II TINJAUAN PUSTAKA 7
2.1 Penelitian Terdahulu 7
2.2 Manajemen Risiko 10
2.3 OCTAVE 12
2.4 Metode Penilaian Risiko 14
2.5 Business Impact Analysis 19
2.6 Business Continuity Management Systems (BCMS) ..22
2.7 Business Continuity Plan (BCP) 23
2.8 Disaster Recovery Plan (DRP).....24
2.9 Hubungan antara BCP dengan DRP 24
2.10 ISO 22301:2012 25
2.11 NIPP Risk Management Framework 27
2.12 BCP pada Chubu Electric Power Company.....29
BAB III METODOLOGI 31
3.1 Identifikasi Permasalahan 32
3.2 Penggalian Kebutuhan terhadap BCP 33
3.3 Formulasi Alur BCP 33
3.4 Wawancara Proses Bisnis 34
3.5 Pengolahan Data dan Informasi 34
3.6 Penyusunan Rekomendasi Aksi BCP 34
3.7 Validasi BCP.....35
3.8 Jadwal Penyusunan Tugas Akhir 35

BAB IV PERANCANGAN 37
4.1 Identifikasi Permasalahan 37
4.2 Penggalian Kebutuhan terhadap BCP 37
4.3 Formulasi Alur BCP..... 41
4.3.1 Kerangka Dasar..... 41
4.3.2 Alur Kerja Terapan 43
4.3.3 Metode Analisis Risiko Teknologi Informasi 45
4.3.4 Metode Analisis Dampak Bisnis..... 48
4.4 Wawancara Proses Bisnis..... 49
4.5 Pengolahan Data dan Informasi 50
4.6 Penyusunan Rekomendasi Aksi BCP..... 57
4.6.1 Perancangan untuk Strategi Keberlangsungan Bisnis 58
4.6.2 Perancangan untuk Penyusunan Daftar Prosedur... 59
4.6.3 Kebutuhan untuk Pelatihan dan Pengujian 59
4.6.4 Audit Pelaksanaan BCP 61
4.6.5 Peninjauan Pihak Manajemen..... 62
4.6.6 Peningkatan Secara Terus- Menerus..... 62
4.7 Validasi BCP..... 63
BAB V IMPLEMENTASI 65
5.1 Identifikasi Permasalahan 65
5.2 Penggalian Kebutuhan terhadap BCP 66
5.2.1 Konteks Organisasi 68
5.2.2 Ruang Lingkup BCP 69
5.2.3 Penentuan Peran dan Tanggung Jawab 69
5.2.4 Tujuan Pelaksanaan BCP 70
5.2.5 Sumber Daya..... 71
5.2.6 Alur Komunikasi..... 72
5.3 Formulasi Alur BCP..... 73
5.4 Wawancara Proses Bisnis..... 83
5.5 Pengolahan Data dan Informasi 86
5.1.1 Identifikasi dan Analisis Risiko 86
5.1.2 Analisa Dampak Bisnis..... 91
5.1.3 Prioritisasi 91
5.6 Penyusunan Rekomendasi Aksi BCP..... 92
5.7 Validasi BCP..... 93
5.8 Hambatan dan Kendala 93

BAB VI HASIL DAN PEMBAHASAN 95
6.1 Fase Perencanaan (*Plan*).....95
6.1.1 Menentukan Konteks Organisasi 95
6.1.2 Menentukan Ruang Lingkup 102
6.1.3 Menentukan Peran dan Tanggung Jawab 103
6.1.4 Menentukan Tujuan Perencanaan Keberlangsungan Bisnis 106
6.1.5 Menentukan Sumber Daya Perusahaan 107
6.1.6 Menentukan Alur Komunikasi.....108
6.2 Fase Pengerjaan (*Do*).....111
6.2.1 Identifikasi dan Analisis Risiko Teknologi Informasi 112
6.2.2 Analisis Dampak Bisnis.....149
6.2.3 Prioritisasi 157
6.2.4 Strategi BCP 164
6.2.5 Prosedur BCP.....171
6.2.6 Pengujian BCP.....177
6.3 Fase Pemeriksaan.....182
6.3.1 Audit Pelaksanaan BCP 182
6.3.2 Peninjauan Pihak Manajemen.....187
6.4 Fase Penindakan.....187
BAB VII KESIMPULAN DAN SARAN 190
7.1 Kesimpulan.....190
7.2 Saran 192
DAFTAR PUSTAKA 194
BIODATA PENULIS 196
DAFTAR LAMPIRAN 198
LAMPIRAN A A-1
LAMPIRAN B B-1
LAMPIRAN C C-1
LAMPIRAN D D-1
LAMPIRAN E E-1
LAMPIRAN F.....F-1
LAMPIRAN G G-1
LAMPIRAN H H-1
LAMPIRAN I.....I-1
LAMPIRAN J J-1

LAMPIRAN K K-1
LAMPIRAN L L-1

DAFTAR GAMBAR

Gambar 2.1 Tahap Kerangka Metode OCTAVE 13
Gambar 2.2 Tahap 2 kerangka kerja OCTAVE 14
Gambar 2.3 Diagram Alur FMEA..... 15
Gambar 2.4 Siklus BCMS pada standar BIA ISO 22317..... 23
Gambar 2.5 Siklus BCMS berdasarkan ISO 22301:2012 27
Gambar 2.6 NIPP Risk Management Framework..... 28
Gambar 2.7 Alur Kerja Keberlangsungan Bisnis Perusahaan *Chubu Power Electric*..... 30
Gambar 3.1 Metodologi Penelitian Tugas Akhir 32
Gambar 4.1 Kerangka BCMS ISO 22301:2012..... 42
Gambar 4.2 NIPP Risk Management Framework..... 43
Gambar 4.3 Metode Penilaian FMEA..... 47
Gambar 4.4 Visualisasi perancangan Alur Kerja BCP PT PLN (Persero) APD Jateng dan DIY..... 49
Gambar 5.1 Studi Empiris Perancangan Alur Kerja BCP..... 65
Gambar 5.2 Visualisasi Penyesuaian dengan Kebutuhan dan Keinginan Organisasi..... 73
Gambar 5.3 Visualisasi Perancangan Alur Kerja BCP 76
Gambar 5.4 Hasil Alur Kerja BCP..... 76
Gambar 6.1 Alur Kerja BCP PT PLN (Persero) APD Jateng dan DIY – Fase Plan..... 95
Gambar 6.2 Gambar Wilayah Kerja PT PLN (Persero) APD Jateng dan DIY 97
Gambar 6.3 Proses Bisnis PT PLN (Persero) APD Jateng dan DIY 101
Gambar 6.4 Struktur Organisasi PT PLN (Persero) APD Jateng dan DIY 102
Gambar 6.5 Struktur Komite BCP 104
Gambar 6.6 Alur Komunikasi BCP..... 109
Gambar 6.7 Alur Kerja BCP PT PLN (Persero) APD Jateng dan DIY – Fase Do 111
Gambar 7.1 Hasil Perancangan Alur Kerja BCP PLN APD Jateng dan DIY 191

Halaman ini sengaja dikosongkan

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu 7
Tabel 2.2 Daftar ranking tingkat keparahan (*Severity*) 16
Tabel 2.3 Daftar Tingkat frekuensi kejadian (*Occurance*)... 17
Tabel 2.4 Daftar Nilai Deteksi Kejadian (*Detection*)..... 18
Tabel 2.5 Level Risiko berdasarkan hasil RPN..... 19
Tabel 2.6 Dampak terhadap Produk dan Layanan 21
Tabel 2.7 Aspek Proses Bisnis Internal..... 21
Tabel 2.8 Perbedaan BCP dengan DRP 25
Tabel 3.1 Jadwal Penelitian dan Pengerjaan Tugas Akhir ... 35
Tabel 4.1 Tabel Interview Protocol Penggalian Kebutuhan Proses Bisnis 38
Tabel 4.2 Rancangan Tabel Penilaian Risiko TI..... 50
Tabel 4.3 Daftar Nilai untuk Tingkat Keparahan (*Severity*) 50
Tabel 4.4 Daftar Penilaian Tingkat Frekuensi Kejadian (*Occurance*)..... 52
Tabel 4.5 Daftar Penilaian Tingkat Deteksi Kejadian (*Detection*)..... 52
Tabel 4.6 Klasifikasi Hasil Penilaian Berdasarkan *Risk Priority Number* 54
Tabel 4.7 Tabel Hasil Klasifikasi Risiko..... 55
Tabel 4.8 Penilaian Dampak Berdasarkan Aspek Produk dan Layanan 55
Tabel 4.9 Penilaian Dampak Berdasarkan Aspek Proses Bisnis Internal 56
Tabel 4.10 Tabel Matriks Level Risiko TI dan Dampak Bisnis 57
Tabel 4.11 Tabel Rancangan Kebutuhan Strategi BCP 58
Tabel 4.12 Rancangan Tabel dari Kebutuhan Daftar Prosedur 59
Tabel 4.13 Tabel Kerangka untuk Modul Pelatihan BCP 60
Tabel 4.14 Tabel Kerangka untuk Modul Pengujian BCP 61
Tabel 4.15 Rancangan Tabel Kebutuhan Audit Pelaksanaan BCP 62
Tabel 4.16 Kebutuhan Peningkatan secara terus menerus 63

Tabel 5.1 Tabel Identitas Responden Wawancara Kebutuhan BCP 66
Tabel 5.2 Daftar Kebutuhan Pelaksanaan BCP 67
Tabel 5.3 Dokumen untuk Kebutuhan Penelitian.....68
Tabel 5.4 Pemetaan Kebutuhan Organisasi 73
Tabel 5.5 Pemetaan Standar pada Alur Kerja BCP 77
Tabel 5.6 Standar ISO 27002 Terlaksana 86
Tabel 5.7 Standar ISO 27002 terlaksana 88
Tabel 5.8 Tabel Penentuan Prioritas Aset TI.....91
Tabel 5.9 Contoh Tabel Kebutuhan Prosedur.....92
Tabel 6.1 Pembagian Peran dan Tanggung Jawab Komite BCP 104
Tabel 6.2 Aset Kritis PT PLN (Persero) APD Jateng dan DIY 107
Tabel 6.3 Daftar Aset Kritis 112
Tabel 6.4 Kebutuhan keamanan aset kritis 113
Tabel 6.5 Daftar Ancaman pada Kategori Ancaman.....118
Tabel 6.6 Implementasi Aksi Penanggulangan Risiko TI ..119
Tabel 6.7 Daftar Standar ISO 27002 Tidak Terlaksana beserta Daftar Kerentanan 123
Tabel 6.8 Daftar Komponen Utama Aset TI 128
Tabel 6.9 Daftar Kerentanan Infrastruktur 130
Tabel 6.10 Pembagian Nomor Identifikasi Risiko Aset Kritis 138
Tabel 6.11 Daftar Jumlah Kritikalitas Aset Berdasarkan Tingkat RPN 144
Tabel 6.12 Daftar Klasifikasi Risiko padaAset TI.....144
Tabel 6.13 Tabel Analisa Dampak Bisnis 149
Tabel 6.14 Penggunaan Aset TI pada tiap Level Kritikalitas Proses Bisnis.....155
Tabel 6.15 Daftar Pengelompokan Aset TI berdasarkan Kritikalitas Risiko TI.....158
Tabel 6.16 Pemetaan pada Tabel Metrics untuk Aset TI.....159
Tabel 6.17 Pemetaan Identifikasi Aset TI berdasarkan Kritikalitas Proses Bisnis.....160
Tabel 6.18 Metrics Prioritas Aset TI berdasarkan Risiko TI dan Dampak Bisnis.....162

Tabel 6.19 Hasil Kritikalitas Dampak Bisnis 163
Tabel 6.20 Hasil Prioritisasi Aset TI berdasarkan pada Metrics 163
Tabel 6.21 Daftar Prioritas Utama Aset TI dan Kritikalitasnya 165
Tabel 6.22 Daftar Kritikalitas berdasarkan Prioritas Utama Aset TI..... 165
Tabel 6.23 Contoh Strategi Preventif..... 166
Tabel 6.24 Contoh Strategi Detektif 169
Tabel 6.25 Contoh Strategi DRP kesalahan Konfigurasi SCADA 170
Tabel 6.26 Contoh Strategi korektif saat Kejadia pada Gangguan SCADA 171
Tabel 6.27 Tabel Kebutuhan Prosedur 172
Tabel 6.28 Tabel Pengujian Alur Komunikasi BCP 177
Tabel 6.29 Hambatan Pengujian Strategi Keberlangsungan Bisnis..... 180
Tabel 6.30 Rekap Keberhasilan Pengujian..... 181

Halaman ini sengaja dikosongkan

DAFTAR LAMPIRAN

Berikut ini adalah lampiran dari beberapa dokumentasi pada penelitian Tugas Akhir ini. Dokumen yang dilampirkan tersebut merupakan bukti dari pengerjaan penelitian ini. Hasil selengkapnya dari peneliian ini telah disampaikan dalam dokumen produk BCP PT PLN (Persero) APD Jateng dan DIY.

Kode Lampiran	Lampiran
A	Kuesioner formulir wawancara proses bisnis
B	Hasil wawancara penggalian kebutuhan bisnis dengan Asisten Manajer SCADA
C	*Checklist* kontrol ISO 27002:2005
D	Kalkulasi Penilaian analisis risiko teknologi informasi
E	Analisis dampak bisnis
F	Strategi Keberlangsungan Bisnis berbasis Risiko
G	Gambaran umum modul pelatihan dan pengujian
H	Validasi keseuaian alur kerja BCP
I	Validasi keseseuaian penilaian risiko dan analisis dampak bisnis
J	Validasi hasil pengujian
K	Validasi kesesuaian dokumen produk BCP

Halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

Pada bab ini, akan dijelaskan tentang Latar Belakang Masalah, Perumusan Masalah, Batasan Masalah, Tujuan Tugas Akhir, dan Relevansi serta Manfaat Kegiatan Tugas Akhir.

1.1 Latar Belakang Masalah

PT PLN (Persero) adalah perusahaan listrik milik negara yang memberikan jasa untuk bidang kelistrikan di Indonesia dan merupakan salah satu Badan Usaha Milik Negara yang memiliki rencana strategis yaitu "*Diakui sebagai perusahaan kelas dunia yang bertumbuh kembang, unggul, dan terpercaya pada potensi insani*" . Dalam rangka mencapai visi tersebut, PT PLN membagi fokus kerjanya pada setiap unit kerja yang terbagi dalam beberapa wilayah di Indonesia. Salah satu unit kerja PT PLN (Persero) yaitu unit kerja area penyalur distribusi yang terdapat di Jawa Timur, yaitu PT PLN (Persero) Area Pengatur Distribusi Jawa Tengah dan DIY. Organisasi PLN APD Jateng dan DIY merupakan organisasi PLN setingkta area yang berada di bawah pengawasan oleh PT PLN Distribusi Jateng dan DIY berdasarkan SK Direksi PLN nomor 260.K/DIR/2007. Fungsi dan tugas pokok PT PLN APD Jateng dan DIY adalah melakukan perencanaan, melaksanakan, mengevaluasi serta membuat laporan atas kegiatan operasi SCADA dan telekomunikasi sistem distribusi dan gardu secara efisien. SCADA (*Supervisory Control and Data Aquisition*) merupakan sistem informasi yang dijadikan sebagai media pengawasan, pengendalian, dan pengumpulan data dari gardu induk maupun dari pembangkit secara otomatis dan *real time* [1].

Dalam rangka mencapai visi dan misi, perusahaan dan organisasi membutuhkan dukungan sistem dan layanan TI dalam menjalankan proses bisnisnya. Namun dalam penggunaan sistem dan layanan TI tersebut tidak terlepas dari risiko TI yang berdampak pada keberlangsungan bisnis. Oleh

karena itu perlunya perusahaan dalam merencakanan kebutuhan untuk keberlangsungan bisnis perusahaan untuk menanggapi, memulihkan, melanjutkan proses bisnis setelah adanya gangguan. Perencanaan keberlangsungan bisnis perusahaan dapat didokumentasikan dalam dokumen BCP (*Business Continuity* Plan) dimulai dengan mengetahui terlebih dahulu dampak bisnis perusahaan dalam aspek finansial maupun operasional apabila proses bisnis perusahaan terhenti atau terhambat, serta penggunaan layanan TI serta risiko dalam sistem dan layanan TI tersebut. Lalu penyusunan dokumen BCP dapat disusun dengan menetapkan kebijakan dan prosedur aksi manajemen untuk kejadian bencana.

Pada saat ini, PT PLN (Persero) APD Jateng dan DIY masih belum memiliki perencanaan strategi dan pengelolaan untuk keberlangsungan bisnis berbasis risiko yang terdokumentasi dan tersusun sesuai dengan standar praktis berdasarkan ISO maupun standar praktis dari perusahaan yang telah menerapkan pengelolaan keberlangsungan bisnis untuk perusahaan. Selain itu, dalam rangka menjaga data serta sistem dan layanan TI perusahaan dari keadaan pra dan pasca bencana, saat ini masih belum terdapat alur untuk penanganan *backup* dan *recovery* data PT PLN (Persero) APD Jateng dan DIY. Namun saat ini untuk menanggulangi adanya risiko dan dampak bisnis yang mengancam proses bisnis perusahaan, PT PLN (Persero) telah memiliki prosedur praktis yang tertuang dalam dokumen rencana jangka panjang untuk penilaian risiko dan dampak bisnis perusahaan. Sehingga dalam tugas akhir ini, penulis bermaksud untuk menyusun bentuk dari perencanaan keberlangsungan bisnis perusahaan (*Business Continuity Planning*) PT PLN (Persero) APD Jateng dan DIY dengan berangkat dari penyusunan alur kerja dari pengelolaan keberlangsungan bisnis perusahaan (*Business Continuity Management)* yang disusun dari formulasi antara ISO 22301: 2012 dan bentuk yang alur kerjan BCM yang telah diterapkan perusahaan lain yaitu *Chubu Electric Power Company Group* dan DHS *Energy*. Hasil akhir dari tugas akhir ini adalah rekomendasi pelaksanaan untuk strategi perusahaan dalam

melaksanakan keberlangsungan bisnis perusahaan, rekomendasi strategi tersebut didapatkan dari beberapa standar untuk pelaksanaan mitigasi risiko yang telah didefinisikan, diantaranya yaitu ISO 22701 serta bentuk praktis yang telah diterapkan oleh perusahaan lain dengan memperhatikan kebutuhan dari PT PLN (Persero) APD Jateng dan DIY. Hasil akhir tersebut akan disusun dan didokumentasikan dalam dokumen BCP PT PLN (Persero) APD Jateng dan DIY.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang yang dikemukakan di atas, rumusan masalah yang menjadi fokus utama dalam usulan tugas akhir ini adalah:

1. Apa hasil dari analisis kritikalitas risiko dari sistem dan layanan TI yang digunakan oleh PT PLN (Persero) Jateng dan DIY?
2. Apa hasil dari analisis kritikalitas dampak proses bisnis pada PT PLN (Persero) APD Jateng dan DIY?
3. Bagaimana bentuk rancangan alur kerja yang dapat digunakan untuk pengelolaan keberlangsungan bisnis berbasis risiko pada PT PLN (Persero) APD Jateng dan DIY?
4. Bagaimana hasil akhir dari rekomendasi strategi untuk perencanaan keberlangsungan bisnis PT PLN (Persero) APD Jateng dan DIY?

1.3 Batasan Masalah

Dari perumusan masalah yang telah disebutkan di atas, batasan masalah dalam tugas akhir ini adalah:

1. Perencanaan keberlangsungan bisnis akan menggunakan alur mundur atau berbasis pada risiko.
2. Hasil akhir dari tugas akhir ini adalah bentuk alur kerja untuk pelaksanan keberlangsungan bisnis PT PLN

(Persero) APD Jateng dan DIY beserta dengan strategi untuk keberlangsungan bisnis perusahaan berbasis risiko.

3. Bentuk alur pengelolaan keberlangsungan bisnis dan hasil dari perencanaan keberlangsungan bisnis akan menggunakan studi kasus pada penggunaan teknologi dan informasi pada PT PLN (Persero) APD Jateng dan DIY.
4. BCP yang dibuat akan berdasarkan pada formulasi kerangka kerja BCMS 22301:2012, Metode OCTAVE dan strategi praktis yang telah diterapkan oleh perusahaan *Department of Energy* United States dengan beberapa rekomendasi aksi manajemen dari standar dan *best practice*.
5. Penilaian dampak bisnis perusahaan menggunakan metode penilaian dampak yang telah dimiliki oleh PT PLN (Persero) pada buku buku Prosedur Penyusunan Risiko dan Kajian Risiko dengan melihat kriteria sesuai fokus utama dari bisnis PT PLN unit area penyalur distribusi.
6. Proses pengerjaan BCP akan difokuskan pada layanan TI yang berada pada prioritas utama dalam hasil analisa dampak bisnis dan pada level risiko TI tinggi dan menengah.
7. Pemberian rekomendasi strategi dan prosedur terbatas pada ISO 27002 dan penerapan pada *Department of Energy* United States.

1.4 Tujuan Tugas Akhir

Dari rumusan masalah yang disebutkan sebelumnya, tujuan yang akan dicapai melalui tugas akhir ini adalah:

1. Mengetahui kritikalitas risiko dari sistem dan layanan TI yang digunakan oleh PT PLN (Persero) Jateng dan DIY.
2. Mengetahui kritikalitas dari dampak proses bisnis PT PLN (Persero) APD Jateng dan DIY.
3. Mengetahui rancangan alur kerja yang dapat digunakan untuk pengelolaan keberlangsungan bisnis berbasis risiko pada PT PLN (Persero) APD Jateng dan DIY.

4. Menghasilkan rekomendasi strategi manajemen untuk perencanaan keberlangsungan bisnis PT PLN (Persero) APD Jateng dan DIY.

1.5 Manfaat Tugas Akhir

Melalui tugas akhir ini diharapkan dapat memberi manfaat yaitu:

Bagi akademis

1. Memberikan sumbangsih pengetahuan mengenai pembuatan usulan pada aktifitas perencanaan keberlangsungan bisnis dengan studi kasus perusahaan energi yaitu PT PLN (Persero) APD Jateng dan DIY.

Bagi perusahaan

1. Memberikan dokumentasi mengenai keadaan proses bisnis dan dampak bisnis dari proses bisnis PT PLN saat ini sehingga dapat dijadikan rekomendasi untuk evaluasi perusahaan yang bersangkutan.
2. Memberikan rekomendasi penggunaan alur kerja pengelolaan keberlangsungan bisnis serta memberikan rekomendasi untuk strategi manajemen dalam perencanaan keberlangsungan bisnis perusahaan berbasis risiko TI PT PLN (Persero) APD Jateng dan DIY.

1.6 Relevansi

Topik yang diangkat dalam pengerjaan tugas akhir ini adalah mengenai perencanaan keberlangsungan bisnis (*business continuity plan)* dengan menggunakan alur mundur yaitu berbasis pada risiko teknologi informasi perusahaan. Topik ini relevan dengan mata kuliah manajemen risiko dan perencanaan keberlangsungan bisnis, dimana perencanaan keberlangsungan bisnis merupakan salah satu mata kuliah pilihan untuk laboratorium Manajemen Sistem Informasi (MSI).

Halaman ini sengaja dikosongkan

BAB II
TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai Studi Penelitian Terdahulu, Literatur Studi dan metode- metode tertentu yang akan dijadikan acuan pada tugas akhir ini.

2.1 Penelitian Terdahulu

Penelitian mengenai *Business Continuity Plan* telah berkembang dan telah dijadikan sebagai topik dalam penelitian baik berupa penggunaan, rekomendasi alur kerja BCP, serta efektifitas BCP.

Tabel 2.1 Penelitian Terdahulu

Judul Penelitian	*Business Continuity Management (BCM) Applied to Transpetro's National Operational Control Center - CNCO*
Penulis	Dilmar de Castro Alves
Hasil Penelitian	Perusahaan Transpetro merupakan perusahaan energi dengan produk utama yaitu gas dan minyak bumi. Melalui CNCO perusahaan ini melalukan operasi dan *monitoring* penyaluran minyak dan gas alam ke perusahaan minyak di Brazil yaitu Petrobas dan beberapa perusahaan yang lainnya. Dalam penelitian ini akan disusun dan dikemukakan hasil dari kinerja implementasi *Business Continuity Management* perusahaan Transpetro dalam penyaluran distribusi energi dan minyak [2]. Hasil dari penelitian ini adalah melalui implementasi BCM, CNCO dapat mengetahui kebutuhan perusahaan dalam menghadapi kemungkinan dari kejadian bencana dan mengetahui sistemasi bagaimana untuk menanggapi dan

	mengelola kejadian bencana untuk melindungi aset TI perusahaan
Hubungan dengan Tugas Akhir	Penelitian ini memberikan pandangan mengenai implementasi dari perencanaan keberlangsunganbisnis untuk perusahaan energi yang telah diterapkan oleh perusahaan Transpetro.
Judul Penelitian	*Guide to Industrial Control Systems (ICS) Security*
Penulis	Stouffer K
Hasil Penelitian	Penelitian tersebut berfokus pada penerapan BCP yang sudah dilaksanakan di perusahaan energi yaitu perusahaan ABC mengenai pelaksanaan BCP dan DRP pada perusahaan yang disertai rekomendasi untuk *best practices.*
Hubungan dengan Tugas Akhir	Penelitian tersebut memberikan gambaran mengenai keadaan nyata pada penerapan BCP dan DRP perusahaan energi dan juga memberikan *best pratices* yang dapat diterapkan oleh perusahaan energi yang lain. Namun kekurangan dari penelitian ini adalah kurang runtut dan terstrukturnya penjelasan mengenai penerapan BCP perusahaan [3].
Judul Penelitian	*A Framework for Business Continuity Management*
Penulis	Forbes Gibb
Hasil Penelitian	Penelitian ini menghasilkan rekomendasi kerangka kerja untuk pelaksanaan *Business Continuity Management* pada perusahaan pada umumnya [4]. Hasil BCP yang direkomendasikan dari penelitian ini masih bersifat general dan tidak berfokus pada bidang tertentu.

Hubungan dengan Tugas Akhir	Kelebihan dari penelitian ini adalah penelitian ini bersifat general tidak berfokus pada satu perusahaan bidang tertentu, namun yang menjadi kelemahan adalah karena bersifat general maka perlu banyak penyesuaian apabila akan diterapkan pada perusahaan bidang tertentu, seperti contohnya PT PLN sebagai perusahaan energi.
Judul Penelitian	Kerangka Kerja *Business Continuity Plan* (BCP) Teknologi Informasi Perusahaan Studi Kasus : PDAM Kota Surabaya
Penulis	Giovanny Praisukma Pertiwi
Hasil Penelitian	Penelitian ini menghasilkan kerangka kerja BCP pada perusahaan BUMN yang berfokus pada pelayanan pelanggan yaitu PDAM kota Surabaya dengan acuan ISO 22301 dan kerangka kerja PDAM kota Padang [5].
Hubungan dengan Tugas Akhir	Pembuatan kerangka kerja BCP untuk PT PLN bisa mengacu dari dasar- dasar pembuatan BCP dari penelitian tersebut karena PT PLN dan PDAM merupakan perusahaan BUMN dan berfokus pada pelayanan pelanggan, namun langkah praktisnya tetap berbeda karena PT PLN merupakan perusahaan berbasis energi dan PDAM merupakan perusahaan bidang penyaluran air bersih untuk pelanggan.
Judul Penelitian	Konsep Penyusunan Kerangka Kerja *Business Continuity Plan* Teknologi dan Sistem Informasi
Penulis	Anindita Alisia
Hasil Penelitian	Penelitian ini menghasilkan kerangka kerja BCP untuk perusahaan perbankan dengan studi kasus yaitu Bank Surya Yudha

	Banjarnegara dengan melakukan formulasi antara BCP milik Bank of Japan dan Dutch Financial Sector serta ISO 22301: 2012 yang dikaitkan dengan kebutuhan dan tujuan Bank Surya Yudha Banjarnegara. [6]
Hubungan dengan Tugas Akhir	Penelitian ini memberikan referensi untuk langkah – langkah atau metodologi dalam pembuatan kerangka kerja perencanaan keberlangsungan bisnis perusahaan yang dapat disesuaikan pada kebutuhan organisasi.
Judul Penelitian	Perancangan Kerangka Kerja Business Continuity Plan untuk Teknologi Informasi pada Studi Kasus STIE PERBANAS
Penulis	Sabrina Leviana Putri
Hasil Penelitian	Penyusunan kerangka kerja yang dilakukan adalah dengan melakukan formulasi antara kebutuhan dan tujuan organisasi berdasarkan ISO 22301:2012 dan kerangka kerja BCM Universitas Griffith dengan menyesuaikan terhadap kebutuhan dari dampak dan risiko TI STIE Perbanas. [7]
Hubungan dengan Tugas Akhir	Penelitian ini memberikan referensi untuk langkah – langkah atau metodologi dalam formulasi penyusunan kerangka kerja perencanaan keberlangsungan bisnis perusahaan yang dapat disesuaikan pada kebutuhan organisasi.

2.2 Manajemen Risiko

Risiko merupakan kemungkinan (*likelihood*) terjadinya ancaman (*threat-source*) yang mengancam kerentanan (*vulner-ability*) dari sistem, serta menghasilkan dampak (*impact*)

berupa kejadian yang merugikan bagi organisasi atau perusahaan. Menurut Basyaid [8], risiko didefinisikan sebagai peluang terjadinya hasil yang tidak diinginkan, sehingga risiko hanya terkait dengan situasi yang memungkinkan munculnya hasil negatif yang berkaitan dengan perkiraan kemungkinan terjadinya hasil negatif tersebut.

Menurut ISO 31000, manajemen risiko merupakan sekumpulan aktivitas dan metode yang terkoordinasi untuk mengarahkan dalam mengkontrol risiko yang bisa mempengaruhi pencapaian tujuan perusahaan [9]. Menurut Blokdijk [10], tugas manajemen risiko adalah mengelola risiko suatu proyek untuk risiko. Tujuan dan manfaat yang dari pelaksanaan manajemen risiko oleh perusahaan adalah untuk mencegah perusahaan dari kegagalan, mengurangi pengeluaran yang berlebihan dari hasil dampak atau risiko yang terjadi.

Terdapat 4 pilihan dalam penanganan risiko yang terdapat pada alur manajemen risiko, yaitu:

- *Take*

  Penanganan ini dilakukan apabila risiko yang dirasakan cukuo besar dan tidak dapat dihindari, sehingga risiko yang terjadi akan mengakibatkan dampak bagi perusahaan sehingga perusahaan harus menerima keadaan risiko. Misalnya adalah kejadian bencana alam yang tidak dapat dihindari oleh perusahaan.
- *Treat*

  Penanganan risiko ini dilakukan untuk menurunkan tingkat risiko dengan cara mengambil tindakan berupa *control* atau *treat* dari risiko tersebut.
- *Terminate*

  Penanganan risiko dengan cara ini adalah apabila risiko yang dirasakan terlalu besar sehingga organisasi atau perusahaan perlu untuk melakukan tindakan pembatalan agar risiko tersebut tidak terjadi. Contoh risiko seperti ini adalah pembuatan produk TI yang baru untuk perusahaan yang akan merugikan perusahaan, maka dalam rangka

untuk menghundari risiko maka perlunya diadakan pembatalan untuk rencana pembuatan produk TI tersebut.

- *Transfer*

  Bentuk penanganan risiko dengan cara *transfer* adalah dengan mengalihkan risiko pada pihak lain, misalnya adalah pada pihak asuransi perusahaan.

Dalam proses manajemen risiko SI/ TI, terdapat proses penilaian risiko untuk aset SI/ TI. Proses penilaian dan pengendalian risiko yang sesuai dengan *best practices* adalah penilaian risiko dengan *standard* OCTAVE dan metode FMEA.

2.3 OCTAVE

Kerangka kerja OCTAVE (*Operationally Critical Threat, Assets and Vulnerability Evaluation)* adalah merupakan pendekatan yang digunakan untuk menilai kebutuhan kemanan informasi organisasi. Kerangka kerja ini memanfaatkan pengetahuan masyarakat yang berhubungan dengan praktek kemanan dan proses organisasi untuk mengetahui keamanan dalam organisasi [11].

Berikut merupakan tahapan yang terdapat dalam OCTAVE untuk manajemen risiko:

- Tahap 1: Menentukan aset berdasarkan profil ancaman

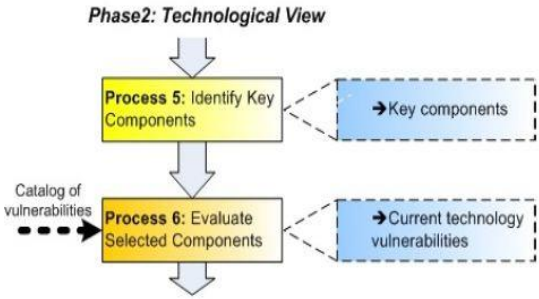
  Pada tahap ini yang dilakukan adalah menentukan aset kritis dan ancaman serta yang saat ini sudah dilakukan dalam rangka melindungi aset tersebut. Dalam fase ini terdapat 4 sub- tahap atau proses, yaitu:
  - Proses 1: Mengidentifikasi pengetahuan dari senior manajemen terhadap aset dan area untuk manajemen risiko TI, kebutuhan keamanan untuk SI/ TI serta mengidentifikasi kerentanan organisasi saat ini.
  - Proses 2: Mengidentifikasi pengetahuan dari manajemen operasional berkaitan dengan aset dan area untuk manajemen risiko TI, kebutuhan keamanan

untuk SI/ TI serta mengidentifikasi kerentanan organisasi saat ini.

- Proses 3: *Identify Staff Knowledge*. Para peserta dalam proses ini adalah anggota staf organisasi. Anggota staf TI biasanya berpartisipasi dalam workshop terpisah dari yang dihadiri oleh anggota staf umum.
- Proses 4: Membuat profil ancaman, yaitu dengan menentukan aset kritis, kebutuhan keamanan untuk aset kritis, serta mengidentifikasi ancaman yang terdapat pada aset kritis.

Gambar 2.1 Tahap Kerangka Metode OCTAVE

- Tahap 2: Mengidentifikasi kerentanan infrastruktur
- Pada tahap kedua, yang harus dilakukan adalah melakukan identifikasi terhadap kerentanan infrastruktur pada aset kritis. Berikut adalah proses yang terdapat pada tahap 2 kerangka kerja OCTAVE:
  - Proses 5: Mengidentifikasi komponen penting yang akan diperiksa untuk kerentanan infrastruktur.
  - Proses 6: Mengevaluasi Komponen Terpilih. Tujuan dari proses ii adalah untuk mengetahui kerentanan teknologi yang terdapat pada komponen infrastruktur.



Gambar 2.2 Tahap 2 kerangka kerja OCTAVE

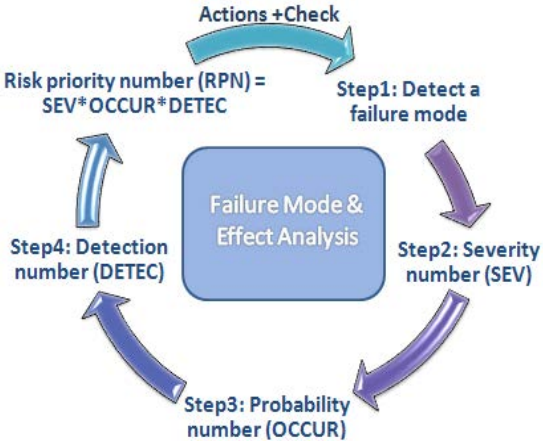
- Tahap 3: Mengembangkan strategi dan rencana keamanan Tahap ini adalah membuat strategi oerlindungan bagi organisasi dan bentuk rencana untuk mitgasi risiko yang diperlukan. Dalam tahap ini terdapat 2 proses yaitu:
  - Proses 7: Analisis risiko. Proses 7 meliputi 3 aktifitas, yaitu mengidentifikasi dampak dari ancaman terhadap aset kritis, membuat kriteria evaluasi risiko, dan mengevaluasi dampak dari ancaman terhadap aset kritis.
  - Proses 8: Pengembangan strategi pengamanan. Tujuan dari proses 8 adalah untuk mengembangkan strategi perlindungan bagi organisasi, rencana mitigasi untuk risiko terhadap aset kritis, dan daftar tindakan tindakan jangka pendek.

2.4 Metode Penilaian Risiko

Failure Modes Effect and Analysis (FMEA) adalah pendekatan langkah demi langkah untuk mengidentifikasi semua kegagalan yang mungkin terjadi dalam proses manufaktur atau perakitan, atau produk atau layanan [12]. Tujuan dari penilaian FMEA adalah untuk melakukan identifikasi terhadap 3 hal, yaitu penyebab kegagalan, efek yang ditimbukan dari kegagalan, serta mengetahui tingkat kritikalitas efek dari kegagalan tersebut. Dalam mengidentifikasi risiko, OCTAVE

memiliki kekurangan pada penilaiannya. Dengan demikian, ditambahakan metode FMEA agar dapat melengkapi kekurangan tersebut.

Berikut merupakan tahapan dari proses FMEA:



Gambar 2.3 Diagram Alur FMEA

- FMEA *Pre- Work.*
  Pada tahap ini yang harus dilakukan adalah mendefinisikan pemangku kepentingan yang terlibat dalam aktifitas manajemen risiko, mengetahui batasan dan ruang lingkup kerja, serta melakukan pengumpulan data dan informasi yang berkaitan dengan aktifitas manajemen risiko.
- Tahap 1: Mendeteksi mode kegagalan.
  Pada tahap ini yang dilakukan adalah melakukan identifikasi terhadap kejadian risiko yang potensial yang menimbulkan efek penyebab dari kegagalan.
- Tahap 2: Menentukan angka keparahan yang ditimbulkan dari kegagalan (*severity number).*

Memberikan peringkat untuk masing- masing penyebab kegagalan sesuai dengan prioritasnya mulai dari angka 1 (*minor)* hingga 10 (*terberat*).

Tabel 2.2. Daftar ranking tingkat keparahan (*Severity*)

Jenis	Keterangan	Nilai
Minor	Kejadian tidak dirasakan dampaknya atau tidak mempengaruhi kinerja.	1
	Menyebabkan gangguan kecil tetapi tidak mempengaruhi kinerja	2
Low	Menyebabkan gangguan kecil dan mempengaruhi sedikit kinerja	3
	Menyebabkan gangguan kecil dan menyebabkan kerugian kecil pada operasional	4
Moderate	Menyebabkan penurunan kinerja dan kerugian operasional yang masih dapat diatasi	5
	Menyebabkan penurunan kinerja dan kerugian operasional yang masih dapat diatasi, serta menimbulkan keluhan pelanggan	6
High	Mempengaruhi beberapa proses bisnis dan menimbulkan keluhan pelanggan	7
	Mempengaruhi seluruh proses bisnis dan menimbulkan keluhan pelanggan	8
Very High	Menghentikan proses bisnis.	9
	Menghentikan proses bisnis dan mempengaruhi sistem keamanan.	10

- Tahap 3: Menentukan angka probabilitas kejadian (*Occurance*).
  Memberikan peringkat masing masing penyebab sesuai dengan probabilitas terjadinya mulai 1 (*none*) sampai 10 (yang terberat).

Tabel 2.3. Daftar Tingkat frekuensi kejadian (*Occurance*)

Jenis Kejadian	Keterangan	Nilai
Minor	Tidak pernah, atau satu kali dalam kurun waktu 10 tahun	1
	Satu kali dalam kurun waktu 5 tahun	2
Low	Satu kali dalam kurun waktu 12 bulan	3
	Satu kali dalam kurun waktu 8 bulan	4
Moderate	Satu kali dalam kurun waktu 5 bulan	5
	Satu kali dalam kurun waktu 3 bulan	6
High	Satu kali dalam kurun waktu 1 bulan	7
	Satu kali dalam kurun waktu 2 minggu	8
Very High	Satu kali dalam kurun waktu 3 hari	9
	Terjadi setiap hari	10

- Tahap 4: Menentukan angka kemungkinan dari kejadian risiko (*Detection*)
  Setelah mengidentidikasi tingkat keparahan dan frekuensi kejadian dari risikom selanjutnya adalah memperkirakan kemungkinan kejadian risiko tersebut datang dan mengancam organisasi. Semakin rendah

peringkatnya maka semakin mudahnya risiko tersebut dapat dideteksi.

Tabel 2.4 Daftar Nilai Deteksi Kejadian (*Detection*)

Jenis Kejadian	Keterangan	Nilai
Minor	Tidak pernah, atau satu kali dalam kurun waktu 10 tahun	1
	Satu kali dalam kurun waktu 5 tahun	2
Low	Satu kali dalam kurun waktu 12 bulan	3
	Satu kali dalam kurun waktu 8 bulan	4
Moderate	Satu kali dalam kurun waktu 5 bulan	5
	Satu kali dalam kurun waktu 3 bulan	6
High	Satu kali dalam kurun waktu 1 bulan	7
	Satu kali dalam kurun waktu 2 minggu	8
Very High	Satu kali dalam kurun waktu 3 hari	9
	Terjadi setiap hari	10

- Menghitung RPN (*Risk Priority Number)*

Setelah melakukan identifikasi dengan menggunakan angka dan ranking pada tiap *severity, occurence* dan *detection,* selanjutnya adalah melakukan operasi perhitungan RPN dengan rumus sebagai berikut :

$$\mathbf{RPN = S \times O \times D}$$

Keterangan :
S = *Severity Number* (Angka Tingkat Keparahan)
O = *Occurrence Number* (Angka Tingkat Probabilitas Kejadian)
D = *Detection Number* (Angka Tingkat Deteksi)

Level dari risiko dapat diketahui dari hasil dari perhitungan RPN pada tabel di bawah ini

Tabel 2.5. Level Risiko berdasarkan hasil RPN

RPN	Level Resiko
200>	*Very High*
151-200	*High*
101-150	*Medium*
51-100	*Low*
0-50	*Very Low*

2.5 Business Impact Analysis

Busines Impact Analysis (BIA) atau analisa dampak bisnis merupakan proses yang dilakukan untuk menentukan proses bisnis dan fungsi bisnis yang kritis dari adanya risiko yang menimbulkan dampak yang terjadi pada organisasi/ perusahaan [13]. Analisa dampak bisnis akan didokumentasikan dalam dokumen BIA. Menurut ISACA, tujuan adanya BIA adalah untuk mengidentifikasikan unit- unit bisnis dan proses bisnis yang penting bagi perusahaan dilihat dari kritikalitasnya dari dampak untuk kejadian bencana [14]. Dalam tahapan penyusunan BCP, BIA adalah langkah awal untuk mengidentifikasikan aktifitas, penilaian dampak, membuat prioritasi serta mengidentifikasikan adanya ketergantungan antar sumber daya [15].

Penentuan kritikalitas pada dampak bisnis tersebut dapat ditinjau dari berbagai aspek, beberapa aspek yang sering digunakan untuk mengukur kritikalitas dampak bisnis adalah aspek finansial, operasional, aspek pelanggan, aspek *public*

image, dan lain- lain. Pihak yang berhak untuk menentukan kritikalitas proses bisnis adalah pihak manajemen strategis pada perusahaan atau pada tiap fungsi bisnis perusahaan. Setelah ditentukan angka kritikalitas proses bisnis pada tiap aspek yang digunakan, maka hasil dari penjumlahan angka tersebut akan di ranking dan ditentukan tingkat kritikalitasnya. Pada tugas akhir ini tingkat kritikalitas yang akan digunakan adalah kritikalitas yang *low* (rendah), *moderate* (menengah), *high* (tinggi kritikalitasnya).

Dengan adanya proses analisa dampak bisnis, maka perusahaan dapat mengetahui apa yang perlu diprioritaskan dalam hal perbaikan saat keadaaan bencana. Luaran yang dihasilkan dari analisa dampak bisnis adalah sebagai berikut:

- Mendapatkan gambaran dari ruang lingkup BCM yang akan dilaksanakan oleh perusahaan.
- Identifikasi mengenai kebutuhan peraturan, hukum, kebijakan dan kontrak yang memiliki dampak untuk keberlangsungan bisnis perusahaan.
- Identifikasi hubungan dari semua produk/ layanan, proses, aktifitas dan sumber daya perusahaan.
- Identifikasi ketergantungan setiap hubungan dari system dan layanan serta fungsi bisnis pada proses bisnis yang berjalan untuk perusahaan.
- Hasil evaluasi dari dampak bisnis dengan parameter waktu dan kapabilitas yang dapat ditanggulangi perusahaan.

Penyusunan BIA akan berdasarkan pada teknis dan praktis yang telah dijalankan oleh PT PLN (Persero) berdasarkan pada kebijakan direksi sesuai KEPDIR 537.K.DIR/2010 sebagai fokus implementasi pada *risk awareness* dalam penguatan kontrol internal [16]. Langkah praktis yang telah diterapkan oleh PT PLN (Persero) adalah menggunakan perhitungan untuk ancaman pada risiko bisnis. Pada tabel 2.6 dan 2.7 merupakan profil untuk kriteria tingkat dampak yang terdapat pada buku Prosedur Penyusunan Risiko dan Kajian Risiko [17]. Dampak bisnis ditinjau dari 2 aspek,

yaitu aspek produk dan layanan, dan aspek proses bisnis internal.

Tabel 2.6 Dampak terhadap Produk dan Layanan

Tingkat Dampak	Keterangan	Nilai
Tidak Signifikan	Mengakibatkan pemadaman sesaat selama <15 menit pada satu waktu	1
Minor	Mengakibatkan pemadaman sesaat selama 15 menit – 1 jam pada satu waktu	2
Medium	Mengakibatkan pemadaman selama 1 – 3 jam pada satu waktu	3
Signifikan	Mengakibatkan pemadaman selama 3 jam – 1 hari pada satu waktu	4
Malapetaka	Mengakibatkan pemadaman selama lebih dari 1 hari dan/ atau Mengakibatkan pemadaman bergilir pada watu waktu (*blackout system)*	5

Tabel 2.7 Aspek Proses Bisnis Internal

Tingkat Dampak	Keterangan	Nilai
Tidak Signifikan	Kegiatan proses bisnis perusahaan tidak terganggu	1
Minor	Mengakibatkan kegiatan proses bisnis perusahaan terganggu secara terbatas dalam 1 unit dan tidak mempengaruhi pelayanan	2

Tingkat Dampak	Keterangan	Nilai
Medium	Mengakibatkan kegiatan proses bisnis perusahaan terganggu secara terbatas dalam 1 unit dan mempengaruhi pelayanan	3
Signifikan	Mengakibatkan kegiatan proses bisnis perusahaan terganggu secara terbatas dalam beberapa unit	4
Malapetaka	Mengakibatkan kegiatan proses bisnis perusahaan terganggu secara terbatas dalam secara luas	5

2.6 Business Continuity Management Systems (BCMS)

Business Continuity Management merupakan proses holistik yang dimulai dari proses identifikasi dampak dan risiko dari kegiatan bisnis hingga melakukan respon untuk menanggulangi dan mengurangi risiko bencana. *Business Continuity Management Systems* merupakan sekumpulan elemen dari keseluruhan sistem manajemen yang saling berkaitan untuk melaksanakan implementasi, operasi, pengawasan, *review*, menjaga dan meningkatkan keberlangsungan bisnis perusahaan [18].

Gambar 2.4 Siklus BCMS pada standar BIA ISO 22317

Proses dalam BCM saling terkait satu sama lain dan tidak dapat dipisahkan. Berikut merupakan hubungan dari setiap proses yang terdapat dalam BCM, dimana di dalamnya juga terdapat proses BIA dan BCP.

2.7 Business Continuity Plan (BCP)

*Business Continuity Plan (*BCP) Master Plan adalah dokumen manajemen yang menjelaskan metodologi untuk merangkai panduan aktifitas perencanaan untuk keberlangsungan bisnis (BCP), pemeliharaan, dan bagaimana BCP dieksekusi untuk mengembalikan operasi organisasi/ perusahaan setelah terjadi bencana. Dokumen BCP harus dilakukan revisi dan diperbaharui secara periode yang kontinyu untuk menyesuaikan perubahan dari manajemen organisasi dan bisnis.

BCP memiliki 2 buah metode yaitu metode maju dan metode mundur, dimana pada pengerjaan kali ini kita akan menggunakan metode mundur. Metode perangkaian BCP mundur yang dimaksud adalah metode perangkaian BCP berbasis resiko, dimana dalam tahap perangkaiannya digunakan metode

– metode analisa resiko untuk mengidentifikasi hal – hal dan langkah – langkah yang harus dilakukan saat BCP dieksekusi.

BCP metode mundur atau berbasis risiko, dalam proses pembuatannya membutuhkan penilaian risiko TI dan analisa dari dampak bisnis terlebih dahulu sebelum menentukan aksi untuk pengelolaan risiko. Salah satu acuan yang dapat digunakan untuk melakukan penyusunan perencanaan keberlangsungan bisnis berbasis risiko adalah dengan ISO 22301: 2012 yaitu *Plan, Do, Check*, dan *Action.*

2.8 Disaster Recovery Plan (DRP)

Menurut Brooks [19], DRP merupakan rencana yang dibuat oleh organisasi dalam penanganan terhadap pemulihan kinerja sistem, aplikasi yang berfokus pada penggunaan TI ketika terjadi situasi darurat yang mengancam organisasi. Sedngkan menurut National Institute of Standard and Technology, DRP merupakan perencanaan untuk melaksanakan kondisi pengganti atau alternatif pada saat kondisi bencana atau gangguan terhadap sistem, perangkat atau layanan TI. Sehingga dari kedua sumber tersebut, DRP merupakan bentuk aksi perencanaan yang dibuat sebagai aksi pemulihan khususnya pada suatu sistem atau perangkat TI pada kejadian bencana.

2.9 Hubungan antara BCP dengan DRP

Menurut buku *Disaster Recovery Strategies with Tivoli Storage Management* [19] menjelaskan bahwa BCP merupakan perencanaan yang dilakukan oleh perusahaan yang menghasilkan kebutuhan detail- detail dari prosedur untuk menanggulangi kejadian risiko atau bencana, sedangkan DRP dihasilkan dari kebutuhan detail prosedur untuk keberlangsungan pada operasional TI. Sehingga dari keterangan tersebut dapat disimpulkan bahwa DRP merupakan subset atau bagian dari proses BCP. Selain itu, dalam rangka memenuhi kebutuhan bisnis yang dapat berubah maka kedua perencanaan

ini butuh untuk dilakukan pembaharuan secara periodik pada tiap tahun.

Dalam rangka mempermudah pengertian mengenai BCP dan DRP, berikut dalam tabel akan diberikan perbedaan dari BCP dan DRP berdasarkan kategori yang diidentifikasikan sebagai berikut:

Tabel 2.8. Perbedaan BCP dengan DRP

Kategori	BCP	DRP
Tujuan	Pemeliharaan keberlangsungan dari proses bisnis	Penanganan bencana pada operasional TI
Ruang lingkup perencanaan	Dibuat dengan mempertimbangkan satu atau keseluruhan proses bisnis	Dibuat dengan mempertimbangkan gangguan pada operasional TI
Waktu pemberlakuan	Dibutuhkan saat, sebelum dan setelah kejadian gangguan	Dibutuhkan saat, dan setelah kejadian gangguan

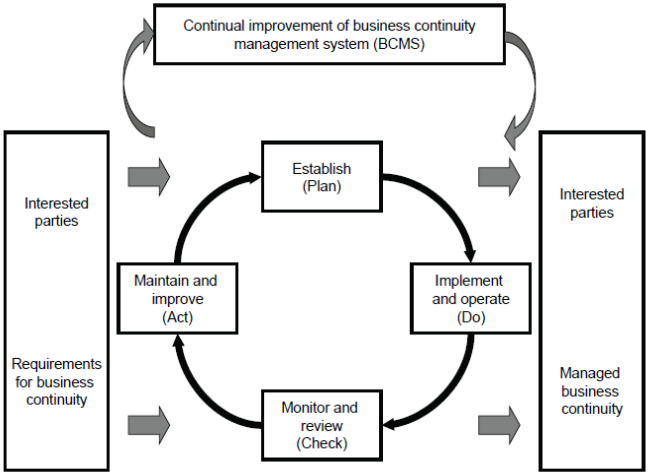
2.10 ISO 22301:2012

ISO 22301: 2012 merupakan salah satu acuan standard untuk perencanaan keberlangsungan bisnis berbasis risiko dengan menggunakan tahap –tahap yaitu *Plan*, *Do*, *Check*, dan *Action*. ISO 22301 merupakan hasil dari pengembangan dari British Standard 25999-2:2007. Standar tersebut digunakan dalam rangka menjaga keberlangsungan bisnis dari adanya gangguan yang berpotensi mengancam bisnis perusahaan. Standar ini banyak digunakan oleh perusahaan – perusahaan karena bersifat umum. Sehingga dalam penelitian ini selain menggunakan standar ISO 22301 juga akan menggunakan contoh penerapan dari kerangka BCP yang telah diterapkan

oleh perusahaan energi lain agar dapat disesuaikan dengan kebutuhan bisnis perusahaan yang dicontohkan dalam BCP perusahaan tersebut.

Tahap- tahap yang terdapat pada acuan standard untuk perencanaan keberlangsungan bisnis berbasis risiko pada ISO 22301: 2012 adalah sebagai berikut:

- *Plan*
  Pada tahap ini yang dilakukan oleh tim analisis adalah menentukan kebijakan, tujuan, target, kontrol, proses dan prosedur untuk aktifitas keberlangsungan bisnis pada perusahaan.
- *Do*
  Pada tahap ini *Do* yang dilakukan adalah pelaksanaan dari kebijakan, tujuan, target, kontrol, proses dan prosedur yang telah direncanakan pada tahap *Plan.*
- *Check*
  Tahap *Check* merupakan tahap untuk melakukan review dan pengawasan pada pelaksanaan keberlangsungan bisnis perusahaan yang disertai dengan laporan yang disertai dengan rekomendari untuk perbaikan dari sistem untuk rencana keberlangsungan bisnis perusahaan.
- *Action*
  Tahap *Action* merupakan tahap untuk pemeliharaan dan perbaikan pengelolaan sistem keberlangsungan bisnis dengan membuat aksi korektif berdasarkan pada hasil laporan review dari pengawasan keberlangsungan bisnis.



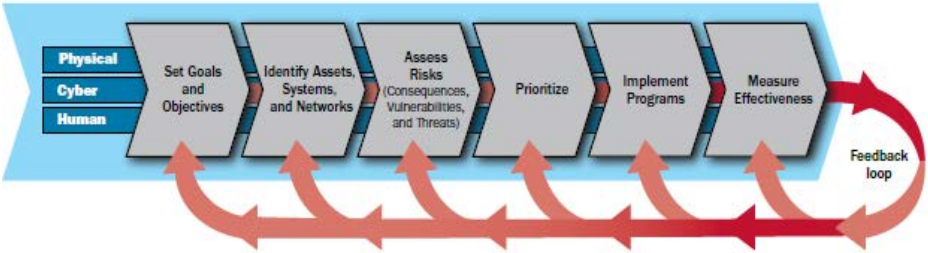
Gambar 2.5 Siklus BCMS berdasarkan ISO 22301:2012

2.11 NIPP Risk Management Framework

Pada tahun 2006, *Department of Homeland Security* (DHS) mengeluarkan sebuah kerangka kerja untuk pengelolaan risiko dan keberlangsungan bisnis perusahaan untuk perusahaan sektor industri, energi dan layanan publik di United States yang terdapat dalam *Sector Specific Agencies* (SAA). Kerangka kerja tersebut dinamakan *National Infrastructure Protection Plan* (NIPP).

Kerangka kerja pengelolaan risiko NIPP telah diterapkan oleh salah satu sektor dari SSA yaitu sektor energi oleh *The US Department of Energy* (DOE). DOE merupakan organisasi atau perusahaan dari pemerintahan United States untuk mengatur sektor energi dan sector perminyakan di United States [19]. Tugas DOE dalam pengaturan sektor energi tersebut beberapa diantaranya adalah dengan melakukan pengawasan secara rutin mengenai penyaluran energi listrik dan minyak di United States. Selain menerapkan kerangka kerja ini, DOE juga melakukan penyesuaian dengan kebutuhan perusahaan dan pelayanan yang

diberikan kepada publik. Tujuan DOE dalam penerapan kerangka kerja pengelolaan risiko ini adalah agar dalam pencapaian tugas dan tanggung jawab perusahaan terhadap publik dapat berlangsung secara aman, memiliki informasi yang reliabel, adanya koordinasi yang lebih baik antar anggota perusahaan, serta terciptanya hubungan dengan publik dan *private*



Gambar 2.6 NIPP Risk Management Framework

partner perusahaan yang terpercaya.

Dalam kerangka kerja yang telah digunakan oleh DOE terdapat beberapa tahap di dalamnya yaitu sebagai berikut:

- Menentukan sasaran dan tujuan
  Pada tahap ini perusahaan harus mendefinisikan terlebih dahulu apa tujuan dari penerapan BCP, profil sektor perusahaan, dan *partnership* dengan pihak lain.
- Mengidentifikasi aset, sistem, dan jaringan
  Tujuan dari tahap ini adalah perusahaan mengetahui keberadaan dari aset, sistem dan jaringan yang digunakan pada proses bisnis perusahaan. Pada tahap ini, yang perlu dilakukan adalah menjelaskan aset, sistem dan jaringan perusahaan yang digunakan pada aktifitas proses bisnis.
- Menilai risiko
  Pada tahap ini perusahaan perlu mengetahui terlebih dahulu risiko- risiko yang mengancam perusahaan serta mengetahui dampak yang ditimbulkan dari risiko tersebut dari *human impact, economic impact, impact on public confidence,* serta *impact on government capability*. Setelah mengetahui dampak atau konsekuensi dari risiko, yang

harus dilakukan adalah melakukan penilaian terhadap ancaman (*threat*) dan kerentanan (vulnerabilities) pada aset, sistem dan jaringan.

Metode yang digunakan dalam penilaian risiko pada kerangka kerja ini adalah R = f (C, T, V) dimana fungsi risiko dari aset (f) merupakan konsekuensi (C) yang menyerang dan mengganggu proses bisnis perusahaan, yang sering menjadi ancaman (T) pada aset perusahaan dan aset perusahaan yang memiliki kerentanan (V).

- Menentukan prioritas

  Pada tahap ini, proritas yang ditentukan berdasarkan kondisi internal dan kritikalitas bisnis perusahaan, serta kondisi program pemerintahan yang membutuhkan alokasi sumber daya pada prioritisasi tersebut.
- Pelaksanaan program

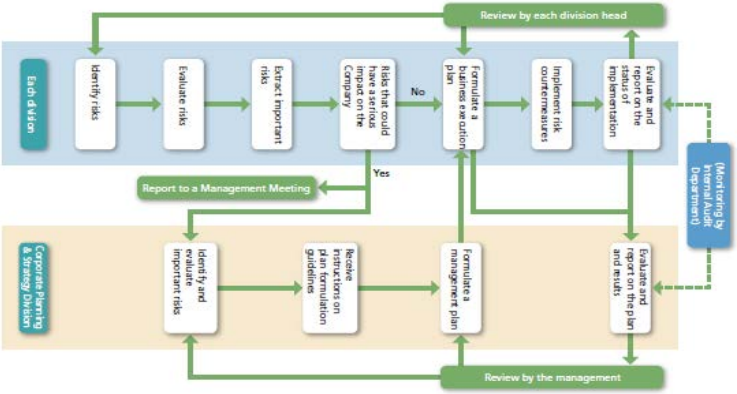
  Pelaksanaan program pada tahap ini berupa program evaluasi, prioritisasi kebutuhan, dan pelaksanaan.
- Mengukur efektifitas

  Pengukuran efektifitas dapat memberikan identifikasi pada beberapa metriks yang digunakan untuk meningkatkan performa kerja perusahaan. Dalam pengukurna efektifitas ini perusahan harus menentukan kunci keberhasilan dari aktifitas mitigasi risiko, menentukan metriks dari aktifitas mitigasi dan program keberlangsungan bisnis pada perusahan.

2.12 BCP pada Chubu Electric Power Company

Ruang lingkup BCP yang diterapkan oleh *Chubu Electric Power* memiliki lebih banyak ruang lingkup apabila dibandingkan dengan bentuk manajemen bencananya [21]. Karena dalam BCP yang telah disusun juga menyertakan apa saja risiko bisnis yang ditimbulkan dari bencana dengan proritas utama adalah mengamati aspek operasional bisnis seperti kegiatan untuk memasok listrik, pembayaran dan pembiayaan mitra bisnis, penyelamatan lingkungan dari radiasi kimia dan lain- lain.

Berikut merupakan gambar dari alur *Business Continuity Plan* pada perusahaan *Chubu Electric Power*:



Gambar 2.7 Alur Kerja Keberlangsungan Bisnis Perusahaan *Chubu Power Electric*

LAMPIRAN A
Kuesioner Formulir Wawancara Proses Bisnis

1. Informasi Umum

Tujuan:

Memperoleh pemahaman secara menyeluruh pada setiap unit bisnis Perusahaan.

Cara pengisian kuesioner :

1. Isilah data personal, seperti nama, no telepon dan alamat email.
2. Isilah nama kelompok kerja/ bagian/ unit kerja Anda
3. Isilah dengan posisi Anda dalam kelompok kerja/bagian/unit kerja ini.

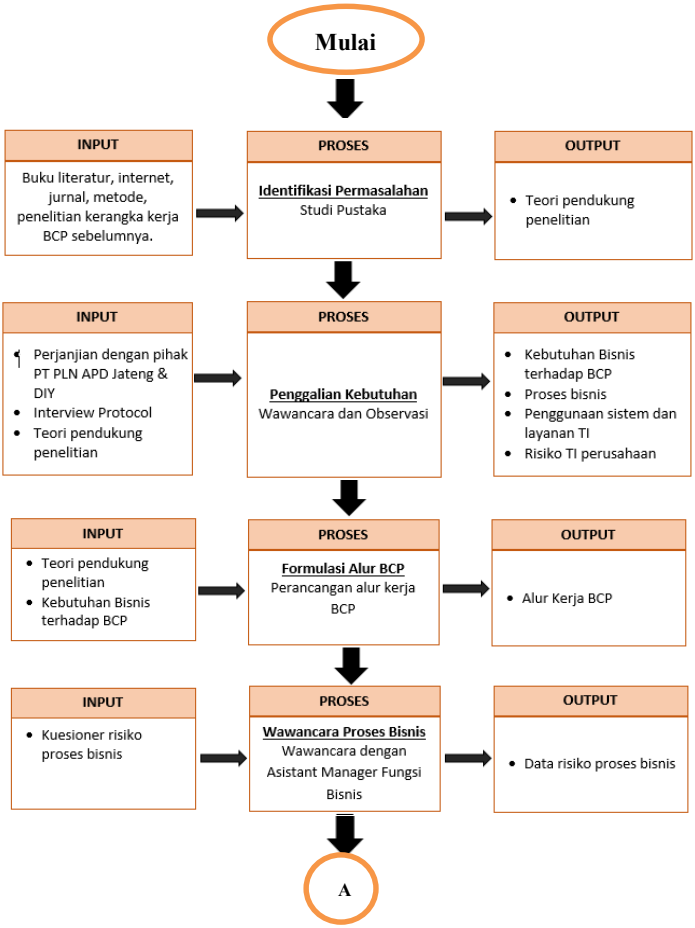
Kuesioner B*usiness Impact Analysis* (BIA)

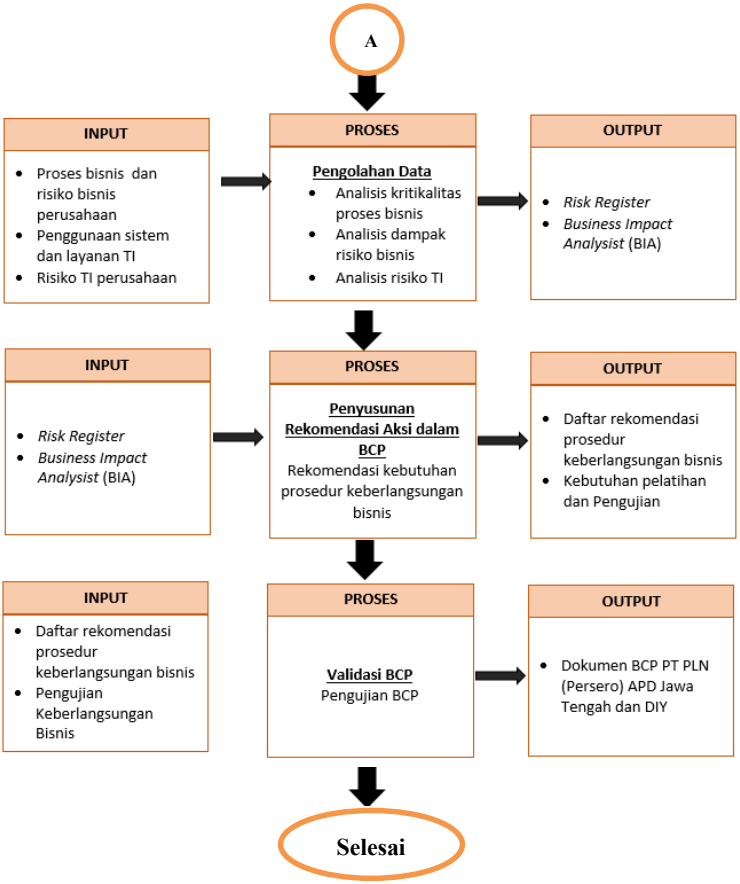
Nama : _____
No Telepon (Kantor/HP) : _____
Alamat Email : _____
Jabatan : _____
Bagian : _____
Fungsi : _____

BAB III
METODOLOGI

Bab ini menjelaskan metodologi yang akan digunakan dalam pengerjaan tugas akhir. Metodologi diperlukan sebagai panduan urutan pengerjaan yang disusun secara sistematis untuk tugas akhir yang diusulkan.

Berikut merupakan gambaran mengenai metodologi yang akan digunakan pada tahap penyusunan tugas akhir.





Gambar 3.1 Metodologi Penelitian Tugas Akhir

3.1 Identifikasi Permasalahan

Tahap pertama dalam pengerjaan tugas akhir ini adalah dengan melakukan studi pustaka pada sumber literatur berupa buku, jurnal penelitian atau report CSR perusahaan yang berkaitan dengan kerangka dan alur kerja untuk kegiatan dalam perencanaan keberlangsungan bisnis berbasis risiko pada perusahaan energi yang berfokus pada layanan distribusi penyaluran tenaga listrik untuk pelanggan. Selain itu, tahap ini juga mengidentifikasikan proses bisnis yang berkaitan dengan

menggunakan masukan dari buku Rencana Jangka Panjang PLN APD Jateng dan DIY [22] yang berisi visi, misi serta proses bisnis yang dilaksanakan oleh PLN APD Jateng dan DIY.

Keluaran dari tahap ini berupa teori pendukung untuk melakukan penelitian mengenai model untuk alur kerja dari proses pengelolaan keberlangsungan bisnis yang dapat diterapkan oleh PT PLN (Persero) APD Jateng.

3.2 Penggalian Kebutuhan terhadap BCP

Proses ini dilakukan untuk mengetahui kebutuhan dari PT PLN (Persero) APD Jateng dan DIY terhadap penerapan BCP pada perusahaan. Metode yang dilakukan dalam penggalian kebutuhan terhadap BCP ini adalah wawancara dengan Asisten Manajer SCADA dan Telekomunikasi serta observasi dari dokumen- dokumen yang berkaitan dengan manajemen risiko atau keberlangsungan bisnis perusahaan. Masukan dari proses ini adalah interview protocol serta teori pendukung penelitian, khususnya ISO 22301:2012 dan metode OCTAVE. Keluaran dari proses ini adalah kebutuhan bisnis terhadap BCP, proses bisnis dan fungsi bisnis yang terdapat di perusahaan, penggunaan sistem dan layanan TI serta risiko TI perusahaan yang mengancam keberlangsungan bisnis perusahaan.

3.3 Formulasi Alur BCP

Setelah mengetahui kebutuhan dan teori untuk pelaksanaan BCP, maka penelitian dapat dilanjutkan dengan melakukan formulasi dari beberapa teori pendukung yang telah didapatkan dengan kondisi dan kebutuhan dari PLN APD Jateng dan DIY. Hasil dari proses ini adalah beru[a rekomendasi pelaksanaan alur kerja BCP untuk PLN APD Jateng dan DIY yang nantinya perlu untuk diverifikasi terlebih dahulu oleh pihak manajemen SCADA dan Telekomunikasi.

3.4 Wawancara Proses Bisnis

Tahap ini adalah tahap pengumpulan data dan informasi yang tujuannya adalah untuk mendapatkan data dan informasi yang berkaitan dengan pengerjaan tugas akhir ini.

Metode yang dapat dilakukan dalam proses pengumpulan data adalah dengan melakukan wawancara dan observasi terhadap proses bisnis dalam perusahaan. Data- data yang dibutuhkan dalam pengerjaan tugas akhir ini antara lain data mengenai fungsi bisnis serta proses bisnis yang terdapat dalam perusahaan, penggunaan sistem dan layanan TI pada perusahaan, serta risiko dari sistem dan layanan TI perusahaan.

Masukan dari proses ini adalah berupa kuesioner untuk ditanyakan pada Asisten Manajer tiap fungsi Bisnis serta checklist penerapan ISO 27002 yang akan dilakukan oleh staff SCADA dan Telekomunikasi untuk selanjutnya diverifikasi oleh Asisten Manajer SCADA dan Telekomunikasi.

3.5 Pengolahan Data dan Informasi

Data yang telah didapatkan dari proses 3 yaitu pengumpulan data dan informasi akan digunakan sebagai proses olah data yaitu untuk menentukan kritikalitas proses bisnis, analisis dampak dari risiko bisnis, serta analisis dari risiko sistem dan layanan TI perusahaan. Keluaran dari proses ini adalah berupa dokumen *business impact analysist* dan berupa *risk register* dari risiko sistem dan layanan TI perusahaan.

3.6 Penyusunan Rekomendasi Aksi BCP

Pada tahap ini akan dilakukan kegiatan untuk menyusun dokumen bentuk manajemen aksi dari kejadian bencana.

Aktivitas yang akan dilaksanakan dalam proses ini adalah menyusun daftar strategi dan kebutuhan keberlangsungan bisnis sebagai bentuk manajemen aksi dalam BCP serta menganalisa ulang alur kerja untuk pengelolaan keberlangsungan bisnis PT PLN (Persero) APD Jateng dan DIY. Keluaran dari proses ini

adalah berupa daftar rekomendasi prosedur keberlangsungan bisnis serta kebutuhan pelatihan dan pengujian BCP.

3.7 Validasi BCP

Pada tahap ini akan dilakukan validasi terhadap usulan bentuk dokumentasi BCP berbasis risiko pada perusahaan PT PLN yang telah disusun oleh penulis. Pada proses ini, yang akan dilakukan adalah dengan melakukan pengujian dari hasil dokumen BCP yang telah disusun untuk diujikan pada perusahaan dan melakukan pertemuan dengan pihak manajemen PT PLN (Persero) APD Jateng dan DIY untuk pengesahan dokumen BCP PT PLN (Persero) apabila dokumen BCP yang dihasilkan telah sesuai. Tujuan diadakannya proses validasi adalah untuk memberikan kepastian bahwa bentuk dari alur dalam pengelolaan dan perencanaan keberlangsungan bisnis untuk PT PLN (Persero) APD Jateng sudah sesuai dengan kondisi dan keadaan kultur perusahaan sehingga dapat diterapkan oleh PT PLN (Persero).

3.8 Jadwal Penyusunan Tugas Akhir

Bab ini menjelaskan mengenai rencana penjadwalan untuk penyusunan tugas akhir yang berjudul "Perencanaan Keberlangsungan Bisnis Teknologi Informasi Berbasis Risiko (Studi Kasus: PT PLN (PERSERO) APD Jateng dan DIY)"

Tabel 3.1 Jadwal Penelitian dan Pengerjaan Tugas Akhir

No	Kegiatan	Maret				April				Mei				Juni			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Studi Pustaka																
2.	Penyusunan proposal tugas akhir																

No	Kegiatan	Maret				April				Mei				Juni			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
3.	Sidang proposal tugas akhir																
4.	Analisis teori pendukung																
5.	Pengumpulan data dan infor-masi																
6.	Pengolahan data dan informasi																
7.	Penyusunan dokumen BCP																
8.	Validasi BCP																
9.	Penyusunan buku tugas akhir																
10.	Sidang Tugas Akhir																

BAB IV
PERANCANGAN

Pada bab ini akan menjelaskan mengenai perancangan dalam proses penelitian Tugas Akhir sesuai dengan metodologi yang telah dijabarkan pada Bab III.

4.1 Identifikasi Permasalahan

Identifikasi permasalahan dilakukan dengan melakukan p melakukan studi pustaka pada sumber literatur berupa buku, jurnal penelitian atau report CSR perusahaan yang berkaitan dengan kerangka dan alur kerja untuk kegiatan dalam perencanaan keberlangsungan bisnis berbasis risiko pada perusahaan energi yang berfokus pada layanan distribusi penyaluran tenaga listrik untuk pelanggan. Selain itu, tahap ini juga mengidentifikasikan proses bisnis yang berkaitan dengan menggunakan masukan dari buku Rencana Jangka Panjang PLN APD Jateng dan DIY [22] yang berisi visi, misi serta proses bisnis yang dilaksanakan oleh PLN APD Jateng dan DIY.

4.2 Penggalian Kebutuhan terhadap BCP

Penggalian kebutuhan bisnis dilakukan dengan proses wawancara dengan manajemen yang berfokus pada teknologi informasi di perusahaan. Pada PT PLN (Persero) APD Jateng dan DIY, pihak manajemen yang menangani dan mengawasi penggunaaan teknologi informasi adalah Asisten Manajer SCADA dan Telekomunikasi. Hasil yang diharapkan dari proses ini adalah berupa ketentuan untuk konteks organisasi, ruang lingkup BCP, pembagian peran dan tanggung jawab, alur komunikasi pelaksanaan BCP, serta tujuan pelaksanaan BCP.

Interview protocol yang dibuat berdasarkan pada metode OCTAVE untuk mengidentifikasikan kebutuhan dan keperluan perusahaan dalam penanganan risiko TI. Berikut merupakan interview protocol dari wawancara dengan Asisten Manajer

SCADA dan Telekomunikasi untuk menggali kebutuhan bisnis perusahaan:

Tabel 4.1 Tabel Interview Protocol Penggalian Kebutuhan Proses Bisnis

A. Data Narasumber

Nama :
Jabatan :
Fungsi :
Waktu :
Lokasi :

B. Keadaan Terkini Manajemen Risiko PT PLN (Persero) APD Jateng dan DIY

1. PT PLN (Persero) sudah memiliki buku prosedur untuk penyusunan profil risiko dan kajian risiko perusahaan, apakah PT PLN (Persero) APD Jateng sudah melaksanakan prosedur untuk mendaftar risiko dan melakukan kajian risiko tingkat perusahan?

   _____
   _____

2. Seperti apakah bentuk dari alur komunikasi yang telah dilakukan oleh perusahaan dalam penanganan gangguan terhadap layanan TI?

   _____
   _____

3. Apakah terdapat dokumentasi atau pencatatan terhadap log gangguan pada layanan TI?

   _____
   _____

4. Apakah terdapat beberapa gangguan TI yang berkaitan langsung dengan aplikasi tertentu yang bukan menjadi tanggung jawab secara langsung dari tim TI?

   _____
   _____

5. Dalam buku prosedur untuk penyusunan profil risiko dan kajian risiko PT PLN (Persero) sudah mendefinisikan risiko- risiko yang mengancam perusahaan, hanya saja belum secara spesifik mendefinisikan risiko Teknologi Informasi.
   Misalnya pada point O.9.1 Bencana Lokal, apakah dapat ditambahkan dengan profil risiko O.9.4 Risiko Bencana Tingkat Perusahaan dengan lebih dispesifikkan lagi dengan O.9.4.1 Kebakaran tingkat perusahaan, O.9.1.2 Kebakaran Server, O.9.1.3 Listrik Mati, dan lain sebagainya sesuai dengan standar acuan teknologi informasi yang akan disesuaikan dengan PT PLN dengan pertimbangan dari pihak Manager APD?

   _____
   _____

C. <u>Identifikasi Risiko Keamanan Teknologi Informasi</u>

1. Siapa sajakah yang berkaitan langsung terhadap layanan TI yang terdapat di PLN APD Jateng dan DIY?

   _____
   _____

2. Apa saja perangkat lunak atau aplikasi yang diidentifikasikan sebagai aset TI kritis pada PLN APD Jateng dan DIY?

   _____
   _____

3. Apa saja perangkat keras yang diidentifikasikan sebagai aset TI kritis pada PLN APD Jateng dan DIY?

   _____

   _____

4. Apa saja komponen jaringan yang diidentifikasikan sebagai aset TI kritis pada PLN APD Jateng dan DIY?

   _____

   _____

5. Apa saja identifikasi dan deskripsi spesifik dari data yang diidentifikasikan sebagai aset TI kritis pada PLN APD Jateng dan DIY?

   _____

   _____

D. Penggalian Kebutuhan Keamanan Aset TI Kritis

1. Apakah PT PLN (Persero) APD Jateng sudah memiliki bentuk langkah antisipasi manajemen risiko khusus untuk Teknologi Informasi perusahaan?

   Jika jawaban **Ya,** apakah langkah manajemen risiko sudah didokumentasikan dalam bentuk dokumen manajemen risiko? Sejauh apa bentuk dokumentasi manajemen risiko tersebut?

   _____

   _____

Selain dengan metode wawancara, yang dilakukan dalam aktifitas ini adalah melakukan observasi dari dokumen rencana jangka panjang PT PLN (Persero) untuk mengetahui fleksibilitas dan aktifitas terkini dari perusahaan dalam penanganan risiko bisnis dan risiko TI.

Konteks organisasi yang dimaksud adalah proses bisnis yang terdapat pada perusahaan serta alur atau keterkaitan antar proses bisnis. Keterkaitan proses bisnis tersebut didapatkan dari observasi dokumen rencana jangka panjang PT PLN (Persero) APD Jateng dan DIY [22] yang dipublikasikan pada internal perusahaan pada tahun 2013. Oleh karena tidak ter-*update*nya buku rencana jangka panjang tersebut, maka penelitian tugas akhir pada bagian ini diperlukan untuk konfirmasi pada pihak asisten manajer untuk memastikan bahwa keterkaitan dan proses bisnis tersebut sesuai dengan kondisi dan keadaan yang terdapat pada PT PLN (Persero) APD Jateng dan DIY.

Penetapan ruang lingkup dilakukan berdasarkan pada standar salah satu alur kerja terapan yang dilakukan pada perusahaan lain dengan kondisi perusahaan. Sedangkan untuk tujuan pelaksanaan BCP didapatkan dari pemetaan yang diinginkan dan kebutuhan perusahaan terhadap BCP.

4.3 Formulasi Alur BCP

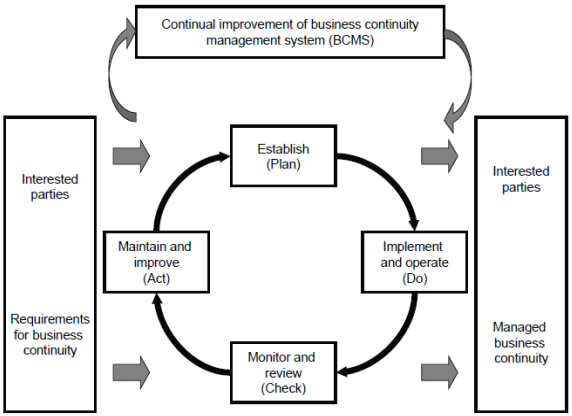
Perancangan alur kerja BCP untuk PT PLN (Persero) APD Jateng dan DIY akan dibuat dengan menggunakan pendekatan alur mundur atau berbasis risiko. Sehingga dalam hal ini, perlu dilakukan penggalian kebutuhan perusahaan terlebih dahulu berdasarkan keinginan manajemen terhadap pelaksanaan BCP pada PT PLN (Persero) APD Jateng dan DIY. Perancangan alur kerja dilakukan berdasarkan standar dan kerangka *best practice* yang telah diterapkan pada sebuah perusahaan.

Sub bab berikut ini merupakan pemetaan penggunaan teori penunjang dalam formulasi kerangka kerja BCP:

4.3.1 Kerangka Dasar

Dalam proses perancangan alur kerja Business Continuity Plan untuk PT PLN (Persero) APD Jateng dan DIY akan menggunakan kerangka dasar *Business Continuity Management Systems* ISO 22301:2012 sebagai acuan utama

dalam pembuatan alur kerja. ISO 22301:2012 digunakan sebagai kerangka dasar dalam perancangan ini karena kerangka ISO 22301:2012 merupakan kerangka kerja yang bersifat iteratif atau tidak terputus pada satu proses akhir sehingga akan memudahkan perusahaan dalam melakukan pelaksanaan, pemantauan serta pengembangan BCP. Kerangka kerja ini bersifat iteratif karena standar PDCA (*Plan, Do, Check, Act)* dilakukan secara terus menerus atau tidak terputus oleh satu proses tertentu.



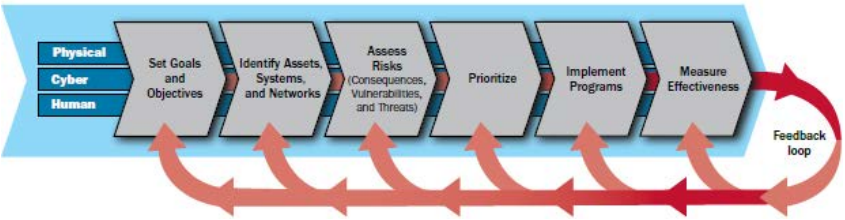
Gambar 4.1 Kerangka BCMS ISO 22301:2012

Kerangka ISO 22301 digunakan sebagai kerangka dasar untuk perancangan alur kerja sesuai kebutuhan PT PLN (Persero) APD Jateng dan DIY dengan kombinasi satu contoh terapan alur kerja BCP yang dilakukan oleh perusahaan lain, yaitu *The US Department of Energy*. Kerangka dasar ISO 22301 akan dijadikan sebagai pondasi awal dalam pembuatan alur kerja BCP untuk PT PLN (Persero) APD Jateng dan DIY.

4.3.2 Alur Kerja Terapan

Kerangka kerja 22301:2012 dianggap terlalu kaku karena tidak memiliki sifat yang sederhana atau terlalu sulit untuk dimengerti [6] maka diperlukan sebuah alur kerja yang telah diuji dan diterapkan oleh organisasi lain dalam pelaksanaan BCP.

Alur kerja terapan yang akan digunakan adalah alur kerja BCP milik *The US Department of Energy* yang merupakan perusahaan energi untuk energi listrik dan gas di United States. Alur kerja ini dibuat oleh *Department of Homeland Security* (DHS) sebagai alur kerja untuk perusahaandi sektor industri, energi dan layanan publik di United States. Kerangka atau alur kerja ini diberikan nama *National Infrastructure Protection Plan* (NIPP)



Gambar 4.2 NIPP Risk Management Framework

Dalam alur kerja yang digunakan oleh DOE tersebut terdapat beberapa tahap sebagai berikut:

- Menentukan sasaran dan tujuan
  Pada tahap ini organisasi harus mendefinisikan terlebih dahulu apa tujuan dari penerapan BCP, profil sektor perusahaan, dan *partnership* dengan pihak lain.
- Mengidentifikasi aset, sistem, dan jaringan
  Pada tahap ini yang dilakukan organisasi adalah mengidentifikasikan aset, sistem dan jaringan yang digunakan pada setiap proses bisnis pada organisasi atau perusahaan.

- Melakukan penilaian risiko
  Setelah melakukan identifikasi risiko, organisasi atau perusahaan melakukan penilaian risiko untuk dapat menentukan prioritas dalam malaksanakan strategi keberlangsungan bisnis. Penilaian risiko yang dilakukan oleh DOE berdasarkan pada konsekuensi yang menyerang dan mengganggu proses bisnis perusahaah, ancaman terhadap aset perusahaah serta kerentanan yang dimiliki oleh aset.
- Menentukan prioritas
  Pada tahap ini, proritas yang ditentukan berdasarkan kondisi internal dan kritikalitas bisnis perusahaan, serta kondisi program pemerintahan yang membutuhkan alokasi sumber daya pada prioritisasi tersebut.
- Melaksanakan program strategi BCP
  Pelaksanaan program pada tahap ini berupa program evaluasi, prioritisasi kebutuhan, dan pelaksanaan.
- Melakukan pengukuran efektifitas BCP
  Pengukuran efektifitas dapat memberikan identifikasi pada beberapa metriks yang digunakan untuk meningkatkan performa kerja perusahaan. Dalam pengukurna efektifitas ini perusahan harus menentukan kunci keberhasilan dari aktifitas mitigasi risiko, menentukan metriks dari aktifitas mitigasi dan program keberlangsungan bisnis pada perusahan.

Alur kerja tersebut juga memiliki sifat iteratif yang berulang dari tahap akhir pada tahap awal. Namun kekurangan dari alur kerja ini adalah bahwa alur kerja ini hanya melakukan identifikasi risiko berdasarkan pada 3 komponen, yaitu pada aset fisik, cyber, dan manusia. Sedangkan komponen aset kritis TI adalah sebanyak 5 komponen sistem informasi diantaranya adalah manusia, perangkat keras (*hardware),* perangkat lunak *(software)*, data, serta jaringan.

4.3.3 Metode Analisis Risiko Teknologi Informasi

Analisis risiko teknologi informasi yang dilakukan adalah berupa proses identifikasi risiko dan proses penilaian risiko. Telah dijelaskan pada bagian 4.1.2 mengenai alur kerja penerapan BCP pada DOE bahwa dalam alur kerja tersebut melakukan identifikasi aset hanya berdasarkan pada 3 komponen saja, serta pada tahap penilaian risiko yang berdasarkan pada konsekuensi, ancaman terhadap aset, dan kerentanan yang dimiliki oleh aset. Oleh karena PT PLN (Persero) APD Jateng dan DIY menginginkan acuan standar dan metode yang dapat diterapkan oleh perusahaan, maka pada identifikasi aset kritis teknologi informasi dan penilaian risiko akan menggunakan metode dan standar yang lebih adaptif atau mudah digunakan oleh PT PLN (Persero) serta sesuai dengan acuan standar.

4.3.3.1 Metode untuk Identifikasi Risiko

Bagian ini akan menjelaskan metode yang dilakukan untuk identifikasi aset kritis dan risiko TI perusahaan. Berikut merupakan penjelasannya:

Identifikasi Risiko

Metode identifikasi risiko akan menggunakan metode kerangka kerja OCTAVE (*Operationally Critical Threat, Assets and Vulnerability*) sebagai pendekatan untuk penilaian kebutuhan keamanan informasi perusahaan.

Tahap pada OCTAVE adalah sebagai berikut:

1. Menentukan aset berdasarkan profil ancaman
   - Mengidentifikasi pengetahuan manajer PT PLN (Persero) APD Jateng dan DIY mengenai kebutuhan keamanan teknologi informasi.
   - Mengidentifikasi pengetahuan asistant manajer SCADA dan Telekomunikasi PT PLN (Persero) APD Jateng dan DIY mengenai kebutuhan keamanan teknologi informasi.

- Mengidentifikasi pengetahuan staff, terutama staff SCADA dan Telekomunikasi PT PLN (Persero) APD Jateng dan DIY mengenai kebutuhan keamanan teknologi informasi.
- Membuat profil ancaman yaitu dengan menentukan aset kritisTI yang terdapat pada PT PLN (Persero) APD Jateng dan DIY.

Output dari tahap 1 ini adalah berupa daftar identifikasi aset kritis TI yang digunakan oleh setiap proses bisnis.Mengidentifikasi kerentanan Infrastruktur

- Mengidentifikasi komponen pada tiap infrastruktur yang digunakan oleh operasional proses bisnis pada PT PLN (Persero) APD Jateng dan DIY.
- Melakukan evaluasi terhadap komponen terpilih agar dapat mengetahui kerentanan teknologi pada komponen infrastruktur yang telah diidentifikasi. Pada proses identifikasi kerentanan ini juga menggunakan ISO 27002 yang akan didaftar ketentuan rekomendasi kontrol berdasarkan standar ISO 27002 lalu diberikan pada staff SCADA dan telekomunikasi yang nantinya akan di*checklist* bagian- bagain yang sudah dijalani sehingga dapat mengetahui *gap* antara standar acuan yang seharusnya dengan keadaan nyata yang dilakukan oleh perusahaan. *Gap* pada kondisi yang tidak dilakukan oleh perusahaan maka akan diidentifikasi menjadi kerentanan aset TI perusahaan.

Output dari tahap2 ini adalah berupa daftar identifikasi kerentanan aset TI.

2. Mengembangkan strategi dan rencana keamanan
   - Mengidentifikasi dampak dari ancaman kerentanan aset kritis TI yang telah diidentifikasi pada tahap 2 dengan membuat kriteria evaluasi untuk penilaian risiko. Penilaian risiko aset kritis TI akan menggunakan penilaian FMEA yang dinilai

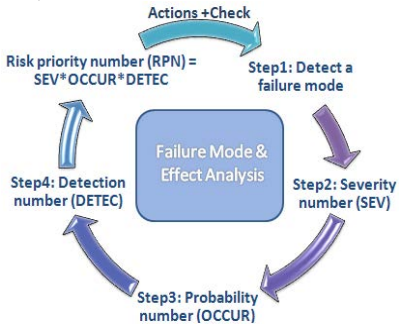
berdasarkan pada dampak (*severity*), nilai probabilitas atau frekuensi kejadian (*occurence*), sertanilai deteksi terhadap risiko (d*etection*) nilai deteksi dapat diperoleh berdasarkan kesiapan perusahaan terhadap penanganan dan penanggulangan risiko aset kritis TI yang telah diidentifikasi pada tahap 2.

Output dari tahap 3 adalah berupa hasil klasifikasi terhadap kritikalitas risiko aset kritis TI. Penilaian kritikalitas risko TI akan menggunakan metode FMEA yang akan dijelaskan pada bagian selanjutnya. Dalam tahap ini seharusnya masih terdapat proses untuk strategi keamanan informasi, namun proses ini tidak akan digunakan sesuai dengan ketentuan metode OCTAVE, melainkan dengan ISO 22301 karena strategi yang dikaji dalam penelitian ini adalah strategi untuk keberlangsungan bisnis.

Metode Penilaian Risiko FMEA

Penilaian FMEA yang dilakukan untuk mengidentifikasi terhadap 3 aspek, yaitu dari aspek dampak, frekuensi kejadian, serta deteksi terhadap kejadian bencana/ gangguan.

Berikut merupakan dari metode *Failure Mode Effect Analysis* (FMEA):



Gambar 4.3 Metode Penilaian FMEA

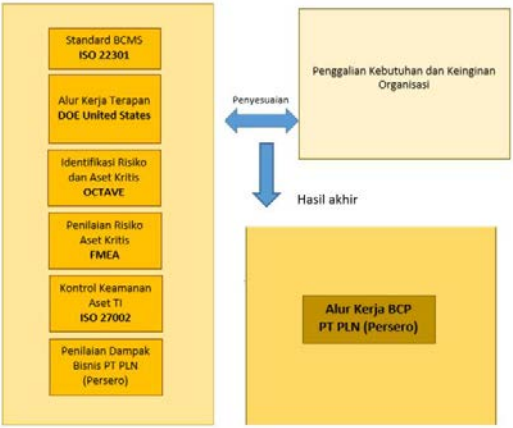
- Tahap 1: Mendeteksi mode kegagalan.
  Pada tahap ini yang dilakukan adalah melakukan identifikasi terhadap kejadian risiko yang potensial yang menimbulkan efek penyebab dari kegagalan.
- Tahap 2: Menentukan angka keparahan yang ditimbulkan dari kegagalan (*severity number).*
  Memberikan peringkat untuk masing- masing penyebab kegagalan sesuai dengan prioritasnya mulai dari angka 1 (*minor)* hingga 10 (terberat).
- Tahap 3: Menentukan angka probabilitas kejadian (*Occurance*).
  Memberikan peringkat masing masing penyebab sesuai dengan probabilitas terjadinya mulai 1 (*none*) sampai 10 (paling sering).
- Tahap 4: Menentukan angka kemungkinan dari kejadian risiko (*Detection*)
  Setelah mengidentidikasi tingkat keparahan dan frekuensi kejadian dari risikom selanjutnya adalah memperkirakan kemungkinan kejadian risiko tersebut datang dan mengancam organisasi. Semakin rendah peringkatnya maka semakin mudahnya risiko tersebut dapat dideteksi.
- Menghitung RPN (*Risk Priority Number)*
  Setelah melakukan identifikasi dengan menggunakan angka dan ranking pada tiap *severity, occurence* dan *detection,* selanjutnya adalah melakukan operasi perhitungan RPN atau angka prioritas dari hasil penilaian risiko. Rumus dan keterangan tingkat penilaian risiko akan diklasifikasikan pada bab ini sub bab Pengolahan Data dan Informasi.

4.3.4 Metode Analisis Dampak Bisnis

Penilaian dampak bisnis menggunakan klasifikasi dampak bisnis yang telah ditetapkan oleh PT PLN (Persero) APD Jateng dan DIY dan tertuang dalam buku . Dalam penyusunan Tugas Akhir ini, dari 5 sudut pandang dampak aspek bisnis hanya akan

menggunakan 2 aspek bisnis, yaitu pada produk dan layanan serta proses bisnis internal perusahan.

Berikut merupakan visualisasi dari perancangan alur kerja BCP berdasarkan beberapa metode yang telah disiapkan:



Gambar 4.4 Visualisasi perancangan Alur Kerja BCP PT PLN (Persero) APD Jateng dan DIY

Setelah memiliki persiapan dalam perancangan alur kerja, maka selanjutnya adalah melakukan penggalian kebutuhan dan keinginan organisasi yang nantinya akan disesuaikan. Selanjutnya berdasarkan kerangka dasar ISO 22301 akan disusun beberapa alur untuk *Plan, Do, Check, dan Act.*

4.4 Wawancara Proses Bisnis

Wawancaraa proses bisnis dilakukan dengan melakukan wawancara dengan setiap fungsi bisnis yang melakukan proses bisnis dalam perusahaan. Wawancara pada aktifitas ini dilakukan dengan tiap manajemen tertinggi tiap fungsi bisnis atau pihak *middle management* pada perusahaan, dimana dalam hal ini adalah Asisten Manajer tiap fungsi bisnis.

Interview protocol dari wawancara proses bisnis ini terlampir pada lampiran A.

4.5 Pengolahan Data dan Informasi

Pengolahan data dan informasi dari tahap ini adalah penilaian resiko TI dan penilaian dampak bisnis serta proses prioritisasi dari ast kritis TI yangtelah dilakukan penilaiannya.

Penilaian Risiko TI

Penilaian risiko TI menggunakan metode penilaian FMEA (*Failure Mode Effect Analysis).* Berikut merupakan rancangan dari kebutuhan tabel yang akan dijadikan sebagai media penilaian risiko TI:

Tabel 4.2 Rancangan Tabel Penilaian Risiko TI

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		

Klasifikasi penilaian risiko untuk penilaian aspek dampak (*severity* atau s) adalah sebagai berikut:

Tabel 4.3 Daftar Nilai untuk Tingkat Keparahan (*Severity*)

Jenis dampak	Keterangan	Nilai
Minor	Kejadian tidak dirasakan dampaknya atau tidak mempengaruhi kinerja.	1
	Menyebabkan gangguan kecil tetapi tidak mempengaruhi kinerja	2

Jenis dampak	Keterangan	Nilai
Low	Menyebabkan gangguan kecil dan mempengaruhi sedikit kinerja	3
	Menyebabkan gangguan kecil dan menyebabkan kerugian kecil pada operasional	4
Moderate	Menyebabkan penurunan kinerja dan kerugian operasional yang masih dapat diatasi	5
	Menyebabkan penurunan kinerja dan kerugian operasional yang masih dapat diatasi, serta menimbulkan keluhan pelanggan	6
High	Mempengaruhi beberapa proses bisnis dan menimbulkan keluhan pelanggan	7
	Mempengaruhi seluruh proses bisnis dan menimbulkan keluhan pelanggan	8
Very High	Menghentikan proses bisnis.	9
	Menghentikan proses bisnis dan mempengaruhi sistem keamanan.	10

Berikut adalah tabel klasfikasi untuk penilaian pada aspek penilaian probabilitas kejadian atau *occurence* (o). Penilaian ini dilakukan dengan meilihat log dari history gangguan yang telah terdokumentasi dari perusahaan.

Tabel 4.4 Daftar Penilaian Tingkat Frekuensi Kejadian (*Occurance*)

Jenis Kejadian	Keterangan	Nilai
Minor	Tidak pernah, atau satu kali dalam kurun waktu 10 tahun	1
	Satu kali dalam kurun waktu 5 tahun	2
Low	Satu kali dalam kurun waktu 12 bulan	3
	Satu kali dalam kurun waktu 8 bulan	4
Moderate	Satu kali dalam kurun waktu 5 bulan	5
	Satu kali dalam kurun waktu 3 bulan	6
High	Satu kali dalam kurun waktu 1 bulan	7
	Satu kali dalam kurun waktu 2 minggu	8
Very High	Satu kali dalam kurun waktu 3 hari	9
	Terjadi setiap hari	10

Penilaian risiko pada aspek deteksi atau *detection* (d) dilakukan dengan melakukan gap antara kondisi ideal pada ISO 27002 terhadap kondisi eksisting yang dilaksanakan oleh PT PLN (Persero) APD Jateng dan DIY. Berikut merupakan tabel penilaian untuk aspek deteksi:

Tabel 4.5 Daftar Penilaian Tingkat Deteksi Kejadian (*Detection*)

Jenis Deteksi	Keterangan	Nilai
Minor	Tidak adanya deteksi dari organisasi terhadap ancaman risiko	10

Jenis Deteksi	Keterangan	Nilai
	Terdapat metode deteksi (berupa alat atau alarm) namun tidak terdapat deteksi waktu dan perencanaan atau prosedur tertulis secara jelas	9
Low	Terdapat metode deteksi) terhadap ancaman risiko dan tidak terdapat prosedur tertulis dan tidak ada rencana pengecekan atau pengujian secara berkala	8
	Terdapat metode deteksi terhadap ancaman risiko dan terdapat prosedur tertulis namun tidak terlaksana rencana pengecekan atau pengujian secara berkala	7
Moderate	Terdapat metode deteksi terhadap ancaman risiko dan tidak terdapat prosedur tertulis namun terlaksana rencana pengecekan atau pengujian secara berkala	6
	Terdapat metode deteksi terhadap ancaman risiko dan terdapat prosedur tertulis serta terlaksana rencana pengecekan atau pengujian secara berkala	5
High	Metode deteksi memiliki kemungkinan cukup tinggi dalam mendeteksi kegagalan pada 41%-50% kejadian dan terlaksana rencana pengecekan atau pengujian secara rutin	4
	Metode deteksi memiliki kemungkinan cukup tinggi dalam mendeteksi kegagalan 31% - 40% kejadian dan terlaksana rencana	3

Jenis Deteksi	Keterangan	Nilai
	pengecekan atau pengujian secara rutin	
Very High	Metode deteksi sangat efektif dalam mendeteksi 21% - 30% kejadian dan terlaksana rencana pengecekan atau pengujian secara rutin	2
	Metode deteksi sangat efektif dalam mendeteksi <20% kejadian dan terlaksana rencana pengecekan atau pengujian secara rutin	1

Setelah melakukan identifikasi dengan menggunakan angka dan ranking pada tiap *severity, occurence* dan *detection,* selanjutnya adalah melakukan operasi perhitungan RPN dengan rumus sebagai berikut :

$$\mathbf{RPN = S \times O \times D}$$

Keterangan :

S : ***Severity Number* (Angka Tingkat Keparahan)**
O : ***Occurrence Number* (Angka Tingkat Probabilitas Kejadian)**
D : ***Detection Number* (Angka Tingkat Deteksi)**

Level dari risiko dapat diketahui dari hasil dari perhitungan RPN pada tabel di bawah ini:

Tabel 4.6 Klasifikasi Hasil Penilaian Berdasarkan *Risk Priority Number*

RPN	Level Resiko
200>	*Very High*
151-200	*High*
101-150	*Medium*
51-100	*Low*
0-50	*Very Low*

Hasil penilaian risiko diurutkan dan ditunjukkan berdasarkan level kritikalitas risiko. Tujuannya adalah untuk memudahkan dalam klasifikasi dalam pembacaan level risiko.

Tabel 4.7 Tabel Hasil Klasifikasi Risiko

Nomor Identif-ikasi Risiko	Aset TI	Penyebab Kega-galan	Klasifikasi Risiko
			High
			Medium
			Low

Metode Analisis Dampak Bisnis

Penilaian dampak bisnis menggunakan klasifikasi dampak bisnis yang telah ditetapkan oleh PT PLN (Persero) APD Jateng dan DIY dan tertuang dalam buku Prosedur Penyusunan Profil dan Kajian Risiko PT PLN (Persero) APD Jateng dan DIY. Dalam penyusunan Tugas Akhir ini, dari 5 sudut pandang dampak aspek bisnis hanya akan menggunakan 2 aspek bisnis, yaitu pada produk dan layanan serta proses bisnis internal perusahan. Berikut merupakan klasifikasi tinglat penilaian terhadap aspek dampak bisnis produk dan layanan:

Tabel 4.8 Penilaian Dampak Berdasarkan Aspek Produk dan Layanan

Tingkat Dampak	Keterangan	Nilai
Tidak Signifikan	Mengakibatkan pemadaman sesaat selama <15 menit pada satu waktu	1
Minor	Mengakibatkan pemadaman sesaat selama 15 menit – 1 jam pada satu waktu	2
Medium	Mengakibatkan pemadaman selama 1 – 3 jam pada satu waktu	3

Tingkat Dampak	Keterangan	Nilai
Signifikan	Mengakibatkan pemadaman selama 3 jam – 1 hari pada satu waktu	4
Malapetaka	Mengakibatkan pemadaman selama lebih dari 1 hari dan/ atau Mengakibatkan pemadaman bergilir pada watu waktu (*blackout system)*	5

Berikut merupakan klasifikasi penilaian untuk klasifikasi dampak bisnis pada aspek proses bisnis internal:

Tabel 4.9 Penilaian Dampak Berdasarkan Aspek Proses Bisnis Internal

Tingkat Dampak	Keterangan	Nilai
Tidak Signifikan	Kegiatan proses bisnis perusahaan tidak terganggu	1
Minor	Mengakibatkan kegiatan proses bisnis perusahaan terganggu secara terbatas dalam 1 unit dan tidak mempengaruhi pelayanan	2
Medium	Mengakibatkan kegiatan proses bisnis perusahaan terganggu secara terbatas dalam 1 unit dan mempengaruhi pelayanan	3
Signifikan	Mengakibatkan kegiatan proses bisnis perusahaan terganggu secara terbatas dalam beberapa unit	4
Malapetaka	Mengakibatkan kegiatan proses bisnis perusahaan terganggu secara terbatas dalam secara luas	5

Setelah penilaian risiko TI dan dampak bisnis dilakukan, selanjutnya perlu dilakukan prioritisasi aset kritis TI. Prioritisasi TI dilakukan dengan tujuan untuk mengetahui kebutuhan prioritas risiko yang harus didahulukan oleh perusahaan dalam penanggulangan risiko. Berikut tabel 4.9 merupakan rancangan dari metode pelaksanaan prioritisasi dimana pada rancangan berikut merupakan hasil dari perpotongan antara level risiko TI dan level kritikalitas dampak bisnis:

Tabel 4.10 Tabel Matriks Level Risiko TI dan Dampak Bisnis

Risiko TI / Dampak Bisnis	*Very High dan High*	*Medium*	*Low* dan *Very Low*
High			
Medium			
Low			

4.6 Penyusunan Rekomendasi Aksi BCP

Hasil yang diharapkan dari proses ini adalah hasil dari strategi keberlangsungan bisnis, modul pelatihan dan pengujian, audit pelaksanaan BCP, serta peninjauan manajemen untuk peningkatan BCP.

4.6.1 Perancangan untuk Strategi Keberlangsungan Bisnis

Strategi keberlangsungan bisnis yang dibuat berdasarkan pada rekomendasi ISO 27002 dan penerapan pada implementasi pada DOE United States. Strategi BCP yang dilakukan akan berdasarkan pada beberapa strategi berikut ini:

Tabel 4.11 Tabel Rancangan Kebutuhan Strategi BCP

Jenis Strategi	Keterangan
Strategi Preventif	Jenis strategi yang dilakukan untuk mengurangi risiko dan/ atau dampak yang ditimbulkan dari gangguan. Strategi preventif dilakukan agar perusahaan memiliki persiapan dalam rangka menghadapi gangguan yang akan terjadi.
Strategi DRP	Jenis strategi DRP merupakan strategi berupa tindakan yang dilakukan pada saat itu juga untuk memulihkan kejadian gangguan. Strategi DRP ini dilaksanakan oleh tim DRP yang merupakan staff SCADA dan Telekomunikasi PT PLN (Persero) APD Jateng dan DIY.
Strategi Detektif	Strategi detektif merupakan aktifitas yang dapat dilakukan untuk megidentifikasikan adanya kejadian bencana atau gangguan. Pelaksanaan kontrol detektif harus diletakkan pada daerah aset untuk mengidentifikasikan gangguan/ bencana.

Jenis Strategi	Keterangan
Strategi Korektif	Strategi korektif dilakukan saat organisasi melihat adanya ketidak sesuaian dari pelaksanaan BCP sehingga strategi korektif berguna bagi perusahaan untuk melakukan perbaikan kinerja dari perencanaan BCP.

4.6.2 Perancangan untuk Penyusunan Daftar Prosedur

Setelah dibuat daftar strategi yang dilakukan, maka berikutnya akan didaftarkan kebutuhan prosedur yang dihasilkan dari strategi yang tekah direncanakan. Dikarenakan keterbatasan ruang lingkup yang telah ditentukan pada Bab I buku Tugas Akhir ini, maka yang dapat dilakukan oleh penyusun tugas akhir ini hanya terbatas pada pemberian daftar prosedur yang dibutuhkan berdasarkan pada strategi yang telah disusun pada bagian proses strategi BCP. Dalam daftar prosedur ini, diperlukan keterangan yang menjelaskan referensi risiko dan kebutuhan standar yang dibutuhkan sebagai contoh atau rekomendasi pelaksanaan penagnggulangan risiko. Berikut merupakan rancangan tabel dari kebutuhan daftar prosedur:

Tabel 4.12 Rancangan Tabel dari Kebutuhan Daftar Prosedur

No	Kebutuhan Prosedur	ID. Strategi	Risiko yang Di-tangani	Acuan yang digunakan	
				ISO 27002:2005	Penerapan Department of Energy

4.6.3 Kebutuhan untuk Pelatihan dan Pengujian

Setelah daftar prosedur dan strategi disusun, maka selanjutnya perlu bentuk rekomendasi untuk pelaksanaan dan pengujian yang dibutuhkan oleh perusahaan. Proses penyusunan kebutuhan untuk pelatihan dan pengujian

berdasarkan pada hasil strategi dan prosedur BCP yang telah ditetapkan. Pada tiap daftar strategi dan prosedur tersebut, hal yang harus dilakukan adalah melakukan peninjauan ulang terhadap daftar- daftar yang membutuhkan pelatihan dan pengujian untuk pelaksanaan keberlangsungan bisnis perusahaan. Selain daftar kebutuhan pengujian dari daftar strategi dan prosedur, kebutuhan lain yang harus disiapkan dalam rangka penyusunan pelatihan dan pengujian BCP adalah menyiapkan daftar pemegang peran pelaksanaan pengujian dan pelatihan, waktu pelaksanaan, lokasi pelaksanaan, serta tahap pelaksanaan untuk pengujian dan pelatihan yang dibutuhkan.

Pelatihan dan pengujian terbagi menjadi pelatihan dan pengujian terhadap ketentuan alur komunikasi BCP pada dokumen ini serta pelatihan dan pengujian terhadap strategi keberlangsungan bisnis yang telah dibuat. Tujuan dari pelatihan adalah untuk memastikan bahwa pihak organisasi memahami strategi yang dibuat, sedangkan tujuan dari pengujian adalah untuk memastikan bahwa strategi yang dibuat telah sesuai dengan kebutuhan perusahan.

Tabel 4.13 Tabel Kerangka untuk Modul Pelatihan BCP

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PELATIHAN KEBERLANJU-TAN BISNIS**
Nama Pelatihan	
Jenis Pelatihan	
Deskripsi Pelatihan	
Sasaran Pelatihan	
Materi Umum	

Dalam pelatihan ini akan diberikan materi yaitu sebagai berikut :

Berikut merupakan kerangka dari pembuatan untuk modul pengujian keberlangsungan bisnis.

Tabel 4.14 Tabel Kerangka untuk Modul Pengujian BCP

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PENGUJIAN KEBERLANJUTAN BISNIS**	
Pengujian		
Pelaku dan pembagian peran	1.	
	2.	
	3.	
Skenario pengujian		

4.6.4 Audit Pelaksanaan BCP

Audit pelaksanaan BCP dilakukan untuk memeriksa efektitifitas dari implementasi BCP yang telah dibuat. Penilaian akan dilakukan dengan melakukan penilaian terhadap kesesuaian BCP yang dilaksanakan oleh perusahaan. Namun dikarenakan keterbatasan waktu dan batasan masalah, pada peelitian tugas akhir ini tidak sampai pada proses *assesment* pada *checklist* audit. Penelitian tugas akhir pada bagian ini

hanya akan sampai pada pembuatan checklist pada kebutuhan audit pelaksanaan BCP.

Proses ini membutuhkan hasil dari prosedur BCP dan formulir atau *checklist* untuk pelaksanaan audit. Bermula dari kolom tujuan yang mengacu pada tujuan pelaksanaan BCP, diikuti dengan pernyataan yang sesuai dengan proses atau aktifitas dalam BCP, yang diisi dengan pernyataan Ya, Tidak atau Parsial. Pernyataan 'Ya' digunakan untuk pelaksanaan pada pernyataan BCP yang dilakukan oleh perusahaan, pernyataan 'Tidak' diisikan pada pernyataan pelaksanaan aktifitas BCP yang tidak dilaksanakan oleh perusahaan, sedangkan pada pernyataan 'Parsial' diberikan pada pernyataan yang telah melakukan sebagian dari aktifitas pelaksanaan BCP dengan menyertakan bukti atau berkas pelaksanaan pada prosedur yang telah disusun.

Tabel 4.15 Rancangan Tabel Kebutuhan Audit Pelaksanaan BCP

Tujuan	Pernyataan	Ya	Tidak	Parsial	Bukti

4.6.5 Peninjauan Pihak Manajemen

Proses perancangan untuk peninjauan pihak manajemen dilakukan dengan menjelaskan cakupan yang akan digunakan dalam peninjauan pihak manajemen. Cakupan tersebut terdiri dari hasil audit dan kebutuhan perubahan terbaru dari perusahaan seperti kebijaka terbaru, prosedur terbaru, layanan dan aset TI terbaru, dan lain- lain.

4.6.6 Peningkatan Secara Terus- Menerus

Pada proses ini perlu dilakukan rekomendasi untuk perusahaan ntuk melakukan proses peningkatan terhadap pelaksanaan BCP pada perusahaan. Pada proses ini akan diberikan rekomendasi

untuk peningkatan berdasarkan pada dua sisi kebutuhan, yaitu kebutuhan dari sisi internal dan kebutuhan dari sisi eksternal.

Tabel 4.16 Kebutuhan Peningkatan secara terus menerus

Sisi Internal	Sisi internal merupakan cakupan yang masih terdapat pada alur kerja BCP PT PLN (Persero) APD Jateng dan DIY yang dilaksanakan pada fase pemeriksanaan (*Check*).
Sisi Eksternal	Sisi eksternal yang merupakan bagian diluar cakupan alur kerja BCP PT PLN (Persero) APD Jateng dan DIY.

4.7 Validasi BCP

Dalam rangka memastikan kesesuaian alur kerja BCP dan kebenaran analisis maka diperlukan aktifitas verifikasi dan validasi terhadap tiap hasil dari proses alur kerja BCP yang telah dibuat. Proses verifikasi dan validasi penyusunan alur dan dokumentasi BCP akan dilakukan pada tiap proses berikut ini:

- Kesesuaian alur kerja BCP
- Kebenaran dan kesesuaian penilaian risiko
- Kebenaran dan kesesuaian analisa dampak bisnis
- Kebenaran dan kesesuaian strategi dan prosedur BCP

Selain proses verifikasi kebenaran mengenai alur kerja dan analisis hasill data untuk dokumentasi BCP, diperlukan pula aktifitas pelatihan dan pengujian terhadap BCP yang telah dibuat. Pelatihan dan pengujian tersebut dilakukan untuk memastikan bahwa proses dokumentasi BCP yang telah dilakukan telah sesuai dengan kebutuhan keamanan aset TI PT PLN (Persero) APD Jateng dan DIY.

Halaman ini sengaja dikosongkan

2. Proses Bisnis Perusahaan

Identifikasi Proses Bisnis

Pada kuesioner ini akan dilakukan identifikasi terhadap proses bisnis atau aktifitas yang terdapat pada fungsi/ bagian Anda.

Dalam hal ini, Proses bisnis merupakan suatu kumpulan **aktifitas** yang saling terkait **yang dilakukan oleh tiap fungsi bisnis** dalam suatu perusahaan dalam menyelesaikan atau menghasilkan produk atau layanan dalam perusahaan.

Proses Bisnis :	Penjelasan singkat & jelas mengenai alur proses bisnis :
1.	1.
2.	2.
3.	3.

3. Potensi Kerugian Terganggunya Proses Bisnis

Identifikasi Potensi Kerugian

Pada kuesioner ini akan dilakukan penilaian tingkat kerugian perusahaan akibat bencana yang dapat menghentikan proses bisnis atau aktifitas bisnis pada fungsi/ bagian Anda, dimulai dari saat terjadi bencana sampai dengan penanganan bencana. Asumsi yang digunakan adalah bencana yang terjadi menyebabkan proses bisnis pada fungsi/ bagian Anda berhenti beroperasi.

Tujuan

Untuk mengidentifikasi tingkat kerugian dari dampak pada fungsi/ bagian/ proses bisnis yang terjadi gangguan.

Cara Pengisian

1. Isilah Nama proses bisnis pada baris 'Proses Bisnis', sesuai proses bisnis yang telah diisi di bagian **2. Proses Bisnis Perusahaan**
2. Isilah dengan angka 1 atau 2 atau 3 atau 4 atau 5 yang sesuai antara pernyataan di kolom kriteria dan kolom Durasi berhentinya proses bisnis

A-4

Contoh Pengisian :

Kategori Risiko	Kriteria	Durasi proses bisnis berhenti beroperasi setelah terjadi bencana					
		< 1 Jam	4 Jam	1 Hari	7 Hari	1 Bu-lan	> 1 Bu-lan
Proses Bisnis 1 : Monitoring SCADA							
Produk dan Layanan	1. Tidak memiliki dampak terhadap produk/ layanan atau mengakibatkan pemadaman selama **kurang dari 15 menit** 2. Mengakibatkan pemadaman selama **15 menit – 1 jam** pada satu waktu 3. Mengakibatkan pemadaman selama **1- 3 jam** pada satu waktu 4. Mengakibatkan pemadaman selama **3 – 24 jam** pada satu waktu 5. Mengakibatkan pemadaman selama **lebih dari 1 hari** atau mengakibatkan pemadaman bergilir pada satu waktu/ *blackout* sistem	1	2	3	3	4	4

Kategori Risiko	Kriteria	Durasi proses bisnis berhenti beroperasi setelah terjadi bencana					
		< 1 Jam	4 Jam	1 Hari	7 Hari	1 Bu-lan	> 1 Bu-lan
Proses Bisnis : _____							
Produk dan Layanan	1. Tidak memiliki dampak terhadap produk/ layanan atau mengakibatkan pemadaman selama **kurang dari 15 menit** 2. Mengakibatkan pemadaman selama **15 menit – 1 jam** pada satu waktu 3. Mengakibatkan pemadaman selama **1- 3 jam** pada satu waktu 4. Mengakibatkan pemadaman selama **3 – 24 jam** pada satu waktu 5. Mengakibatkan pemadaman selama **lebih dari 1 hari** atau mengakibatkan pemadaman bergilir pada satu waktu/ *blackout* sistem						
Proses Bisnis In-ternal	1. Kegiatan perusahaan tidak terganggu						

	2. Kegiatan perusahaan **terganggu secara terbatas dalam 1 unit** dan **tidak mempengaruhi pelayanan** 3. Kegiatan perusahaan **terganggu secara terbatas dalam 1 unit** dan **mempengaruhi pelayanan** 4. Kegiatan perusahaan **terganggu secara terbatas di beberapa unit** 5. Kegiatan perusahaan terganggu secara luas						

4. Penggunaan Sistem dan Layanan TI

Tujuan

Untuk mengetahui sistem dan layanan TI yang digunakan dalam aktifitas bisnis yang dilakukan oleh fungsi bisnis serta mendefinisikan risiko sistem dan layanan TI yang digunakan oleh fungsi bisnis serta kritikalitas kebutuhan sistem/ layanan bagi aktifitas bisnis.

Cara Pengisian

1. Isikan sistem dan layanan TI yang digunakan dalam aktifitas bisnis dalam kolom Aplikasi Sistem dan Layanan IT
2. Beri tanda check (√) pada bagian yang dirasa benar sesuai dengan kebutuhan pada sistem layanan TI yang dibutuhkan pada aktifitas proses bisnis tersebut.
3. Isikan kolom tingkat keparahan yang ditimbulkan terhadap proses bisnis apabila layanan tersebut mati. Tingkat keparahan dikelompokkan sebagai berikut :

Jenis Dampak	Keterangan	Nilai
Minor	Tidak mempengaruhi performasi	1-2
Low	Mempengaruhi performasi sedikit	3-4
Moderate	Pada level ini, pelanggan juga merasakan dampak dan ketidaknya-manan yang disebabkan.	5-6

High	Menghentikan proses bisnis	7-8
Very High	Menghentikan proses bisnis dan mempengaruhi sistem keamanan	9-10

4. Contoh pengisian: Pada proses bisnis monitoring SCADA membutuhkan aplikasi SKADA dan apabila aplikasi SCADA mati maka akan menimbulkan akibat yang mempengaruhi berjalannya proses bisnis yaitu proses bisnis terhenti. Sehingga dalam hal ini aplikasi SCADA memiliki jenis dampak *High*. Berikut contoh pengisiannya :

Aplikasi Sistem dan Layanan IT	**Tingkat Keparahan**					**Tingkat Keparahan**				
	Mi-nor	Low	Moder-ate	High	Very High	Mi-nor	Low	Moder-ate	High	Very High
	Proses Bisnis 1 : Monitoring SCADA					Proses Bisnis 2 :				
Sistem SCADA										

LAMPIRAN B
Transkrip Hasil Wawancara dengan Asisten Manager SCADA dan Telekomunikasi

E. Data Narasumber

Nama : Angga Rajasa
Jabatan : Asisten Manajer
Fungsi : SCADA dan Telekomunikasi
Waktu : Rabu, 27 April 2016
Lokasi : Kantor PLN APD Jateng dan DIY (Semarang)

F. Keadaan Terkini Manajemen Risiko PT PLN (Persero) APD Jateng dan DIY

6. PT PLN (Persero) sudah memiliki buku prosedur untuk penyusunan profil risiko dan kajian risiko perusahaan, apakah PT PLN (Persero) APD Jateng sudah melaksanakan prosedur untuk mendaftar risiko dan melakukan kajian risiko tingkat perusahan?

   Keterangan narasumber:
   PLN pusat memang sudah memiliki buku prosedur untuk penyusunan profil risiko dan kajian risiko perusahaan yang sekarang ini sudah dilakukan oleh tiap fungsi bisnis untuk menilai level atau kritikalitas risiko proses bisnis dan setiap bulan selalu di review mengenai ketercapaian tiap penanganan proses bisnis yang bersangkutan oleh setiap asisten manager dan manager APD.

7. Seperti apakah bentuk dari alur komunikasi yang telah dilakukan oleh perusahaan dalam penanganan gangguan terhadap layanan TI?

   Keterangan narasumber:
   Media komunikasi utama yang digunakan saat mengalami gangguan adalah HT. Baik gangguan jaringan distribusi atau gangguan lainnya media

komunikasi tercepat adalah HT. Selain itu PLN APD juga menggunakan SpeedJarDist untuk pelaporan gangguan secara spesifik seperti misalnya gangguan SCADA ataupun pada HT itu sendiri.
Apabila terdapat gangguan dari layanan TI maka fungsi bisnis yang bersangkutan melaporkan pada tim TI dan Telekomunikasi atau melalui Asistem Manager SCADA dan Telekomunikasi, lalu AsMan SCADA dan Telekomunikasi yang telah menerima laporan gangguan layanan TI memberikan instruksi pada tim TI dan Telekomunikasi tergantung dari fokus gangguan apakah dari SCADA dan Data atau pada Aplikasi dan bagain telekomunikasi. Karena apabila bagian yang bersangkutan adalah gangguan SCADA dan Data maka yang memiliki tuas dalam pelaksanaan perbaikan adalah tim TI, dan apabila yang terkena gangguan adalah layanan aplikasi dan telekomunikasi maka yang bersangkutan adalah bagian telekomunikasi. Apabila gangguan telah berhasil ditangani maka Asisten Manajer SCADA dan Telekomunikasi wajib memberikan laporan pada Manager APD bahwa telah terjadi gangguan dan gangguan tersbut telah ditangani dengan deskripsi umum langkah yang telah dilakukan. Apabila tidak dapat dilakukan dalam waktu singkat maka tim melakukan tindakan sekunder dalam menyelamatkan aktivitas bisnis seperti misal apabila listrik mati maka perlu menyalakan UPS, dan lain- lain sesuai dengan insruksi asisten manajer SCADA dan Telekomunikasi terkait gangguan.

8. Apakah terdapat dokumentasi atau pencatatan terhadap log gangguan pada layanan TI?

   Keterangan narasumber:
   Sejauh ini masih belum ada pencatanan khusus atau baku hanya untuk gangguan TI, namun untuk log gangguan SCADA dan server dapat secara otomatis

terekam dan teridentifikasi oleh sistem SCADA dan sever. Sedangkan untuk aplikasi lain lognya dapat dilihat dalam pelaporan pada SpeedJarDist.

9. Apakah terdapat beberapa gangguan TI yang berkaitan langsung dengan aplikasi tertentu yang bukan menjadi tanggung jawab secara langsung dari tim TI?

   Keterangan narasumber:
   Ya, beberapa diantaranya yaitu pada saluran komunikasi yaitu telepon, HT, internet, dan fiber optic menjadi tanggung jawab pihak Telkom yang telah bekerja sama dengan PLN. Apabila terdapat gangguan terkait kesalahan pada jaringan telepon, internet tidak tersambung maka tim TI dan Telekomunikasi hanya dapat menerima dan meneruskan pesan gangguan pada pihak PT Telkom. Selain itu juga pada peralatan Gardu Induk yang terpasang dan terkoneksi secara real time pada SCADA merupakan tanggung jawab dari fungsi bisnis GI, bukan SCADA dan Telekomunikasi. Sehingga sebaiknya studi kasus yang dilakukan pada penelitian Anda lebih spesifik pada TI saja sehingga tidak membingungkan dalam penafsiran tim TI dan Telekomunikasi.

10. Dalam buku prosedur untuk penyusunan profil risiko dan kajian risiko PT PLN (Persero) sudah mendefinisikan risiko- risiko yang mengancam perusahaan, hanya saja belum secara spesifik mendefinisikan risiko Teknologi Informasi.
    Misalnya pada point O.9.1 Bencana Lokal, apakah dapat ditambahkan dengan profil risiko O.9.4 Risiko Bencana Tingkat Perusahaan dengan lebih dispesifikkan lagi dengan O.9.4.1 Kebakaran tingkat perusahaan, O.9.1.2 Kebakaran Server, O.9.1.3 Listrik Mati, dan lain sebagainya sesuai dengan standar acuan

teknologi informasi yang akan disesuaikan dengan PT PLN dengan pertimbangan dari pihak Manager APD?

Keterangan narasumber:
Sebaiknya didefinisikan dalam daftar risiko yang terpisah saja sehingga dapat dibedakan dimana yang merupakan risiko TI dengan risiko tingkat bisnis yang berkaitan langsung dengan perusahaan dan juga harapannya nanti dapat digunakan sebagai rekomendasi untuk mengetahui bahwa terdapat risiko- risiko TI yang belum kami perhatikan atau sadari.

G. Identifikasi Risiko Keamanan Teknologi Informasi

6. Siapa sajakah yang berkaitan langsung terhadap layanan TI yang terdapat di PLN APD Jateng dan DIY?

   Keterangan narasumber:
   Pihak yang berkaitan langsung dengan layanan TI PLN APD Jateng dan DIY adalah dari tim SCADA dan Telekomunikasi, tim dari fungsi bisnis selain SCADA dan Telekomunikasi, serta administrator dari layanan baik dari internal maupun dari pihak eksternal seperti PLN Distribusi.

7. Apa saja perangkat lunak atau aplikasi yang diidentifikasikan sebagai aset TI kritis pada PLN APD Jateng dan DIY?

   Keterangan narasumber:
   Software atau aplikasi yang digunakan di PLN APD Jateng diantaranya yaitu sistem SCADA, AMS atau Aplikasi Manajemen Surat atau Email PLN, SAP yang digunakan pada beberapa fungsi bisnis tertentu, Web Jaringan Distribusi, SpeedJarDist untuk pelaporan gangguan pada SCADA khususnya.

8. Apa saja perangkat keras yang diidentifikasikan sebagai aset TI kritis pada PLN APD Jateng dan DIY?

   Keterangan narasumber:
   Software atau aplikasi yang digunakan di PLN APD Jateng diantaranya yaitu sistem SCADA, AMS atau Aplikasi Manajemen Surat atau Email PLN, SAP yang digunakan pada beberapa fungsi bisnis tertentu, Web Jaringan Distribusi, SpeedJarDist untuk pelaporan gangguan pada SCADA khususnya.

9. Apa saja komponen jaringan yang diidentifikasikan sebagai aset TI kritis pada PLN APD Jateng dan DIY?

   Keterangan narasumber:
   Jika yang dimaksud adalah jaringan internet maka komponennya antara lain *switch*, *router*, jaringan LAN, Access Point, Fiber Optic, dan Jaringan WAN.

10. Apa saja identifikasi dan deskripsi spesifik dari data yang diidentifikasikan sebagai aset TI kritis pada PLN APD Jateng dan DIY?

    Keterangan narasumber:
    Data yang dimiliki oleh PLN APD antara lain data tegangan dimana terdapat data tegangan trafo, data tegangan jaringan, lalu data beban yang diantaranya terdapat data beban penyulang serta data beban trafo. Lalu data frekuensi, data pelanggan (menjadi tanggung jawab pihak PLN Distribusi), data war factor, data gangguan GI, data aset proteksi, data cubical, data cable, data administrasi milik fungsi adkeu yang diantaranya adalah data evaluasi jam kerja, data evaluasi struktur, serta data penilaian pekerja atau talent karyawan.

H. <u>Penggalian Kebutuhan Keamanan Aset TI Kritis</u>

2. Apakah PT PLN (Persero) APD Jateng sudah memiliki bentuk langkah antisipasi manajemen risiko khusus untuk Teknologi Informasi perusahaan?
   Jika jawaban **Ya,** apakah langkah manajemen risiko sudah didokumentasikan dalam bentuk dokumen manajemen risiko? Sejauh apa bentuk dokumentasi manajemen risiko tersebut?

   Keterangan narasumber:

   PLN sudah memiliki langkah antisipasi manajemen risiko TI yang dilaksanakan oleh tim SCADA dan Telekomunikasi, khususnya tim di bagian TI dan Telekomunikasi dengan pengawasan langsung yang dilakukan oleh asisten manajer fungsi SCADA dan telekomunikasi. Manager APD juga berperan dalam menerima review dan laporan dari asisten manajer SCADA dan Telekomunikasi mengenai tindakan dan penanganan gangguan layanan TI yang telah dilakukan oleh tim.

   Sebagian besar dari tindakan antisipasi terhadap risiko TI masih belum sesuai standar ISO yang dapat diterapkan untuk TI di PLN karena kami belum mengetahui secara spesifik kebutuhan khusus dari manajemen keamanan untuk TI di perusahaan seperti apa.

   Seperti yang sudah dijelaskan sebelumnya, bahwa bentuk antsipasi terhadap ancaman dari risiko TI masih belum disesuaikan dengan standar manajemen keamanan yang seharusnya, dokumentasi manajemen risiko khusus SCADA telah dibuat oleh PLN pusat namun belum mengacu standar apapun. Selain itu, untuk manajemen risiko TI pada telekomunikasi telah ditetapkan pada buku pedoman telekomunikasi. Sedangkan untuk aplikasi spesifik yang lainnya masih belum memiliki pedoman atau dokumen manajemen risiko secara khusus.

Harapannya dengan adanya penelitian terhadap manajemen risiko dan keberlangsungan bisnis yang dilakukan terhadap TI di PLN APD dapat memberikan rekomendasi strategi yang mengacu pada standar tertentu atau ISO yang dapat diaplikasikan oleh kondisi perusahaan.

Halaman ini sengaja dikosongkan

LAMPIRAN C

***Checklist* Penerapan Kontrol ISO 27002**

Kuesioner ini diajukan untuk mengetahui kondisi pelaksanaan aksi penanggulangan risiko teknologi informasi pada PT PLN (Persero) dengan mengacu pada standar ISO 27002 mengenai sistem manajemen keamanan informasi.

Mohon berikan tanda centang (√) pada bagian yang saat ini telah dilaksanakan oleh PT PLN (Persero) APD Jateng dan DIY dalam menaggulangi risiko TI.

Penanggulangan risiko terhadap *human error* pada aset TI

No	Aksi Penanggulangan Risiko TI	Pelaksanaan
1.	Setiap staff memiliki hak akses yang berbeda satu sama lain tergantung dari peran staff terhadap layanan TI yang digunakan	√
2.	Akses yang digunakan setiap pengguna layanan TI di perusahaan selalu disertai *password* dan ID yang harus didaftarkan terlebih dahulu	√
3.	Adanya larangan tertulis terhadap akses tertentu yang dilarang oleh para karyawan yang bukan menjadi hak aksesnya.	√
4.	Adanya pernyataan persetujuan yang telah disepakati oleh tiap staff atau administrator yang bertanggung jawab terhadap layanan tertentu untuk menghindari penyalahgunaan hak akses.	√
5.	Adanya pembukuan khusus untuk *user guide* dalam installasi ***hardware*** yang disebarkan kepada seluruh karyawan PT PLN (Persero) APD Jateng dan DIY	-

6.	Adanya pembukuan khusus untuk *user guide* dalam installasi dan penggunaan ***software*** yang disebarkan kepada seluruh karyawan PT PLN (Persero) APD Jateng dan DIY	-
7.	Adanya training khusus bagi karyawan yang berhubungan langsung dengan *hardware* atau *software* tertentu.	√
8.	Adanya pemberian status pada tiap staff dalam penggunaan akses ruang, hardware, software (status aktif saat masih menjadi staff/ pengguna, status non aktif ketika sudah tidak memegang jabatan dalam perusahaan atau non karyawan sehingga harus di*block*)	-
9.	Adanya pengecekan terhadap status karyawan sebagai pengguna aset TI (aktif pengguna atau non aktif pengguna)	-
10.	Adanya log tertulis terhadap status karyawan sebagai pengguna aset TI.	-
11.	Adanya dokumentasi tertulis mengenai hak yang dimiliki oleh tiap karyawan dan administrator.	√
12.	Adanya *session time out* secara otomatis saat terdapat penggunaan yang tidak lagi aktif dalam jangka waktu tertentu.	-

Penanggulangan risiko terhadap keamanan aset fisik TI – Server

No	Aksi Penanggulangan Risiko TI	Pelaksanaan
1.	Adanya parameter kemunculan api di wilayah kerja dan wilayah fisik aset TI (seperti detector asap, atau yang lainnya)	√

2.	Adanya parameter atau alarm bahwa server sedang dalam keadaan overheat.	-
3.	Adanya parameter mengenai keadaan suhu ruang server. (suhu panas - suhu normal seharusnya)	-
4.	Adanya peringatan tertulis mengenai larangan membawa makanan/ minuman, rokok, pemantik api/ korek, kamera dan bahan kimia berbahaya ke dalam ruang server.	√
5.	Adanya pembatasan hak akses terhadap ruang server.	-
6.	Di dalam ruang server terbebas dari ancaman air (seperti atap bocor, air ac, dan lain- lain)	√
7.	Pembatasan hak akses ruang server dilakukan dengan memberikan kartu kontrol atau PIN yang **hanya** dapat digunakan oleh orang tertentu untuk masuk dalam ruang server.	-
8.	Adanya laporan log mengenai orang-orang yang masuk ke dalam ruang server baik secara manual maupun otomatis dengan sistem.	-
9.	Terdapat peralatan pemadam api di area ruang server	-
10.	Di dalam ruang server **penggunaan saklar** pada sambungan listrik **tidak bertumpuk**.	-
11.	Kabel di dalam ruang server dilapisi oleh bahan khusus untuk menghindari kabel yang putus atau diserang oleh serangga atau tikus. (pelaksanaan: dilapisi kabel pelindung spiral)	-

Penanggulangan risiko terhadap keamanan aset fisik TI – PC, Finger Print, HT, Telepon Kantor, Amplifier,kondisi fisik router, kondisi fisik switch.

No	Aksi Penanggulangan Risiko TI	Pelaksanaan
1.	Kabel fisik selalu tertata rapi, tidak menghalangi akses jalan (tertata dibawah lantai atau diberikan alat khusus agar tidak terinjak)	√
2.	Kabel fisik tertata dan diberikan pembeda antara kabel satu dengan yang lain (antara kabel telepon, kabel PC, dan lain- lain)	-
3.	Adanya pengecekan rutin terhadap kondisi kabel tiap periode tertentu.	√
4.	Kabel fisik dilapisi oleh bahan yang tidak menghantarkan arus listrik (selain dari produk asli kabel) untuk menghindari konslet dan gigitan tikus atau serangga	-
5.	Adanya dokumentasi untuk **log installasi** *hardware*	-
6.	Adanya dokumentasi khusus terjadinya gangguan pada *hardware*	-
7.	Adanya peraturan untuk peminjaman atau pemindahan *hardware* (batas waktu peminjaman, prosedur pemindahan, penanggung jawab peminjam atau pemindah, pembukuan peminjaman dan pemindahan dari awal dilakukan peminjaman atau pemindahan hingga selesai)	-
8.	Adanya staff khusus yang menangani permasalahan gangguan pada hardware atau aset fisik TI	√

9.	Adanya larangan untuk makan, minum, dan merokok dalam ruangan yang terdapat aset fisik TI.	√
10.	Hardware atau aset fisik TI terletak di dalam ruangan yang aman dan tidak dengan mudah diakses oleh orang asing non karyawan.	√
11.	Adanya aktifitas rutin untuk melakukan perawatan dan *service* terhadap *hardware* dalam periode tertentu sesuai dengan *user guide* pada hardware.	-
12.	Adanya perlindungan khusus terhadap kondisi fisik router dan switch dari ancaman pencurian (diberikan tambahan pengamanan khusus seperti dilindungi dengan pagar besi atau kurungan besi dan dikunci)	-
13.	Tersedianya sumber listrik cadangan atau genset untuk menanggulangi listrik padam dalam kegiatan operasional perusahaan.	√
14.	Fisik aset TI yang berada di luar ruangan terlindung dari ancaman pencurian, petir, dan hujan	√

Penanggulangan risiko terhadap keamanan aset TI – *Software*

No	Aksi Penanggulangan Risiko TI	Pelaksanaan
1.	Adanya dokumentasi untuk **log installasi** *software* pada tiap *personal computer*	-
2.	Adanya dokumentasi khusus terjadinya gangguan pada *software*	√

No	Aksi Penanggulangan Risiko TI	Pelaksanaan
3.	Adanya staff khusus yang menangani permasalahan gangguan pada *software*.	√
4.	Adanya pembatasan hak akses terhadap penggunaan *software* antara satu karyawan dengan karyawan yang lain	√
5.	Adanya perlindungan terhadap virus pada sistem operasi dengan menginstallasi anti virus pada setiap *personal computer*.	√
6.	Adanya pemberian kriptografi pada tiap aplikasi untuk menanggulangi adanya serangan hak akses yang tidak sah.	√
7.	Adanya pembukuan untuk buku manual instalasi atau konfigurasi aplikasi yang digunakan oleh tiap proses bisnis	-
8.	Adanya prosedur dan dokumentasi tertulis sebagai log instalasi aplikasi	-

Penanggulangan risiko terhadap keamanan aset TI – Data

No	Aksi Penanggulangan Risiko TI	Pelaksanaan
1.	Adanya pembatasan hak akses terhadap akses database yang berisi data penting perusahaan	√
2.	Adanya pengelompokan kebutuhan keamanan terhadap data perusahaan (*Confidential, Integrity, Available*)	-
3.	Diberikannya sistem enkripsi pada data perusahaan.	√
4.	Adanya perlindungan *firewall* untuk menghindari pencurian data dari pihak asing.	√

5.	Adanya *back up* pada setiap data perusahaan dengan periode tertentu berdasarkan *security requirements* data.	√
6.	Pemberlakuan pengujian *back up* dilakukan pada periode tertentu untuk memastikan bahwa *back up* dapat dilakukan tanpa adanya gangguan atau hambatan.	-
7.	Pemberlakuan back up data pada lokasi lain yang lebih aman dari ancaman lingkungan (tidak dapat dihindari)	√
8.	Untuk *restore* data, diberlakukan prosedur khusus dengan memberikan pengecekan dan pengujian untuk memastikan efektifitas *restore* data	-
9.	Terdapat email khusus internal perusahaan untuk mencegah adanya kesalahan dalam pengiriman email	√
10.	Adanya prosedur khusus untuk pendaftaran ID dan *password* email perusahaan.	√

Penanggulangan risiko terhadap keamanan aset fisik TI – Jaringan TI dan telekomunikasi

No	Aksi Penanggulangan Risiko TI	Pelaksanaan
1.	Pengkabelan untuk jalur kabel tenaga listrik dan kabel *network and telecommunication* dibedakan dengan identifikasi khusus	√
2.	PT PLN (Persero) APD Jateng dan DIY telah menggunakan jalur *network and telecommunication* pada *fiber optic*	√

3.	Adanya prosedur khusus untuk memberikan akses yang sah pada lingkungan jaringan internet pada PT PLN dengan memberikan masukan ID dan *password* sebelum penggunaan jaringan internet	√
4.	Adanya pengujian pada periode tertentu untuk memastikan jaringan keamanan internet perusahaan	-

LAMPIRAN D

Kalkulasi Penilaian Risiko Aset TI

Hasil dari penilaian dampak, kejadian dan langkah deteksi risiko TI berdasarkan hasil wawancara dan observasi yang telah dilakukan:

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		
People	Staff SCADA dan Telekomunikasi, Staff non SCADA dan Telekomunikasi, Administrator	Penyalahgunaan hak akses dan data organisasi	Penyalahgunaan hak akses	P.1	4	1	8	32	*Very Low*
			Penyalahgunaan data perusahaan	P.2	5	1	8	40	*Very Low*

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		
Software	Aplikasi SCADA	SCADA tidak dapat dioperasikan atau gangguan operasi	Kesalahan konfigurasi pada SCADA	S.1	9	8	7	504	*Very High*
			Server untuk SCADA mengalami *downtime*	S.2	9	8	7	504	*Very High*
			Tidak tersedianya jaringan listrik	S.3	9	4	6	216	*Very High*
			Pengaruh pada peralatan komponen gardu induk	S.4	9	6	4	216	*Very High*
	SAP	Penyalahgunaan hak akses	Penyalahgunaan hak akses pada aplikasi	S.6	3	3	8	72	*Low*

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		
		Tidak tersedianya server	Server down	S.7	2	5	7	70	*Low*
	Email PLN	Penyalahgunaan hak akses	Penyalahgunaan hak akses pada aplikasi	S.8	8	2	7	112	*Medium*
		Tidak tersedianya server	Server down	S.9	7	4	6	168	*High*
	Web jaringan distribusi	Penyalahgunaan hak akses	Penyalahgunaan hak akses pada aplikasi	S.10	5	1	7	35	*Very Low*
		Tidak tersedianya server	Server down	S.11	4	4	6	96	*Low*
	SpeedJardist	Penyalahgunaan hak akses	Penyalahgunaan hak akses pada aplikasi	S.12	5	1	7	35	*Very Low*

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		
		Tidak tersedianya server	Server down	S.13	4	4	6	96	*Low*
Hardware	Server	Tidak tersedianya jaringan listrik	Listrik Mati	H.1	9	4	6	216	*Very High*
			Kerusakan pada genset	H.2	9	4	6	216	*Very High*
		Kerusakan pada server	Gempa bumi	H.3	9	1	10	90	*Low*
			Kebocoran	H.4	9	1	10	90	*Low*
			Kebakaran	H.5	9	1	10	90	*Low*
			Badai/ Petir	H.6	8	1	10	80	*Low*
			Kabel server digigit serangga atau tikus	H.7	8	3	7	168	*High*
		Server Down	Terbatasnya *space* memori pada server	H.8	9	3	6	162	*High*

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		
			Kesalahan pada konfigurasi server	H.9	9	3	6	162	*High*
		Terganggunya operasional server	Pencurian aset fisik pada server	H.10	10	2	6	120	*Medium*
			Server dalam keadaan overheat	H.11	9	5	7	315	*Very High*
	PC	PC tidak dapat dioperasikan	Tidak tersedianya jaringan listrik untuk PC	H.12	8	4	4	128	*Medium*
			Adanya kesalahan konfigurasi pada aset fisik PC	H.13	8	2	3	48	*Very Low*
		Ancaman kelalaian manusia	Pencurian aset fisik peralatan PC	H.14	4	1	10	40	*Very Low*

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		
			Kelalaian aktifitas di area peralatan (seperti makan dan minum di ruangan)	H.15	6	2	7	84	*Low*
		Kerusakan pada PC	Serangan *virus* atau *worm*	H.16	5	3	5	75	*Low*
	Telepon Kantor	Gangguan pada jaringan komunikasi telepon kantor	Kerusakan pada telepon	H.18	7	2	6	84	*Low*
Data	Seluruh data perusahaan	Penyalahgunaan hak akses	Penyalahgunaan hak akses pada data	D.1	5	1	8	40	*Very Low*

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		
		terhadap data perusahaan	Penyebaran data atau informasi perusahaan	D.2	6	1	8	48	*Very Low*
			Data perusahaan di *hacking* dan *cracking*	D.3	5	1	8	40	*Very Low*
		Data tidak dapat digunakan/ diakses	Kesalahan pada konfigurasi backup	D.4	6	1	6	36	*Very Low*
			Kesalahan pada konfigurasi *backup* dan *restore* data	D.5	6	3	6	108	*Medium*
Network	Jaringan internet pada perusahaan	Terputusnya jaringan Internet	Kabel LAN terputus	N.1	8	3	6	144	*Medium*
			Pencurian aset fisik jaringan	N.2	10	1	8	48	*Very Low*

Kategori Aset	Aset	Potensi Kegagalan	Penyebab Potensi Kegagalan	Id Risiko	Penilaian			RPN	Klasifikasi Risiko
					S	O	D		
			Kesalahan konfigurasi atau instalasi jaringan internet	N.3	7	2	6	84	*Low*
		Cyber crime melalui jaringan internet	Pencurian *bandwidth*	N.4	5	1	9	45	*Very Low*
			Serangan *hacker* melalui jaringan internet perusahaan	N.5	10	2	8	160	*High*

LAMPIRAN E

Kalkulasi Penilaian Dampak Terhentinya Proses Bisnis

No.	Fungsi Bisnis	Proses Bisnis	Dampak	Durasi proses bisnis saat terjadi bencana					Level Risiko
				<1 jam	4 jam	1 hari	7 hari	> 1 Bulan	
1.	Pemeliharaan Gardu Induk	Pemeliharaan Korektif	Produk dan Layanan	4	5	4	5	5	*High*
			Proses Bisnis Internal	4	5	4	4	5	
		Pemeliharaan Intensif	Produk dan Layanan	2	2	3	3	4	*Medium*
			Proses Bisnis Internal	2	2	3	3	4	
		Proteksi dan Meter	Produk dan Layanan	2	2	3	3	4	*Medium*

No.	Fungsi Bisnis	Proses Bisnis	Dampak	Durasi proses bisnis saat terjadi bencana					Level Risiko
				<1 jam	4 jam	1 hari	7 hari	> 1 Bulan	
			Proses Bisnis Internal	2	2	3	3	4	
2.	Operasional Sistem DIstribusi	Operasional	Produk dan Layanan	5	5	5	5	5	*High*
			Proses Bisnis Internal	4	4	4	4	5	
		Perencanaan	Produk dan Layanan	2	2	2	3	4	*Low*
			Proses Bisnis Internal	2	2	2	3	4	
		Pengelolaan data dan Gambar	Produk dan Layanan	2	2	2	3	3	*Low*

No.	Fungsi Bisnis	Proses Bisnis	Dampak	Durasi proses bisnis saat terjadi bencana					Level Risiko
				<1 jam	4 jam	1 hari	7 hari	> 1 Bulan	
			Proses Bisnis Internal	2	2	2	3	4	
3.	SCADA dan telekomunikasi	Menyiapkan Keperluan Operasi SCADA	Produk dan Layanan	3	3	4	5	5	*High*
			Proses Bisnis Internal	3	3	4	5	5	
		Remote Terminal Unit	Produk dan Layanan	3	3	4	5	5	*High*
			Proses Bisnis Internal	3	4	4	4	5	
		Pengelolaan TI dan telekomunikasi	Produk dan Layanan	2	2	3	3	5	*Medium*

No.	Fungsi Bisnis	Proses Bisnis	Dampak	Durasi proses bisnis saat terjadi bencana					Level Risiko
				<1 jam	4 jam	1 hari	7 hari	> 1 Bulan	
			Proses Bisnis Internal	2	2	3	4	4	
4.	Administrasi dan Keuangan	Administrasi dan K3	Produk dan Layanan	1	1	1	1	1	*Low*
			Proses Bisnis Internal	1	1	1	1	1	
		Kesiapan SDM	Produk dan Layanan	1	1	1	1	1	*Low*
			Proses Bisnis Internal	1	1	1	1	1	
		Keuangan	Produk dan Layanan	1	1	1	1	1	*Low*

No.	Fungsi Bisnis	Proses Bisnis	Dampak	Durasi proses bisnis saat terjadi bencana					Level Risiko
				<1 jam	4 jam	1 hari	7 hari	> 1 Bulan	
			Proses Bisnis Internal	1	1	1	1	1	

LAMPIRAN F

Strategi Keberlangsungan Bisnis terhadap Gangguan

Berikut merupakan strategi BCP untuk tiap risiko yang telah diidentifikasikan berdasarkan prioritas utama dalam keberlangsungan bisnis PT PLN (Persero) APD Jateng dan DIY:

Strategi Keberlangsungan Bisnis terhadap Gangguan SCADA		
Penyebab Risiko Kegagalan: Kesalahan Konfigurasi pada SCADA ID Strategi : SCADA 01		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Prosedur konfigurasi dan integrasi sistem SCADA dengan *software* atau aplikasi lain	Sebagai bentuk identifikasi terhadap konfigurasi sistem SCADA dengan software atau aplikasi lain yang terintegrasi dengan sistem SCADA.	Lakukan identifikasi terhadap keseluruhan *software* atau aplikasi sistem SCADA. Apakah software tersebut digunakan dalam lingkup APD Jateng dan DIY saja atau digunakan juga oleh vendor atau PLN pusat. Selain itu juga diperlukan metode kontrol pembatasan hak akses dan penggunaan kapasitas memory untuk *software* lain yang terintegrasi terhadap sistem SCADA.

		(*Dokumen FISMA CM 6- Configuration Settings – Implementasi pada DOE*)
Pemberlakuan pembukuan terhadap buku panduan untuk installasi SCADA	Buku panduan installasi digunakan pada pelaku instalasi sebagai panduan untuk menhindari kesalahan pada saat instalasi	Proses instalasi harus didampingii dengan buku panduan yang diberikan dari vendor produk. *Dokumen FISMA CM 6- Configuration Settings – Implementasi pada DOE*)
Pemberlakuan kontrol atau metode secara tertulis/terdokumentasi untuk installasi SCADA	Metode/ kontrol tertulis diperlukan sebagai panduan untuk pelaksanaan instalasi terhadap SCADA pada PT PLN (Persero) APD Jateng dan DIY yang dapat ditinjau perusahaan.	Dalam prosedur ini, diperlukan pula metode dokumentasi untuk log waktu pelaksanaan instalasi atau upgrade serta dokumentasi pelaku installasi SCADA. (*ISO 27002:2005 – 12.4.1 Control of Operational Software*) Selain itu, dalam prosedur instalasi juga diperlukan pemberlakuan pengujian terhadap sistem untuk memastikan kehandalan sistem SCADA yang telah diinstalasi.

		Setelah pengujian selesai dilakukan, perlu dilakukan *check list* instalasi berdasarkan dokumentasi keberhasilan pengujian SCADA (*Dokumen FISMA CM 6- Configuration Settings – Implementasi pada DOE*)
Pencatatan kontrak persetujuan dengan vendor produk terhadap peraturan upgrade sistem pada SCADA	Sebagai bentuk persetujuan, pengetahuan serta kontrak pihak PT PLN (Persero) dengan vendor produk yang bersangkutan	Perusahaan menjadi lebih mengetahui jadwal upgrade sistem sehingga dapat menghindari adanya kegagalan konfigurasi terhadap sistem SCADA. *(Access restriction for change, Configuration Management 7 FISMA – Implementasi pada DOE)*
Penyusunan **prosedur penanganan gangguan pada sistem SCADA**	Sebagai pedoman dalam melakukan pencegahan dan penanganan gangguan pada sistem SCADA	Dalam perencanaan yang telah dibuat oleh NIPP, hal yang harus diperhatikan dalam upaya pencegahan dan penanganan adalah sebagai berikut:

		• Risiko pada dimensi *cyber* • Perlindungan terhadap ancaman bencana hazard • Ketergantungan terhadap peraturan sektor pada departemen lain di United States • Penanganan recovery saat gangguan (dokumen NIPP Plan untuk Department of Energy United States)

Strategi Detektif untuk kejadian kesalahan konfigurasi pada Server	
Strategi Detektif	**Keterangan**
Melakukan pemeriksaan dari dokumentasi log instalasi	Mengantisipasi kegagalan dari instalasi
Strategi DRP pada kesalahan konfigurasi SCADA	
Strategi saat gangguan terjadi	**Keterangan**

Identifikasi penyebab gangguan	Saat menerima laporan mengenai gangguan SCADA, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi lebih lanjut pada pihak yang bertanggung jawab.
Pemeriksaan kesalahan konfigurasi	Melakukan pemeriksaan terhadap kondisi gangguan pada SCADA sesuai dengan identifikasi pada laporan.
Penyelamatan data dan informasi sementara	Melakukan upaya untuk menangani penyelamatan data dan informasi terakhir yang telah diperoleh dari sistem SCADA.
Strategi Korektif pada Gangguan SCADA	
Strategi Korektif	**Keterangan**
Melakukan evaluasi prosedur penanganan gangguan dari dokumentasi insiden	Evaluasi prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

Strategi Keberlangsungan Bisnis terhadap Gangguan SCADA		
Penyebab Risiko Kegagalan: Kerusakan pada Peralatan Gardu Induk ID Strategi : SCADA 02		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Prosedur Perawatan dan pemeriksaan Komponen Gardu Induk	Sebagai pedoman dalam perawatan dan peeriksaan pada gardu induk	Bagian ini tidak dilaksanakan oleh fungsi SCADA dan Telkomunikasi, melainkan pada fungsi bisnis Gardu Induk, sehingga pada prosedur ini akan mengacu pada prosdur yang telah ditetapkan oleh fungsi Gardu Induk
Strategi Detektif Kerusakan pada Peralatan Gardu Induk		
Strategi Detektif		**Keterangan**
Berdasarkan ketentuan **Prosedur Perawatan dan pemeriksaan Komponen Gardu Induk**		Bagian ini tidak dilaksanakan oleh fungsi SCADA dan Telkomunikasi, melainkan pada fungsi bisnis Gardu Induk, sehingga pada prosedur ini akan mengacu pada prosdur yang telah ditetapkan oleh fungsi Gardu Induk
Strategi DRP pada Kerusakan pada Peralatan Gardu Induk		
Strategi saat gangguan terjadi		**Keterangan**
Berdasarkan ketentuan **Prosedur Perawatan dan pemeriksaan Komponen Gardu Induk**		Bagian ini tidak dilaksanakan oleh fungsi SCADA dan Telkomunikasi, melainkan pada fungsi bisnis Gardu Induk, sehingga pada prosedur ini akan mengacu pada prosdur yang telah

	ditetapkan oleh fungsi Gardu Induk
Strategi Korektif pada Gangguan SCADA	
Strategi Korektif	**Keterangan**
Berdasarkan ketentuan **Prosedur Perawatan dan pemeriksaan Komponen Gardu Induk**	Bagian ini tidak dilaksanakan oleh fungsi SCADA dan Telkomunikasi, melainkan pada fungsi bisnis Gardu Induk, sehingga pada prosedur ini akan mengacu pada prosdur yang telah ditetapkan oleh fungsi Gardu Induk

Strategi Keberlangsungan Bisnis terhadap Gangguan SCADA		
Penyebab Risiko Kegagalan : Tidak Tersedianya Jaringan Listrik ID Strategi : SCADA 03		
Strategi DRP Tidak tersedianya Jaringan Listrik		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Penyusunan Kebijakan Pengkabelan dan Peralatan Listrik	Sebagai acuan dalam penyusunan prosedur operasional terhadap pengkabelan dan peralatan listrik	Prosedur pengkabelan ini dapat mengacu pada standar ISO *ISO 27002:2005 9.2.3 Cabling Security* dan langkah implementasi yang telah dilaksanakan Department of Energy United States terhadap pelaksanaan standar FISMA bagian *Power Equipment and Cabling* .
Penyusunan **Prosedur Pengkabelan dan Peralatan Listrik**	Sebagai pedoman bagi pemasangan, perlindungan, serta pemasalahan pengkabelan yang terkait dengan sumber	Berikut merupakan contoh metode yang dapat diterapkan pada prosedur pemasangan: • Adanya pemisahan jalur kabel listrik dengan kabel yang lain secara fisik (*Power*

	listrik, jaringan internet serta jaringan telepon.	*Equipment and Cabling 9 FISMA – Implementasi pada DOE United States*) • Adanya identifikasi khusus pada tiap jenis kabel (kabel listrik, kabel telepon, kabel LAN) seperti identifikasi warna atau identifikasi isolator pembungkus kabel untuk membedakan kabel agar memberikan kemudahan saat mengidentifikasi pada kejadian gangguan. (*ISO 27002:2005 9.2.3 Cabling Security*)
Penyusunan **prosedur terhadap e*mergency power***	Sebagai pedoman dalam pelaksanaan metode pengadaan sumber energi listrik cadangan sementara dan pemberian metode antisipasi dalam menghadapi risiko gangguan tidak tersedianya sumber daya listrik.	• Menyediakan sumber energi listrik cadangan sebagai sumber energi sementara yang dapat digunakan oleh proses bisnis. (*PE 11 Emergency Power FISMA – Implementasi pada DOE United States* dan *ISO 27002:2005 9.2.2 Supporting Utilities*) • Sumber energi listrik cadangan harus dapat di *maintenance* dengan rutin oleh organisasi (*PE 11 Emergency*

		Power FISMA – Implementasi pada DOE United States)
Pemberlakuan **prosedur *backup data*** secara rutin	Sebagai bentuk antisipasi organisasi apabila sistem SCADA terganggu dan mengancam kehilangan data perusahaan	*Backup* data rutin dilakukan agar apabila sistem SCADA mati data-data yang belum tersimpan memiliki *backup* sehingga tidak hilang ketika SCADA dapat kembali berfungsi.
Menyiapkan strategi pengujian saat jaringan listrik tidak tersedia	Sebagai bentuk kesiapan organisasi saat terjadi gangguan terhadap tidak tersedianya jaringan listrik pada perusahaan.	Pengujian hanya dilakukan apabila kondisi memungkinkan, karena pengujian berdasarkan pada sumber listrik yang merupakan sumber daya utama pada kebutuhan proses bisnis perusahaan.

Strategi DRP terhadap tidak tersedianya jaringan listrik	
Strategi DRP	**Keterangan**
Identifikasi Penyebab gangguan	Saat menerima laporan mengenai gangguan SCADA, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi lebih lanjut pada pihak yang bertanggung jawab.
Pengupayaan untuk menghidupkan sumber daya listrik cadangan	Menghidupkan sumber daya listrik cadangan sebagai metode utama saat jaringan listrik tidak tersedia.

Melakukan *restorasi* data dan informasi yang telah di *backup* secara otomatis	Melakukan upaya untuk mengambil data yang telah diback up sebelumnya dari sistem SCADA.
Strategi Korektif pada Gangguan SCADA	
Strategi Korektif	**Keterangan**
Melakukan evaluasi prosedur penanganan gangguan dari log dokumentasi insiden	Evaluasi kejadian, frekuensi kejadian dan prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

Strategi Keberlangsungan Bisnis terhadap aplikasi Email PLN		
Penyebab Risiko Kegagalan: Penyalahgunaan Hak Akses pada Aplikasi Email Perusahaan ID Strategi : Email 01		
Strategi Preventif Tidak tersedianya Jaringan Listrik		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Pemberlakuan **prosedur manajemen akun**	Untuk memastikan akses pengguna	Penyusunan prosedur ini dapat berdasarkan pada kontrol dokumen FISMA AC 11 Session Lock, AC 2 Account Management, AC 3

	yang sah dan mencegah adanya penggunaan yang tidak sah pada aplikasi	Access Enforcement, AC 1 Access Control Policy and procedures dan ISO 27002:2005 *11.2.1 User Registration, 11.2.23 User Password Management* • Pemberlakuan metode alur administratif/ pendaftaran pengguna pada aplikasi email PLN. Metode tersebut disarankan mencakup: - Ketentuan pemberian nama ID dan kompleksitas *password* - Pemberian lembar persetujuan mengenai ketentuan dan hak untuk penggunaan akses (*ISO 27002:2005 11.2.1 User Registration)* • Pemberlakuan manajemen dalam penggunaan *password* oleh pengguna pada aplikasi email PLN. Metode tersebut mencakup: - Pemberlakuan masa berlaku *password* sehingga mengharuskan pengguna untuk melakukan *update* untuk

		mengubah *pass-word*nya. - Pemberlakuan prosedur untuk verifikasi *pass-word* baru (tidak dapat mengulang *password* lama, dan lain- lain) (*ISO 27002:2005 11.2.23 User Pass-word Management)* • Adanya pemberlakuan *non active sessions* secara otomatis agar tidak dis-alahgunakan saat pengguna meninggalkan aplikasi atau aset TI selama beberapa saat serta pemberlakuan *log out* otomatis saat pengguna keluar dari laman email PLN (*Access Control 11 FISMA – Implementasi pada DOE United States* serta ISO 27002:2005 *11.3.2 Unanttended User Equipment* dan *11.3.3 Clear Desk and Clear Screen Policy)*
Pemberlakuan kebijakan dan **prosedur *Identifier Ac-count Man-agement***	Sebagai upaya pencegahan hak akses yang sudah tidak berlaku atau kadalu-	• Pemberian kontrol atau metode untuk *session ter-mination* atau pemutusan hubungan pada staff non aktif terhadap apilkasi email PLN. (berlaku pada *Account Control 12*

	arsa oleh perusahaan (misalnya staff non aktif, dan lain- lain)	*FISMA- Implementasi pada DOE United States dan ISO 27002:2005 9.2.5 Security of equipment off premises,9.2.7 Removal Property)* • Pemberlakuan identifikasi akun dan pemberian peran pada tiap akses akun seperti misalnya peran untuk public, supervisor, asistant manajer, manajer, *cross organization management*, dan lain-lain (*IA 4 Identifier Management*)

Strategi Detektif pada Penyalahgunaan Hak Akses	
Strategi DRP	**Keterangan**
Pemberlakuan uji *scanning* terhadap sistem keamanan jaringan internet perusahaan	*Scanning* merupakan metode deteksi untuk mengetahui penyalahgunaan hak akses pada jaringan internet. Scanning dapat dilakukan dengan tools yang banyak tersedia secara open sources seperti misalnya Nmap.
Pencatatan atau dokumentasi hasil scanning jaringan keamanan	Lakukan dokumentasi setelah pelaksanaan scanning disertai waktu pelaksanaan dan hasil scanning.

Strategi DRP pada Penyalahgunaan Hak Akses	
Strategi DRP	**Keterangan**
Identifikasi situasi terhadap pelaporan pada gangguan email PLN	Melakukan identifikasi saat terjadi gangguan pada

	email PLN untuk mengatahui penyebab gangguan
Pengamanan aset TI/ SI terutama pada email PLN dan data – data	Lakukan upaya backup dan pengamanan terhadap set TI/ SI
Pemeriksaan terhadap gangguan	Untuk mengetahui keadaan nyata dalam gangguan email PLN dan mengetahu penyebab pasti pada gangguan email PLN. Apabila gangguan terjadi karena penyalahgunaan hak akses, maka diperlukan tindakan terhadap pelaku.
Penindakan pelaku	Penindakan pelaku berdasarkan pada kebijakan yang telah disampaikan pihak PLN
Strategi Korektif pada Gangguan Email PLN	
Strategi Korektif	**Keterangan**
Melakukan evaluasi prosedur penanganan gangguan dari dokumentasi insiden	Evaluasi prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

Strategi Keberlangsungan Bisnis terhadap Server		
Pengkabelan pada Server terputus ID Strategi : Server 01		
Strategi Preventif terhadap terputusya jaringan kabel		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Penerapan **prosedur perlindungan pada peralatan listrik** dan pengkabelan	Sebagai bentuk perlindungan untuk gangguan yang bersumber dari kerusakan kabel	Perusahaan perlu memberikan perlindungan terhadap peralatan elektronik dan kabel dari ancaman gangguan atau kerusakan. Berikut merupakan beberapa cara yang perlu dilakukan: • Adanya pemberian perlindungan khusus pada tiap kabel untuk menghindari kerusakan dari gigitan tikus atau seranga (*Power Equipment and Cabling 9 FISMA – Implementasi pada DOE United States*) • Adanya identifikasi khusus pada tiap jenis kabel (kabel listrik, kabel telepon, kabel LAN) seperti identifikasi warna atau identifikasi isolator pembungkus kabel untuk membedakan kabel agar memberikan kemudahan saat mengidentifikasi pada kejadian gangguan. (*ISO 27002:2005 9.2.3 Cabling Security*)

Pemberlakuan **prosedur *backup data*** secara rutin	Sebagai bentuk antisipasi organisasi apabila sistem SCADA terganggu dan mengancam kehilangan data perusahaan	*Backup* data rutin dilakukan agar apabila sistem SCADA mati data-data yang belum tersimpan memiliki *backup* sehingga tidak hilang ketika SCADA dapat kembali berfungsi.

Strategi DRP terhadap terputusnya jaringan kabel	
Strategi DRP	**Keterangan**
Identifikasi Penyebab gangguan	Saat menerima laporan mengenai gangguan server, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi lebih lanjut pada pihak yang bertanggung jawab.
Pemeriksanaan terhadap gangguan	Tim melakukan inspeksi terhadap gangguan, salah satu pemeriksaan juga dilakukan pada pemantauan kabel yang tersambung dengan server
Melakukan restorasi data dan informasi yang telah di *backup* secara otomatis	Melakukan upaya untuk mengambil data yang telah diback up sebelumnya dari aplikasi terkait.
Strategi Korektif pada Gangguan Server	
Strategi DRP	**Keterangan**

Melakukan evaluasi prosedur penanganan gangguan dari dokumentasi insiden	Evaluasi prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

Strategi Keberlangsungan Bisnis terhadap Server		
Kebutuhan Memori tidak terpenuhi		
Strategi Preventif terhadap kebutuhan memoru yang tidak terpenuhi		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Penyusunan **prosedur Manajemen Kapasitas**	Memberikan batasan, pengawasan serta penyesuaian penggunaan kapasitas memori pada server	• Melakukan *off loading* atau proses yang dilakukan untuk mengamankan data *confidential* dan *integrity* dari server penyimpanan primer ke server penyimpanan sekunder. (AU 4 FISMA - *Implementasi pada DOE United States)* • Mengelola kapasitas penggunaan untuk memastikan bahwa kapasitas masih tersedia dan dapat digunakan oleh operasional bisnis.

		Penyediaan kuota kapasitas dapat berdasarkan pada prioritas proses bisnis, kuota atau partitioning. (*SC 5 FISMA-Implementasi pada DOE United States*)

Strategi DRP terhadap Kebutuhan Memori yang Tidak Terpenuhi	
Strategi DRP	**Keterangan**
Identifikasi Penyebab gangguan	Saat menerima laporan mengenai gangguan server, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi lebih lanjut pada pihak yang bertanggung jawab.
Pemeriksanaan terhadap gangguan	Tim melakukan inspeksi terhadap gangguan, salah satu pemeriksaan juga dilakukan pada pemantauan kapasitas memori pada server
Melakukan *off loading*	*Off loading* yaitu proses yang dilakukan untuk mengamankan data *confidential* dan *integrity* dari server penyimpanan primer ke server penyimpanan sekunder
Melakukan restorasi data dan informasi yang telah di *backup*	Melakukan upaya untuk melakukan percobaan *back up* kembali.
Strategi Korektif pada Gangguan Server	
Strategi DRP	**Keterangan**

Melakukan evaluasi prosedur penanganan gangguan dari dokumentasi insiden	Evaluasi prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

Strategi Keberlangsungan Bisnis terhadap Server		
Server dalam keadaan *overheat* ID Strategi : Server 02		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Pemasangan status temperature ruangan server	Mengetahui temperature ruangan server secara real time	• Pendeteksi temperature ruangan server dipasang dalam ruang server yang di monitoring setiap saat *(PE 14 – FISMA Implementasi pada DOE)*
Pemberian **prosedur terhadap gangguan bencana hazard**	Sebagai acuan dalam keperluan pembuatan prosedur operasional penanganan bencana	Kebijakan ini dapat mengacu pada kebutuhan keamanan PT PL (Persero) APD Jateng dan DIY terhadap standar pada *Physical Equipment* dokumen FISMA implementasi pada Department of Energy United States serta ISO 27002:2005 yaitu pada bagian 9.1 *Secure Areas of Physical and environmental security.*

Pembuatan **prosedur penanganan keadaan server yang *overheat***	Melakukan penanganan gangguan lebih aman sesuai dengan prosedur yang diber-lakukan	*(PE 14 – FISMA Implementasi pada DOE)*

Strategi Detektif untuk kejadian *overheat* pada Server	
Strategi Detektif	**Keterangan**
Pemasangan pendeteksi temperature ru-angan server	• Pendeteksi tem-perature ruangan server dipasang dalam ruang server yang di monitoring setiap saat *(PE 14 – FISMA Implementasi pada DOE)*
Pemasangan alarm atau notifikasi apa-bila temperatur ruangan server terlalu tinggi untuk keamanan server	• Notifikasi dapat berupa alarm yang memberikan status ruangan server dalam keadaan *over-heat,* *(PE 14 – FISMA Implementasi pada DOE)*

Strategi DRP untuk kejadian *overheat* pada Server	
Strategi DRP	**Keterangan**

Identifikasi situasi terhadap alarm pada notifikasi keadaan suhu	Melakukan tindakan penyelamatan terhadap ruang server (apabila kebakaran terjadi sebatas pada ruang server saja)
Pengamanan aset fisik server	Memastikan keadaan server dan ruang server setelah notifikasi muncul lalu melakukan pengamanan awal untuk mengembalikan temperature normal ruang server.
Melaporkan pada koordinator tim BCP keberlangsungan bisnis pada risiko TI	Apabila pengamanan dan pengembalian temperature ruang server tidak selesai dalam 1 jam maka tim pemeriksa melakukan pelaporan pada koordinator tim BCP untuk selajutnya dilaksanakan strategi komunikasi BCP
Penyuluhan terhadap bagian yang terkena dampak	Hal ini dilakukan untuk menginformasikan pada seluruh elemen organisasi mengenai keadaan terkini dari dampak bencana alam terhadap aset dan proses bisnis.
Menonaktifkan sistem sementara	Menon-aktifkan sistem akan mempermudah tim BCP dalam penanggulangan bencana
Mengaktifkan sistem dan restore data	Setelah sistem diaktifkan kembali, tim melakukan upaya untuk melakkan restore data yang tesimpan pada server cadangan.

Strategi Korektif pada Gangguan Server	
Strategi DRP	**Keterangan**
Melakukan evaluasi prosedur penanganan gangguan dari dokumentasi insiden	Evaluasi prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

Strategi Keberlangsungan Bisnis terhadap Server		
Kesalahan Konfigurasi *Server* ID Strategi : Server 03		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Pemberlakuan **prosedur untuk pemasangan perangkat keras**	Prosedur tertulis diperlukan sebagai panduan untuk pelaksanaan instalasi terhadap server pada PT PLN (Persero) APD Jateng	Dalam prosedur ini, diperlukan pula <u>dokumentasi untuk log waktu pelaksanaan</u> instalasi atau upgrade serta <u>dokumentasi pelaku installasi</u> server serta pemasangan atau pelepasan komponen- komponen pada server. (*ISO 27002:2005 – Bab 12.4.1 Control of Operational Software*) Selain itu, dalam prosedur instalasi juga diperlukan <u>pemberlakuan pengujian terhadap sistem</u> untuk memasti-

	dan DIY yang dapat ditinjau perusahaan.	kan kehandalan server yang telah diinstalasi. Setelah pengujian selesai dilakukan, perlu dilakukan *check list* instalasi berdasarkan dokumentasi keberhasilan pengujian server (*Configuration Management 5 FISMA – Implementasi pada DOE*)
Pemberlakuan pembukuan terhadap buku panduan untuk installasi server	Buku panduan installasi digunakan pada pelaku instalasi sebagai panduan untuk menhindari kesalahan pada saat instalasi	Proses instalasi harus didampingii dengan buku panduan yang diberikan dari vendor produk. (*Configuration Management 5 FISMA – Implementasi pada DOE*)

Strategi Detektif untuk kejadian kesalahan konfigurasi pada Server	
Strategi Detektif	**Keterangan**
Melakukan pemeriksaan dari dokumentasi log instalasi dan pengujian	Mengantisipasi kegagalan dari instalasi

Strategi DRP pada kesalahan konfigurasi server	
Strategi saat gangguan terjadi	**Keterangan**
Identifikasi penyebab gangguan	Saat menerima laporan mengenai gangguan server, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi

	lebih lanjut pada pihak yang bertanggung jawab.
Pemeriksaan kesalahan konfigurasi	Melakukan pemeriksaan terhadap kondisi gangguan pada server sesuai dengan identifikasi pada laporan. Apabila penyelamatan kondisi normal server tidak dapat dilakukan pada kurun waktu 1 jam maka selanjutnya tim melaporkan pada ketua tim BCP
Penyuluhan terhadap bagian yang terkena dampak	Hal ini dilakukan untuk menginformasikan pada seluruh elemen organisasi mengenai keadaan terkini dari dampak bencana alam terhadap aset dan proses bisnis.
Penyelamatan data dan informasi sementara	Melakukan upaya untuk menangani penyelamatan data dan informasi terakhir yang telah diperoleh dari server.
Strategi Korektif pada Gangguan Server	
Strategi DRP	**Keterangan**
Melakukan evaluasi prosedur penanganan gangguan dari dokumentasi insiden	Evaluasi prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan

	gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

Strategi Keberlangsungan Bisnis terhadap Server		
Pencurian Aset Fisik ID Strategi: Server 04		
Strategi Preventif pada pencurian aset fisik		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Pembuatan alur dan **prosedur administratif akses ruang server**	Untuk mengetahui segala jenis akses yang dilakukan pada ruang server	Penyusunan prosedur ini dapat berdasarkan pada acuan standar ISO 27002:2005 bagian 9.1.1 Physical Security Perimeter dan bagian 9.1.2 yaitu Physical Entry Control, serta pelaksanaan pada Department of Energy United States yaitu pada dokumen FISMA – NIST bagian *Physical Environmental Protection* – 3 dan *Physical Environmental Protection* – 1.
Strategi Detektif pada pencurian aset fisik		
Strategi Detektif	**Tujuan Strategi detektif**	**Keterangan**
Pemasangan cctv pada pintu masuk dan beberapa sudut ruang server	Untuk memantau aktifitas dan mengetahui aktifitas mencurigakan	Melakukan pengawasan oleh pihak tertentu pada ruang cctv terhadap orang yang aktifitas pada ruang server. (*Physical Environmental Protection* – 3 FISMA)

	dalam ruang server	

Strategi DRP pada Pencurian aset fisik server	
Strategi saat gangguan terjadi	**Keterangan**
Identifikasi penyebab gangguan	Saat menerima laporan mengenai gangguan server, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi lebih lanjut pada pihak yang bertanggung jawab.
Melaporkan pada ketua tim BCP	Melakukan laporan bahwa terjadi pencurian aset fisik server dan pengembalian kondisi normal memungkinkan memakan waktu lebih dari 1 jam.
Penyuluhan terhadap bagian yang terkena dampak	Hal ini dilakukan untuk menginformasikan pada seluruh elemen organisasi mengenai keadaan terkini dari dampak bencana alam terhadap aset dan proses bisnis.
Penyelamatan data dan informasi sementara serta pemulihan data	Melakukan upaya untuk menangani penyelamatan dan pemulihan data dan informasi terakhir yang telah diperoleh dari server.
Pemeriksaan CCTV dan log akses ruag server	Melihat record dari cctv yang terpasang pada

	area ruang server serta memantau log akses ruang server untuk mengetahui pelaku yang memasuki ruang server
Strategi Korektif pada Gangguan Server	
Strategi DRP	**Keterangan**
Melakukan evaluasi prosedur penanganan gangguan dari dokumentasi insiden	Evaluasi prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

Strategi Keberlangsungan Bisnis terhadap Data Perusahaan		
Kesalahan Konfigurasi *Backup* dan *Restore* data ID Strategi : Data 01		
Strategi Preventif pada Kesalahan Konfigurasi		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Penyusunan **prosedur backup**	Sebagai pedoman langkah pelaksanaan backup dan	Prosedur *backup* dapat mengacu pada kontrol yang telah diterapkan oleh Department of Energy United States pada dokumen FISMA – NIST bagian CP 9 – Information System Backup

dan restore data	restore data perusahaan	dan CP 10 Information System Recovery and Reconstruction dan ISO 27002:2005 bagian 10.5.1 mengenai *Information Backup.*
Pengidentifikasian jenis data	Mengetahui tipe data berdasarkan *confidentiality, integrity,* serta *availability* data	• Memberikan identifikasi terhadap setiap data perusahaan berdasarkan *confidentiality, integrity,* serta *availability* data • Memberikan identitas tipe data berdasakan pada reliabilitas data yang dapat ditinjau dari dampak tidak tersedianya jenis aplikasi untuk menginput data tersebut. (*CP 9 FISMA Implementasi pada DOE*)
Pemberlakuan *backup* data secara rutin harian (penggunaan **berdasarkan prosedur backup dan restore data**)	Pemberlakuan *backup* untuk melakukan pencadangan data untuk digunakan kembali yang tersimpan saat data asli hilang.	Strategi backup secara harian merupakan strategi back up yang dapat dilakukan dan mempermudah perusahaan dalam pelaksanaan back up secara rutin terhadap data perusahaan. (DOE Data Center Optimization Plan) • Lokasi penyimpanan data backup harus bebas dari ancaman risiko yang juga mengancam pada lokasi utama. (ISO27002:2005 10.5.1 *Information Backup*)
Strategi Detektif		**Keterangan**

Identifikasi penyebab gangguan	Saat menerima laporan mengenai gangguan server, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi lebih lanjut pada pihak yang bertanggung jawab.
Pengujian *backup* dan *restore* data	Gunakan data sampling untuk melakukan pengujian metode backup dan restore. Tulis hasil pengujian dengan log waktu dan catat keberhasilan backup dan restore data. (*CP 9 FISMA Implementasi pada DOE*) (ISO27002:2005 10.5.1 *Information Backup*)
Strategi DRP pada kesalahan konfigurasi *backup* data	
Strategi DRP	**Keterangan**
Identifikasi penyebab gangguan	Saat menerima laporan mengenai gangguan server, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi lebih lanjut pada pihak yang bertanggung jawab.
Identifikasi jenis data	Melakukan identifikasi jenis data yang ditangani
Pemeriksaan terhadap gangguan	Melakukan pemeriksaan terhadap kondisi gangguan pada server sesuai dengan identifikasi pada laporan. Apabila penyelamatan kondisi normal server tidak dapat dilakukan pada kurun waktu 1 jam maka selanjutnya tim melaporkan pada ketua tim BCP

Penyuluhan terhadap bagian yang terkena dampak	Hal ini dilakukan untuk menginformasikan pada seluruh elemen organisasi mengenai keadaan terkini dari dampak bencana alam terhadap aset dan proses bisnis.
Penyelamatan data dan informasi sementara	Melakukan upaya untuk menangani penyelamatan data dan informasi terakhir yang telah diperoleh diinput dari aplikasi terkait.
Strategi Korektif pada Gangguan terhadap Data Perusahaan	
Strategi Korektif	**Keterangan**
Melakukan dokumentasi hasil penanganan	Dokumentasi hasil penanganan digunakan sebagai bahan pertimbangan langkah korektif berikutnya
Melakukan evaluasi prosedur *backup* data	Evaluasi prosedur back up data untuk mengetahui kesalahan dalam pelaksanaan prosedur
Identifikasi jenis data	Melakukan identifikasi jenis data yang akan ditangani
Melakukan perbaikan terhadap gangguan terkait	Perbaikan dilakukan dengan mengupayakan ketersediaan data cadangan yang telah di *backup* sebelumnya dan melakukan perbaikan pada konfigurasi pada sistem *backup* dan *recovery*

Strategi Keberlangsungan Bisnis terhadap Jaringan Internet		
Serangan *Hacker* ID Strategi: Network 01		
Strategi Preventif pada Serangan *Hacker* Jaringan Internet		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**

Pemberlakuan **kebijakan dan prosedur penggunaan jaringan internet**	Memberikan pedoman dan panduan bagi elemen organisasi terhadap penggunaan jaringan internet dan hak akses tiap elemen organsasi	• (AC 6 *Least Privileged* FISMA DOE) • (ISO 27002:2005 11.4.6 *Network Connection Control*)
Pemasangan *Firewall* pada jaringan internet	Untuk mengantisipasi adanya serangan hacker	• Pemasangan firewall perlu dipasangkan pada koneksi internet, virtual private network, jaringan intranet perusahaan, dan jaringan sambungan dengan SCADA. (*Cybersecurity Risk Management Process for DOE Usnited States)*
Pengujian tingkat keamanan secara periodik	Untuk mengetahui tingkat keamanan yang telah berlaku saat ini	• Sesuai dengan kebijakan dan prosedur yang telah dibuat perusahaan.
Pemberlakuan *backup* data secara harian (penggunaan **berdasarkan prosedur backup dan restore data**)	Untuk mengantisipasi serangan hacker yang mencuri dan meghilangkan hak akses pegawai PLN terhadap data	• Strategi backup secara harian merupakan strategi back up yang dapat dilakukan dan mempermudah perusahaan dalam pelaksanaan back up secara rutin terhadap data perusahaan. (DOE Data Center Optimization Plan)
Strategi Detektif pada Serangan *Hacker*		
Strategi DRP		**Keterangan**

Pemberlakuan *scanning* terhadap sistem keamanan jaringan internet perusahaan	*Scanning* merupakan metode deteksi untuk mengetahui penyalahgunaan hak akses pada jaringan internet. Scanning dapat dilakukan dengan tools yang banyak tersedia secara open sources seperti misalnya Nmap.
Pencatatan atau dokumentasi hasil scanning jaringan keamanan	Lakukan dokumentasi setelah pelaksanaan scanning disertai waktu pelaksanaan dan hasil scanning.
Strategi DRP terhadap Serangan *Hacker*	
Strategi DRP	**Keterangan**
Identifikasi situasi terhadap pelaporan pada gangguan email PLN	Melakukan identifikasi saat terjadi gangguan pada email PLN untuk mengatahui penyebab gangguan
Pengamanan aset TI/ SI	Lakukan upaya backup dan pengamanan terhadap set TI/ SI
Pemeriksaan terhadap gangguan	Untuk mengetahui keadaan pada gangguan jaringan internet PLN dan mengetahu penyebab pasti pada gangguan email PLN. Apabila gangguan terjadi karena penyalahgunaan hak akses, maka diperlukan tindakan terhadap pelaku. Pemeriksaan ini dapat dilakukan dengan melakukan pelaksanaan *nmap*.
Penindakan pelaku	Penindakan pelaku berdasarkan pada kebijakan yang telah disampaikan pihak PLN
Strategi Korektif pada Gangguan Jaringan Internet	
Strategi DRP	**Keterangan**

Melakukan evaluasi prosedur keamanan, manajemen akun	Evaluasi prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Evaluasi terhadap tingkat keamanan pada firewall	Hal ini bertujuan untuk mengetahui celah keamanan dari keamanan pada jaringan internet
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait yaitu peningaktan atau perbaikan celah keamanan jaringan internet
Pengujian dan monitoring hasil perbaikan	Melakukan pengujian dan evaluasi pada hasil perbaikan

Strategi Keberlangsungan Bisnis terhadap Gangguan Jaringan Internet		
Penyebab Risiko Kegagalan : Terputusnya Kabel LAN ID Strategi : Network 02		
Strategi DRP Terputusnya Kabel LAN		
Strategi Preventif	**Tujuan Strategi Preventif**	**Keterangan**
Penyusunan **Kebijakan Pengkabelan dan Peralatan Listrik**	Sebagai acuan dalam penyusunan prosedur operasional terhadap pengkabelan	Prosedur pengkabelan ini dapat mengacu pada standar ISO *ISO 27002:2005 9.2.3 Cabling Security* dan langkah implementasi yang telah dilaksanakan Department of Energy United States terhadap pelaksanaan standar FISMA bagian *Power Equipment and Cabling* .

Penyusunan **Prosedur Pengkabelan dan Peralatan Listrik**	Sebagai pedoman bagi pemasangan, perlindungan, serta pemasalahan pengkabelan yang terkait dengan sumber listrik, jaringan internet serta jaringan telepon.	Berikut merupakan contoh metode yang dapat diterapkan pada prosedur pemasangan: • Adanya pemisahan jalur kabel listrik dengan kabel yang lain secara fisik (*Power Equipment and Cabling 9 FISMA – Implementasi pada DOE United States*) • Adanya identifikasi khusus pada tiap jenis kabel (kabel listrik, kabel telepon, kabel LAN) seperti identifikasi warna atau identifikasi isolator pembungkus kabel untuk membedakan kabel agar memberikan kemudahan saat mengidentifikasi pada kejadian gangguan. (*ISO 27002:2005 9.2.3 Cabling Security*)
Strategi DRP terhadap Terputusnya Kabel LAN		
Strategi DRP		**Keterangan**

Pemeriksaan penyebab gangguan	Saat menerima laporan mengenai gangguan SCADA, lakukan identifikasi terhadap penyebab gangguan tersebut, lalu selanjutnya akan dilakukan pengamanan dan antisipasi lebih lanjut pada pihak yang bertanggung jawab.
Melakukan *restorasi* data dan informasi yang telah di *backup* secara otomatis	Melakukan upaya untuk mengambil data yang telah diback up sebelumnya dari sistem SCADA.
Strategi Korektif pada Terputusnya Kabel LAN	
Strategi Korektif	**Keterangan**
Melakukan evaluasi prosedur penanganan gangguan dari log dokumentasi insiden	Evaluasi kejadian, frekuensi kejadian dan prosedur penanganan gagguan dan dokumentasi insiden kejadian ganguan yang dituliskan oleh tim DRP
Melakukan perbaikan terhadap gangguan terkait	Melakukan upaya perbaikan untuk penanganan gangguan terkait, misalnya seperti kasus tidak ketersediaan listrik mencoba untuk melakukan perbaikan komponen atau ketersediaan jaringan listrik.

LAMPIRAN G
Gambaran Umum Modul Pelatihan dan Pengujian

1. Gambaran Umum Modul Pelatihan

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS**
Nama Pelatihan	Pelatihan Alur Komunikasi BCP PT PLN (Persero) APD Jateng dan DIY
Jenis Pelatihan	Sosialisasi dan praktik
Deskripsi Pelatihan	
Pelatihan ini bertujuan untuk memberi pengetahuan umum dan teknis mengenai *Business Continuity Plan* yang berbasis padar risiko TI yang digunakan oleh tiap proses bisnis dalam perusahaan. Dengan adanya pelatihan ini diharapkan dapat memberikan wawasan pada obyek peneilitan mengenai hal umum dan teknis pelaksanaan *Business Continuity Plan* yang berbasis padar risiko TI.	
Sasaran Pelatihan	Staf SCADA dan Telekomunikasi
Materi Umum	
Dalam pelatihan ini akan diberikan materi yaitu sebagai berikut : • Latar belakang perlunya *Business Continuity Planning* bagi perusahaan • Tujuan pelaksanaan *Business Continuity Planning* bagi perusahaan • Alur kerja *Business Continuity Planning* untuk PT PLN (Persero) APD Jateng dan DIY	

• Prosedur tiap tahap dalam alur kerja BCP • Alur komunikasi BCP untuk PT PLN (Persero) APD Jateng dan DIY

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS**
Nama Pelatihan	Pelatihan Prosedur Manajemen Akun
Jenis Pelatihan	Sosialisasi dan praktik
Deskripsi Pelatihan	
Pelatihan ini bertujuan untuk memberikan pengetahuan pada objek pelatihan mengenai ketentuan dan prosedur untuk manajemen akun. Dengan adanya pelatihan ini diharapkan dapat memberikan wawasan pada objek peneilitan mengenai ketentuan dan prosedur pelaksanaan manajemen akun.	
Sasaran Pelatihan	Seluruh Staff PT PLN (Persero) APD Jateng dan DIY
Materi Umum	
Dalam pelatihan ini akan diberikan materi yaitu sebagai berikut : • Latar belakang perlunya manajemen akun oleh tiap elemen organisasi • Tujuan dari adanya prosedur dan ketentuan manajemen akun • Bentuk prosedur dan ketentuan manajemen akun	

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS**
Nama Pelatihan	Pelatihan Penanganan Gangguan Server
Jenis Pelatihan	Sosialisasi dan praktik
Deskripsi Pelatihan	
Pelatihan ini bertujuan untuk memberi pengetahuan umum dan teknis respon dan penanganan pertama yang harus dilakukan saat terjadi gangguan server. Hal ini dilakukan agar tim penanganan gangguan dapat dengan segera melakukan tindakan saat terjadi gangguan pada server	
Sasaran Pelatihan	Staf SCADA dan Telekomunikasi
Materi Umum	
Dalam pelatihan ini akan diberikan materi yaitu sebagai berikut : • Pembagian peran pada saat gangguan server • Prosedur penanganan • Monitoring server • Solusi penanganan gangguan server	

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS**

Nama Pelatihan	Pelatihan Penanganan Gangguan Jaringan
Jenis Pelatihan	Sosialisasi dan praktik
Deskripsi Pelatihan	
Pelatihan ini bertujuan untuk memberi pengetahuan umum dan teknis respon dan penanganan pertama yang harus dilakukan saat terjadi gangguan jaringan. Hal ini dilakukan agar tim penanganan gangguan dapat dengan segera melakukan tindakan saat terjadi gangguan pada jaringan	
Sasaran Pelatihan	Staf SCADA dan Telekomunikasi
Materi Umum	
Dalam pelatihan ini akan diberikan materi yaitu sebagai berikut : • Pembagian peran pada saat gangguan jaringan • Prosedur penanganan pada gangguan jaringan • Monitoring terhadap jaringan internet • Solusi penanganan gangguan jaringan internet	

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS**
Nama Pelatihan	Pelatihan Penanganan Gangguan Aplikasi
Jenis Pelatihan	Sosialisasi dan praktik
Deskripsi Pelatihan	

Pelatihan ini bertujuan untuk memberi pengetahuan umum dan teknis respon dan penanganan pertama yang harus dilakukan saat terjadi gangguan aplikasi. Hal ini dilakukan agar tim penanganan gangguan dapat dengan segera melakukan tindakan saat terjadi gangguan pada aplikasi sehingga poses bisnis utama tidak mengalami gangguan yang menyebabkan berkurangnya produk dan layanan serta terganggunya proses bisnis internal.	
Sasaran Pelatihan	Staf SCADA dan Telekomunikasi
Materi Umum	
Dalam pelatihan ini akan diberikan materi yaitu sebagai berikut : • Daftar dan jenis aplikasi yang diguankan pada tiap proses bisnis • Pembagian peran pada saat gangguan aplikasi • Prosedur penanganan pada gangguan aplikasi • Monitoring terhadap aplikasi • Solusi penanganan gangguan aplikasi	

2. Gambaran Umum Modul Pengujian

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PENGUJIAN KEBERLANJUTAN BISNIS**
Pengujian	Pengujian kerentanan jaringan internet (*Penetration Testing*) – melakukan uji perlawanan terhadap keamanan sistem

Pelaku dan pembagian peran	1. Pelaku penyalahguna	: diperankan oleh 1 staff scada dan telekomunikasi
	2. Dokumentator pelaksanaan	: diperankan oleh 1 staff scada dan telekomunikasi
	3. Pengawas	: Asisten Manajer SCADA dan telekomunikasi
	4. Pihak tim DRP	: diperankan oleh 1 staff scada dan telekomunikasi
Skenario pengujian	1. Persiapkan prosedur perencanaan pada *security assesment* 2. Lakukan percobaan dengan sql injection pada tiap fitur aplikasi 3. Tim melakukan pencatatan kerentanan fitur 4. Tim DRP melakukan perbaikan sistem terhadap kerentanan keamanan 5. Dokumentator pelaksana mendokumen-tasikan hasil perbaikan sistem	

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PEN-GUJIAN KEBERLANJUTAN BISNIS**	
Pengujian	Penanganan Gangguan Tidak Tersedianya Jaringan Listrik	
Pelaku dan pembagian peran	1. Pencatat hasil pengujian	: diperankan oleh 1 staff scada dan telekomunikasi
	2. Pengarah	: Asisten Manajer SCADA dan telekomunikasi
	3. Pelaksana atau tim DRP	: diperankan oleh 1 staff scada dan telekomunikasi

Skenario pengujian	1. Tim DRP melakukan pemeriksaan terhadap server yang tidak dapat beroperasi 2. Tim DRP melaporkan gangguan pada AsMan SCADA dan Telekomunikasi 3. Tim DRP melakukan backup power dan keberlangsungan proses bisnis utama 4. Tim DRP melakukan pengamatan terhadap masa hidup sumber daya pada genset 5. Dokumentator pelaksana mendokumentasikan hasil pengujian BCP

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PENGUJIAN KEBERLANJUTAN BISNIS**	
Pengujian	Uji Back up dan restore data	
Pelaku dan pembagian peran	4. Pencatat hasil pengujian	: diperankan oleh 1 staff scada dan telekomunikasi
	5. Pengarah	: Asisten Manajer SCADA dan telekomunikasi
	6. Pelaksana atau tim DRP	: diperankan oleh 1 staff scada dan telekomunikasi
Skenario pengujian	1. Staff melakukan prosedur backup data secara manual 2. Staff melakukan prosedur restore data secara manual	

	3. Pencatat melakukan dokumentasi dengan format hari, tanggal, waktu dan keberhasilan

PT. PLN (PERSERO)	**GAMBARAN UMUM MODUL PENGUJIAN KEBERLANJUTAN BISNIS**	
Pengujian	Keberhasilan konfigurasi dan instalasi SCADA	
Pelaku dan pembagian peran	1. Pencatat hasil pengujian	: diperankan oleh 1 staff scada dan telekomunikasi
	2. Pengarah	: Asisten Manajer SCADA dan telekomunikasi
	3. Pelaksana atau tim DRP	: diperankan oleh 1 staff scada dan telekomunikasi
Skenario pengujian	1. Staff melakukan prosedur instalasi yang tlah ditetapkan 2. Staff memastikan bahwa pada setiap fitur dapat berjalan dengan baik 3. Pencatat melakukan dokumentasi dengan format hari, tanggal, waktu dan keberhasilan	

LAMPIRAN H
Validasi Kesesuaian Alur Kerja BCP

SURAT KONFIRMASI
Kesesuaian Alur Kerja *Business Continuity Plan* (BCP)
Untuk PT PLN (Persero) APD Jateng dan DIY

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama : Azmi Afifah Zahra
NRP : 5212100140
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian alur kerja *Business Continuity Plan* (BCP) untuk PT PLN (Persero) APD Jateng dan DIY kepada Asisten Manager SCADA dan Telekomunikasi PLN APD Jateng dan DIY.

Atas perhatian dan kesediaan Bapak/ Ibu, saya ucapkan terima kasih

PERSETUJUAN KONFIRMASI Semarang, Juni 2016	
Mengetahui, Asisten Manager SCADA dan Telekomunikasi PT PLN (Persero) APD Jateng dan DIY Angga Rajasa, S.Kom	Peneliti Tugas Akhir Azmi Afifah Zahra

LAMPIRAN I
Validasi Kesesuaian Identifikasi dan Analisis Risiko TI

SURAT KONFIRMASI

Kesesuaian Hasil Analisis Risiko *Continuity Plan* (BCP)
Untuk PT PLN (Persero) APD Jateng dan DIY

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama : Azmi Afifah Zahra
NRP : 5212100140
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis risiko TI untuk keperluan penyusunan *Business Continuity Plan* (BCP) untuk PT PLN (Persero) APD Jateng dan DIY kepada Asisten Manager SCADA dan Telekomunikasi PLN APD Jateng dan DIY.

Atas perhatian dan kesediaan Bapak/ Ibu, saya ucapkan terima kasih

PERSETUJUAN KONFIRMASI Semarang, Juni 2016	
Mengetahui, Asisten Manager SCADA dan Telekomunikasi PT PLN (Persero) APD Jateng dan DIY Angga Rajasa, S.Kom	Peneliti Tugas Akhir Azmi Afifah Zahra

LAMPIRAN J
Validasi Kesesuaian Analisis Dampak Bisnis

SURAT KONFIRMASI

Kesesuaian Hasil Analisis Dampak Bisnis *Business Continuity Plan* (BCP)
Untuk PT PLN (Persero) APD Jateng dan DIY

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama : Azmi Afifah Zahra
NRP : 5212100140
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis dampak bisnis untuk keperluan penyusunan *Business Continuity Plan* (BCP) untuk PT PLN (Persero) APD Jateng dan DIY kepada Asisten Manager SCADA dan Telekomunikasi PLN APD Jateng dan DIY.

Atas perhatian dan kesediaan Bapak/ Ibu, saya ucapkan terima kasih

PERSETUJUAN KONFIRMASI Semarang, Juni 2016	
Mengetahui, Asisten Manager SCADA dan Telekomunikasi PT PLN (Persero) APD Jateng dan DIY Angga Rajasa, S.Kom	Peneliti Tugas Akhir Azmi Afifah Zahra

LAMPIRAN K
Validasi Hasil Akhir BCP

SURAT KONFIRMASI
Kesesuaian Hasil Analisis Risiko *Continuity Plan* (BCP)
Untuk PT PLN (Persero) APD Jateng dan DIY

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama : Azmi Afifah Zahra
NRP : 5212100140
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis risiko TI untuk keperluan penyusunan *Business Continuity Plan* (BCP) untuk PT PLN (Persero) APD Jateng dan DIY kepada Asisten Manager SCADA dan Telekomunikasi PLN APD Jateng dan DIY.

Atas perhatian dan kesediaan Bapak/ Ibu, saya ucapkan terima kasih

PERSETUJUAN KONFIRMASI Semarang, Juni 2016	
Mengetahui, Asisten Manager SCADA dan Telekomunikasi PT PLN (Persero) APD Jateng dan DIY Angga Rajasa, S.Kom	Peneliti Tugas Akhir Azmi Afifah Zahra

LAMPIRAN L
Kebijakan Penyusunan Strategi Keberlangsungan Bisnis

PT PLN (Persero) APD Jateng dan DIY berkomitmen untuk melaksanakan alur dan strategi keberlangsungan bisnis sebagai bentuk penanggulangan dampak dari risiko TI yang mengancam proses bisnis. Perusahaan berusaha untuk memberikan pelayanan kepada masyarakat dengan produk energi listrik yang handal dan melaksanakan perencanaan keberlangsungan bisnis berbasis pada risiko teknologi informasi perusahaan dengan cara:

1. Mematuhi persyaratan atau peraturan perundang-undangan yang berkaitan dangan mutu, lingkungan dan K3.
2. Mendefinisikan keterkaitan setiap proses bisnis dengan persetujuan atau konfirmasi dari pihak manajemen PT PLN (Persero) APD Jateng dan DIY bahwa keterkaitan proses bisnis telah sesuai.
3. Menetapkan wewenang dan tanggung jawab kepada jajaran SDM PT PLN (Persero) APD Jateng dan DIY untuk menjamin pelaksanaan strategi keberlangsungan bisnis.
4. Menetapkan kritikalitas risiko teknologi informasi berdasarkan penilaian FMEA (*Failure Mode Effect Analysis*) serta penilaian dampak bisnis berdasarkan pada penilaian klasifikasi dampak pada aspek- aspek yang telah ditetapkan pada buku prosedur penyusunan profil risiko yang telah ditetapkan PT PLN.
5. Melakukan perawatan dan penyelamatan pada aset kritis TI berdasarkan prosedur strategi keberlangsungan bisnis terhadap risiko TI perusahaan.
6. Prosedur strategi keberlangsungan bisnis yang disusun berdasarkan pada aset kritis TI dengan prioritas utama yang memiliki nilai risiko *high* dan *medium*.

Referensi:

a. ISO 27002:2005, Manajemen Keamanan Sistem Informasi.
b. Buku Prosedur Penyusunan Profil Risiko dan Kajian Risiko PT PLN.

Semarang, ... 2016
PLN (Persero) APD Jateng dan DIY

Manager

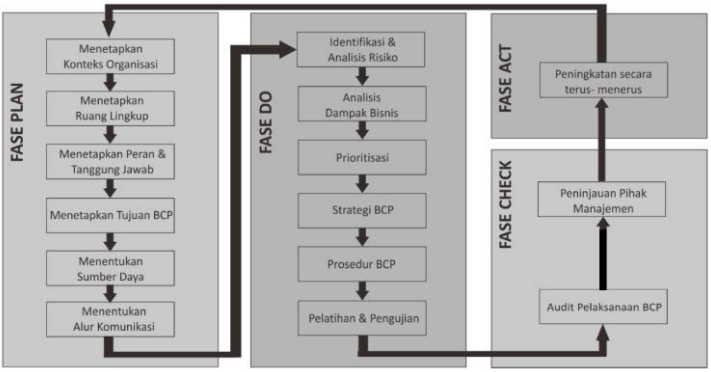
BAB VII
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan mengenai kesimpulan dan saran dari keseluruhan proses dan hasil pengerjaan Tugas Akhir yang telah dilakukan.

7.1 Kesimpulan

Berdasarkan penjelasan latar belakang yang dikemukakan di atas, rumusan masalah yang menjadi fokus utama dalam usulan tugas akhir ini adalah:

1. Hasil dari analisis kritikalitas bisnis menunjukkan bahwa terdapat 6 proses bisnis pada PT PLN (Persero) APD Jateng dan DIY memiliki risiko tinggi dalam kritikalitas bisnis perusahaan. Diantaranya adalah proses bisnis operasional, proses bisnis pengelolaan data dan gambar, proses bisnis persiapan operasi SCADA, proses bisnis Remote Terminal Unit, serta proses bisnis pemeliharaan korektif. Sedangkan pada proses bisnis yang memiliki dampak kritikalitas risiko pada level medium adalah pasa proses bisnis perencanaan, proses bisnis pemeliharaan intensif, serta proses bisnis power dan meter. Sedangkan pada kritikalitas bisnis dengan level *low* adalah pada proses bisnis keuangan, administrasi dan K3, serta kesiapan SDM.
2. Hasil analisis dari prioritisasi pada aset TI berdasarkan pada penilaian dampak bisnis dan penilaian risiko aset TI menunjukkan bahwa terdapat 6 aset TI yang dijadikan sebagai prioritas utama dalam keberlangsungan bisnis, yaitu SCADA, emali PLN, Server, jaringan internet, serta data perusahaan.
3. Hasil perancangan alur kerja untuk PT PLN (Persero) APD Jateng dan DIY adalah sebagai berikut:



Gambar 7.1 Hasil Perancangan Alur Kerja BCP PLN APD Jateng dan DIY

4. Hasil akhir dari rekomendasi strategi (terdapat pada sub bab 6.2.4 dan sub bab 6.2.5) untuk perencanaan keberlangsungan bisnis pada penelitian Tugas Akhir ini menunjukkan bahwa PT PLN (Persero) APD Jateng dan DIY membutuhkan beberapa pelaksanaan strategi dan prosedur terkait pelaksanaan keberlangsungan bisnis. Beberapa contoh prosedur yang perlu dilakukan adalah prosedur konfigurasi dan integrasi sistem SCADA serta prosedur penanganan gangguan pada sistem SCADA yang mengacu pada strategi SCADA 01 yaitu strategi preventif dari risiko kesalahan konfigurasi SCADA. Contoh lainnya adalah prosedur pengkabelan, prosedur terhadap emergency power, prosedur *backup* data yang mengacu pada strategi SCADA 03 untuk risiko tidak tersedianya jaringan listrik. Setiap strategi dan prosedur yang direkomendasikan pada penelitian Tugas Akhir ini telah sesuai dengan acuan standar ISO 27002 dan penerapan dari DOE United States.

DAFTAR PUSTAKA

[1] R. A. Wibawanti, "Pemeliharaan Remote Station SCADA di PT PLN (Persero) APD Jateng," *Jurnal Teknologi,* 2013.

[2] D. d. C. Alves, "Business Continuity Management (BCM) Applied to Transpetro's National Operational Control Center - CNCO," *Journal of Computer Science,* 2015.

[3] S. K, "Guide to Industrial Control Systems (ICS) Security," *Journal of Computer Science,* 2011.

[4] F. Gibb, "A framework for business continuity management," *Journal of Computer Science,* 2005.

[5] G. P. Pertiwi, "Kerangka Kerja Business Continuity Plan (BCP) Teknologi Informasi Perusahaan Studi Kasus : PDAM Kota Surabaya," 2015.

[6] A. Alisia, "Konsep Penyusunan Kerangka Kerja Business Continuity Plan Teknologi dan Sistem Informasi," *Jurnal Sistem Informasi,* 2012.

[7] S. L. Putri, "Perancangan Kerangka Kerja Business Continuity Plan untuk Teknologi Informasi pada Studi Kasus STIE PERBANAS," *Jurnal Teknik,* 2016.

[8] Basyaid, "Manajemen Risiko Organisasi," 2007.

[9] ISO 3100, "ISO 3100 - Risk Management," 2015.

[10] E. Blokdijk, "Risk Management," 2008.

[11] Software Engineering Institute, Operationally Critical Threat, Assets, and Vulnerability Evaluation (OCTAVE) Framework Version 1.0, Canada: SEI Carnegie Mellon University, 1999.

[12] J. Marshall, An Introductioan to Failure Modes Effects and Critically Analysisi (FMEA), Canada, 2012.

[13] P. Ravesh, Business Continuity Plan, Tata Concultancy Service, 2002.

[14] ISACA, "ISACA," 2002. [Online]. Available: https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjigKqL8JHLAhUHGY4KHeb0CF0QFgg2MAM&url=http%3A%2F%2Fwww.isaca.org%2Fgroups%2Fprofessional-english%2Fbusiness-continuity-disaster-recovery-planning%2Fgroupdocuments%. [Accessed 2016].

[15] ISO 22317, ISO 22317, 2015 ed., Stockholm: SIS, 2015.

[16] PT PLN (Persero), "Rencana Jangka Panjang 2014 - 2018," PT PLN (Persero), Jawa Tengah, 2014.

[17] PT PLN (Persero), "Prosedur Penyusunan Profil Risiko dan Kajian Risiko," PT PLN (Persero), Jakarta, 2014.

[18] ISO 22301, ISO 22301, USA, 2012.

[19] C. Brooks, Disaster Recovery Strategy with Tivoli Storage Management, United States: IBM Redbooks, 2002.

[20] United States Department of Energy, "Energy Sector-Specific Plan," Homeland Security, North America, 2010.

[21] Chubu Electric Power Group, Annual Report, Nagoya, 2013.

[22] PT PLN (Persero) APD Jateng dan DIY, Rencana Jangka Panjang PLN APD Jateng dan DIY, Semarang, 2013.

[23] Pertamina RU IV, Business Impact Analysis, Cilacap, 2015.

[24] ISO, ISO 27002, ANSI, 2005.

[25] NIST, Security and Privacy Controls for Federal Information Systems and Organizations, United States: US Department of Commerce, 2013.

BIODATA PENULIS

Penulis lahir pada 3 Maret 1994 di kota Semarang. Penulis dibesarkan oleh orang tua yang selalu mendukung dan memberikan motivasi dalam hidup penulis, mereka adalah Bapak Sumardjiyono dan Ibu Mamik Haryani. Pendidikan formal yang pernah ditempuh oleh penulis sebelum menempuh pendidikan di Jurusan Sistem Informasi ITS adalah SD Rejosari 02 Semarang, SMP Negeri 3 Semarang, dan SMA Negeri Semarang.

Selain menggeluti berbagai aktifitas dan kewajiban akademik, selama ini penulisjuga mengikuti kegiatan akademik untuk melatih *soft skill* dan meningkatkan jalinan saliturahmi dengan sesama. Diantaranya yaitu mengikuti pelatihan LKMM TD, pelatihan LKMM TM, serta memangku amanah sebagai staff OSR BEM FTIf, asisten dirjen Kementerian SOSMAS BEM ITS Kolaborasi, serta sekretaris kementerian SOSMAS BEM ITS Berani.

Saran- saran atau kritik dari penyusunan Tugas Akhir ini maupun untuk penulis, secara langsung dapat melalui alamat email azmiafifahzahra@gmail.com atau azmi12@mhs.is.its.ac.id.