TUGAS AKHIR – KS 141501

FORMULASI STRATEGI UNTUK ACUAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (BCP) BERBASIS TEKNOLOGI INFORMASI DI PT. PERTAMINA REFINERY UNIT IV CILACAP

ULVI RAHMA ISNAINI
NRP 5212100017

Dosen Pembimbing
Dr. Apol Pribadi S., S.T., M.T.
Dito Anggodo Prihastomo, S.T.

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

FINAL PROJECT – KS 141501

STRATEGY FORMULATION FOR BUSINESS CONTINUITY PLAN (BCP) BASED ON INFORMATION TECHNOLOGY IN PT. PERTAMINA REFINERY UNIT IV CILACAP

ULVI RAHMA ISNAINI
NRP 5212100017

Supervisor
Dr. Apol Pribadi S., S.T., M.T.
Dito Anggodo Prihastomo, S.T.

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

LEMBAR PENGESAHAN

FORMULASI STRATEGI UNTUK ACUAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (BCP) BERBASIS TEKNOLOGI INFORMASI DI PT. PERTAMINA REFINERY UNIT IV CILACAP

TUGAS AKHIR

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

Oleh:

ULVI RAHMA ISNAINI
5212 100 017

Surabaya, Juli 2016

KETUA
JURUSAN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M. Kom.
NIP. 196503101991021001

LEMBAR PERSETUJUAN

FORMULASI STRATEGI UNTUK ACUAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (BCP) BERBASIS TEKNOLOGI INFORMASI DI PT. PERTAMINA REFINERY UNIT IV CILACAP

TUGAS AKHIR

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

Oleh :

ULVI RAHMA ISNAINI
5212 100 017

Disetujui Tim Penguji : Tanggal Ujian : Juli 2016
Periode Wisuda : September 2016

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

Dito Anggodo Prihastomo, S.T. **(Pembimbing II)**

Ir. Ahmad Holil Noor Ali, M.Kom. **(Penguji I)**

Hanim Maria Astuti, S.Kom., M.Sc. **(Penguji II)**

FORMULASI STRATEGI UNTUK ACUAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (BCP) BERBASIS TEKNOLOGI INFORMASI DI PT. PERTAMINA REFINERY UNIT IV CILACAP

Nama Mahasiswa : ULVI RAHMA ISNAINI
NRP : 5212 100 017
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing I : Dr. Apol Pribadi S., S.T., M.T.
Dosen Pembimbing II : Dito Anggodo Prihastomo, S.T.

ABSTRAK

Tugas akhir ini membahas mengenai pembuatan dokumen business continuity plan (BCP) pada studi kasus PT. Pertamina Refinery Unit IV Cilacap. Ketergantungan PT. Pertamina RU IV akan aplikasi online, penggunaan internet dan informasi up to date yang digunakan untuk pengambilan keputusan dan menjalankan operasional bisnis sehari-hari menjadi latar belakang dalam pembuatan tugas akhir ini. Business continuity plan sendiri merupakan salah satu solusi terbaik untuk menjamin keberlangsungan kegiatan operasional bisnis perusahaan yang pada akhirnya akan berdampak pada meningkatnya kualitas layanan perusahaan kepada pelanggan.

Elemen yang ada dalam dokumen BCP PT. Pertamina RU IV ditentukan dengan mengacu pada best practice ISO 22301:2012 tentang Business Continuity Management Systems (BCMS), best practice ISO 27031:2011 terkait Business Continuity in ICT, dan penelitian sebelumnya mengenai pembuatan model kerangka kerja BCP. Langkah-langkah pengembangan yang dilakukan mulai dari risk assessment, business impact analysis, sampai dengan pembuatan strategi BCP. Data diperoleh melalui analisis dokumen, observasi, dan wawancara dengan pihak management untuk mendapatkan pengetahuan mengenai risiko apa saja yang

mungkin dihadapi, proses bisnis mana yang kritis untuk keberlangsungan organisasi, dan strategi apa yang dapat diimplementasikan untuk menjamin keberlangsungan bisnis di PT. Pertamina Refinery Unit IV Cilacap.

Hasil dari penelitian ini diharapkan dapat memberikan panduan bagi perusahaan terkait perancangan BCP yang sesuai dengan kebutuhan dan kondisi perusahaan. Hasil dari dokumen BCP juga diharapkan dapat memberikan informasi bagi perusahaan terkait identifikasi risiko teknologi informasi dan penilaian dampak bisnis, serta rencana berbasis teknologi informasi yang harus diterapkan sebagai upaya untuk mempertahankan keberlanjutan operasional bisnis yang ada di PT. Pertamina RU IV. Hasil dari penelitian ini juga menunjukkan bahwa implementasi BCP pada sebuah perusahaan merupakan suatu hal yang unik, karena disesuaikan dengan kebutuhan dan kondisi yang ada pada masing-masing perusahaan.

Kata kunci: Business Continuity Plan (BCP), Business Impact Analysis (BIA), ISO 22301:2012, ISO 31000:2009, Risiko Teknologi Informasi

STRATEGY FORMULATION FOR BUSINESS CONTINUITY PLAN (BCP) DOCUMENT BASED ON INFORMATION TECHNOLOGY IN PT. PERTAMINA REFINERY UNIT IV CILACAP

Name	**: ULVI RAHMA ISNAINI**
NRP	**: 5212 100 017**
Department	**: Information Systems FTIF -ITS**
Supervisor I	**: Dr. Apol Pribadi S., S.T., M.T.**
Supervisor II	**: Dito Anggodo Prihastomo, S.T.**

ABSTRACT

This final project is discussing about creating business continuity plan (BCP) in PT. Pertamina Refinery Unit IV Cilacap. The company's high dependency of online application, the use of internet and up to date information that used to make decision and run daily business operation are the backgrounds of this research. Business continuity plan is the best solution to ensure the sustainability of the company's business operation that will ultimately have an impact on increasing the quality of service that provide by the company to costumer.

Elements that contains in BCP's document of PT. Pertamina RU IV is conducted in accordance of best practice ISO 22301:2012 about Business Continuity Management Systems's (BCMS), best practice ISO 27031:2011 about Business Continuity in ICT, and previous research about framework of BCP. This research was conducted with the method that begins with risk assessment, business impact analysis through desingning the BCP. Data obtained through document's analysis and interview to management to gain knowledge about any IT risk that may be

encountered by the company, business process that critical to the sustainability of the organization, and what strategies that can be implemented to ensure the business continuity in PT. Pertamina Refinery Unit IV Cilacap.

The result of this research are expected to provide guidance for the design of BCP that related to company's needs and condition. Also to provide information that related to risk identification, assessment of business impact, and the plans based on information technology that should be applied to maintain continuity of business operations in PT. Pertamina Refinery Unit IV. The result of this study also showed that the implementation of the BCP in company is a something unique, where each implementation should be adjusted to the business continuity requirements of the company.

Keywords : Business Continuity Plan (BCP), Business Impact Analysis (BIA), ISO 22301:2012, ISO 31000:2009, Information Technology Risk

DAFTAR ISI

DAFTAR TABEL

Halaman ini sengaja dikosongkan

DAFTAR GAMBAR

DAFTAR LAMPIRAN

Berikut ini adalah lampiran dokumen dari penelitian ini. Dokumen-dokumen ini dapat dijadikan sebagai bukti dari pengerjaan penelitian ini. Hasil selengkapnya dari penelitian ini disampaikan dalam dokumen produk perusahaan.

KODE LAMPIRAN	LAMPIRAN
A	Validasi Hasil Analisis Risiko
B	Validasi Dokumen Akhir BCP PT. Pertamina Refinery Unit IV Cilacap
C	Interview Protocol sub-fungsi IT RU IV
D	Interview Protocol sub-fungsi Business Operation and Technology
E	Interview Protocol sub-fungsi Business Support and Infrastructure

Halaman ini sengaja dikosongkan

Halaman ini sengaja dikosongkan

BAB I
PENDAHULUAN

Pada bagian ini akan dijelaskan mengenai latar belakang masalah, rumusan masalah, batasan masalah dan tujuan penelitian yang mendasari penelitian tugas akhir.

1.1 Latar Belakang

Sejak tahun 2012 hingga saat ini, PT. Pertamina telah menjadi produsen minyak dan gas besar di Indonesia di antara korporasi asing seperti Chevron, Total, Conoco Phillips, BP, Exxon Mobil, dsb dengan total produksi sebesar 462 mmboe/d [1]. Dengan produksi sebesar itu, PT. Pertamina bertransformasi menjadi salah satu lokomotif perekonomian bangsa yang bergerak di bidang energi meliputi minyak, gas serta energi baru dan terbarukan.

PT. Pertamina RU IV sebagai salah satu unit pengolahan Pertamina memegang peranan penting dalam menjaga pasokan minyak nasional hingga mencapai 33,3% dari seluruh produksi minyak nasional [2]. Angka tersebut merupakan yang paling besar jika dibandingkan dengan unit-unit pengolahan lainnya. Dengan produksi sebesar itu, Pertamina RU IV harus berusaha untuk menjaga keberlansungan bisnisnya. Salah satu strategi yang mendukung tujuan ini adalah pemanfaatan teknologi informasi (TI). Peranan TI dalam keberlangsungan bisnis di RU IV secara garis besar mencakup layanan operasi komunikasi serta layanan operasi komputer. Adanya ketergantungan proses bisnis di RU IV terhadap layanan TI tentu saja membawa implikasi tersendiri dimana muncul risiko bagi perusahaan apabila terjadi gangguan terhadap layanan TI, baik dari sisi alam, manusia, ataupun secara sistem [2]. Di PT. Pertamina RU IV sendiri, implementasi TI dapat dikatakan sudah meyeluruh. PT. Pertamina RU IV memiliki ketergantungan yang tinggi terhadap aplikasi online, penggunaan internet dan informasi *up to date* yang digunakan untuk pengambilan keputusan dan menjalankan operasional bisnis rutin.

Hal ini dibuktikan dengan hasil dari analisa *business impact analysis* (BIA) tahun 2015 yang menyatakan bahwa lima fungsi bisnis kritikal di PT. Pertamina RU IV memiliki ketergantungan tinggi terhadap layanan TI.

Pada PT. Pertamina RU IV, terutama pada fungsi TI, mulai menyadari akan pentingnya sebuah *business continuity plan*. Kebutuhan dan kepentingan perusahaan akan BCP tentu saja berbeda-beda bergantung dari jenis usahanya. Pada beberapa perusahaan, kebutuhan akan BCP terlihat jelas, terutama pada perusahaan yang memiliki ketergantungan tinggi pada TI dalam menjalankan proses bisnisnya [2]. Perusahaan jenis ini akan mensyaratkan *continuous availability* yang merupakan subset dari BCP yang juga dikenal sebagai *zero-downtime*. Hal ini dikarenakan *cost* dari ketika sebuah sistem tidak berjalan (*down*) sesaat saja akan jauh lebih besar jika dibandingkan biaya investasi perancangan sebuah BCP.

Susan Snedaker [3] mengemukakan hubungan antara biaya perencanaan sebuah BCP dengan biaya yang harus ditanggung oleh perusahaan akibat kegagalan bisnis yang disebabkan oleh bencana. Dari penelitian yang dilakukan oleh Cummings, Haag & McCubbrey pada tahun 2005 terhadap perusahaan yang mengalami kehilangan data skala besar tanpa memiliki BCP didapatkan data sebagai berikut: 43% dari perusahaan ini tidak pernah dibuka kembali, 51% dari perusahaan tersebut ditutup dalam jangka waktu 2 tahun lamanya dan hanya 6% dari perusahaan tersebut yang dapat bertahan dalam jangka waktu yang lama.

PT. Pertamina RU IV membutuhkan sebuah *business continuity plan* (BCP) berbasis teknologi informasi sebagai salah satu aspek yang mendukung keberlanjutan proses bisnis perusahaaan. BCP yang dimiliki setiap perusahaan berbeda-beda tergantung dari kebutuhan yang dimiliki oleh perusahaan, dan hal ini sejalan dengan pendapat Susan Snedaker [3].

1.2 Perumusan Masalah

Dari pemaparan latar belakang dapat ditarik rumusan masalah sebagai berikut:

1. Apa saja elemen atau konten dalam dokumen BCP PT. Pertamina Refinery Unit IV Cilacap?
2. Apa hasil identifikasi risiko teknologi informasi di PT. Pertamina Refinery Unit IV Cilacap?
3. Untuk mendukung pembuatan dokumen BCP, strategi apa yang dapat dijadikan acuan oleh PT. Pertamina Refinery Unit IV Cilacap?

1.3 Batasan Masalah

Dari permasalahan yang disebutkan di atas, batasan masalah dalam tugas akhir ini adalah sebagi berikut:

1. Analisa dampak bisnis mengacu kepada hasil *business impact analysis* (BIA) tahun 2015 yang disusun oleh peneliti saat melakukan kerja praktek.
2. Acuan yang digunakan dalam melakukan analisa risiko adalah ISO 31000:2009, yang menitikberatkan pada fase *risk assessment*.
3. Proses pengerjaan BCP hanya berfokus pada:
   - Proses bisnis kritis (jika proses bisnis terganggu di atas 1 s/d 3 jam akan menurunkan kapasitas olah menjadi s/d 80% atau jika proses bisnis terganggu 1 s/d 3 jam akan mengalami kerugian materiil Rp. 250.000.000 s/d Rp. 1.000.000.000)
   - Risiko TI yang bernilai *very high* (memiliki nilai *risk priority number*≥200) dan risiko yang bernilai *high* (memiliki nilai *risk priority number* diantara 120-199)
4. Strategi BCP yang berupa mitigasi risiko TI mengacu pada standar ISO 27002:2005, *best practice bandwith management* oleh Cisco, dan *best practice high-availability application* dari Microsoft.

5. Strategi DRP yang dibuat terbatas pada strategi pencadangan *(backup)* dan strategi pemulihan *(restore)* untuk aplikasi non-ERP di PT. Pertamina RU IV.

1.4 Tujuan Tugas Akhir

Tujuan yang diharapkan dari penelitian tugas akhir ini antara lain adalah:

1. Mengetahui apa saja elemen dalam dokumen BCP PT. Pertamina Refinery Unit IV
2. Menghasilkan identifikasi risiko dan penilaian risiko pada teknologi informasi di PT. Pertamina Refinery Unit IV
3. Mengetahui strategi apa yang dapat dijadikan acuan oleh PT. Pertamina Refinery Unit IV untuk membuat dokumen BCP

1.5 Manfaat Kegiatan Tugas Akhir

Manfaat yang dapat diperoleh dari pengerjaan tugas akhir ini akan ditinjau dari dua aspek sebagai berikut:

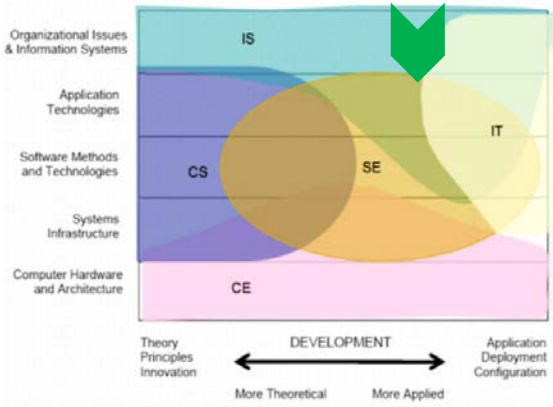
a. Manfaat bagi PT. Pertamina Refinery Unit IV
   Strategi yang dihasilkan diharapkan dapat digunakan sebagai acuan untuk PT. Pertamina Refinery Unit IV dalam membuat dokumen perencanaan keberlangsungan bisnis.
b. Manfaat Akademis
   Penelitian ini diharapkan dapat memperkaya pengetahuan dan dapat dijadikan referensi dalam formulasi strategi untuk pengembangan dokumen *business continuity* plan (BCP) di industri non perbankan di Indonesia.

1.6 Relevansi

Penelitian tugas akhir ini berupa pembuatan dokumen b*usiness continuity plan* (BCP) berdasarkan kondisi kekinian dan kebutuhan perusahaan. Penelitian ini dikatakan layak sebagai tugas akhir tingat S1 karena merupakan bentuk penyelesaian permasalahan nyata yang dihadapi oleh PT. Pertamina Refinery

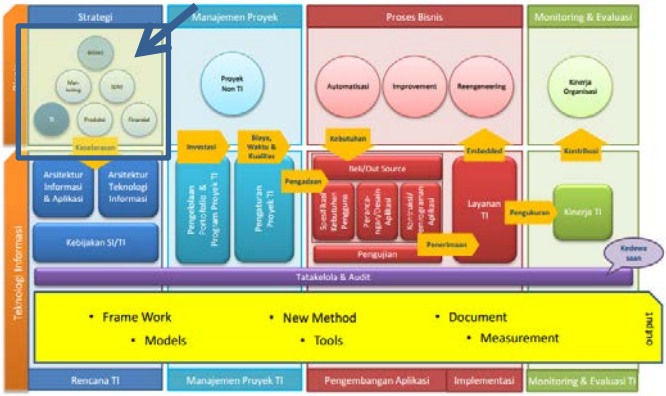
Unit IV Cilacap. Dokumen *business continuity plan* (BCP) ini akan menjadi salah satu solusi dalam mencegah kelumpuhan sistem dan teknologi informasi serta operasional bisnis perusahaan yang pada akhirnya berdampak pada meningkatnya kualitas layanan perusahaan kepada pelanggan.

Dalam 13 topik/area penelitian bidang Sistem Informasi berdasarkan data 1.615 paper [4], penelitian ini masuk ke dalam bidang penelitian Manajemen TI (*IT Management*) dan Manajemen Risiko (*Risk Management*) sebab membantu pihak perusahaan dalam merencanakan dan mengelola aset-aset TI yang ada dalam perusahaan mereka agar keberlangsungan bisnisnya bisa tetap berjalan. Disamping itu, penelitian ini erat hubungannya dengan manajemen risiko (*risk management*) karena menjadi salah satu bagian dalam proses pembuatan dokumen BCP (*business continuity plan*). Pada peta penelitian sistem informasi, topik ini terletak di pertengahan antara teori dan penerapan karena penelitian ini menghubungkan antara teori *best practice* dengan penerapan studi kasus perusahaan. Untuk lebih jelasnya, penelitian ini berada pada posisi seperti gambar di bawah ini:



Gambar 1.1 Peta Penelitian Sistem Informasi (Sumber : SI ITS)

Sedangkan dalam *roadmap* lab MSI Jurusan Sistem Informasi, topik penelitian ini masuk ke dalam area strategi bisnis, karena membantu PT. Pertamina Refinery Unit IV dalam menyusun rencana untuk keberlansungan bisnis mereka.



Gambar 1.2 Road Map Laboratorium MSI (Sumber : SI ITS)

Jika dilihat dari sisi pembelajaran, mata kuliah Jurusan Sistem Informasi yang terkait dengan penelitian ini adalah perencanaan keberlangsungan bisnis dan manajemen risiko.

BAB II
TINJAUAN PUSTAKA

Bab ini akan menjelaskan pustaka atau literatur yang digunakan selama penelitian ini.

2.1 Studi Sebelumnya

Dalam pengerjaan tugas akhir ini, akan digunakan beberapa penelitian sebelumnya sebagai pedoman dan referensi penerjaan. Pada tabel di bawah ini akan dijelaskan deskripsi, hasil, dan hubungan dari penelitian-penelitian sebelumnya dan hubungannya dengan tugas akhir ini.

Tabel 2.1 Penelitian Sebelumnya (Sumber: Peneliti)

IT Service Continuity : Achieving Embeddedness Through Planning [5]	
Nama Peneliti	Marko Niemimma dan Joanna Jarvelainen
Tahun Penelitian	2013
Hasil Penelitian	Dalam penelitian ini menjelaskan langkah-langkah dalam pembuatan *business continuity plan* berbasis teknologi informasi secara general dan bisa diaplikasikan pada hampir seluruh perusahaan. Selain itu, dalam hasil penelitian juga dipaparkan bagaimana cara pengaplikasian BCP ke manajemen perusahaan.
Hubungan penelitian dengan Tugas Akhir	Hasil dari penelitian ini dapat memberikan gambaran terkait bagaimana langkah-langkah pembuatan *business continuity plan* (BCP) berbasis teknologi informasi, dan hal-hal penting (*critical path*) apa yang harus diwaspadai oleh peneliti selama proses pengerjaan tugas akhir ini.
Kerangka Kerja Business Continuity Plan (BCP) untuk Teknologi Informasi Perusahaan	

Studi Kasus : PDAM Kota Surabaya [6]	
Nama Peneliti	Giovanni Prastisukma
Tahun Penelitian	2015
Hasil Penelitian	Penelitian ini menghasilkan kerangka kerja BCP berbasis risiko yang sesuai dengan kondisi PDAM kota Surabaya dan dokumen produk BCP PDAM Kota Surabaya. Dalam pembuatan kerangka kerja BCP, peneliti mengacu pada beberapa standar, antara lain ISO 22301:2012, Cobit 5 (DSS04 : *Manage Continuity*), dan *best practice* kerangka BCP PDAM kota Padang.
Hubungan penelitian dengan Tugas Akhir	Hasil dari penelitian ini dapat memberikan gambaran terkait dengan langkah-langkah formulasi kerangka kerja BCP yang mengacu pada beberapa *standard* dan *best practice* dari perusahaan sejenis.

2.2 Dasar Teori

2.2.1 Risiko

Risiko adalah kemungkinan kejadian atau keadaan yang dapat mengancam pencapaian tujuan dan sasaran organisasi. Definisi resiko menurut ISO (ISO Guide 31000:2009, p9) adalah suatu efek dari ketidakpastian dalam pencapaian suatu tujuan. Mereka menambahkan bahwa efek tersebut bisa bersifat negatif maupun positif, yang merupakan penyimpangan dari sesuatu yang sudah diekspektasikan sebelumnya [7]. Sedangkan menurut William Heins (2011) risiko adalah variansi dari hasil yang terjadi selama periode tertentu dan pada kondisi tertentu. Sehingga risiko tidak dapat dipastikan kapan terjadinya, namun dapat dilihat kemungkinan terjadinya [8].

Menurut PMBOK (*Project Management Body of Knowledge*), risiko adalah sebuah kejadian yang tidak pasti dan tidak dapat diprediksi, atau sebuah kondisi yang apabila terjadi, akan menimbulkan efek setidaknya pada satu tujuan proyek. Tujuan proyek tersebut adalah ruang lingkup (*scope*), penjadwalan proyek (*schedule*), biaya proyek (*cost*), dan kualitas dari proyek yang sedang dikerjakan (*quality*) [9].

Perlu adanya penjelasan mengenai perbedaan antara *risk* (risiko) dengan *uncertainty* (ketidakpastian). Dimana, setiap risiko adalah ketidakpastian, namun tidak semua ketidakpastian adalah risiko. Selain itu, risiko dapat dipelajari cara munculnya, sedangkan ketidakpastian tidak dapat dipelajari, karena bisa muncul secara tiba-tiba.

2.2.1.1 Komponen Risiko

Menurut Talabis dan Martin J, risiko adalah situasi yang memperlihatkan dimana suatu objek menjadi berbahaya. Risiko merupakan suatu pengukuran ketidakpastian. Dalam risiko terdiri dari beberapa komponen, yang terdiri dari *event, asset, outcome,* dan *probability*.

2.2.1.1.1 Event

Event adalah sebuah peluang atau situasi dimana hal tersebut mungkin untuk terjadi, namun tidak dapat dipastikan kejadiannya. *Event* dalam konteks penilaian risiko melihat dari kejadian yang akan datang. Identifikasi *event* merupakan salah satu kunci aktivitas dalam proses penilaian risiko. Dalam proses penilaian risiko, *event-event* risiko dapat berpotensi menjadi ancaman.

2.2.1.1.2 Asset

Aset adalah sumber daya ekonomi yang dikuasai dan/atau dimiliki oleh organisasi sebagai akibat dari peristiwa masa lalu dan

dari mana manfaat ekonomi dan sosial di masa depan diharapkan dapat diperoleh, baik dari pemerintah maupun masyarakat, serta dapat diukur dalam satuan uang, termasuk sumber daya non keuangan yang diperlukan untuk penyediaan jasa bagi masyarakat umum dan sumber-sumber daya yang dipelihara.

Salah satu jenis aset adalah aset informasi. Aset informasi merupakan bagian inti dari aset teknologi informasi. Aset informasi berisikan data dan informasi yang relevan dengan proses bisnis pada suatu organisasi. Aset informasi pada penelitian ini meliputi komponen-komponen pendukung yang meliputi:

1. Orang *(people)*
   Dalam tugas akhir ini komponen yang akan diidentifikasi adalah pengguna aplikasi yang ada di proses bisnis organisasi tersebut.

2. Data
   Dalam dunia teknologi informasi, yang disebut data adalah individu dalam sebuah database, yang disimpan dalam basis data untuk keperluan penyediaan informasi dalam tujuannya untuk mendukung perusahaan dalam menjalankan proses operasional.

3. Perangkat keras *(hardware)*
   Mencakup piranti fisik, seperti komputer, printer, dan monitor. Perangkat ini berperan sebagai media penyimpanan dalam sistem informasi. Setiap perushaaan yang memiliki teknologi informasi yang maju pasti memiliki perangkat keras dalam jumlah yang banyak.

4. Perangkat lunak *(software)*
   Merupakan sekumpulan instruksi yang dapat mempengaruhi kinerja perangkat keras dan memproses data. Tujuan perangkat ini adalah untuk mengolah,

menghitung, dan memanipulasi data agar menghasilkan informasi yang berguna.

5. Jaringan *(network)*
   Merupakan sistem penghubung yang memungkinkan suatu sumber yang digunakan bersamaan dalam waktu dan tempat yang berbeda-beda.

Kemudian kelima komponen tersebut saling menyatu dan berinteraksi sehingga dapat berfungsi sebagai pendukung dan penyedia kebutuhan informasi dalam rangka pengambilan keputusan yang lebih baik.

2.2.1.1.3 Outcome

Outcome merupakan suatu dampak dari event risiko yang terjadi. *Outcome* dari risiko akan selalu merugikan organisasi sebagai akibat dari peristiwa masa lalu dan dari mana manfaat ekonomi dan sosial di masa depan diharapkan dapat diperoleh, baik dari pemerintah maupun masyarakat

2.2.1.1.4 Probability

Probability merupakan peluang terjadinya suatu risiko di masa depan. Tujuan dari penilaian risiko adalah untuk mengukur suatu kemungkinan atau *likelihood* dari event risiko yang akan terjadi di masa depan.

Berikut merupakan keterkaitan hubungan dan interaksi antara keempat komponen risiko yang telah dijelaskan sebelumnya hingga menjadi risiko.

Gambar 2.1 Keterkaitan Komponen Risiko (Sumber: Talabis, Martin J)

Ancaman yang terdiri dari suatu aksi dan non-aksi yang timbul sebagai bentuk negatif dari situasi yang tidak diinginkan. **Kerentanan** adalah sebuah kelemahan atau faktor lingkungan luar yang dapat meningkatkan kemungkinan atau *likelihood* terjadinya ancaman. **Dampak** adalah *outcome* yang berpotensi untuk memicu terjadinya kehilangan atau kerugian akibat adanya ancaman dan kerentanan yang terjadi.

Gambar 2.2 Interaksi Komponen Risiko (Sumber: Talabis, Martin J)

2.2.1.2 Risiko Teknologi Informasi / Sistem Informasi

Teknologi informasi adalah penggunaan mesin dan program elektronik yang digunakan untuk memproses, menyimpan, mengirim, dan menyajikan informasi [10]. Sedangkan sistem informasi adalah kombinasi dari orang, *hardware*, *software*, jaringan komunikasi, data, kebijakan dan prosedur yang menyimpan, mengambil, merubah, dan menyebarkan informasi dalam sebuah organisasi [11].

Implementasi IT/IS di sebuah perusahaan pasti menimbulkan risiko. Risiko tersebut meliputi semua ketidakpastian kejadian yang muncul akibat implementasi IT/IS dalam sebuah organisasi atau perusahaan.

2.2.2 Manajemen Risiko

Manajemen risiko merupakan bagian kegiatan yang digunakan untuk melakukan penilaian, mitigasi risiko dan pengembangan strategi untuk mengurangi dampak yang dihasilkan dari risiko tersebut.

Menurut ISO 31000:2009, manajemen risiko adalah sebuah aktivitas yang terkoordinir untuk menjalankan dan mengawasi sebuah perusahaan atau organisasi dengan pendekatan risiko [12].

Manajemen risiko adalah sebuah bidang ilmu yang membahas bagaimana sebuah perusahaan atau organisasi dapat menerapkan ukuran dalam melakukan pemetaan permasalahan dengan pendekatan manajemen secara komprehensif dan sistematis [13]. Sedangkan menurut *Institute of Risk Management* (IRM) menjelaskan bahwa manajemen risiko adalah sebuah proses yang bertujuan untuk membantu organisasi atau perusahaan dalam memahami, mengevaluasi, dan mengambil tindakan untuk risiko-risiko yang muncul, dengan meningkatkan kemungkinan untuk berhasil dan mengurangi kemungkinan kegagalan.

Sehingga dapat disimpulkan bahwa manajemen risiko adalah proses pengelolaan risiko dalam sebuah organisasi atau perusahaan dengan tujuan untuk meminimalisasi risiko yang mungkin muncul.

2.2.2.1 Manajemen Risiko Teknologi Informasi/Sistem Informasi

Teknologi informasi sudah menjadi bagian penting dari sebuah organisasi dalam menjalankan aktivitas operasional dan pengambilan keputusan strategis dalam sebuah perusahaan. Dalam satu dekade terakhir perkembangan teknologi informasi sangat

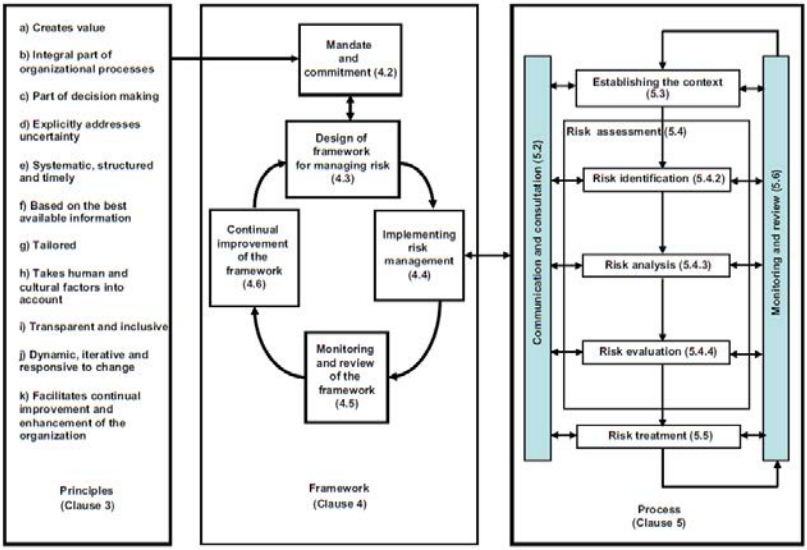
pesat. Hal ini secara tidak langsung menjadikan teknologi informasi sebagai ancaman dan kesempatan untuk sebuah organisasi. Berdasarkan pemahaman itulah, muncul sebuah kebutuhan pengelolaan risiko dalam implementasi teknologi informasi.

Menurut ISACA (2006), manajemen risiko teknologi informasi adalah proses pengidentifikasian *vulnerabilities* (kerentanan) dan ancaman terhadap sumber daya informasi yang digunakan perusahaan untuk mencapai tujuan bisnis [14]. Manajemen risiko teknologi informasi juga digunakan untuk menentukan langkah mitigasi yang harus diambil oleh perusahaan untuk mencegah terjadinya risiko. Manajemen risiko merupakan aksi yang terintegrasi yang mendukung proses bisnis perusahaan dan dapat menghasilkan strategi yang mendukung mitigasi risiko yang terjadi pada organisasi yang bersangkutan.

2.2.3 Framework ISO 31000

ISO 31000:2009, *Risk Management – Principles and Guidelines*, menyediakan prinsip, kerangka kerja, dan proses yang dapat digunakan untuk mengelola risiko [15]. ISO 31000 ini bersifat generik, dapat diaplikasikan ke hampir semua organisasi tanpa memandang ukuran organisasi, aktivitas, ataupun sektor. Penggunaan ISO 31000 dapat membantu organisasi dalam mencapai tujuan, meningkatkan kesempatan untuk menghadapi ancaman, dan mengalokasikan sumber daya untuk menghadapi risiko yang mungkin muncul.

Secara garis besar, pemaparan manajemen risiko dalam ISO 31000 memiliki tiga bagian utama, yaitu prinsip, kerangka kerja dan proses.



Gambar 2.3 Hubungan antara Prinsip, Kerangka, dan Proses Manajemen Risiko (Sumber: ISO 31000)

Berikut merupakan penjelasan beberapa aspek yang terdapat di ISO 31000:

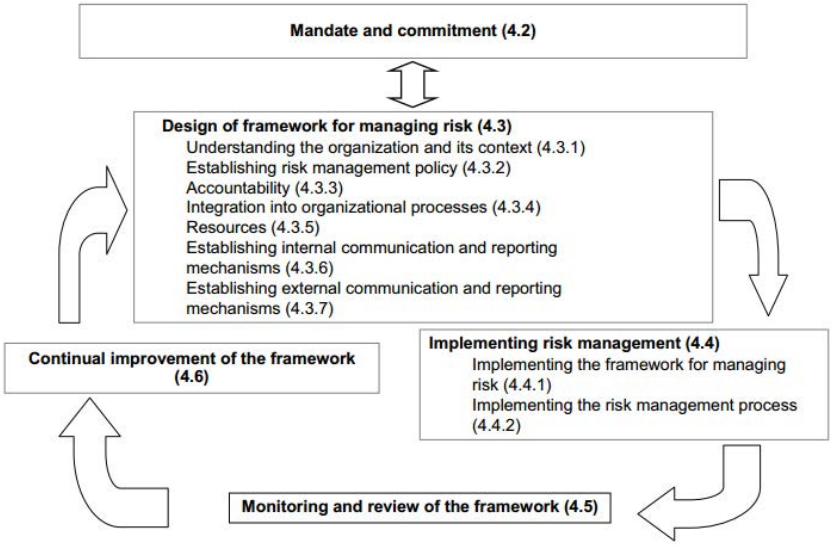
2.2.3.1 Prinsip

Untuk penerapan manajemen risiko yang efektif, organisasi harus patuh terhadap prinsip-prinsip sebagai berikut:

a. Manajemen risiko menciptakan nilai tambah (*creates value*)
b. Manajemen risiko adalah bagian integral proses dalam organisasi (*an integral part of all organizational processes*)
c. Manajemen risiko adalah bagian dari pengambil keputusan (*part of decision making*)
d. Manajemen risiko secara eksplisit menangani ketidakpastian (*explicitly addresses uncertainty*)
e. Manajemen risiko bersifat sistematis, terstruktur, dan tepat waktu (*systematic, structured, and timely*)

f. Manajemen risiko berdasarkan informasi terbaik yang tersedia (*based on the best available information*)
g. Manajemen risiko dibuat sesuai kebutuhan (*tailored*)
h. Manajemen risiko memperhitungkan faktor manusia dan budaya (*takes human and cultural factors into account*)
i. Manajemen risiko bersifat transparan dan inklusif (*transparent and inclusive*)
j. Manajemen risiko bersifat dinamis, iterative, dan responsive terhadap perubahan (*dynamic, iterative, and responsive to change*)
k. Manajemen risiko memfasilitasi perbaikan dan pengembangan berkelanjutan organisasi (*facilitates continual improvement and enhancement of the organization*)

2.2.3.2 Kerangka Kerja



Gambar 2.4 Hubungan antara Komponen dari Kerangka Kerja Manajemen Risiko (Sumber: ISO 31000)

Kerangka kerja ini bukan ditujukan untuk menentukan sistem manajemen, namun lebih kepada membantu organisasi dalam mengintegrasikan manajemen risiko pada keseluruhan sistem manajemen yang ada pada organisasi terkait. Namun demikian, organisasi harus mengadaptasi komponen yang terdapat dalam kerangka kerja ini dan disesuaikan dengan keinginan dan kebutuhan mereka. Berikut ini merupakan komponen dari kerangka kerja ISO 31000:

1. Pemberian mandat dan komitmen (*mandate and commitment*)
2. Perencanaan kerangka kerja manajemen risiko
3. Penerapan manajemen risiko
4. Monitoring dan *review* terhadap kerangka kerja manajemen risiko
5. Perbaikan kerangka kerja manajemen risiko secara berkelanjutan

2.2.3.2 Proses Manajemen Risiko

Proses manajemen risiko merupakan kegiatan yang kritikal dalam manajemen risiko karena merupakan penerapan dari prinsip-prinsip dan kerangka yang telah dibangun sebelumnya. Proses manajemen risiko yang terdapat pada ISO 31000:2009 terdapat pada klausa 5. Proses dan tahapan tersebut adalah sebagai berikut:

1. Umum
2. Komunikasi dan konsultasi
3. Menetapkan konteks
   3.1 Umum
   3.2 Menetapkan konteks eksternal
   3.3 Menetapkan konteks internal
   3.4 Menetapkan konteks dari proses manajemen risiko
   3.5 Mengembangkan kriteria risiko
4. Menilai risiko (*risk assessment*)
   4.1 Umum
   4.2 Identifikasi risiko

4.3 Analisis risiko
4.4 Evaluasi risiko
5. Perlakuan risiko (*risk treatment*)
5.1 Umum
5.2 Seleksi pilihan-pilihan perlakuan risiko
5.3 Persiapan dan implementasi rencana-rencana perlakuan risiko
6. Pemantauan dan peninjauan ulang (*monitoring and review*)
7. Perekaman atau pencatatan proses manajemen risiko

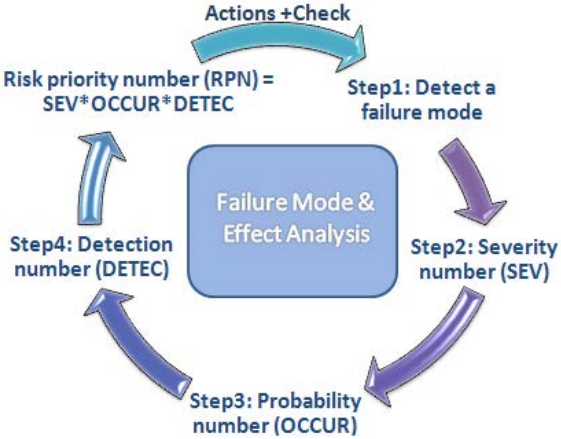
Pada penelitian ini fase yang digunakan sesuai dengan ISO 31000:2009 adalah fase penilaian risiko (identifikasi, analisis, dan evaluasi risiko). Fase inilah yang akan tercakup dalam kerangka kerja BCP yang sesuai dengan kebutuhan perusahaan studi kasus.

2.2.4 Metode *Failure Mode and Effect Analysis* (FMEA)

Failure Mode and Effect Analysis atau FMEA merupakan metode yang digunakan untuk melakukan identifikasi dan analisis suatu kegagalan beserta akibatnya. Tujuan dari FMEA adalah untuk menghindari terjadi kegagalan. Menurut Chrysler (1995), FMEA dapat dilakukan dengan cara:

1. Mengenali dan mengevaluasi kegagalan potensi suatu produk dan efeknya
2. Mengidentifikasi tindakan yang bisa menghilangkan atau mengurangi kesempatan dari potensi kegagalan
3. Pencatatan proses sehingga dokumen perlu di update secara teratur agar dapat digunakan untuk mencegah dan mengantisipasi terjadinya kegagalan

Proses yang dilakukan dalam penerapan FMEA adalah mengukur potensi terjadinya kegagalan tersebut melalui tiga komponen. Tahapan dari FMEA digambarkan pada diagram alur berikut [16] :



Gambar 2.5 Proses FMEA (Sumber: FMEA)

Komponen kegagalan tersebut antara lain:

1. *Severity* (tingkat keparahan) / *Impact*
   Tingkat keparahan merupakan pengukuran dalam memperkirakan subjektif numerik dari seberapa para pekerja/pihak ketiga/*customer* akan merasakan efek dari risiko yang terjadi.

Tabel 2.2 Kriteria Penilaian Severity (Sumber: FMEA)

Dampak	Dampak dari Efek	Rangking
Akibat berbahaya	Melukai pelanggan atau karyawan atau meningkatkan total biaya proyek lebih besar dari 25%	10
Akibat serius	Aktivitas yang ilegal atau meningkatkan total biaya proyek lebih besar dari 20%	9
Akibar ekstrim	Mengubah produk atau jasa menjadi tidak	8

Dampak	Dampak dari Efek	Rangking
	layak digunakan atau meningkatkan total biaya proyek sebesar 15%	
Akibat major	Menyebabkan ketidakpuasan pelanggan secara ekstrim atau meningkatkan total biaya proyek sebesar 10%	7
Akibat signifikan	Menghasilkan kerusakan parsial secara moderat atau meningkatkan total biaya proyek sebesar 5-10%	6
Akibat moderat	Menyebabkan perununan kinerja dan mengakibatkan kerugian atau meningkatkan total biaya proyek sebesar 5%	5
Akibat minor	Menyebabkan sedikit kerugian atau meningkatkan total biaya proyek sebesar <5%	4
Akibat ringan	Menyebabkan gangguan kecil yang dapat diatasi tanpa kehilangan sesuatu atau meningkatkan total	3

Dampak	Dampak dari Efek	Rangking
	biaya proyek sebesar <5%	
Akibat sangat ringan	Tanpa disadari : terjadi gangguan kecil pada kinerja atau tidak meningkatkan total biaya proyek	2
Tidak ada akibat	Tanpa disadari dan tidak mempengaruhi kinerja atau tidak meningkatkan total biaya proyek	1

2. *Occurance* (tingkat kejadian) / *Likelihood*
   Tingkat waktu adalah pengukuran dalam memperkirakan tentang probabilitas penyebab kemungkinan terjadinya risiko akan menghasilkan modus kegagalan yang menyebabkan akibat tertentu.

Tabel 2.3 Kriteria Penilaian Occurance (Sumber: FMEA)

Kemungkinan Kegagalan	Kemungkinan	Rangking
Very high: Kegagalan hampir/tidak dapat dihindari	Lebih dari satu kali tiap harinya	10
Very high: Kegagalan selalu terjadi	Satu kali setiap 3-4 hari	9
High: Kegagalan sering terjadi	Satu kali dalam seminggu	8
High:	Satu kali dalam sebulan	7

Kemungkinan Kegagalan	Kemungkinan	Rangking
Kegagalan sering terjadi		
Moderatly high: Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan	6
Moderate: Kegagalan terjadi sekali waktu	Satu kali setiap 6 bulan	5
Moderate low: Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relatif kecil	Satu kali dalam 1-3 tahun	3
Very low: Kegagalan terjadi relatif kecil dan sangat jarang	Satu kali dalam 3-6 tahun	2
Remote: Kegagalan tidak pernah terjadi	Satu kali dalam 6-50 tahun	1

3. *Detection* (deteksi) / *Cause*
   Tingkat deteksi, ini adalah seberapa besar tingkat risiko tersebut dapat dideteksi sebelumnya. Pengukuran ini merupakan sebuah penilaian subjektif numerik untuk dapat melakukan deteksi akan penyebab dari sebuah risiko dapat terjadi.

Tabel 2.4 Kriteria Penilaian Detection (Sumber: FMEA)

Dampak	Dampak dari Efek	Rangking
Hampir tidak mungkin	Tidak ada metode deteksi	10

Dampak	Dampak dari Efek	Rangking
Sangat kecil	Metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontigensi	9
Kecil	Metode deteksi tidak terbukti untuk mendeteksi tepat waktu	8
Sangat rendah	Metode deteksi tidak andal dalam mendeteksi tepat waktu	7
Rendah	Metode deteksi memiliki tingkat efektivitas yang rendah	6
Sedang	Metode deteksi memiliki efektivitas yang rata-rata	5
Cukup tinggi	Metode deteksi memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan	4
Tinggi	Metode deteksi memiliki kemungkinan tingga untuk dapat mendeteksi kegagalan	3
Sangat tinggi	Metode deteksi sangat efektif untuk dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontigensi	2
Hampir pasti	Metode deteksi hampir pasti dapat mendeteksi dengan waktu yang cukup	1

Dampak	Dampak dari Efek	Rangking
	untuk melaksanakan rencana kontigensi	

Ketiga komponen tersebut kemudian dibobotkan sehingga didapatkan hasil *Risk Priority Number* (RPN). RPN adalah hasil ukuran yang digunakan ketika menilai risiko untuk membantu mengidentifikasi "*critical failure modes*". Nilai RPN berkisar dari 1 (terbaik mutlak) hingga 1000 (absolut terburuk). Cara untuk melakukan perhitungan RPN adalah:

$$RPN = S \times O \times D$$

Keterangan:
S = *Severity number* (angka tingkat keparahan)
O = *Occurence number* (angka tingkat probabilitas kejadian)
D = *Detection number* (angka tingkat deteksi)

Setelah menghitung RPN maka langkah selanjutnya adalah dengan mengurutkan risiko dari RPN yang paling tinggi ke rendah. Nilai RPN tersebut kemudian diklasifikasikan berdasarkan level prioritas kesalahan yang memerlukan penanganan lanjut, sebagai berikut:

Tabel 2.5. RPN (Sumber: FMEA)

Level Risiko	Skala RPN
Very High	≥ 200
High	120-199
Medium	80-119
Low	20-79
Very Low	0-19

2.2.5 *Business Impact Analysis* (BIA)

Business Impact Analysis (BIA) merupakan suatu dokumen yang mengidentifikasi proses bisnis kritikal, perkiraan dampak bencana terhadap unit bisnis, dan kebutuhan sumber daya yang

diperlukan dalam pemulihan [17]. Dalam BIA, sumber daya kritis yang saling bergantung (*stakeholder*, produk, dan layanan utama) dan level kepentingannya terhadap aktivitas kritis (proses kunci dalam sebuah *valuechain*) dianalisis. Sementara itu, tujuan utama dari penggunaan BIA oleh semua organisasi adalah untuk mengoptimasi kinerja dari pemulihan dan waktu yang dibutuhkan untuk pemulihan ini. Menurut *Business Continuity Institute* (BCI), sebuah organisasi dalam BCMS dan sertifikasi, ada empat tujuan dari BIA, antara lain:

a. Mendapatkan pemahaman tentang tujuan organsiasi, prioritas dari masing-masing tujuan dan jangka waktu untuk melanjutkan kembali dari sebuah gangguan yang tidak direncanakan.
b. Menginformasikan keputusan manajemen mengenai *maximum tolerable outage* (MTO) dari setiap fungsi.
c. Menyediakan sumber daya informasi bagaimana sebuah strategi pemulihan yang sesuai dapat ditentukan/ direkomendasikan
d. Menguraikan ketergantungan yang ada baik dari internal maupun eksternal unuk mencapai tujuan bisnis.

2.2.5.1 Kerugian *Upstream* dan *Downstream*

Selain gangguan bisnis seperti banjir, gempa bumi, dsb., terdapat dampak tidak langsung yang harus dipertimbangkan, yaitu kerugian *upstream* dan kerugian *downstream* [3] yang akan dijelaskan sebagai berikut :

a. Kerugian *upstream* adalah kerugian yang terjadi ketika salah satu *supplier* utama terpengaruh oleh adanya bencana/gangguan dan perusahaan mengandalkan pengiriman regular dari produk atau layanan dari *supplier* utama tersebut. Hal ini akan menyebabkan perusahaan tidak dapat memberikan produk atau layanan meskipun perusahaan tersebut tidak mengalami bencana secara langsung.

b. Kerugian *downstream* adalah kerugian yang terjadi saat pelanggan utama atau lingkungan di sekitar perusahaan terpengaruh oleh bencana/gangguan, sementara perusahaan tidak menyediakan layanan yang kritis sehingga pelanggan utama lebih fokus pada bagaimana menangani dampak daripada menggunakan produk atau layanan yang disediakan oleh perusahaan.

2.2.5.2 *Impact Criticality*

Tujuan dilakukannya fase ini adalah untuk mengidentifikasi fungsi-fungsi mana yang kritis, mana yang penting, dan mana yang kurang penting sehingga bisa diabaikan atau ditunda proses pemulihannya. Pengelompokan kritikalitas proses bisnis dan kriterianya berdasarkan acuan konsultan Veda Praxis [17] dideskripsikan sebagai berikut :

Tabel 2.6 Kriteria Penilaian Kritikalitas Proses Bisnis Veda Praxis (Sumber: Pertamina RU IV)

Kategori Proses Bisnis	Dampak Operasional / Finansial	Keterangan
Kritikal	Dampak no 3 atau lebih tinggi pada saat proses bisnis terhenti dengan durasi waktu kurang dari 1 hari.	Dampak no. 3 adalah: OPR: Terganggu operasi di atas 1 s/d 3 jam dan atau kapasitas olah menjadi s/d 80%. atau FIN : Terjadi kerugian materiil Rp 250.000.000,00 s/d Rp 1.000.000.000,00
Moderat	Dampak no 3 atau lebih tinggi pada saat proses bisnis terhenti dengan durasi waktu lebih dari 1 hari hingga 7 hari	
Non Kritikal	Dampak no 3 atau lebih tinggi pada saat proses bisnis terhenti dengan	

Kategori Proses Bisnis	Dampak Operasional / Finansial	Keterangan
	durasi waktu lebih dari 7 hari	

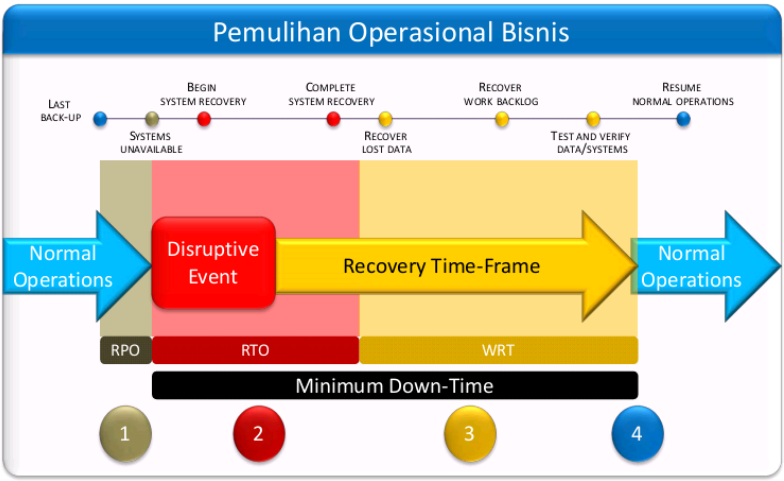
2.2.5.2 Kebutuhan Waktu Pemulihan

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

- ***Maximum torelable downtime* (MTD)**, yang pada beberapa literatur disebut juga sebagai *maximum tolerable period of distrupment* (MTPD) sesuai namanya adalah besar waktu maksimum sebuah bisnis dapat menoleransi ketidakadaan sebuah fungsi bisnis. Semakin kritis fungsi bisnis biasanya akan memiliki MTD yang semakin kecil.
- ***Recovery time objective* (RTO)** adalah maksimum waktu yang diperbolehkan untuk sebuah proses tidak beroperasi karena kejadian darurat. RTO adalah waktu yang digunakan untuk memulihkan layanan. Situasi untuk menandai mulai dan selesainya durasi RTO harus disepakati terlebih dahulu. RTO biasanya didefinisikan dalam satuan waktu jam.
- ***Work recovery time* (WRT)** adalah langkah-langkah tambahan yang perlu dilakukan supaya bisnis dapat berjalan kembali setelah sistem (perangkat lunak, perangkat keras, dan konfigurasi) dikembalian (*restore*)
- ***Recovery point objective* (RPO)** adalah maksimum durasi waktu yang diperbolehkan data aplikasinya hilang akibat tidak ter-*cover* oleh jadwal backup yang ditentukan. RPO didefinisikan dalam satuan waktu jam. Sebagai contoh jika sebuah perusahaan melakukan *backup* secara *realtime* maka dapat disimpulkan toleransi kehilangan data di perusahaan

tersebut hampir tidak ada. Sementara itu jika sebuah perusahaan melakukan *backup* setiap satu minggu sekali maka toleransi kehilangan data perusahaan tersebut maksimal adalah satu minggu.

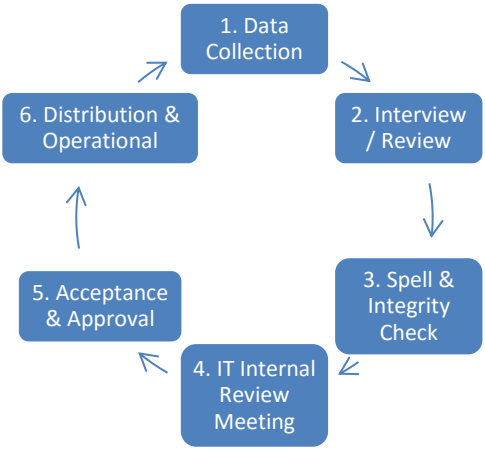
Berikut ini merupakan diagram yang menunjukkan hubungan antara keempat terminologi tersebut:



Gambar 2.6 Kerangka Waktu Pemulihan (Sumber: BIA 2015 RU IV)

2.2.5.3 Proses *Business Impact Analysis* (BIA)

Proses penyusunan BIA menurut kerangka kerja PT. Pertamina [18] digambarkan sebagai berikut :



Gambar 2.7 Langkah Pengerjaan BIA (Sumber: Pertamina)

Terdapat 6 langkah dalam penyusunan dokumen BIA menurut Pertamina, dimulai dari:

1. *Data Collection*
   IT menentukan secara lebih detil update data yang diperlukan dan mengumpulkan data terbaru dari dokumen yang tersedia
2. *Interview / Review*
   IT mereview update data dengan melakukan wawancara / mengumpulkan kuesioner dari *data owner*.
3. *Spell & Integrity Check*
   IT menyusun update data dan melakukan cek terkait integritas data dan tata bahasa
4. *IT Internal Review Meeting*
   IT melakukan rapat internal untuk mereview isi BIA dan merekomendasikan update data
5. *Acceptance & Approval*
   IT memproses persetujuan update data
6. *Distribution & Operational*
   IT mendistribusikan BIA yang telah update dan melakukan rekomendasi yang diperlukan sesuai hasil update isi BIA

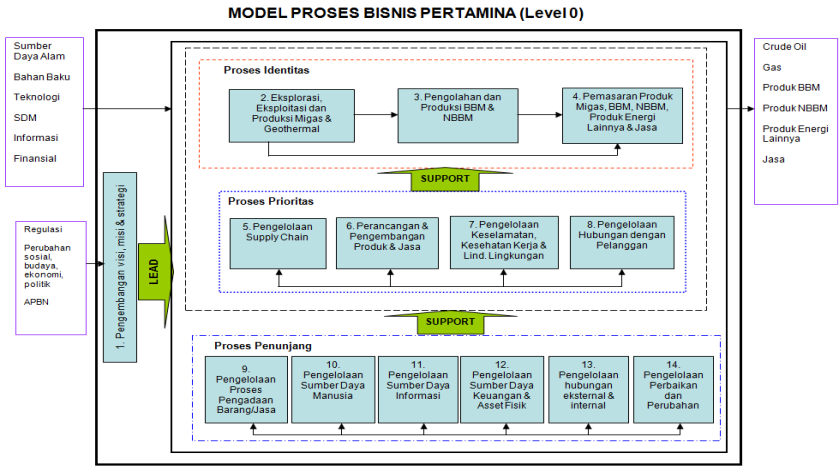
2.2.5.4 Hasil *Business Impact Analysis* (BIA) PT. Pertamina Refinery Unit IV 2015

2.2.5.4.1 Proses Bisnis

a. Identifikasi Proses Bisnis

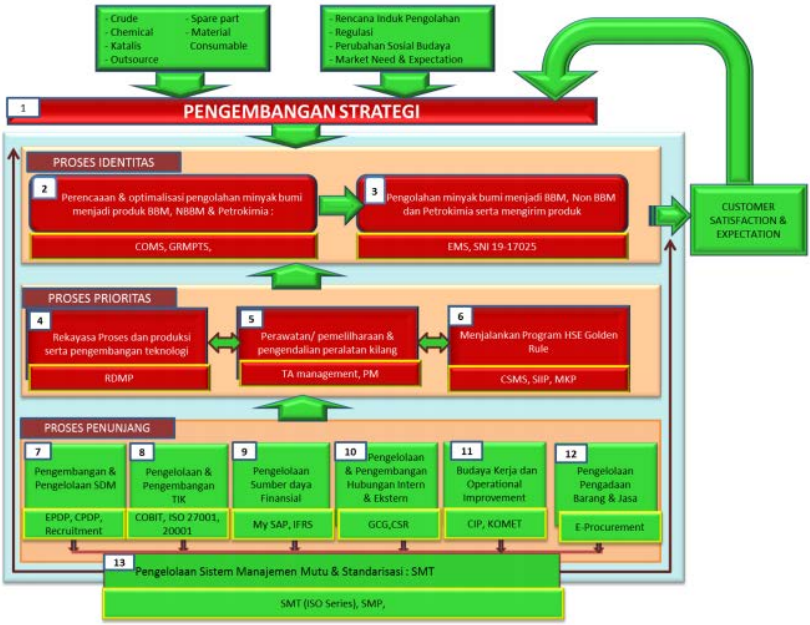
Proses bisnis Pertamina secara garis besar tertuang di SK Direksi No. Kpts-011/2007, terbagi menjadi 3 kelompok, yaitu proses identitas, proses prioritas, dan proses penunjang. Proses identitas meliputi:

1. Proses eksplorasi, eksploitasi, dan produksi migas & geothermal
2. Proses pengolahan dan produksi BBM & Non BBM
3. Pemasaran produk migas, BBM, non BBM, produk energi lainnya dan jasa



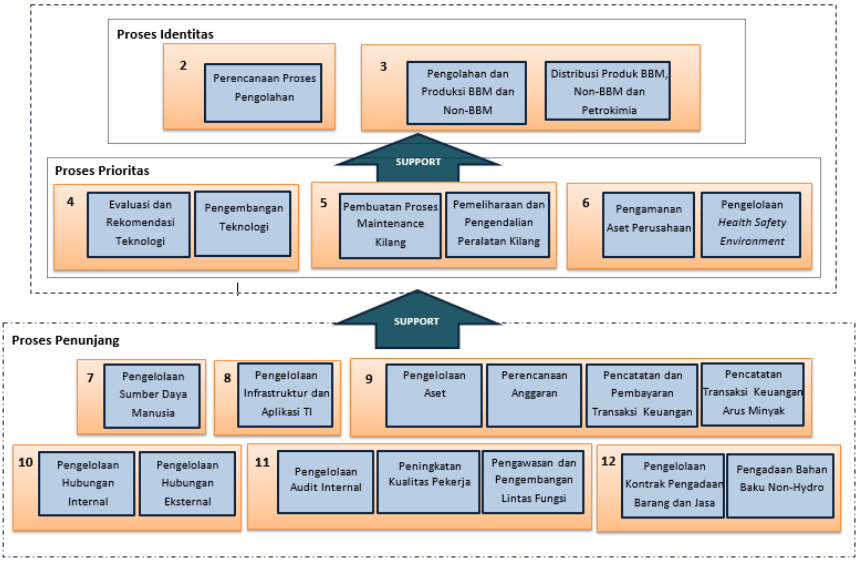
Gambar 2.8 Model Bisnis Pertamina Level 0 (Sumber: BIA 2015 RU IV)

Sedangkan menurut dokumen Pertamina Refinery Unit IV Quality Assessment Tahun 2014, proses bisnis yang ada di Pertamina Refinery Unit IV terbagi menjadi sebagai berikut :



Gambar 2.9 Model Bisnis Pertamina Level 1 (Sumber: BIA 2015 RU IV)

Setelah di-*break down* lebih kecil, proses bisnis di RU IV meliputi proses-proses sebagai berikut :



Gambar 2.10 Model Bisnis Pertamina Level 2 (Sumber: BIA 2015 RU IV)

Berikut merupakan penjelasan dari proses bisnis level 1 PT Pertamina (PERSERO) RU IV yang menjelaskan detail deskripsi, input kerja, output dan pembagian kerja tiap fungsi yang melaksanakan proses bisnis tersebut.

Tabel 2.7. Tabel Deskripsi Proses Bisnis level 1 PT Pertamina RU IV (Sumber: BIA 2015 RU IV)

No	Proses Bisnis	Sub Proses	Deskripsi	Funsgsi Terkait	Input	Output
1	Perencanaan Proses Pengolahan	Perencanaan Proses Pengolahan	Merencanakan proses pengolahan untuk prosuksi BBM, NBBM dan petrokimia	RPO		Perencanaan untuk proses pengolahan yang matang dan efisien, serta bahan baku minyak mentah yang siap diolah menjadi BBM, NBBM dan petrokimia
		Optimalisasi Proses Pengolahan	Melaksanakan tugas optimalisasi sehingga proses bisnis pengolahan minyak bumi dapat berjalan secara efisien	**Optimalisasi Proses Pengolahan** Shipping Kapal: Marine Quality Control: Production 2		
		Pengadaan Bahan Baku Hydrocarbon	Melaksanakan tugas pengadaan hydrocarbon sebagai bahan baku proses pengolahan minyak menjadi BBM. NBBM dan petrokimia	Procurement		
2	Pengolahan dan Produksi BBM dan non-BBM	Pengolahan dan produksi BBM	Melaksanakan proses operasional untuk produksi minyak bumi menjadi BBM	Production 1	Perencanaan untuk proses pengolahan yang matang dan efisien, serta bahan baku minyak	Produk BBM, NBBM dan petrokimia
		Pengolahan dan produksi NBBM	Melaksanakan proses operasional untuk produksi minyak bumi menjadi NBBM dan petrokimia	Production		

No	Proses Bisnis	Sub Proses	Deskripsi	Funsgsi Terkait	Input	Output
					mentah yang siap diolah menjadi BBM, NBBM dan petrokimia	
3	Distribusi Produk BBM, NBBM dan Petrokimia	Perencana Distribusi Produk BBM, NBBM dan Petrokimia	Melakukan perencanaan untuk pengiriman produk hasil olahan pada saluran distribusi	RPO	Data Distribusi Minyak	Laporan Perencanaan Distribusi
		Shipping Distribusi Produk BBM, NBBM dan Petrokimia	Mengirimkan produk hasil olahan pada saluran distribusi	Marine	Laporan Perencanaan Distribusi	Produk BBM, NBBM dan petrokimia yang telah didistribusikan
4	Evaluasi dan Rekomendasi Teknologi	Engineering Development	Melakukan analisa problem, spesifikasi kilang dan memastikan bahwa energi yang digunakan efisien	Engineering Development	Data Kilang	Laporan Efisiensi Kinerja kilang
5	Pengembangan Teknologi	Engineering Development	Melaksanakan proyek pengembangan kilang	Engineering Development	Data Proyek Pengembangan Kilang	Laporan Proyek Pengembangan Kilang
6	Pembuatan Program	General Planning	Merencanakan proses pemeliharaan dan perbaikan peralatan kilang baik secara	Reliability	Data Kilang	Perencanaan untuk Jadwal Peralatan

No	Proses Bisnis	Sub Proses	Deskripsi	Funsgsi Terkait	Input	Output
	Maintenance Kilang		insidential maupun pemeliharaan rutin pada refinery unit			kilang yang terawat dan terpelihara
		Specific Planning	Melakukan perencanaan proses pemeliharaan dan perbaikan peralatan kilang secaa lebih spesifik untuk pemeliharaan rutin dan insidentil pada refinery unit	MPS, TA		
7	Pemeliharaan dan Pengendalian Peralatan Kilang	Pemeliharaan rutin harian dan insidential	Melaksanakan proses pemeliharaan dan perbaikan peralatan kilang baik secara insidential maupun pemeliharaan rutin harian pada refinery unit	ME	Data Kilang	Peralatan kilang yang terawat dan terpelihara
		Pemeliharaan tahunan	Melaksanakan proses pemeliharaan dan perbaikan peralatan kilang baik secara rutin tahunan dan 4 tahunan pada refinery unit	TA		
8	Pengelolaan HSSE Golden Rule	Pengamanan Aset Perusahaan	Membuat perencanaan dan pengamanan aset perusahaan terhadap risiko keamanan aset	General Affair		Aset dan dokumen perusahaan yang disimpan dengan aman

No	Proses Bisnis	Sub Proses	Deskripsi	Funsgsi Terkait	Input	Output
		Pengelolaan Health Safety Environment	mempromosikan aspek HSSE pada seluruh fungsi agar proses operasi kilang berjalan lancar agar risiko kecelakaan kerja dapat diminimalisir	Leader dan kontrol pengamanan HSSE : HSE Pengaman area minyak di kapal dan lepas laut: Marine Penanganan K3: PHC		Personil kerja, lingkungan dan kegiatan operasional kilang yang aman dan sehat
9	Pengelolaan Sumber Daya Manusia	Pengelola: Human Resources	Mengelola sumber daya manusia dalam perusahaan dengan memberikan reward pada pekerja, penanganan TKJP, pengembangan karier serta kompetensi pekerja perusahaan	Pengelola: Human Resources	Data Pekerja Pertamina RU IV	Sumber daya manusia yang handal dan kompeten untuk kemajuan perusahaan
10	Pengelolaan Infrastruktur dan Aplikasi TI	Pelaksana : IT	Melakukan pengelolaan dan pengembangan untuk infrastruktur dan aplikasi teknologi informasi untuk efisiensi kinerja pada perusahaan	Pelaksana : IT	Data kebutuhan perbaikan atau layanan TI baru pada tiap fungsi bisnis	Infrastruktur dan layanan TI yang memadai dan memberikan efisiensi kerja pada proses bisnis dan risiko proses bisnis

No	Proses Bisnis	Sub Proses	Deskripsi	Funsgsi Terkait	Input	Output
11	Pengelolaan Aset	Pengelolaan aset dan material	Mengelola aset perusahaan yang berupa aset dan material milik perusahaan	Finance		Aset material dan aset fisik perusahaan yang aman dan taat pajak
		Pengelolaan aset fisik (tanah dan bangunan)	Mengelola aset fisik perusahaan yang berupa tanah dan bangunan milik perusahaan	Asset		
12	Perencanaan Anggaran	Finance	Mengelola keuangan perusahaan	Finance		Anggaran Keuangan perusahaan yang sesuai dengan kebutuhan bisnis
13	Pembayaran dan Pencatatan Transaksi Keuangan Umum	Finance	Mengelola dokumentasi pada proses transaksi keuangan	Finance		Dokumentasi Transaksi Keuangan
14	Pencatatan Transaksi Keuangan Arus Minyak	Finance dan RPO	Mengelola dokumentasi pada proses transaksi keuangan	Finance dan RPO		Dokumentasi Transaksi Keuangan
15	Pengelolaan Hubungan Internal	Publikasi informasi internal	Menyebarkan dan memberikan informasi mengenai kondisi proses bisnis internal RU IV	General Affair		Hubungan baik yang terjalin dengan pihak internal perusahaan

No	Proses Bisnis	Sub Proses	Deskripsi	Funsgsi Terkait	Input	Output
		Hubungan kerja internal	Mengelola dan meningkatkan hubungan dengan pihak industrial pada internal perusahaan	Human Resources		
16	Pengelolaan Hubungan Eksternal	Hubungan kontrak kerja eksternal	Mengelola dan meningkatkan hubungan dengan pihak eksternal perusahaan	Human Resources		Hubungan baik yang terjalin dengan pihak eksternal perusahaan
		Penanganan Kasus Pekerja	Mengambil tindakan untuk menghadapi adanya penanganan kasus pada pekerja terhadap pihak eksternal perusahaan	Legal		
17	Pengelolaan Audit Internal	Penetapan Standar	Menetapkan standar untuk pemberlakuan dalam penilaian audit performa kerja	Quality Management	Data operasional kerja tiap fungsi bisnis	Standard penilaian kinerja dan operasional perusahaan
		Pelaksanaan Audit	Melakukan audit dan penilaian performa kerja untuk mendapatkan evaluasi yang dapat dijadikan sebagai acuan untuk peningkatan budaya kerja dan operasional perusahaan	RIA		Evaluasi untuk peningkatan budaya kerja dan operasional perusahaan

No	Proses Bisnis	Sub Proses	Deskripsi	Funsgsi Terkait	Input	Output
18	Peningkatan Kualitas Pekerja	Peningkatan Kualitas Budaya Kerja	Memberikan program kerja untuk tiap pekerja di Pertamina RU IV dengan tujuan untuk memberikan motivasi peningkatan kerja dan menemukan inovasi baru untuk perusahaan	Pelaksana : OPI dan Quality Management		Program usulan dari pekerja untuk penignkatan kinerja RU IV
19	Pengawasan dan Pengembangan Lintas Fungsi	Penetapan Standar	Mengawasi dan mengembangkan kinerja pada tiap fungsi Pertamina RU IV dengan memberikan penetapan standar	Quality Management		Standard budaya kerja dan operasional perusahaan
		Konsultasi	Mengawasi dan mengembangkan kinerja pada tiap fungsi Pertamina RU IV melalui pelaksanaan konsultasi untuk tiap fungsi bisnis yang bersangkutan	RIA		Peningkatan kinerja pada tiap fungsi bisnis
		Monitoring	Mengawasi dan mengembangkan kinerja pada tiap fungsi Pertamina RU IV melalui pelaksanaan monitoring	OPI		Kegiatan rapat dan Pelaporan untuk reminder tiap fungsi bisnis

No	Proses Bisnis	Sub Proses	Deskripsi	Funsgsi Terkait	Input	Output
20	Pengelolaan Kontrak Pengadaan Barang dan Jasa	Procurement	Pengadaan layanan dan kontrak jasa dan pengelolaan gudang	Procurement	Permintaan untuk pengadaan	Kontrak Kerja untuk pengadaan barang dan jasa
21	Pengadaan Bahan Baku non-hydro	Procurement	Proses pembelian material dengan melakukan sistem tender	Procurement	Permintaan untuk pengadaan bahan baku non hydro	Penerimaan bahan baku non hydro

b. Kritikalitas Proses Bisnis

Untuk mengetahui kritikalitas suatu proses bisnis dapat ditentukan dari beberapa besar dampak atau kerugian yang harus ditanggung jika proses bisnis tersebut terhenti. Semakin besar kerugian maka semakin kritis proses bisnis tersebut.

Pengelompokan kritikalitas proses bisnis dan kriterianya berdasarkan acuan konsultan Veda Praxis dideskripsikan sebagai berikut:

Tabel 2.8 Kriteria Pengelompokan Kritikalitas Proses Bisnis Veda Praxis (Sumber: PT. Pertamina RU IV)

Kategori Proses Bisnis	Dampak Operasional / Finansial	Keterangan
Kritikal	Dampak no 3 atau lebih tinggi pada saat proses bisnis terhenti dengan durasi waktu kurang dari 1 hari.	Dampak no. 3 adalah: OPR: Terganggu operasi di atas 1 s/d 3 jam dan atau kapasitas olah menjadi s/d 80%. atau FIN : Terjadi kerugian materiil Rp 250.000.000,00 s/d Rp 1.000.000.000,00
Moderat	Dampak no 3 atau lebih tinggi pada saat proses bisnis terhenti dengan durasi waktu lebih dari 1 hari hingga 7 hari	
Non Kritikal	Dampak no 3 atau lebih tinggi pada saat proses bisnis terhenti dengan durasi waktu lebih dari 7 hari	

Identifikasi Kritikalitas Proses Bisnis

Tabel 2.9 Identifikasi Kritikalitas Proses Bisnis (Sumber: BIA 2015 PT. Pertamina RU IV)

Urutan Proses	Proses Bisnis dan Durasi Waktu	Dampak Maksimum OPR	Dampak Maksimum FIN	Kritikalitas
1	Perencanaan Proses Pengolahan			Kritikal
	< 1 Hari	5	5	

Urutan Proses	Proses Bisnis dan Durasi Waktu	Dampak Maksimum OPR	FIN	Kritikalitas
	1-7 Hari	5	5	
	> 7 hari	5	5	
2	Pengolahan dan Produksi BBM dan non-BBM			Kritikal
	< 1 Hari	5	5	
	1-7 Hari	5	5	
	> 7 hari	5	5	
3	Distribusi Produk BBM, NBBM dan Petrokimia			Kritikal
	< 1 Hari	5	4	
	1-7 Hari	5	5	
	> 7 hari	5	5	
7	Pemeliharaan dan Pengendalian Peralatan Kilang			Kritikal
	< 1 Hari	5	5	
	1-7 Hari	5	5	
	> 7 hari	5	5	
8	Pengelolaan Health Safety Environment			Kritikal
	< 1 Hari	2	3	
	1-7 Hari	2	3	
	> 7 hari	3	5	
4	Evaluasi dan Rekomendasi Teknologi			Moderat
	< 1 Hari	2	2	
	1-7 Hari	4	2	
	> 7 hari	5	3	
5	Pengembangan Teknologi			Moderat
	< 1 Hari	2	2	
	1-7 Hari	2	3	
	> 7 hari	3	3	
6	Pembuatan Program Maintenance Kilang			Moderat
	< 1 Hari	2	2	
	1-7 Hari	3	2	
	> 7 hari	5	5	
10	Pengelolaan Infrastruktur dan Aplikasi TI			Moderat
	< 1 Hari	2	1	
	1-7 Hari	3	1	
	> 7 hari	4	1	
14	Pencatatan Transaksi Keuangan Arus Minyak			Moderat
	< 1 Hari	1	2	
	1-7 Hari	4	3	
	> 7 hari	4	3	
21	Pengadaan Bahan Baku non-hydro			Moderat

Urutan Proses	Proses Bisnis dan Durasi Waktu	Dampak Maksimum OPR	FIN	Kritikalitas
	< 1 Hari	2	2	
	1-7 Hari	2	3	
	> 7 hari	4	4	
9	Pengelolaan Sumber Daya Manusia			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	1	1	
11	Pengelolaan Aset			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	1	1	
12	Perencanaan Anggaran			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	1	3	
13	Pencatatan Transaksi Keuangan Umum			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	2	1	
15	Pengelolaan Hubungan Internal			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	1	1	
16	Pengelolaan Hubungan Eksternal			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	1	1	
17	Pengelolaan Audit Internal			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	2	2	
18	Peningkatan Kualitas Pekerja			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	1	1	
19	Pengawasan dan Pengembangan Lintas Fungsi			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	1	1	
	> 7 hari	3	1	

Urutan Proses	Proses Bisnis dan Durasi Waktu	Dampak Maksimum OPR	FIN	Kritikalitas
20	Pengelolaan Kontrak Pengadaan Barang dan Jasa			Non Kritikal
	< 1 Hari	1	1	
	1-7 Hari	2	2	
	> 7 hari	3	2	

2.2.5.4.2 Layanan IT dalam Proses Bisnis

Keberlangsungan proses bisnis di RU IV Cilacap tidak terlepas dari layanan fungsi IT. Layanan IT yang menjadi ruang lingkup dalam konteks BIA meliputi layanan komunikasi maupun layanan komputer yang dirasakan customer di masing – masing proses bisnis.

a. Layanan Aplikasi

Tabel 2.10 Layanan Aplikasi TI (Sumber: BIA 2015 RU IV)

No	Nama Aplikasi	Penggunaan	User
1	Aplikasi Biodata Security	Menyimpan data pekerja, pihak ketiga, OJT, PKL	Security
2	Aplikasi Notulen Rapat	Aplikasi yang digunakan untuk membantu pencatatan saat rapat operasi dan kehandalan dan menyebarkannya ke seluruh fungsi	OPI
3	Audit Management System	Membantu menyimpan hasil audit dan rekomendasi untuk perbaikan fungsi	RIA
4	Autocad	Membuat gambar mesin	Engineering Development
5	Billing System	Aplikasi keuangan operasional rumah sakit pertamina	PHC
6	Budget Monitor	Monitoring budget untuk maintenance kilang	Reliability
7	Daftar Telfon	Menyimpan data nomor telfon kantor dan sekretaris fungsi RU IV	Seluruh fungsi
8	Daily Tanker Position	Pelaporan pergerakan tanker datang dan pergi di area RU IV	Marine
9	DEHI (Daily Equipment Highlight)	Mencatat kondisi peralatan kritis/butuh perhatian lebih lanjut	OPI Reliability

No	Nama Aplikasi	Penggunaan	User
10	E-Correspondence	Aplikasi yang membantu pengiriman memo antar fungsi di Pertamina	Seluruh fungsi
11	E-Mis (Event Management Information System)	Agenda kegiatan rapat beserta penggunaan ruang rapat dan peserta yang diundang	HR
12	Engineering Drawing	Menyimpan data desain kilang	Engineering Development MPS
13	Fingerprint Mitra Kerja	Absensi mitra kerja	Seluruh fungsi
14	Fingerprint pekerja	Absensi karyawan	Seluruh fungsi
15	GRTMPS	Analisa harian rencana RPO	RPO
16	HIPER (Health Information Pertamina)	Menyimpan informasi kesehatan pekerja	PHC
17	HIRAC	Identifikasi hazard	Seluruh fungsi
18	Hysis	Aplikasi yang digunakan untuk simulasi efisiensi energi (ECLC)	Engineering Development
19	IM	Untuk pembuatan medical card dan claim deklarasi karyawan Pertamina	PHC
20	iTools	Sistem inventory perlatan bagian komunikasi IT	IT
21	LIMS	Monitoring kegiatan laboratorium	Engineering Development RPO Production II
22	Material Catalog	Data kode dan nama material yang digunakan dalam proses bisnis RU IV	Procurement
23	MCU Online	Aplikasi pemanggilan MCU berkala tahunan dan khusus sekaligus digunakan untuk mengeluarkan surat pemanggilan MCU pekerja	PHC
24	MMHM (Material Master Hydro Movement)	Aplikasi pelaporan arus minyak kapal	Marine
25	Monitoring Cuti	Untuk memonitoring cuti dan SIJ pekerja dan mencetak formnya	HR

No	Nama Aplikasi	Penggunaan	User
26	Monitoring Data Purchasing	Sistem monitoring data purchasing	Procurement
27	Monitoring Hazard	Sistem monitoring paparan hazard pekerja	HSE
28	MySAP	Layanan ERP korporat	Seluruh fungsi
29	PIMS	Project & Initiative Management System	OPI RPO
30	People review		HR
31	Primavera	Manajemen proyek untuk TA, memantau pelaksanaan TA setiap hari saat TA sedang berlangsung	TA MPS
32	Procure 2 Pay	Pembayaran pengadaan barang / jasa	Finance Marine Procurement
33	RDP	Rumah dinas perusahaan	HR
34	Readiness Tools	Informasi mengenai peralatan di bengkel TA	TA
35	ROAS	Mencatat pergerakan arus minyak	OPI RPO
36	Saprodu (Sistem Informasi Penjadwalan Terpadu)	Surat Izin Penyaluran/Pemompaan/Penyerahan	RPO
37	SIKA (Surat Ijin Kerja Aman) Online	Dokumen kontrol bahaya administratif	HSE
38	SIMOPS	Portal seluruh web dan aplikasi Pertamina RU IV Cilacap	Seluruh fungsi
39	Simulasi Framingham	Untuk mengetahui kategori resiko kemungkinan terkena penyakit kardiovaskuler dalam 10 tahun mendatang	PHC
40	SMS Emergency	Aplikasi yang digunakan sebagai SMS emergency apabila terjadi keadaan darurat	HSE
41	SPC APP	Aplikasi pusat untuk share processing center	Finance
42	TADB (Turn Around Database)	Database peralatan dan bom of material untuk TA	TA

No	Nama Aplikasi	Penggunaan	User
43	Tank Vision	Monitoring pergerakan tanki yang ada di area RU IV	RPO Production II
44	Thinkcell	Aplikasi pembuatan presentasi berupa chart dari data yang cepat dan interaktif	Engineering Development MPS
45	TIMS	Publikasi progress pengerjaan TA saat TA berlangsung	TA
46	USD Online	Deklarasi UMK dan SP3	Finance
47	Web Finance	Website finance	Finance
48	Web HR	Website HR	HR
49	Email Pertamina	Layanan penyedia surat elektronik untuk perusahaan pertamina.	Seluruh fungsi
50	Web HSE	Website HSE	HSE
51	Web ME	Website ME	ME
52	Web MPS	Website MPS	MPS
53	Web OPI	Website OPI	OPI
54	Web Procurement	Website Procurement	Procurement
55	Web QM	Website QM	QM
56	Web Reliability	Website Reliability	Reliability
57	Web RIA	Website RIA	RIA

b. Layanan Non Aplikasi

a. Informasi Sistem Hardware

Tabel 2.11 Layanan Non Aplikasi (Sumber: BIA 2015 RU IV)

No	Hardware	Lingkungan Hardware	Jumlah
1	Server	Data Center	17 Unit
2	PC	Seluruh lokasi kerja RU IV	1096 Unit
3	Jaringan telepon dan telepon meja	Seluruh lokasi kerja RU IV	
4	CCTV (Closed Circuit Television)	Area kilang Area Marine 70 Area Perkantoran Head Office Komperta	152 Camera
5	Facsimile Distribusi	Head Office RU IV	100 buah
6	Intercom kilang		11 sistem
7	Fire Emergency System	Area Kilang RU IV Area Head Office Pertamina Hospital Cilacap Area Marine 70	6 Node (Kilang) 1 Node (Area 70) 1 Node (PHC) 1 Node (HO)

8	HT/Radio		
9	Public Addressor	Area Head Office Pertamina Hospital Cilacap Area Kilang	3 sistem (HO, Kilang, PHC)
10	Trunking system	Kantor Communication Operations	1 Controller 11 Repeater 603 HT 86 Radio mobil
11	Radio Pantai	Area Marine 70	

b. Informasi Jaringan
Kebutuhan/Persyaratan Peralatan Jaringan

Tabel 2.12 Kebutuhan Jaringan (Sumber: BIA 2015 RU IV)

No	Peralatan Jaringan	Jumlah
1	Switch	1 unit
2	Access Point	85 unit
3	WAN	1956 port
4	Internet	2 sistem (main : MPLS Telkom, 10 Mbps, backup Patrakom 4 Mbps)
5	Intranet	2 sistem: 1. Proxy kantor pusat (main) 2. Proxy local (Telkom, backup)

c. Analisis RTO

Metode pemaparan yang akan dilakukan di bagian ini dilakukan dengan 2 tahapan besar, pengelompokan layanan IT sesuai proses bisnis serta dilanjutkan penyusunan matriks prioritas layanan IT. Aktivitas pengelompokan layanan IT dilakukan untuk mengetahui layanan apa saja yang digunakan oleh customer di masing – masing kategori kritikalitas proses bisnis sesuai paparan pada bagian sebelumnya, yaitu kategori kritikal, kategori moderate serta kategori non-critical. Ketika ada layanan IT yang digunakan di lebih dari satu kategori kritikalitas proses bisnis, maka layanan tersebut akan didefinisikan sebagai kelompok layanan dengan level kategori kritikalitas yang lebih tinggi. Misalnya layanan IT MySAP digunakan oleh kategori Critical, Moderate dan Non-

Critical, maka untuk matriks layanan ini akan masuk di kategori Critical.

Suatu proses bisnis dikatakan kritikal tidak berarti semua layanan IT yang digunakannya mendapatkan prioritas utama (*high-priority*), oleh karena itu dibutuhkan matriks priotisasi layanan IT, dengan mempertimbangkan kritikalitas berdasarkan RTO (*Recovery Time Objective*).

Pengelompokan layanan IT yang digunakan masing – masing proses bisnis berdasarkan level kritikalitasnya adalah sebagai berikut:

Tabel 2.13 Pengelompokan Layanan TI berdasarkan Tingkat Kritikalitas (Sumber: BIA 2015 RU IV)

Level Kritikalitas Proses Bisnis	Proses Bisnis	Layanan IT yang Digunakan		
Critical	Perencanaan Proses Pengolahan	Intranet Pertamina	LIMS	Daily Tanker Position
	Pengolahan dan Produksi BBM dan Non-BBM	WAN	PC (Include Ms. Office)	MMHM (Material Master Hydro Movement)
	Distribusi Produk BBM, Non-BBM dan Petrokimia	HT	MySAP	Primavera
	Pemeliharaan dan Pengendalian Peralatan Kilang	Telepon	PIMS	Readiness Tools
	Pengelolaan Health Safety Environment	Radio Pantai	ROAS	TADB (Turn Around Database)
		Fax	Tank Vision	TIMS
		E-mail	Material Catalog	Monitoring Hazard

Level Kritikalitas Proses Bisnis	Proses Bisnis	Layanan IT yang Digunakan		
		Intercom	Monitoring Data Purchasing	SMS Emergency
		CCTV	Procure 2 Pay	MCU Online
		GRTMPS	SIMOPS	SIKA Online
Moderate	Evaluasi Rekomendasi Teknologi Pengembangan Teknologi Pembuatan Program Maintenance Kilang Pengelolaan Infrastruktur dan Aplikasi IT Pencataan Transaksi Keuangan Arus Minyak Pengadaan Bahan Baku Non-Hydro	Intranet Pertamina	Procure 2 Pay	TADB
		WAN	LIMS	TIMS
		HT	Primavera	Readiness Tools
		Telepon	Monitoring Data Purchasing	Material Catalog
		Radio Pantai	Engineering Drawing	SPC APP
		Fax	Think Cell	iTools
		e-mail	Budget Monitoring	Hysis
		CCTV	DEHI	
		PC (Include Ms. Office)	Autocad	
Non Critical	Pengelolaan Aset Pengelolaan Sumber Daya Manusia Perencanaan Anggaran Pencatatan Transaksi Keuangan Umum Pengelolaan Hubungan Internal	Thinkcell	DEHI	Fingerprint pekerja
		Fingerprint Mitra Kerja	iTools	Monitoring Cuti
		RDP	Web HR	Audit Management System
		Web Finance	SPC APP	E-Correspondence
		SIMA	Web RIA	E-Mis
		USD Online	Web OPI	Web QM

Level Kritikalitas Proses Bisnis	Proses Bisnis	Layanan IT yang Digunakan
	Pengelolaan Hubungan Eksternal	Aplikasi Biodata Security
	Pengelolaan Audit Internal	
	Peningkatan Kualitas Pekerja	
	Pengawasan dan Pengembangan Lintas Fungsi	
	Pengelolaan Kontrak Pengadaan Barang dan Jasa	

Keterangan:

Layanan IT yang sudah masuk di kategori high
Layanan IT yang sudah masuk di kategori moderate

RTO *(Recovery Time Objective)* adalah waktu toleransi yang diberikan bagi proses bisnis untuk dapat terus berjalan tanpa menggunakan aplikasi sistem maupun layanan IT. RTO dapat dihubungkan dengan SLA ke User. Berikut ini dipaparkan nilai RTO dari layanan – layanan IT di RU IV yang merupakan nilai maksimum dari masing – masing proses bisnis di RU IV.

Tabel 2.14 RTO Layanan TI (Sumber: BIA 2015 RU IV)

No	Aplikasi Sistem dan Layanan IT (Aplikasi / Telepon / HT)	RTO
1	Intranet Pertamina	< 1 jam
2	WAN	< 1 jam
3	HT	< 1 jam
4	Telepon	< 1 jam
5	Radio Pantai	< 1 jam

No	Aplikasi Sistem dan Layanan IT (Aplikasi / Telepon / HT)	RTO
6	CCTV	< 1 jam
7	LIMS	< 1 jam
8	PC (Include Ms. Office)	< 1 jam
9	MySAP	< 1 jam
10	PIMS	< 1 jam
11	ROAS	< 1 jam
12	Material Catalog	< 1 jam
13	Monitoring Data Purchasing	< 1 jam
14	Daily Tanker Position	< 1 jam
15	MMHM (Material Master Hydro Movement)	< 1 jam
16	Historian	< 1 jam
17	E- Corresponden	< 1 jam
18	Fire Emergency Sirene	< 1 jam
19	Server	< 1 jam
20	Hysis	< 1 jam
21	Fax	1 jam
22	Email	1 jam
23	Intercom	1 jam
24	GRTMPS	1 jam
25	Tank Vision	1 jam
26	Procure 2 Pay	1 jam
27	SPC APP	1 jam
28	GLS / SAMK	1 jam
29	SMS Emergency	1 jam
30	WAN	1 jam
31	Telepon Meja	1 jam
32	Saprodu	1 jam
33	SIMOPS	1 hari
34	Primavera	1 hari
35	Readiness Tools	1 hari
36	TADB (Turn Around Database)	1 hari
37	TIMS	1 hari
38	Engineering Drawing	1 hari
39	DEHI	1 hari
40	MCU Online	1 hari
41	Web HSE	1 hari
42	Fingerprint mitra kerja	1 hari
43	Fingerprint Pekerja	1 hari

No	Aplikasi Sistem dan Layanan IT (Aplikasi / Telepon / HT)	RTO
44	SIKA Online	7 hari
45	Autocad	7 hari
46	Budget Monitor	7 hari
47	USD Online	7 hari
48	iTools	7 hari
49	IM	7 hari
50	Pelita	7 hari
51	Simulasi Farmigham	7 hari
52	Monitoring Hazard	1 bulan
53	Monitoring Cuti	1 bulan
54	Web QM	1 bulan
55	Web OPI	1 bulan
56	Aplikasi Biodata Security	1 bulan
57	HIPER	1 bulan
58	HIRAC	1 bulan
59	Daftar Telepon	1 bulan
60	People Review	> 1 bulan
61	Think Cell	> 1 bulan
62	E- corresponden	< 1 jam
63	RDP	7 hari

Namun dalam kegiatan wawancara pada fungsi bisnis, dari sebanyak 57 layanan non aplikasi dan 16 layanan aplikasi hanya sebanyak 52 layanan aplikasi dan 10 layanan non aplikasi yang telah disebutkan. Oleh karena itu dalam dokumen ini juga akan memberikan keterangan RTO untuk layanan aplikasi dan non aplikasi yang tidak disebutkan oleh responden, dengan pertimbangan bahwa layanan yang tidak disebutkan tersebut merupakan aplikasi yang bersifat tidak kritis atau RTO nya hanya berkisar pada 7 hari serta beberapa layanan yang menyangkut untuk koneksi dengan layanan yang kritis maka dalam dokumen ini diberi RTO <1 jam. Berikut merupakan daftar dari layanan tersebut:

Tabel 2.15 RTO Layanan TI (Sumber: BIA 2015 RU IV)

No	Nama Aplikasi	RTO
1	Aplikasi Notulen Rapat	7 hari
2	Audit Management System	7 hari

No	Nama Aplikasi	RTO
3	Billing System	7 hari
4	E-Mis (Event Management Information System)	7 hari
5	Public Addressor	7 hari
6	Trunking system	7 hari
7	Web Finance	7 hari
8	Web HR	7 hari
9	Web ME	7 hari
10	Web MPS	7 hari
11	Web Procurement	7 hari
12	Web Reliability	7 hari
13	Web RIA	7 hari
14	Switch	<1 jam
15	Access Point	<1 jam
16	Internet	<1 jam

Berdasarkan RTO yang sudah diketahui pada tiap layanan maka berikut adalah pengelompokan nilai RTO berdasarkan kategori durasinya :

Tabel 2.16 Pengelompokan RTO Layanan TI (Sumber: BIA 2015 RU IV)

RTO < 1 jam	RTO 1 – 2 jam	RTO s/d 1 hari	RTO s/d 7 hari	RTO s/d 1 bulan	RTO > 1 bulan
Critical		Moderate	Non – Critical		
Intranet Pertamina	Fax	SIMOPS	Autocad	Monitoring Hazard	Think Cell
WAN	Email	Primavera	Budget Monitor	Monitoring Cuti	People Review
HT	Intercom	Readiness Tools	iTools	Web QM	
Telpon	GRTMPS	TADB (Turn Around Database)	USD Online	Web OPI	
Radio Pantai	Tank Vision	TIMS	SIKA Online	Aplikasi Biodata Security	
LIMS	SMS Emergency	DEHI	Audit Management System	HIPER	

RTO < 1 jam	RTO 1 – 2 jam	RTO s/d 1 hari	RTO s/d 7 hari	RTO s/d 1 bulan	RTO > 1 bulan
Critical		**Moderate**	**Non – Critical**		
PC (Include Ms. Office)	SPC APP	MCU Online	Billing System	HIRAC	
MySAP	Telepon Meja	Web HSE	E-Mis (Event Management Information System)	Daftar Telepon	
	Saprodu	Fingerprint mitra kerja			
		Fingerprint Pekerja			
PIMS	Fire Emergency Sirene	Engineering Drawing	Public Addressor		
ROAS	Procure 2 Pay		Trunking system		
Material Catalog			Web Finance		
Monitoring Data Purchasing			Web HR		
Daily Tanker Position			Web HR		
MMHM			Web ME		
Hysis			Web MPS		
SIMOPS			Web Procurement		
Switch			Web Reliability		
Access Point			Web RIA		
Internet			IM		
E-corresponden			Pelita		
Server			Simulasi Farmigham		
			RDP		

Berdasarkan paparan pengelompokan layanan IT berdasarkan kritikalitas proses bisnis serta pengelompokan RTO layanan IT, maka dapat dibuat matriks prioritas layanan IT seperti di bawah.

Tabel 2.17 Prioritas Layanan TI (Sumber: BIA 2015 RU IV)

		Kategori Proses Bisnis		
		Critical	**Moderate**	**Non-Critical**
Kategori Layanan IT berdasarkan RTO	**Critical** **s/d 2 jam**	• Intranet Pertamina • WAN • HT • Telpon • Radio Pantai • CCTV • LIMS • PC (Include Ms. Office) • MySAP • PIMS • ROAS • Material Catalog • Switch • Access Point • Telepon Meja • Monitoring Data Purchasing • Daily Tanker Positio • MMHM • SIMOPS • Fax • Email • Intercom • GRTMPS • Tank Vision • Procure 2 Pay • SMS Emergency • Server • Internet • Saprodu • E-Correspondence	• SPC APP • Hysis • Web HSE • Fingerprint mitra kerja	
	Moderate **s/d 1 hari**	• Primavera Readiness Tools • TADB • TIMS • MCU Online	• Engineering Drawing • DEHI	• Fingerprint pekerja
	Non-Critical **s/d >1 bulan**	• Monitoring Hazard • SIKA Online • Web ME • Web MPS	• Autocad • iTools • USD Online	• Think Cell • Monitoring Cuti • Web QM • Web OPI

			• Budget Monitoring	• Aplikasi Biodata Security • E-Mis • Public Addressor • Trunking system • Web Finance • Web HR • Web Procurement • Web Reliability • Web RIA • IM • Pelita • Simulasi – Farmingham • People review • RDP • Daftar Telepon

Matriks prioritas layanan IT:

Tabel 2.18 Matriks Prioritas Layanan TI (Sumber: BIA 2015 RU IV)

		Kategori Proses Bisnis		
		Critical	Moderate	Non-Critical
Kategori Layanan IT berdasarkan RTO	Critical			
	Moderate			
	Non-Critical			

Keterangan:

Layanan IT dengan ***High-Priority***

Layanan IT dengan ***Medium-Priority***

Layanan IT dengan ***Low-Priority***

d. Analisis RPO

RPO untuk tiap aplikasi bisnis disajikan sebagai berikut:

Tabel 2.19 Hasil Analisa RPO (Sumber: BIA 2015 RU IV)

No	Aplikasi Bisnis	Fungsi Bisnis User	Proses Bisnis	Lokasi Penyimpanan	RPO	RPO Maks
1	LIMS	RPO	Perencanaan Proses Pengolahan	Data Center	1 hari	< 1 jam
		Production II	Pengolahan dan Produksi BBM dan Non-BBM	Data Center	< 1 jam	
		Engineering Development	Evaluasi dan Rekomendasi Teknologi	Data Center	1 hari	
2	MySAP	All	All	Kantor Pusat	< 1 jam	< 1 Jam
3	P2P	All	Perencanaan Proses Pengolahan	Kantor Pusat	< 1 jam	< 1 Jam
			Distribusi Produk BBM, NBBM dan Petrokimia	Kantor Pusat	< 1 jam	
4	MMHM (Material Master Hydro Movement)	Marine	Perencanaan Proses Pengolahan	Kantor Pusat	1 hari	1 hari
			Distribusi Produk BBM, NBBM, dan Petrokimia	Kantor Pusat	1 hari	
5	Monitoring Data Purchasing	Procurement	Perencanaan Proses Pengolahan	Data Center	4 jam	4 jam
			Pengelolaan Kontrak Pengadaan Barang	Data Center	4 jam	

No	Aplikasi Bisnis	Fungsi Bisnis User	Proses Bisnis	Lokasi Penyimpanan	RPO	RPO Maks
			Pengadaan Bahan Baku Non Hydro	Data Center	4 jam	
6	ROAS	Production 1	Distribusi Produk BBM, NBBM, dan Petrokimia	Data Center	< 1 jam	< 1 jam
		OPI	Pengawasan dan Pengembangan Lintas Fungsi	Kantor Pusat	< 1 jam	
		RPO	Perencanaan Proses Pengolahan	Data Center	< 1 jam	
		FInance	Pencatatan Transaksi Keuangan Arus Minyak	Data Center	< 1 jam	
7	Material Catalog	Procurement	Perencanaan Proses Pengolahan	Data Center	1 hari	1 hari
			Pengadaan Bahan Baku Non Hydro	Data Center	1 hari	
8	Web Reliability	Reliability	Pembuatan Program Maintenance Kilang	Data Center	1 bulan	1 bulan
9	Web MPS	ME	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	7 hari	< 1 Jam
		MPS	Pembuatan Program Maintenance Kilang	Data Center	< 1 jam	
10	Engineering Drawing	ME	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	7 hari	1 hari
		Eng&Dev	Pengembangan Teknologi	Data Center	1 hari	
11	SIKA Online	ME	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	1 hari	1 hari
		HSE	Pengelolaan Health Safety Environment	Data Center	7 hari	
		Eng&Dev	Evaluasi dan Rekomendasi Teknologi	Data Center	1 hari	

No	Aplikasi Bisnis	Fungsi Bisnis User	Proses Bisnis	Lokasi Penyimpanan	RPO	RPO Maks
			Pengembangan Teknologi			
12	SIMOPS	All	All	Data Center	1 hari	1 hari
13	Primavera	T/A	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	1 hari	1 hari
14	Billing System PHC	PHC	Pengelolaan Health Safety Environment	Data Center	1 hari	1 hari
15	MCU Online	PHC	Pengelolaan Health Safety Environment	Data Center	1 hari	1 hari
16	Monitoring Hazard	PHC	Pengelolaan Health Safety Environment	Data Center	1 hari	1 hari
		HSE	Pengelolaan Health Safety Environment	Data Center	1 hari	
17	TIMS	T/A	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	1 hari	1 hari
18	Readiness Tools	T/A	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	1 hari	1 hari
19	Web QM	QM	Peningkatan Kualitas Budaya Kerja	Kantor Pusat	7 hari	7 hari
20	DEHI (Daily Equipment Highlight)	OPI	Pengawasan dan Pengembangan Lintas Fungsi	Data Center	7 hari	7 hari
21	Web OPI	OPI	Peningkatan Kualitas Budaya Kerja	Data Center	1 bulan	1 bulan
22	Monitoring Cuti	HR	Pengelolaan Sumber Daya Manusia	Data Center	7 hari	7 hari
23	iTools	IT	Pengelolaan dan Pengembangan TI	Data Center	1 hari	1 hari
24	Aplikasi Biodata Security	GA	Pengelolaan Health Safety Environment	Data Center	1 hari	1 hari

No	Aplikasi Bisnis	Fungsi Bisnis User	Proses Bisnis	Lokasi Penyimpanan	RPO	RPO Maks
25	E-correspondence	All	Seluruh proses bisnis	Kantor Pusat	< 1 jam	< 1 jam
26	Saprodu	RPO	Distribusi produk BBM, NBBM dan Petrokimia	Data Center	1 hari	1 hari
27	Fingerprint mantra kerja	All	All	Data Center	1 hari	1 hari
28	Fingerprint pekerja	All	All	Data Center	1 hari	1 hari
29	Pelita	All	All	Kantor Pusat	1 hari	1 hari
30	Simulasi framingharm	PHC	Pengelolaan HSSE Golden Rule	Data Center	7 hari	7 hari
31	HIPER	PHC	Pengelolaan HSSE Golden Rule	Data Center	7 hari	7 hari
32	HIRAC	HSE	Pengelolaan HSSE Golden Rule	Data Center	7 hari	7 hari
33	Daftar Telepon	All	All	Data Center	7 hari	7 hari
34	People Review	HR	Pengelolaan Sumber Daya Manusia	Data Center	1 hari	1 hari
35	Think cell	All	All	Data Center	1 bulan	1 bulan
36	Aplikasi Notulen Rapat	All	All	Data Center	1 hari	1 hari
37	Billing System	PHC	Pengelolaan HSSE Golden Rule	Data Center	1 hari	1 hari
38	Budget Monitor	Reliability	Pembuatan Program Maintenance Kilang	Data Center	1 hari	1 hari
39	Daily Tanker Position	Marine	Perencanaan dan Optimalisasi Pengolahan Minyak Bumi menjadi Produk	Data Center	< 1 jam	< 1 jam

No	Aplikasi Bisnis	Fungsi Bisnis User	Proses Bisnis	Lokasi Penyimpanan	RPO	RPO Maks
			BBM, NBBM dan Petrokimia			
			Distribusi Produk BBM, NBBM dan Petrokimia	Data Center	< 1 jam	< 1 jam
40	E-Mis	HR	Pengelolaan Sumber Daya Manusia	Data Center	1 hari	1 hari
41	GRTMPS	RPO	Perencanaan dan Optimalisasi Pengolahan Minyak Bumi menjadi Produk BBM, NBBM dan Petrokimia		1 hari	1 hari
42	IM	PHC	Pengelolaan HSSE Golden Rule	Data Center	1 jam	1 jam
43	SPC APP	Finance	Pencatatan dan Pembayaran Transaksi Keuangan Umum	Data Center	< 1 jam	< 1 jam
44	TADB	TA	Pembuatan Program Maintenance Kilang	Data Center	1 hari	1 hari
45	USD Online	Finance	Pencatatan dan Pembayaran Transaksi Keuangan Umum	Kantor Pusat	< 1 jam	< 1 jam
46	Web HR	HR	Pengelolaan Sumber Daya Manusia	Data Center	7 hari	7 hari
47	Web Finance	FInance	Pencatatan dan Pembayaran Transaksi Keuangan Umum	Data Center	7 hari	7 hari
48	Email Pertamina	All	All	Data Center	< 1 jam	< 1 jam
49	Web HSE	HSE	Pengelolaan HSSE Golden Rule	Data Center	7 hari	7 hari

No	Aplikasi Bisnis	Fungsi Bisnis User	Proses Bisnis	Lokasi Penyimpanan	RPO	RPO Maks
50	Web ME	ME	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	7 hari	7 hari
51	Web Procurement	Procurement	Pengadaan Bahan Baku Non-Hydro	Data Center	1 hari	1 hari
52	Web RIA	RIA	Pengelolaan Audit Internal	Data Center	7 hari	7 hari

Hasil dari analisa BIA ini akan menjadi acuan dalam proses perancangan BCP perusahaan. Meskipun yang digunakan adalah BIA tahun 2015, namun tidak terjadi banyak perubahan pada perusahaan di tahun 2016 ini sehingga hasil dari BIA tahun 2015 dapat dikatakan masih *reliable*.

2.2.6 *Business Continuity Management Systems* (BCMS)

Business continuity management systems (BCMS) merupakan salah satu bagian dari sistem manajemen yang ada di organisasi. Menurut ISO 22301 : 2012 [19], BCMS adalah satu set elemen yang saling terkait, yang digunakan oleh organisasi untuk membangun, mengimplementasikan, mengoperasikan, memantau, me-*review*, memelihara, dan meningkatkan kemampuan organisasi dalam menjaga keberlangsungan bisnis. Unsur-unsur ini meliputi manusia, kebijakan, rencana, prosedur, proses, struktur, dan sumber daya [20]

Semua elemen tersebut digunakan untuk memastikan bahwa kegiatan operasional tetap berkelanjutan, semua produk dan layanan tetap bisa dirasakan, dan *brand* yang membentuk *value* perusahaan tetap terlindungi serta reputasi perusahaan tetap terjaga [19].

Dari penjelasan di atas maka dapat disimpulkan bahwa BCMS adalah salah satu sistem manajemen yang ada di organisasi yang menitikberatkan pada upaya keberlanjutan bisnis di perusahaan. Rencana atau langkah yang diambil oleh perusahaan diwujudkan

dalam bentuk *business continuity management* (BCM) yang akan dijelaskan pada poin selanjutnya.

2.2.7 *Business Continuity Management* (BCM)

Menurut standar ISO 22301:2012, *business continuity management* (BCM) adalah sebuah proses berkelanjutan yang digunakan untuk memastikan bahwa kegiatan operasional tetap berkelanjutan, semua produk dan layanan tetap bisa dirasakan, dan *brand* yang membentuk *value* perusahaan tetap terlindungi serta reputasi perusahaan tetap terjaga. Hal ini dapat diraih dengan cara mengidentifikasi ancaman potensial, melakukan analisa dampak yang mungkin terjadi, dan mengambil langkah untuk meningkatkan ketahanan perusahaan [21]. Sedangkan menurut *Business Continuity Institute* (BSI), BCM adalah sebuah proses manajemen berkelanjutan yang mengidentifikasi dampak potensial yang mengancam organisasi dan menyediakan kerangka kerja untuk membentuk ketahanan dan kemampuan perusahaan untuk merespon ancaman secara efektif sehingga dapat melindungi stakeholder, citra perusahaan, dan produk [22].

2.2.8 *Business Continuity Plan* (BCP)

Dewasa ini, *business continuity plan* bukan lagi menjadi kemewahan, namun menjadi suatu elemen esensial dalam program manajemen risiko organisasi [23]. BCP diperlukan bagi perusahaan sebagai tindak lanjut pada resiko yang mungkin terjadi. *Business continuity plan* (BCP) merupakan bagian dari information risk management, yang masuk ke dalam fase *risk mitigation* (pencegahan risiko). Menurut Fang Zhao, BCP merupakan sebuah rencana praktis yang menjadi panduan bagi organisasi untuk memulihkan sebagaian atau keseluruhan fungsi kritikal yang terganggu setelah terjadinya bencana atau gangguan [24]. Dengan kata lain, BCP adalah sebuah panduan perencanaan bagi perusahaan dalam menentukan respon terhadap terjadinya sebuah risiko yang dapat terjadi setiap waktu.

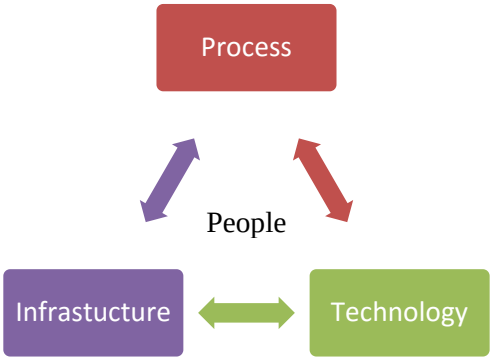
Menurut standar yang dikeluarkan oleh British Standart Institute (2006), langkah yang harus diambil oleh organisasi dalam menyusun BCP antara lain adalah, mengidentifikasi aktivitas/proses yang mendukung proses bisnis utama organisasi, dilanjutkan dengan mengidentifikasi hubungan dan ketergantungan antara aktivitas/proses, dan yang terakhir adalah mengevaluasi dampak dari berhentinya atau tidak beroperasinya proses bisnis yang kritikal terhadap organisasi yang bersangkutan, yang dilakukan dalam fase *business impact analysis* (BIA)

Sedangkan menurut ISO 22301:2012 [19] yang membahas mengenai *business continuity management systems* (BCMS), BCP adalah prosedur terdokumentasi yang dapat digunakan sebagai panduan organisasi untuk merespon, memulihkan, melanjutkan dan mengembalikan kegiatan operasional pada keadaan sebelum gangguan terjadi. Biasanya yang menjadi perhatian utama adalah sumber daya, layanan, atau aktivitas yang sifatnya kritikal pada organisasi yang bersangkutan.

Kejadian atau hal-hal yang menahan proses bisnis adalah segala sesuatu gangguan keamanan yang terduga dan tak terduga yang bisa mematikan operasi normal bisnis dalam kurun waktu tertentu [25]. Tujuan dari BCP adalah untuk meminimalisir efek dari kejadian atau bencana tersebut dalam sebuah perusahaan atau organisasi. Manfaat utama dari *business continuity plan* adalah untuk mereduksi risiko kerugiaan keuangan dan meningkatkan kemampuan perusahaan untuk memulihkan diri dari bencana atau gangguan sesegera mungkin. Perencanaan keberlangsungan bisnis juga harus dapat membantu meminimalisir biaya dan mengurangi risiko sehubungan dengan kejadian bencana tersebut.

2.2.8.1 Komponen Bisnis BCP

Snedaker mem-*breakdown* elemen bisnis menjadi tiga kategori sederhana yaitu manusia (*people*), proses (*process*) dan teknologi (*technology*).



Gambar 2.11 Interaksi Komponen Bisnis BCP (Sumber: Snedaker 2007)

a. Manusia

Sebuah krisis yang dikelola secara baik akan menyebabkan karyawan utama dalam perusahaan tersebut merasa aman dan terlindungi, sehingga meminimalisir kemungkinan karyawan tersebut mencari pekerjaan di tempat lain yang pada akhirnya akan membuat karyawan tersebut lebih fokus pada pekerjaan mereka. Krisis yang dikelola secara baik juga akan meningkatkan reputasi perusahaan, tentang bagaimana perusahaan tersebut dapat menangani kondisi pada masa-masa kritis sekalipun. Memiliki pengelolaan keadaan kritis yang baik juga dapat mengurangi stress yang diderita oleh karyawan secara signifikan, sehingga mereka dapat bekerja kembali lebih cepat, kembali ke operasi bisnis yang normal dan menghasilakan keuntungan bagi perusahaan.

b. Proses

Perencanaan *business continuity* dapat menjadikan kesempatan bagi perusahaan untuk mengevaluasi dan meningkatkan bisnis prosesnya. Seringkali dalam penyusunuan *business continuity*, tim menemukan cara baru untuk merampingkan proses atau meningkatkan keamanan sistem dengan mengidentifikasi titik lemah dalam sistem.

c. Teknologi

Menangani isu teknologi secara acak/pada saat terjadinya bencana akan jauh lebih mahal daripada ketika sebuah organisasi sudah memiliki sebuah rencana penanganan bencana yang matang disaat sebelum kejadian. Negosiasi di awal terhadap layanan darurat dapat menghasilkan harga yang lebih murah dan ROI yang lebih tinggi untuk proses BCP di perusahaan.

2.2.8.2 Kebutuhan akan *Business Continuity Plan*

Mengapa BCP dibutuhkan oleh perusahaan? Level kebutuhan dan kepentingan BCP di perusahaan akan berbeda-beda tergantung dari jenis usahanya. Bagi beberapa perusahaan kebutuhan akan BCP terlihat jelas, terutama bagi perusahaan yang sangat bergantung pada TI untuk menjalankan proses bisnisnya. Contoh umum yang sering kita ketahui adalah bank. Perusahaan seperti ini akan mensyaratkan *continuous availability* yang merupakan subset dari BCP yang juga dikenal sebagai *zero-downtime*. Hal ini dikarenakan *cost* dari sebuah sistem yang tidak berjalan (*down*) sesaat saja akan jauh lebih besar daripada investasi perancangan sebuah BCP. Sementara pada organisasi lain memiliki toleransi yang lebih besar, misalnya pada perusahaan retailer brick and mortar. Perusahaan jenis ini tidak begitu merasakan kerugian jika sistemnya down di luar jam kerjanya. Signifikasi dari sebuah BCP dalam sebuah perusahaan secara garis besar bergantung pada besarnya ketergantungan suatu organisasi kepada komunikasi data [26].

Sedangkan menurut Dr. Nasser, menekankan pentingnya BCP jika ditinjau dari sisi kompetitif. Tingkat kompetensi sebuah perusahaan dapat dilihat oleh seorang konsumen, bagaimana sebuah perusahaan bereaksi ketika sebuah bencana terjadi. Para konsumen mengharapkan informasi mereka tetap aman meskipun suatu kejadian luar biasa terjadi dan mereka juga mengharapkan pemulihan secepat mungkin [27]. Kemampuan ini dikenal dengan istilah *maximum tolerable period of disruption* (MTPD) yaitu

waktu *downtime* maksimum yang dapat diterima untuk menjamin keberlangsungan bisnis sebuah perusahaan.

2.2.9 Perbedaan Antara BCM dan BCP

Terdapat banyak ambiguitas dalam terminologi BCM dan BCP. Sebelum perusahaan dapat mengimplementasikan *business continuity management* (BCM), proses *business continuity plan* (BCP) harus diambil terlebih dahulu. Sehingga secara sederhana dapat diartikan bahwa BCP merupakan bentuk lebih "sederhana" dari BCM. Berikut merupakan beberapa perbedaan antara BCM dan BCP yang dirilis oleh *Business Continuity Institute* (BSI):

Tabel 2.20 Perbedaan BCP dan BCM (Sumber: BSI)

***Business Continuity Planning* (BCP)**	***Business Continuity Management* (BCM)**
• Mengidentifikasi tim manajemen BCM • Mengembangkan kebijakan BCM perusahaan • Mengidentifikasi tim yang bekerja dalam BCM • Melakukan penilaian risiko dan penilaian dampak bisnis • Mendefinisikan *scope* dan strategi *recovery* • Mengembangkan dokumentasi BCP	• Menanamkan BCM ke budaya perusahaan • Menjaga rencana (*change control*) • Memimpin percobaan regular • Menyediakan training (pelatihan) BCM • Mengadakan audit rutin

2.2.10 *Disaster Recovery Plan* (DRP)

Disaster Recovery Plan (DRP) adalah kumpulan dari serangkaian prosedur, kebijakan dan proses yang berkaitan dengan

persiapan untuk melakukan pemulihan yang berkelanjutan dari infrastruktur teknologi setelah bencana (alam dan manusia). Setiap perusahaan memiliki kebutuhan yang spesifik atas proses dan tujuan bisnis yang dilakukannya. Oleh karena DRP antar satu perusahaan dengan perusahaan yang lain berbeda, disesuaikan dengan kebutuhan masing-masing perusahaan [28].

National Institute of Standard and Technology (NIST) memandang bahwa DRP adalah sebuah perencanaan yang berfokus pada sistem informasi, yang didesain untuk memulihkan operasional sistem, aplikasi atau fasilitas infrastruktur komputer pada kondisi pengganti (*alternate*) setelah muncul gangguan.

Sedangkan menurut Usep [25], DRP adalah prosedure yang dijalankan saat BCP berlangsung (*in action*) berupa langkah-langkah untuk penyelamatan dan pemulihan (*recovery*) khususnya terhadap fasilitas IT dan sistem informasi. *Disaster recovery plan* merupakan pengaturan yang komprehensif, berisikan tindakan-tindakan konsisten yang harus dilakukan sebelum, selama, dan setelah adanya kejadian (bencana) yang mengakibatkan hilangnya sumber daya sistem informasi. DRP berisikan prosedur untuk merespon kejadian darurat, menyediakan operasi backup cadangan selama sistem terhenti, dan mengelola proses pemulihan serta penyelamatan sehingga mampu meminimalisir kerugian yang dialami oleh organisasi.

DRP ini berfokus pada sistem informasi atau teknologi informasi yang ada pada perusahaan [6]. Sehingga, dapat disimpulkan bahwa terdapat hubungan antara *disasater recovery plan* (DRP) dengan *business continuity plan* (BCP). Tujuan pembuatan DRP antara lain adalah [29]:

- Memaksimalkan efektifitas pemulihan layanan IT dengan perencanaan yang matang;
- Merancang kontrol pencegahan untuk mereduksi atau mencegah terjadinya risiko gangguan pada sistem-sistem yang dicakup dokumen ini;

- Mengidentifikasi kegiatan, sumber daya, dan prosedur untuk memulihkan dan menjalankan pemrosesan di sistem cadangan pasca bencana;
- Menjamin pemeliharaan dan pengujian rencana dari waktu ke waktu mengikuti perkembangan bisnis, sistem, dan organisasi.

2.2.11 Hubungan BCP dengan DRP

National Institute of Standards and Technology (NIST) mengeluarkan sebuah pedoman perencanaan peristiwa yang mungkin terjadi yang dikhususkan pada bagian sistem informasi di pemerintah pusat Amerika Serikat (*Contingency Planning Guide for Federal Information Systems*). Didalamnya juga memuat perbedaan antara BCP dan DRP. Berikut ini merupakan perbedaan dan keterkaitan antara BCP dan DRP menurut NIST:

Tabel 2.21 Hubungan BCP dan DRP (Sumber: NIST)

Perencanaan	Tujuan	Ruang Lingkup	Fokus
Business Continuity Plan (BCP)	Prosedur untuk mempertahankan operasional bisnis perusahaan, selama dan setelah gangguan muncul.	Dapat dibuat untuk mengatasi gangguan pada sebuah unit bisnis terpenting atau seluruh unit bisnis di perusahaan.	Fokus pada proses bisnis perusahaan.
Disaster Recovery Plan (DRP)	Prosedur untuk relokasi operasional sistem informasi ke lokasi alternatif.	Dibuat untuk mengatasi gangguan pada sistem informasi yang membutuhkan relokasi.	Fokus pada sistem informasi perusahaan.

Sedangkan menurut Usep Solehudin [25], tujuan akhir dari *business continuity plan* dan *disaster recovery plan* adalah sama,

yaitu untuk menjamin keberlangsungan proses bisnis penting atau utama. DRP merupakan bagian atau subset dari strategi yang ada pada BCP dalam menghadapi bencana yang mengancam keberlangsungan proses bisnis penting. Pada saat bisnis *requirement* berubah dan mengharuskan adanya pemulihan/penyiapan dari fungsi-fungsi bisnis yang penting, maka solusi atau rencana yang dibuat adalah BCP. Dalam banyak kasus, BCP tidak dikontrol oleh unit TI, namun biasanya ditangani oleh bagian sekuriti atau keuangan. Sedangkan pada DRP adalah murni domain dari teknologi informasi (TI). Bagian TI-lah yang menghasilkan *disaster recovery plan*. Segala sesuatu yang berhubungan dengan DRP umumnya berfokus kepada "bagaimana memulihkan sistem data". Namun demikian perencanaan memerlukan keterlibatan unit lain dan dukungan dari DRP yang scopenya lebih besar. *Disaster recovery plan* hanya berfokus pada sumberdaya TI, sedangkan BCP sifatnya lebih luas dengan merencanakan secara menyeluruh keberlanjutan sebuah bisnis. BCP mempertimbangkan akses ke berbagai fasilitas, ketersediaan orang, proses bisnis serta pemulihan TI.

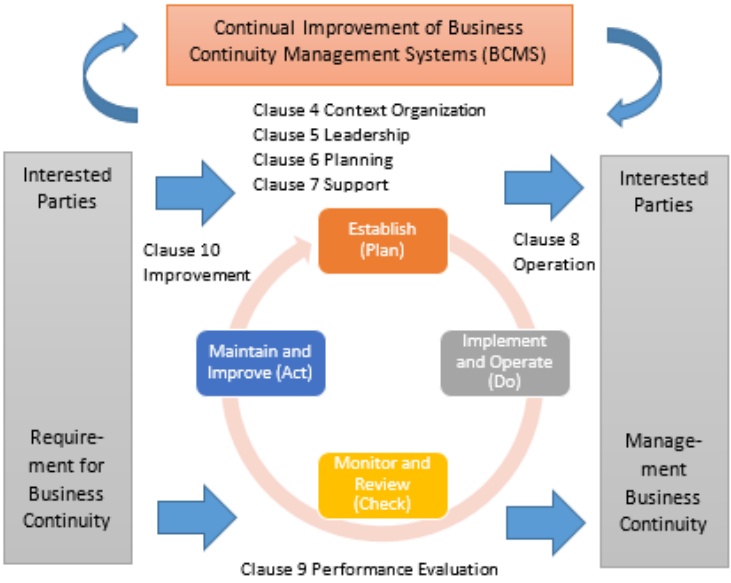
2.2.12 Framework ISO 22301:2012

ISO 22301:2012 merupakan sebuah standar internasional yang dibuat sebagai panduan untuk mengelola sistem pengelolaan keberlangsungan bisnis atau *Business Continuity Management Systems* (BCMS). BCMS adalah bagian dari keseluruhan pengelolaan sistem yang mendirikan, mengimplementasikan, mengoperasikan, memantau, meninjau, mengelola, dan meningkatkan keberlanjutan bisnis [21]. ISO 22301:2012 ini sendiri dikeluarkan oleh ISO (*The International Organization for Standardization*), sebuah badan yang mengatur standar di seluruh dunia.

Di dalam ISO 22301:2012 terdapat penjabaran terkait kerangka BCMS (*business continuity management systems*) serta apa yang harus dipenuhi oleh organisasi atau perusahaan agar

sistem pengelolaan keberlangsungan bisnis di perusahaan mereka dapat berjalan dengan baik.

Kerangka BCMS pada ISO 22301:2012 menerapkan model PDCA (*Plan-Do-Check-Act*) untuk merencanakan, mendirikan, mengimplementasikan, mengoperasikan, memantau, meninjau, mengelola, dan meningkatkan efektivitas secara terus-menerus dalam BCMS organisasi atau perusahaan [13]. Berikut ini merupakan model PDCA yang diaplikasikan pada proses BCMS :



Gambar 2.12 Model PDCA BCMS (Sumber : ISO 22301)

Penjelasan dari model tersebut sebagai berikut :

1. *Plan (Establish)*
   Di dalamnya berisikan kebijakan keberlanjutan bisnis, objektif, target, kontrol, proses, dan prosedur yang relevan yang digunakan untuk meningkatkan keberlanjutan bisnis.

2. *Do (Implement and Operate)*
   Dalam tahap ini berisikan hasil implementasi dan pengoperasian kebijakan keberlansungan bisnis, kontrol, proses, dan prosedur yang telah dibuat.
3. *Check (Monitor and Review)*
   Tahapan ini meliputi peninjauan performa yang tidak sesuai dengan kebijakan dan tujuan keberlangsungan bisnis, melaporkan hasil kepada pihak manajemen untuk dilakukan peninjauan dan perbaikan dalam peningkatan performa.
4. *Act (Maintain and Improve)*
   Pemeliharaan dan peningkatan pada BCMS dilakukan dengan mengambil perbaikan tindakan, berdasarkan peninjauan pengelolaan.

Dalam *best practice* ISO 22301:2012 bab 8.4.4 mengenai *business continuity plan*, dijelaskan bahwa organisasi harus menyediakan sebuah prosedur terdokumentasi sebagai panduan dalam menghadapi gangguan atau insiden yang bisa mengancam keberlangsungan bisnis dalam kurun waktu yang telah disepakati. Dokumen BCP menurut ISO 22301:2012 harus mengandung hal-hal sebagai berikut:

a. Pendefinisian peran dan tanggung jawab pada orang atau tim yang memiliki wewenang selama dan setelah insiden terjadi
b. Proses dalam aktivasi rencana
c. Rincian untuk mengelola konsekuensi langsung dari insiden yang terjadi, dengan memperhatikan:
   1. Kesejahteraan individu
   2. Pilihan strategis, taktis, dan operasional untuk merespon kerusakan, dan
   3. Mencegah kerusakan yang lebih parah pada aktivitas kritikal organisasi
d. Rincian tentang bagaimana dan dalam keadaan apa organisasi akan berkomunikasi dengan karyawan, stakeholder, dan bagian-bagian terkait dengan organisasi lainnya

e. Bagaimana organisasi akan melanjutkan atau memperbaiki aktivitas kritikal pada kurun waktu yang telah disepakati
f. Rincian tentang bagaimana bagian media organisasi akan merespon insiden, termasuk diantaranya
    1. Strategi komunikasi
    2. Teknis penjelasan antar muka *(preferred interface)* yang lebih disukai
    3. Panduan atau template untuk draft pemberian statement dihadapan media
    4. Juru bicara yang sesuai
g. Proses untuk berdiri di bawah ketika insiden selesai

Setiap rencana harus mendefinisikan:

1. Tujuan dan ruang lingkup
2. Kriteria aktivasi dan prosedur
3. Peran, tanggung jawab dan wewenang
4. Kebutuhan komunikasi dan prosedur
5. Kebutuhan sumber daya
6. Alur informasi dan proses terdokumentasi

2.2.13 Framework ISO 27031:2011

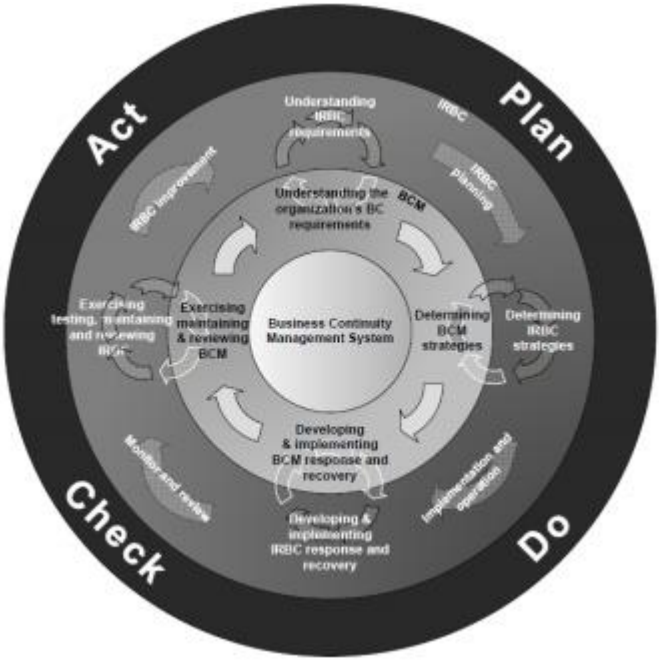
Selama bertahun-tahun, teknologi informasi dan komunikasi telah telah menjadi bagian penting dari banyak proses bisnis serta menjadi elemen penting dari bagian infrastruktur perusahaan. Ditambah dengan dukungan aplikasi online, internet dan layanan jaringan elektronik lainnya, ketergantungan perusahaan akan teknologi informasi dan komunikasi menjadi lebih besar.

Sementara itu, kebutuhan akan *business continuity management* (BCM), termasuk kesiapan menghadapi insiden, *disaster recovery planning*, dan manajemen tanggap darurat telah menjadi diakui dan didukung dengan domain pengetahuan dan keahlian yang spesifik, serta diatur secara lebih rinci pada standar ISO 22301 mengenai *Business Continuity Management Systems* [30].

Jika ditinjau dari ketergantungan perusahaan akan layanan TI, gangguan seperti kegagalan dalam memberikan layanan TI, termasuk isu terkait gangguan sistem dan serangan *malware* tentu saja akan berdampak pada keberlangsungan bisnis. Di sebagian besar kasus, yang memiliki ketergantungan tinggi dengan TI adalah fungsi bisnis yang bersifat kritikal. Hal ini berarti gangguan dengan TI akan menjadi risiko yang dapat menurunkan citra perusahaan. Kesiapan TI (*ICT rediness*) merupakan komponen penting bagi banyak organisasi dalam implementasi *business continuity management* dan *information security management* [30].

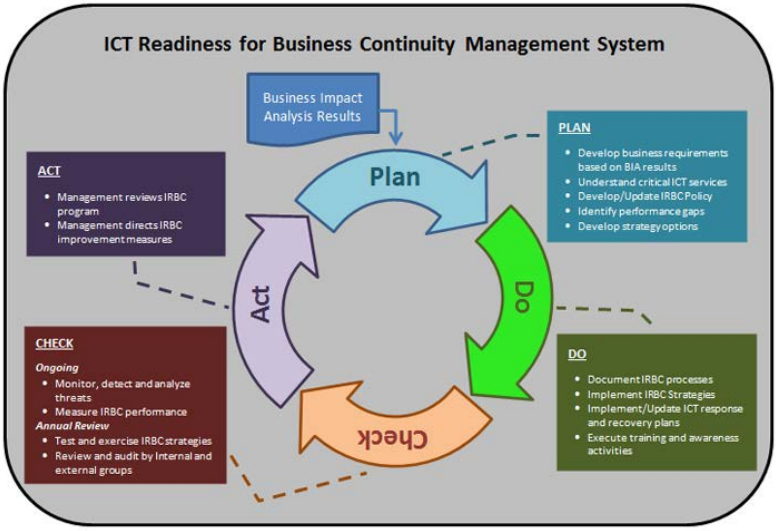
ISO 27031:2011 menyediakan pedoman untuk keberlangsungan binsis dan *IT disaster recovery professionals*, tentang bagaimana merencanakan keberlangsungan dan pemulihan TI sebagai bagian dari *business continuity management sistems* (BCMS) yang lebih komprehensif. Standar ini membantu personel TI untuk mengindentifikasi kebutuhan untuk keberlangsungan teknologi informasi dan komunikasi (TIK) dan menerapkan strategi untuk mengurangi risiko gangguan, serta mengenali, menanggapi, dan memulihkan layanan TI dari gangguan [30].

Gambar di bawah ini merupakan integrasi dan hubungan antara IRBC *(ICT rediness business continuity)* yang dijelaskan dalam ISO 27031:2011 dan BCMS *(business continuity management systems)* yang dijelaskan dalam ISO 22301:2012.



Gambar 2.13 Integrasi antara BCMS dan IT Rediness for Business Continuity (Sumber: ISO 27031)

ISO 27031:2011 menggunakan sistem dasar PDCA yang sama digunakan dalam ISO 22301:2012 namun menyesuaikan agar sesuai dengan sifat teknis dalam IRBC *(IT Rediness for Business Continuity)*. Selain menyesuaikan sifat PDCA, ISO 27031:2011 juga bergantung pada hasil analisis BIA *(business impact analysis)* yang telah dikembangkan dan disetujui oleh pihak manajemen. Berikut merupakan gambaran umum dari sistem PDCA yang ada pada ISO 27031:2011:



Gambar 2.14 Penjelasan Tahap PDCA ISO 27031 (Sumber: ISO 27031)

Penjelasan dari masing-masing tahap PDCA ISO 27031:2011 adalah sebagai berikut:

1. *Plan*
   Pada tahap ini dilakukan pembuatan dan pembaharuan struktur tata kelola untuk keseluran sistem manajemen IRBC. Keluaran utama dari tahap ini adalah kebijakan IRBC, tujuan, target, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan kesiapan IT untuk mendukung tujuan dan kebijakan keberlangsungan bisnis perusahaan.
2. *Do*
   Mengimplementasikan dan mengoperasikan kebijakan IRBC, kontrol, proses dan prosedur yang telah dibuat pada tahap sebelumnya. Keluaran utama dari tahap ini adalah implementasi strategi, serta hasil pelaksanaan kegiatan pelatihan dan kesadaran untuk mempromosikan pentingnya kontinuitas keberlangsungan layanan TI di sebuah perusahaan.
3. *Check*

Pada tahap ini dilakukan penilaian dan, jika dimungkinkan, mengukur proses kinerja berdasarkan kebijakan IRBC, tujuan, dan pengalaman praktikal serta melaporkan hasilnya pada pihak manajemen untuk mendapatkan review.

4. *Act*
   Pada tahap ini diberikan kesempatan bagi manajemen untuk meninjau kinerja IRBC dengan pengambilan langkah korektif dan preventif, untuk mencapai perbaikan terus menerus *(continual improvement)* dan mengurangi risiko gangguan yang mungkin terjadi di masa depan dari IRBC.

Dalam ISO 27031:2011 bab 7.4.2 menjabarkan terkait apa yang harus ada dalam sebuah dokumen rencana keberlangsungan bisnis berbasis TI. Sebuah organisasi dapat memiliki satu atau lebih dokumen yang mencakup seluruh rencana kegiatan pemulihan layanan TI. Rencana respon dan pemulihan rencana TI harus singkat dan dapat diakses orang dengan tanggung jawab yang ditetapkan didalamnya [30]. Rencana harus berisi sebagai berikut:

a. Tujuan dan ruang lingkup
   Tujuan dan ruang lingkup harus didefinisikan, disepakati oleh top management, dan dipahami oleh orang-orang yang terlibat dalam rencana. Rencana yang dibuat juga harus dikorelasikan dengan dokumen-dokumen lain dalam organisasi. Setiap rencana pemulihan layanan TI dalam organisasi harus mempertimbangkan:
   - Layanan TI kritis yang harus dipulihkan
   - Batas waktu pemulihan layanan TI
   - Kriteria aktivasi rencana pemulihan TI

   Rencana mungkin juga mengandung, jika diperlukan, prosedur dan daftar periksa yang mendukung proses kajian pasca insiden.

b. Peran dan tanggung jawab
   Peran dan tanggung jawab individu dan tim yang memiliki otoritas (dalam hal pengambilan keputusan dan definisi sumber daya) selama dan setelah insiden harus jelas didokumentasikan.

c. Kriteria aktivasi rencana
   Dalam dokumen rencana harus terdefinisikan dengan jelas apa kriteria aktivasi rencana pemulihan layanan TI dan kapan rencana itu dilaksanakan. Hal ini dilakukan untuk meminimalisir kerugian dan meluasnya dampak yang ditimbulkan akibat insiden atau bencana yang terjadi. Rencana tersebut juga harus mencakup deskripsi yang jelas dan akurat dari:
   - Bagaimana mobilisasi orang atau tim yang ditugaskan
   - Poin pertemuan langsung
   - Tempat pertemuan tim disertai dengan tempat pertemuan alternatif
   - Keadaan dimana organisasi menanggap bahwa gangguan dalam TI bisa diabaikan, misalnya, kesalahan dan intrupsi kecil, dsb.

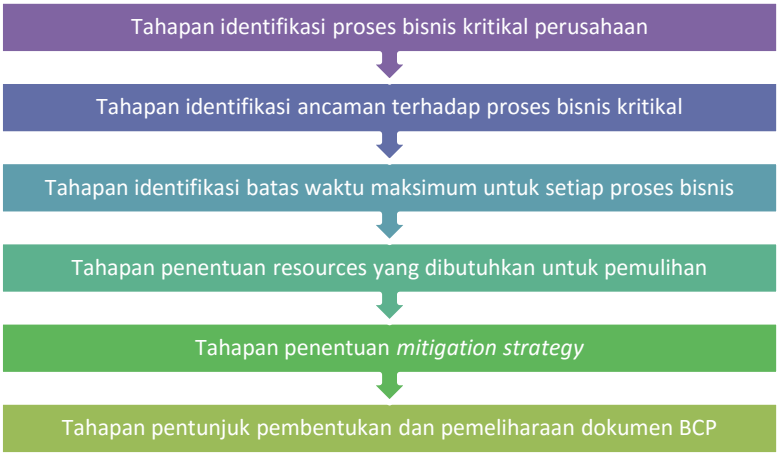
d. Pemilik dan pengeloa rencana respon dokumentasi dan pemulihan TI
   Manajemen harus menunjuk pemilik untuk respon rencana dan pemulihan TI sehingga orang yang telah ditunjuk tersebut bertanggung jawab untuk meninjau dan memperbaharui dokumen secara teratur. Serta harus menggunakan sistem kontrol versi dokumen formal sehingga perubahan dalam dokumen dapat diketahui oleh seluruh pihak yang terlibat

e. Kontak
   Dokumen rencana harus memuat data referensi kontak penting bagi semua pemangku kepentingan untuk memudahkan alur komunikasi di saat insiden terjadi.

2.2.14 Model Kerangka Kerja Business Continuity Plan berdasarkan Penelitian Sebelumnya

Terdapat beberapa penelitian sebelumnya yang dapat digunakan sebagai referensi dalam penelitian ini. Salah satunya adalah penelitian dari Kartini Slamet [31], dengan judul Thesis

"Pembentukan Kerangka Kerja Business Continuity Plan pada Bank Ritel X". Penelitian ini menghasilkan serangkaian tahapan penting dalam penyusunan dokumen BCP. Tahapan tersebut antara lain adalah:



Gambar 2.15 Tahapan Penyusunan Dokumen BCP (Sumber: Kartini, 2004)

Dalam penelitian ini juga dijelaskan bahwa dokumen BCP harus selalu ditinjau ulang dan diperbaharui secara berkala agar tetap relevan dengan keadaan perusahaan [31]. Contohnya jika ada penambahan proses bisnis yang baru maka dokumen BCP juga harus diubah sehingga jika bencana terjadi sewaktu-waktu, perusahaan bisa siap menghadapinya.

2.2.15 Framework ISO 27002

Standar ini merupakan penamaan ulang dari standar ISO/IEC 17799:2005. Standar ini dapat digunakan sebagai titik awal dalam penyusunan dan pengembangan ISMS *(Information Security Management Systems)* [32]. Standar ini memberikan panduan dalam perencanaan dan implementasi suatu program dalam

melindungi aset-aset informasi. Standar ini mengatur beberapa penerapan ISMS sebagai berikut:

- Semua kegiatan harus sesuai dengan tujuan dan proses pengamanan informasi yang didefinisikan dengan jelas dan didokumentasikan dalam suatu kebijakan dan prosedur
- Standar ini memberikan kontrol pengamanan, yang dapat digunakan oleh organisasi untuk diimplementasikan berdasarkan kebutuhan spesifik bisnis organisasi
- Semua pengukuran pengamanan yang digunakan dalam ISMS harus diimplementasikan sebagai hasil dari analisis risiko untuk mengeliminasi alat untuk mengurangi level risiko hingga level yang dapat diterima.
- Suatu proses harus dapat memaastikan adanya verifikasi secara berkelanjutan terhadap semua elemen sistem pengamanan melalui audit dan review
- Suatu proses harus dapat memastikan *continous improvement* dari semua elemen informasi dan sistem manajemen pengamanan.

Tujuan ISO/IEC 27002 adalah untuk memberikan rekomendasi manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab dalam inisiasi, implementasi, atau pengelolaan keamanan informasi pada organisasinya [32]. ISO/IEC 27002 terdiri atas 127 kendali dalam 11 kategori keamanan informasi:

- *Security policy*
- *Organization of information security*
- *Asset management*
- *Human resource security*
- *Physical and enviromental security*
- *Communication and operations management*
- *Access control*
- *Information systems acquisition development and maintenance*

- *Information security incident management*
- *Business continuity management*
- *Compliance*

Dalam penulisan tugas akhir ini, tidak semua bagian pada ISO 27002 dipakai, namun disesuaikan antara risiko yang telah teridentifikasi dengan sub-bab yang ada pada ISO 27002.

2.2.16 *Best Practice Bandwith Management* CISCO

Cisco adalah sebuah perusahaan global dalam bidang telekomunikasi yang berpusat di San Jose, California, Amerika Serikat. Cisco memiliki dua bidang usaha, usaha yang pertama adalah berkutat pada pembuatan *hardware* dan *software* yang berhubungan dengan jaringan komputer, dan yang kedua adalah dalam bidang pendidikan yaitu Cisco Networking Academy (CNA) [33].

Selain berfokus pada pembuatan *hardware* dan *software*, Cisco juga pernah beberapa kali mengeluarkan *best practice* maupun rekomendasi terkait proses pengelolaan *hardware* dan *software* itu sendiri. Salah satunya adalah *best practice* terkait *bandwith management* yang digunakan sebagai salah satu acuan rekomendasi mitigasi untuk risiko lambatnya akses jaringan [34].

Dalam *best practice* tersebut dijelaskan terkait bagaimana cara mengurangi latensi dalam jaringan yang digunakan dalam proses bisnis kritikal.

2.2.17 *Best Practice High-Availability Application* Microsoft

Microsoft adalah sebuah perusahaan multinasional Amerika Serikat yang mengembangkan, membuat, memberi lisensi, dan mendukung beragam produk dan jasa terkait dengan komputer. Microsoft merupakan pembuat perangkat lunak terbesar di dunia. Menurut pendapatannya, Microsoft juga merupakan salah satu perusahaan paling bernilai di dunia [35].

Sebagai perusahaan pembuat peralatan lunak terbesar di dunia, Microsoft sering mengeluarkan *best practice* maupun

rekomendasi terkait bagaimana cara mengembangkan perangkat lunak. Salah satu rekomendasi yang dikeluarkan oleh Microsoft adalah terkait dengan *high-availability application*, yaitu bagaimana cara mengembangkan aplikasi dengan tingkat availabilitas yang tinggi.

Dalam rekomendasinya, Microsoft membagi kelompok-kelompok aplikasi disesuaikan dengan kebutuhan organisasinya, antara lain adalah *non-commercial*, *commercial*, *business-critical*, dan *mission-critical* [36].

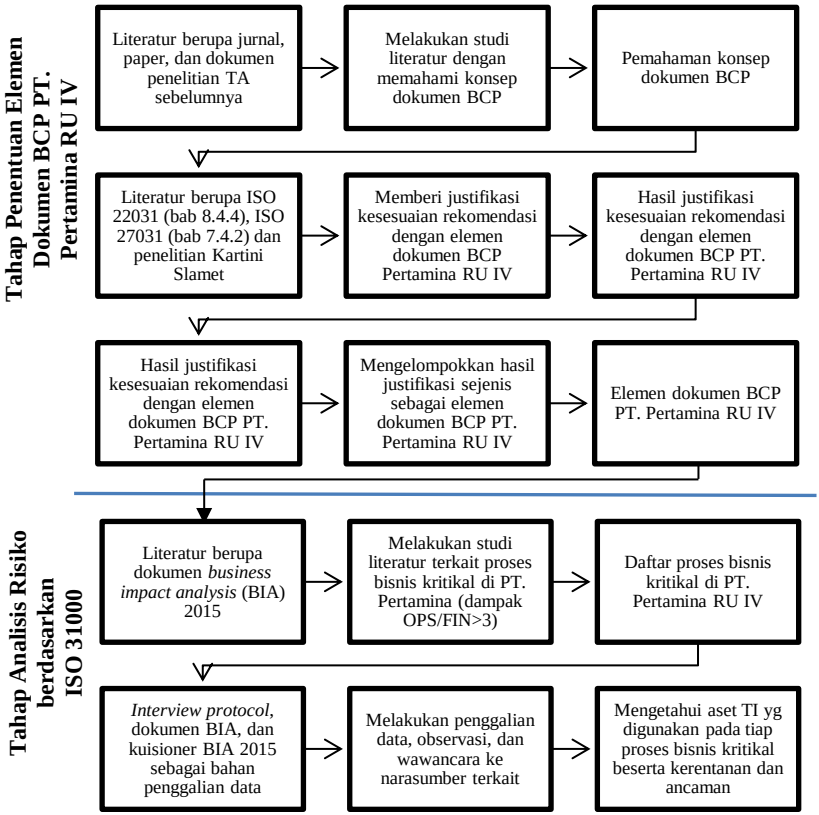
Yang digunakan sebagai acuan dalam rekomendasi mitigasi untuk risiko kegagalan aplikasi adalah kelompok aplikasi yang digunakan dalam *business-critical*.

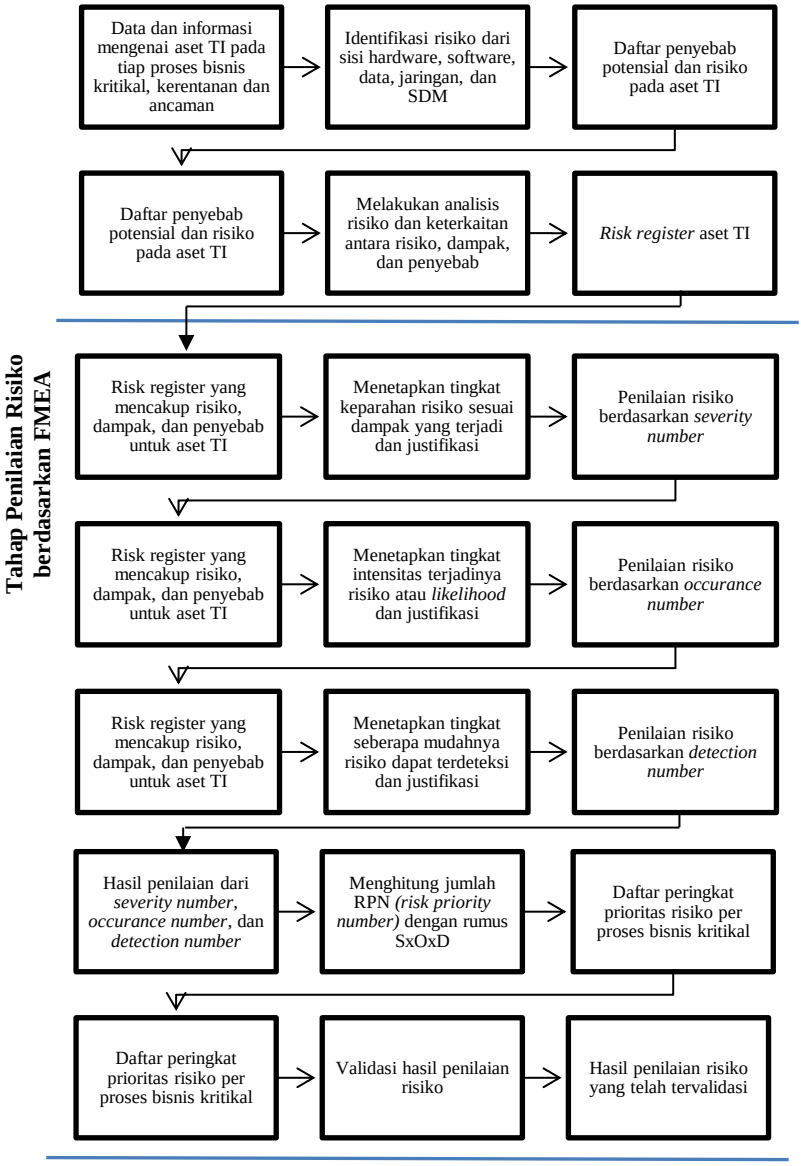
Halaman ini sengaja dikosongkan

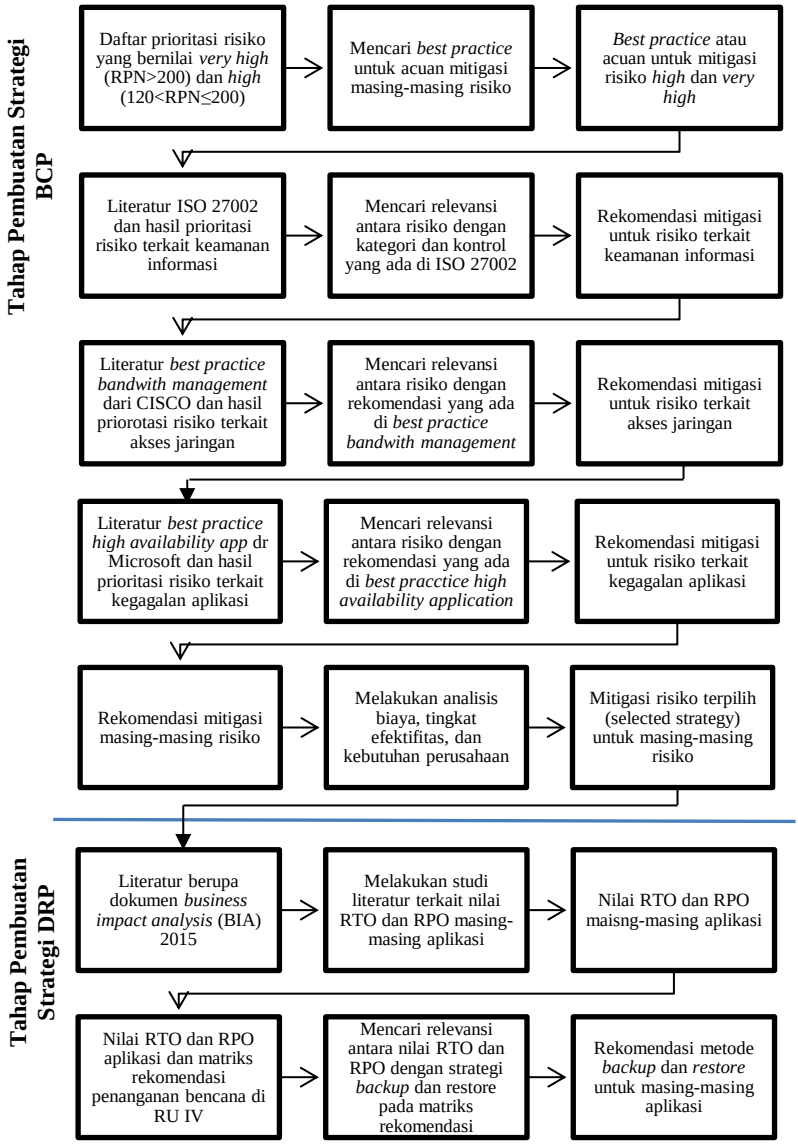
BAB III
METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai metodologi yang digunakan dalam pengerjaan tugas akhir ini. Metodologi tersebut berupa tahap yang memiliki proses.

3.1 Gambaran Metodologi




Data dan informasi mengenai aset TI pada tiap proses bisnis kritikal, kerentanan dan ancaman
Identifikasi risiko dari sisi hardware, software, data, jaringan, dan SDM
Daftar penyebab potensial dan risiko pada aset TI
Daftar penyebab potensial dan risiko pada aset TI
Melakukan analisis risiko dan keterkaitan antara risiko, dampak, dan penyebab
Risk register aset TI
Tahap Penilaian Risiko berdasarkan FMEA
Risk register yang mencakup risiko, dampak, dan penyebab untuk aset TI
Menetapkan tingkat keparahan risiko sesuai dampak yang terjadi dan justifikasi
Penilaian risiko berdasarkan *severity number*
Risk register yang mencakup risiko, dampak, dan penyebab untuk aset TI
Menetapkan tingkat intensitas terjadinya risiko atau *likelihood* dan justifikasi
Penilaian risiko berdasarkan *occurance number*
Risk register yang mencakup risiko, dampak, dan penyebab untuk aset TI
Menetapkan tingkat seberapa mudahnya risiko dapat terdeteksi dan justifikasi
Penilaian risiko berdasarkan *detection number*
Hasil penilaian dari *severity number*, *occurance number*, dan *detection number*
Menghitung jumlah RPN *(risk priority number)* dengan rumus SxOxD
Daftar peringkat prioritas risiko per proses bisnis kritikal
Daftar peringkat prioritas risiko per proses bisnis kritikal
Validasi hasil penilaian risiko
Hasil penilaian risiko yang telah tervalidasi



Gambar 3.1 Metodologi Penelitian (Sumber : Peneliti)

3.2 Uraian Metodologi

Berikut ini merupakan uraian metodologi yang dikerjakan dalam tugas akhir ini dari awal hingga akhir:

3.2.1 Tahap Penentuan Elemen Dokumen BCP

Tahapan ini bertujuan untuk menentukan elemen atau konten apa saja yang terdapat pada dokumen BCP PT. Pertamina RU IV. Langkah-langkah dalam tahapan ini akan dijelaskan sebagai berikut:

1. **Melakukan Studi Literatur dengan Memahami Konsep Dokumen BCP**
   Melakukan studi literatur dengan mempelajari jurnal, paper dan penelitian TA sebelumnya untuk mendapatkan gambaran dan pemahaman mengenai konsep BCP dan apa-apa saja yang harus ada dalam sebuah dokumen BCP.

2. **Memberi Justifikasi Kesesuaian Rekomendasi dengan Isi Dokumen BCP PT. Pertamina RU IV**
   Setelah memahami konsep BCP, maka penelitian dilanjutkan dengan menentukan konten dari dokumen BCP PT. Pertamina RU IV. Dalam menentukan konten dokumen BCP PT. Pertamina RU IV, peneliti menggunakan acuan *best practice* ISO 22301 (Bab 8.4.4 *Business Continuity Plan*), ISO 27031 (Bab 7.4.2 *Business Continuity Plan*), dan Thesis dari Kartini Slamet dengan judul "Pembentukan Kerangka Kerja Business Continuity Plan pada Bank Ritel X". Rekomendasi dari masing-masing *best practice* akan dianalisis dan diberi justifikasi terkait alasan mengapa konten tersebut harus ada pada dokumen BCP PT. Pertamina RU IV. Justifikasi diberikan secara subjektif, terbatas pada pengetahuan peneliti terkait dokumen BCP. Untuk penjelasan masing-masing rekomendasi *best practice* dapat dilihat pada **Bab 4.3.1 Perancangan Elemen Dokumen BCP PT. Pertamina RU IV.**

3. **Mengelompokkan Hasil Justifikasi Sejenis sebagai Elemen dalam Dokumen BCP PT. Pertamina RU IV**
   Setelah dilakukan analisis dan justifikasi pada tiap rekomendasi konten dokumen BCP dari beberapa *best practice*, maka tahap selanjutnya adalah mengelompokkan rekomendasi sejenis untuk membentuk elemen dalam dokumen BCP PT. Pertamina RU IV. Tujuan dari tahapan ini adalah agar isi dokumen BCP yang akan dibuat runtut dan tidak redundan antara satu poin dengan poin lainnya.

3.2.2 Tahap Analisis Risiko berdasarkan ISO 31000

Tahap analisis risiko berdasarkan ISO 31000 merupakan tahap kedua dalam pengerjaan tugas akhir ini. Tahapan ini meliputi proses identifikasi dan analisis risiko. Langkah-langkah dalam tahapan analisis risiko akan dijelaskan sebagai berikut:

1. **Menentukan Ruang Lingkup Analisis Risiko**
   Ruang lingkup dalam analisis risiko pada tugas akhir ini dibatasi pada risiko TI di proses bisnis kritikal (memiliki dampak OPS/FIN>3) PT. Pertamina RU IV. Penentuan proses bisnis apa saja yang masuk ke dalam kategori kritikal mengacu pada hasil analisis dokumen *business impact analysis* (BIA) tahun 2015.

2. **Melakukan Penggalian Data dan Wawancara ke Narasumber Terkait**
   Setelah menentukan ruang lingkup analisis risiko, maka dilakukan penggalian data untuk menentukan risiko TI apa saja yang ada pada proses bisnis kritikal PT. Pertamina RU IV. Dalam melakukan penggalian data kebutuhan tugas akhir ini dilakukan dengan tiga tahapan, yaitu wawancara, mempelajari dokumen perusahaan, dan observasi. Wawancara dilakukan untuk menggali informasi lebih terkait dengan aset TI serta risiko TI apa saja yang mungkin terjadi dengan menggunakan *interview protocol*. Narasumber dalam

proses wawancara ini adalah tiga karyawan pada fungsi IT RU IV yang merepresentasikan setiap sub fungsi TI pada fungsi IT RU IV. Sedangkan dokumen yang akan dipelajari adalah dokumen BIA 2015, aset TI 2015, serta kuisioner untuk penggalian data dokumen BIA 2015. Semua informasi yang berhubungan dan relevan akan digunakan untuk kebutuhan identifikasi risiko, analisis risiko, dan penilaian risiko.

3. **Identifikasi Kerentanan dan Ancaman Aset TI dari sisi *Hardware, Software,* Jaringan, Data, dan Sumber Daya Manusia**

   Dalam tahapan ini akan diidentifikasikan aset TI apa saja yang digunakan pada proses bisnis kritikal, beserta kerentanan dan ancaman yang dapat menjadi penyebab potensial pada proses bisnis kritikal yang didapat dari hasil wawancara, dokumen perusahaan, serta observasi peneliti. Dalam melakukan identifikasi risiko, aset TI akan dibagi menjadi lima kategori yaitu *hardware, software*, jaringan, data, dan sumber daya manusia. Tahap identifikasi risiko ini mencakup permasalahan yang terjadi, kerentanan yang dimiliki, ancaman yang dihadapi, penyebab potensial terjadinya risiko, dan dampak yang ditimbulkan dari terjadinya risiko. Dalam melakukan proses identifikasi, risiko akan diidentifikasi per proses bisnis kritikal dan akan dikategorikan berdasarkan komponen sistem informasi.

4. **Menganalisis Risiko Aset TI pada Proses Bisnis Kritikal**

   Berdasarkan daftar risiko yang telah teridentifikasi, maka akan dilakukan proses analisis risiko untuk melakukan penilaian risiko secara kuantitatif dan kualitatif dengan tujuan untuk mementukan risiko mana yang paling berbahaya dan membutuhkan prioritas lebih dari perusahaan. Analisis risiko dilakukan untuk mengetahui keterkaitan antara risiko, penyebab, dan dampak. Hasil dari tahapan analisis risiko

adalah *risk register* yang menjadi masukan dalam proses penilaian risiko.

3.2.3 Tahap Penilaian Risiko berdasarkan FMEA

Setelah dilakukan identifikasi dan analisis risiko, tahapan selanjutnya adalah penilaian risiko secara kuantitatif untuk mementukan risiko mana yang paling berbahaya dan membutuhkan perhatian lebih dari perusahaan. Langkah-langkah dalam melakukan penilaian risiko adalah sebagai berikut:

1. **Menentukan *Severity Number* dan Justifikasi**
   Tahap ini dilakukan untuk menetapkan nilai *severity number* atau tingkat keparahan dari suatu risiko dilihat dari dampak yang ditimbulkan jika risiko tersebut benar terjadi pada proses bisnis kritikal. Dari efek yang ditimbulkan akan diprioritaskan dari level 1 sebagai dampak yang tidak parah hingga level 10 yang bisa mengakibatkan dampak yang sangat parah. Kriteria untuk masing-masing level dapat dilihat pada Bab II. Tinjauan Pustaka. Selain pemberian nilai untuk *severity number*, dilakukan pula pemberian justifikasi. Justifikasi bertujuan untuk mengetahui alasan pemberian nilai pada setiap risiko. Justifikasi diberikan berdasarkan hasil observasi dari kondisi nyata perusahaan yang dilakukan oleh peneliti.

2. **Menentukan *Occurance Number* dan Justifikasi**
   Tahap ini dilakukan untuk menetapkan nilai *occurance number* atau tingkat kemungkinan risiko tersebut terjadi. Penentuan nilai *occurance number* dilihat dari penyebab *(causes)* dan tingkat kemungkinan *(probability)* munculnya suatu risiko yang akan menghasilkan kegagalan dan akibat tertentu bagi perusahaan. Dari kemungkinan kejadian akan diprioritaskan dari level 1 sebagai "yang paling tidak mungkin terjadi", hingga level 10 sebagai "yang paling sering terjadi". Kriteria untuk masing-masing level dapat dilihat pada Bab II. Tinjauan Pustaka. Selain pemberian nilai untuk *severity number*, dilakukan pula pemberian justifikasi. Justifikasi

bertujuan untuk mengetahui alasan pemberian nilai pada setiap risiko. Justifikasi diberikan berdasarkan hasil observasi dari kondisi nyata perusahaan yang dilakukan oleh peneliti.

3. **Menentukan *Detection Number* dan Justifikasi**
   Tahap ini dilakukan untuk menetapkan nilai *detection number* yang merupakan tingkat yang menunjukkan sejauh mana peluang potensi kegagalan tersebut dapat dideteksi oleh perusahaan. Penentuan nilai *detection number* didasarkan pada implementasi kontrol yang telah diterapkan untuk mencegah atau mendeteksi penyebab kegagalan sebelum kegagalan tersebut terjadi. Dari setiap efek yang ditimbulkan akan diprioritaskan dari level 1 sebagai efek yang mudah terdeteksi hingga level 10 sebagai efek yang paling tidak mudah terdeteksi. Kriteria untuk masing-masing level dapat dilihat pada Bab II. Tinjauan Pustaka. Selain pemberian nilai untuk *severity number*, dilakukan pula pemberian justifikasi. Justifikasi bertujuan untuk mengetahui alasan pemberian nilai pada setiap risiko. Justifikasi diberikan berdasarkan hasil observasi dari kondisi nyata perusahaan yang dilakukan oleh peneliti.

4. **Menghitung Jumlah *Risk Priority Number***
   Tahapan selanjutnya setelah menetapkan nilai *severity number, occurance number,* dan *detection number* adalah menentukan nilai *risk priority number* (RPN). RPN adalah ukuran yang digunakan ketika menilai risiko untuk membantu mengidentifikasi risiko mana yang harus diprioritaskan. Proses pembobotan RPN menggunakan rumus sebagai berikut:

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

   Keterangan:
   S = *Severity number* (angka tingkat keparahan)
   O = *Occurence number* (angka tingkat probabilitas kejadian)
   D = *Detection number* (angka tingkat deteksi)

Setelah menghitung RPN maka langkah selanjutnya adalah dengan mengurutkan risiko dari RPN yang paling tinggi ke rendah. Nilai RPN tersebut kemudian diklasifikasikan berdasarkan level prioritas kesalahan yang memerlukan penanganan lanjut, sebagai berikut:

Tabel 3.1. RPN (Sumber: FMEA)

Level Risiko	Skala RPN
Very High	≥ 200
High	120-199
Medium	80-119
Low	20-79
Very Low	0-19

5. **Melakukan Validasi Hasil Analisis Risiko**
   Tahap selanjutnya setelah menilai tiap risiko per proses bisnis dan melakukan prioritasi risiko adalah mengajukan validasi ke perusahaan terkait hasil analisis risiko yang telah dilakukan. Tujuan dari validasi ini adalah untuk menyatakan bahwa analisis risiko yang dibuat sudah benar dan sesuai dengan kondisi perusahaan. Validasi dituangkan dalam bentuk surat konfirmasi yang diajukan pada bagian TI perusahaan.

3.2.4 Tahap Pembuatan Strategi BCP

Setelah menyelesaikan tahapan analisis risiko, maka akan dilanjutkan dengan pembuatan strategi BCP. Untuk langkah-langkah yang dilakukan pada tahapan ini akan dijelaskan sebagai berikut:

1. **Mencari Best Practice untuk Acuan Mitigasi Masing-Masing Risiko High dan Very High**
   Risiko yang bernilai *very high* (RPN≥200) dan *high* (RPN 120-199) menjadi masukan untuk tahap pembuatan strategi. Strategi yang dibuat dibedakan menjadi dua, yaitu strategi

dalam bentuk aksi manajemen dan strategi dalam bentuk mitigasi risiko. Strategi untuk aksi manajemen bersifat subjektif, yaitu hasil pemikiran peneliti, sedangkan untuk strategi yang berupa mitigasi risiko merupakan hasil rekomendasi *best practice*. Hasil analisis risiko yang bernilai *very high* (RPN≥200) dan *high* (RPN 120-199) menentukan *best practice* apa yang digunakan sebagai acuan.

2. **Menyusun Mitigasi Risiko berdasarkan Rekomendasi ISO 27002**
   Untuk risiko yang berkaitan dengan keamanan jaringan, digunakan acuan *best practice* ISO 27002:2005. ISO 27002 merupakan sebuah standar internasional yang membahas mengenai *information security management systems* (ISMS). Dalam proses penyusunan strategi mitigasi, prosesnya adalah dengan mencari relevansi antara risiko dengan kategori risiko yang ada di ISO 27002, lalu kemudian dicari kontrol yang harus diterapkan sebagai upaya mitigasi untuk risiko terkait. Selain kontrol untuk mitigasi risiko, juga terdapat pentunjuk implementasi *(implementation guidance)* yang dapat digunakan sebagai petunjuk perusahaan jika ingin menerapkan kontrol yang dimaksud.

3. **Menyusun Mitigasi Risiko berdasarkan Rekomendasi Bandwith Management dari Cisco**
   Untuk risiko yang berkaitan dengan akses jaringan, digunakan *best practice* manajemen bandwith dari Cisco. Strategi mitigasi untuk risiko yang berkaitan dengan akses jaringan mengacu pada rekomendasi dari Cisco terkait dengan bagaimana metode pengaturan bandwith untuk menghindari lambatnya akses jaringan.

4. **Mitigasi Risiko berdasarkan Rekomendasi High Availability dari Microsoft**

Untuk risiko yang berkaitan dengan kegagalan aplikasi, digunakan *best practice high availability application* dari Microsoft. Strategi mitigasi untuk risiko yang berkaitan dengan kegagalan aplikasi mengacu pada rekomendasi dari Microsoft terkait dengan bagaimana metode pengembangan aplikasi dengan tingkat availabilitas yang tinggi.

5. **Melakukan Analisis Biaya, Tingkat Efektifitas, dan Kebutuhan Perusahaan pada masing-masing Opsi Mitigasi Risiko**
   Setelah mendapatkan rekomendasi mitigasi dari *best practice* untuk masing-masing risiko, maka dilanjutkan dengan memilih strategi mana yang paling tepat dan dapat diaplikasikan oleh perusahaan. Proses pemilihan strategi dilakukan dengan melakukan analisis biaya, tingkat efektifitas, serta kebutuhan dan kesanggupan perusahaan dalam mengaplikasian strategi tersebut. Acuan yang digunakan untuk memberikan justifikasi adalah rencana pengembangan TI tahun 2016 PT. Pertamina RU IV.

3.2.5 Tahap Pembuatan Strategi DRP

Setelah menentukan strategi BCP, maka dilanjutkan dengan menentukan strategi DRP. Strategi DRP dibatasi pada strategi pencadangan *(backup)* dan strategi pemulihan *(restore)* untuk layanan aplikasi non-ERP saja. Untuk langkah-langkah yang dilakukan pada tahap ini antara lain adalah:

1. **Menentukan Nilai RTO dan RPO Aplikasi**
   Dalam menentukan strategi pencadangan dan pemulihan aplikasi diperlukan informasi terkait nilai RTO dan RPO masing-masing aplikasi. Informasi ini didapatkan dari hasil analisis dokumen *business impact analysis* (BIA) 2015. Pada bagian analisis RTO dan RPO aplikasi.

2. **Menentukan Strategi Backup dan Restore Aplikasi**

Setelah mengetahui nilai RTO dan RPO masing-masing aplikasi, dilanjutkan dengan menentukan strategi pencadangan dan pemulihan yang sesuai. Cara penentuannya adalah dengan menggunakan bantuan matriks penanggulangan bencana RU IV hingga menghasilkan rekomendasi pencadangan dan pemulihan untuk masing-masing aplikasi. Berikut merupakan bentuk matriks penganggulangan bencana di RU IV:

Tabel 3.2 Matriks Rekomendasi Strategi Pencadangan dan Pemulihan (Sumber: Pertamina RU IV)

		RTO (Recovery Time Objective)		
		High	Medium	Low
RPO (Recovery Point Objective)	< 1 Jam	*Electronic Vaulting (Active - Active)*	*Electronic Vaulting (Active - Standby)*	*Offsite Vaulting*
		Mirroring	Incremental Backup – Scheduled	Normal Backup – Daily
	1 - 24 Jam	*Electronic Vaulting (Active – Active)*	*Electronic Vaulting (Active - Standby)*	*Offsite Vaulting*
		Incremental Backup – Scheduled	Incremental Backup - Scheduled	Normal Backup – Daily
	> 24 Jam	*Electronic Vaulting (Active – Active)*	*Electronic Vaulting (Active - Standby)*	*Offsite Vaulting*
		Normal Backup – Daily	Normal Backup - Daily	Normal Backup – Daily

BAB IV
PERANCANGAN

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

4.1 Perancangan Studi Kasus

Dalam pengerjaan tugas akhir ini, dibutuhkan perancangan studi kasus untuk menentukan dan memahami alasan penggunaan studi kasus dalam tugas akhir ini.

4.1.1 Tujuan Studi Kasus

Pada penelitian ini dilakukan pembuatan *business continuity plan* (BCP) sebagai salah satu upaya untuk mitigasi risiko. Penelitian ini membutuhkan studi kasus yang digunakan sebagai objek untuk menggali lebih dalam terkait keadaan dan kebutuhan terkait BCP itu sendiri. Menurut Yin, studi kasus adalah sebuah cara unik untuk mengamati suatu fenomena alam yang ada dalam satu set data [37]. Yin mengemukakan bahwa ada tiga jenis studi kasus, antara lain adalah, eksploratoris (menggali) yaitu melakukan eksplorasi terhadap fenomena apapun dalam data yang berfungsi sebagai tempat tujuan untuk meneliti, deskriptif yaitu digunakan untuk mengambarkan fenomena alamiah yang terjadi pada data dalam bentuk narasi, dan eksplanatoris (memperjelas) yaitu menjelaskan fenomena dalam data mulai dari hal yang dasar hingga dalam dan menjelaskan hubungan klausal dalam konteks kehidupan nyata.

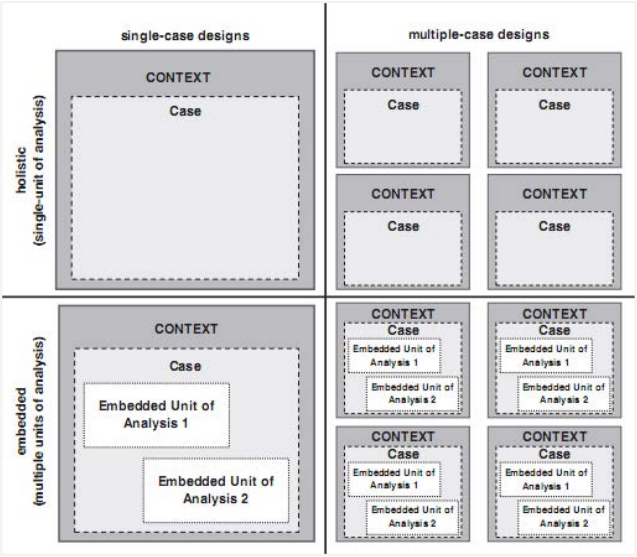
Dalam penelitian tugas akhir ini, kategori studi kasus yang digunakan adalah jenis ekplanatoris (menggali). Studi kasus

eksplanatoris digunakan dalam penelitian ini karena diperlukan sebuah objek yang akan dieksplorasi atau digali mengenai pembuatan dokumen *business continuity plan* (BCP) di perusahaan. Tujuan dari penggunaan studi kasus eksplanatoris ini adalah untuk menjawab rumusan masalah berikut:

1. Apa saja elemen dalam dokumen BCP PT. Pertamina Refinery Unit IV Cilacap?
2. Apa hasil identifikasi risiko teknologi informasi di PT. Pertamina Refinery Unit IV Cilacap?
3. Bagaimana hasil *business continuity plan* (BCP) berbasis risiko yang sesuai dengan kebutuhan PT. Pertamina Refinery Unit IV?

4.1.2 *Unit of Analyis*

Perancangan studi kasus terbagi menjadi dua, yaitu *single case design* dan *multiple-case design*. Perbedaan keduanya terletak pada jumlah studi kasus yang dijadikan objek. Pada jenis *single case design* hanya menggunakan satu kasus untuk diuji, sedangkan pada *multiple case design* menggunakan dua atau lebih kasus untuk diuji. Dari kedua jenis tersebut dibagi menjadi empat tipe yang disesuaikan dengan banyaknya *unit of analysis* yang digambarkan pada gambar di bawah ini:



Gambar 4.1 Unit of Analysis (Sumber: Yin R)

Single case dapat digunakan pada penelitian dengan kasus yang kritis atau unik, mengkaji teori yang telah dirumuskan, dan melakukan eksplorasi. Sedangkan pada *multiple case* digunakan untuk penelitian eksplorasi dengan tujuan untuk menemukan replikasi temuan di seluruh kasus.

Perancangan studi kasus yang digunakan dalam penelitian tugas akhir ini adalah *single case* (satu studi kasus) dengan dua konteks *unit of analysis*. Single case dipilih karena penelitian ini bertujuan untuk melakukan eksplorasi atau menggali yang berfokus pada studi kasus dengan mempertimbangkan dua konteks, yaitu dari analisis risiko dan penilaian risiko.

4.2 Perancangan Pengumpulan Data dan Informasi

Pada bagian ini akan menjelaskan mengenai tahapan persiapan pengumpulan data dan informasi yang nantinya akan diolah untuk dapat menjawab rumusan masalah. Terdapat beberapa

teknik yang digunakan dalam mengumpulkan data dan informasi, antara lain adalah *interview* atau wawancara, analisis dokumen perusahaan dan observasi.

4.2.1 Wawancara

Proses wawancara akan dilakukan pada fungsi IT RU IV. Diharapkan setelah melakukan wawancara akan didapatkan informasi terkait risiko TI yang dihadapi oleh perusahaan.

Tabel 4.1 Rencana Wawancara Risiko TI (Sumber: Peneliti)

Nama Proses	Pengumpulan Data dan Informasi
Teknik	*Interview*/Wawancara Teknik wawancara akan dilakukan dengan metode tanya jawab langsung dengan narasumber. Wawancara akan dilakukan secara terstruktur, dimana peneliti telah menyiapkan pertanyaan-pertanyaan yang dibutuhkan terlebih dahulu.
Objek	Aset TI dan risiko TI perusahaan
Kebutuhan proses	• *Interview protocol* • Laptop • Alat tulis
Tahapan pelaksanaan	Tahapan dalam melakukan wawancara adalah sebagai berikut: • Menetapkan tujuan dan jumlah wawancara • Menentukan narasumber • Membuat *interview protocol* • Memulai proses wawancara • Mendokumentasikan hasil wawancara

4.2.2.1 Jumlah dan Tujuan Wawancara

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

Tabel 4.2 Rencana Jumlah dan Tujuan Wawancara (Sumber: Peneliti)

Wawancara Ke-	Narasumber	Tujuan Wawancara
1	Bagian IT unit RU IV (IT RU IV)	Wawancara ini bertujuan untuk mengetaui aset dan risiko TI apa saja yang ada pada bagian IT unit RU IV. Pada wawancara ini akan digali lebih dalam terkait identifikasi aset TI, kebutuhan keamanan, serta kontrol keamanan TI apa yang sudah diterapkan. Selain melakukan wawancara, peneliti juga melakukan observasi pada ruang kerja dan lingkungan kantor untuk mendapatkan hasil dan intrepetasi yang lebih akurat.
2	Bagian Business Operation and Technology (IT RU IV)	Wawancara ini bertujuan untuk mengetaui aset dan risiko TI apa saja yang ada pada bagian *business operation and technology*. Pada wawancara ini akan digali lebih dalam terkait identifikasi aset TI,

		kebutuhan keamanan, serta kontrol keamanan TI apa yang sudah diterapkan. Selain melakukan wawancara, peneliti juga melakukan observasi pada ruang kerja dan lingkungan kantor untuk mendapatkan hasil dan intrepetasi yang lebih akurat.
3	Bagian Business Support and Infrastructure (IT RU IV)	Wawancara ini bertujuan untuk mengetaui aset dan risiko TI apa saja yang ada pada bagian *business support and infrastructure*. Pada wawancara ini akan digali lebih dalam terkait identifikasi aset TI, kebutuhan keamanan, serta kontrol keamanan TI apa yang sudah diterapkan. Selain melakukan wawancara, peneliti juga melakukan observasi pada ruang kerja dan lingkungan kantor untuk mendapatkan hasil dan intrepetasi yang lebih akurat.

4.2.2.2 Profil Narasumber Wawancara

Sebelum melakukan wawancara, peneliti terlebih dahulu harus menentukan narasumber. Narasumber yang dipilih tentu saja harus sesuai dengan tujuan wawancara serta berada dalam kapasitas objek wawancara. Hal ini bertujuan agar narasumber

dapat memberikan informasi yang valid dan sesuai serta relevan dengan cakupan wawancara itu sendiri. Berikut merupakan profil narasumber yang akan diwawancara dalam penelitian ini:

Tabel 4.3 Profil Narasumber (Sumber: Peneliti)

Nama	Jabatan
Dito Anggodo Prihastomo	Assisstant Data Center Operation and Automation
Satrio Wahyu Pratomo	Junior Assisstant Computer Development and Creative Technology
Indri Setyowati	Assisstant Fixed and Mobile Communication

4.2.2.2 Daftar Pertanyaan Wawancara (*Interview Protocol*)

Tabel 4.4 Daftar Pertanyaan Wawancara (Sumber: Peneliti)

No	Tujuan Pertanyaan	Detail Ringkas Pertanyaan
1	Untuk mengetahui kondisi umum fungsi TI di PT. Pertamina RU IV	• Kondisi umum fungsi TI RU IV • Pembagian sub fungsi IT RU IV • Tupoksi masing-masing fungsi
2	Untuk menggali informasi terkait aset kritis teknologi dan sistem informasi yang diterapkan perusahaan	• Proses umum penerapan TI di Pertamina RU IV • Fungsional bisnis pengguna layanan TI • Aset TI yang digunakan dalam proses bisnis kritikal • Aset TI kritikal yang dapat memberikan ancaman bagi

		keberlangsungan proses bisnis kritikal • Komponen vital pendukung layanan TI
3	Untuk menggali informasi mengenai identifikasi ancaman, kerentanan, dan risiko aset teknologi dan informasi	• Ancaman pada aset TI • Kerentanan pada aset TI
4	Untuk menggali informasi terkait praktik keamanan yang telah diterapkan serta kelemahan perusahaan	• Kontrol keamanan yang diterapkan untuk mengantisipasi terjadinya risiko

4.2.2 Analisis Dokumen

Selain proses wawancara, teknik lain yang dilakukan dalam pengumpulan data dan informasi adalah dengan melakukan analisis dokumen RU IV yang dapat mendukung penelitian.

Tabel 4.5 Rencana Analisis Dokumen (Sumber: Peneliti)

Nama Proses	Pengumpulan Data dan Informasi
Teknik	Analisis Dokumen Pada proses ini akan dilakukan analisis terkait dokumen-dokumen yang dimiliki oleh PT. Pertamina RU IV terkait dengan pembuatan BCP dan hanya jika dokumen tersebut diperbolehkan untuk dianalisis oleh pihak manajemen.
Tujuan	Tujuan analisis dokumen adalah untuk mengetahui lebih lanjut mengenai profil organisasi, aset TI apa saja yang

	digunakan, risiko TI, dan kondisi kekinian dari Pertamina RU IV
Objek	• Dokumen RJPP (rencana jangka panjang) TI 2015 • Daftar aset TI 2015 • Daftar risiko TI 2014 • Dokumen *business impact analysis* (BIA) 2015 • Rencana tindak lanjut mitigasi risiko TI 2015 • Dokumen PQA (*Pertamina Quality Assessment)* 2014 • Dokumen CMDB (*Configuration Management Database*) IT RU IV versi 1.0 • Kuisioner BIA 2015 • Rencana pengembangan TI 2016
Tahapan pelaksanaan	Tahapan dalam melakukan analisis dokumen adalah sebagai berikut: 1. Menetapkan tujuan dan dokumen yang dibutuhkan 2. Mengkonsultasikan daftar dokumen yang diperlukan 3. Melakukan analisis dari dokumen-dokumen yang telah didapatkan 4. Mendokumentasikan hasil analisis dokumen

4.3 Perancangan Pengolahan Data

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

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

4.3.1 Perancangan Elemen Dokumen BCP PT. Pertamina RU IV

Perancangan dalam menentukan elemen atau bagian yang terkandung dalam dokumen BCP PT. Pertamina RU IV mencakup proses sebagai berikut:

1. Elemen dokumen BCP PT. Pertamina RU IV akan mengacu pada rekomendasi elemen dokumen prosedur yang terkandung dalam ISO 22301:2012 *(business continuity management systems)* dan ISO 27031:2011 *(business continuity in ICT)* serta penelitian sebelumnya terkait model kerangka kerja *business continuity plan*.
2. Rekomendasi elemen dari standar acuan akan dipilih dan disesuaikan dengan keadaan dan kondisi yang ada di PT. Pertamina RU IV sehingga menghasilkan dokumen BCP PT. Pertamina RU IV.

4.3.1 Perancangan Analisis Risiko

Perancangan dalam melakukan analisis risiko mencakup langkah-langkah sebagai berikut:

1. Proses bisnis kritikal hasil analisis BIA 2015 menjadi acuan dalam melakukan analisis risiko. Analisis risiko dibatasi hanya pada risiko TI yang ada pada proses bisnis kritikal.
2. Hasil wawancara, survei, dan dokumen perusahaan terkait risiko TI kemudian dipetakan sehingga menghasilkan kerentanan, ancaman, serta penyebab potensial.
3. Setelah mengetahui penyebab potensial, maka penyebab potensial tersebut akan dipetakan menjadi risiko-risiko TI yang terdapat pada masing-masing proses bisnis kritikal.
4. Risiko-risiko TI yang teridentifikasi tersebut selanjutnya akan dianalisis dengan memberikan nilai *severity*, *occurance* dan *detection* hingga menghasilkan nilai RPN

(risk priority number) untuk masing-maisng risiko. Nilai RPN ini selanjutnya akan diurutkan dari yang paling besar untuk menghasilkan prioritasi risiko per proses bisnis kritikal.

5. Hasil dari analisis risiko akan dikonfirmasi ke pihak perusahaan sebagai bentuk persetujuan terhadap hasil analisis yang telah dibuat.

4.3.2 Perancangan Strategi BCP

Perancangan dalam menentukan strategi BCP mencakup langkah-langkah sebagai berikut:

1. Risiko TI yang bernilai *very high* akan menjadi dasar dalam menentukan strategi BCP. Strategi BCP yang dibuat akan dibatasi pada risiko TI yang bernilai *very high* (memiliki nilai RPN≥200) dan risiko yang bernilai high (RPN: 120-199)
2. Pembuatan strategi BCP akan dibedakan menjadi dua, yaitu strategi yang berupa aksi manajemen dalam menghadapi BIA dan strategi yang merupakan upaya mitigasi risiko dengan acuan ISO 27002:2005 (*Information Technology – Security Techniques – Code of Practice for Information System Security Management), best practice bandwith management* dari Cisco, dan *best practice high availability* aplikasi dari Microsoft. Hasil rekomendasi dari setiap *best practice* kemudian akan dianalisis dari segi biaya, tingkat efektifitas dan kebutuhan perusahaan hingga menghasilkan strategi mitigasi risiko yang paling tepat dan dapat diaplikasikan pada PT. Pertamina RU IV.
3. Selain membuat strategi BCP, dibuat pula strategi DRP yang merupakan subset dari strategi BCP dengan menggunakan parameter RTO dan RPO masing-masing aplikasi. Strategi DRP yang dibuat hanya mencakup pada strategi pencadangan *(backup)* dan strategi pemulihan *(restore).*

4.4 Rencana Validasi BCP

Tahapan validasi merupakan tahapan yang dilakukan untuk memastikan bahwa hasil analisa yang dilakukan sudah benar dan sesuai dengan keadaan perusahaan. Tahapan ini dilakukan sebagai konfirmasi bahwa apa yang dikerjakan oleh peneliti telah sesuai dengan kebutuhan PT. Pertamina RU IV. Proses validasi dilakukan dengan mengajukan surat konfirmasi pada perwakilan manajemen RU IV. Berikut merupakan tabel rencana validasi yang akan diajukan pada pihak PT. Pertamina RU IV:

Tabel 4.6 Rencana Validasi BCP (Sumber: Peneliti)

No	Nama Validasi	Deskripsi Validasi
1	Validasi kesesuaian analisis risiko PT. Pertamina RU IV	Tujuan dari validasi ini adalah untuk memastikan bahwa analisis risiko yang dibuat oleh peneliti telah sesuai dengan keadaan organisasi berdasarkan penggalia data dan batasan yang dilakukan di PT. Pertamina RU IV. Validasi ini ditujukan pada perwakilan manajemen dengan menggunakan surat konfirmasi sebagai bukti kesesuaian analisis dengan kondisi sebenernya.
2	Validasi dokumen akhir BCP pada PT. Pertamina RU IV	Validasi ini bertujuan untuk memastikan bahwa dokumen akhir BCP yang telah dibuat oleh peneliti telah sesuai dengan kebutuhan dan kondisi PT. Pertamina RU IV.

BAB V
IMPLEMENTASI

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

5.1 Hasil Pengumpulan Data dan Informasi

Proses pengumpulan data dan informasi dilakukan dengan menggunakan dua metode, yaitu dengan melakukan wawancara dan melakukan analisis dokumen.

5.1.1 Hasil Wawancara

Pengumpulan data menggunakan metode wawancara dilakukan kepada beberapa pihak terkait di PT. Pertamina RU IV. Berikut merupakan keterangan dari pelaksanaan tahap pengumpulan data dan informasi dengan menggunakan metode wawancara:

Tabel 5.1 Hasil Wawancara (Sumber: Peneliti)

Wawancara 1		
Narasumber	:	Dito Anggodo Prihastomo
Jabatan	:	Assistant Data Center Operation and Automation
Tanggal	:	17 Februari 2016
Lokasi	:	Head Office PT. Pertamina RU IV
Topik	:	Identifikasi aset TI, identifikasi risiko TI apa saja yang mungkin terjadi, kebutuhan keamanan, dan kontrol keamanan TI apa yang telah diterapkan.
Hasil	:	Lampiran C
Wawancara 2		
Narasumber	:	Satrio Wahyu Pratomo

Jabatan	:	Junior Assistant Computer Development and Creative Technology
Tanggal	:	18 Februari 2016
Lokasi	:	Head Office PT. Pertamina RU IV
Topik	:	Identifikasi aset TI, identifikasi risiko TI apa saja yang mungkin terjadi, kebutuhan keamanan, dan kontrol keamanan TI apa yang telah diterapkan.
Hasil	:	Lampiran D
Wawancara 3		
Narasumber	:	Indri Setyowati
Jabatan	:	Assisstant Fixed and Mobile Communication
Tanggal	:	19 Februari 2016
Lokasi	:	Gedung Telekomunikasi dan Jaringan PT. Pertamina RU IV
Topik	:	Identifikasi aset TI, identifikasi risiko TI apa saja yang mungkin terjadi, kebutuhan keamanan, dan kontrol keamanan TI apa yang telah diterapkan.
Hasil	:	Lampiran E

* ***Keterangan***: Hasil wawancara terdokumentasi pada bagian lampiran.

5.1.2 Hasil Analisis Dokumen

Selain melalui wawancara, tahapan pengumpulan data dan informasi juga dilakukan dengan melakukan analisis data dari dokumen terkait penelitian yang dimiliki oleh perusahaan. Berikut merupakan dokumen yang dianalisis pada penelitian tugas akhir ini:

1. **Dokumen RJPP (Rencana Jangka Panjang) TI 2015**
   Dokumen rencana jangka panjang IT RU IV merupakan suatu dokumen yang memuat mengenai strategi-strategi

yang telah direncanakan oleh IT RU IV dalam kurun waktu 2013 hingga 2017. Analisis yang dilakukan akan difokuskan pada strategi-strategi yang berkaitan dengan mitigasi risiko TI atau langkah yang diambil manajemen dalam merencanakan keberlanjutan bisnis di RU IV.

2. **Daftar Aset TI 2015**
   Dokumen aset TI 2015 memuat daftar aset-aset TI yang ada di dalam PT. Pertamina RU IV pada tahun 2015. Aset TI dalam dokumen ini dibagi menjadi lima kelompok, yaitu data/informasi, *software*, *physical* atau *hardware*, people, intangible. Karena dokumen ini terakhir diupdate pada tahun 2015, maka perlu dilakukan adanya penyesuaian penambahan dan pengurangan aset dengan melalui proses wawancara dengan pihak terkait. Harapannya, analisis yang dilakukan akan lebih akurat karena disesuaikan dengan kondisi kekinian perusahaan.

3. **Daftar Risiko TI 2014**
   Dokumen risiko TI 2014 adalah sebuah dokumen yang memuat mengenai analisis risiko TI di PT. Pertamina RU IV pada tahun 2014. Disesuaikan dengan daftar aset TI, dokumen risiko TI 2014 juga dibagi menjadi lima kelompok, yaitu data/informasi, *software*, *physical* atau *hardware*, people, intangible. Namun demikian, perlu adanya analisis ulang yang lebih mendalam terkait risiko TI yang ada di perusahaan. Hal ini dikarenakan hanya terdapat satu analisis risiko pada setiap aset di perusahaan. Hal ini tentu saja berbeda dengan kondisi *real*, dimana untuk satu aset TI, terdapat beberapa risiko yang mungkin terjadi.

4. **Dokumen *Business Impact Analysis* (BIA) 2015**
   Dokumen BIA 2015, yang dikerjakan oleh penulis saat melaksanakan kerja praktek, berisi analisis terkait fungsi bisnis apa saja yang ada di Pertamina RU IV, bagaimana

dampak atau kerugian yang dialami oleh perusahaan jika proses bisnis itu berhenti, hingga menghasilkan proses bisnis urutan kritikalitas proses bisnis, dari yang bersifat kritikal, moderat, hingga yang bersifat rendah. Dalam dokumen BIA juga dilakukan analisis terkait aset SI/TI apa saja yang digunakan oleh tiap-tiap fungsi bisnis dan bagaimana urgensitasnya. Hasil dari BIA 2015 akan dijadikan acuan dalam penelitian ini. Walaupun yang dijadikan acuan adalah BIA 2015, namun proses bisnis dan fungsi bisnis di PT. Pertamina RU IV sekarang ini bisa dikatakan tidak mengalami banyak perubahan sehingga hasil analisis BIA 2015 bisa dikatakan masih relevan dan dapat digunakan sebagai acuan dalam pembuatan dokumen BCP.

5. **Rencana Tindak Lanjut Mitigasi Risiko TI 2015**
   Dokumen ini berisi rencana mitigasi risiko TI yang mengacu pada hasil analisis risiko TI 2015. Rencana mitigasi dalam dokumen ini merupakan rencana mitigasi yang sudah disesuaikan dengan kondisi dan *budget* yang dimiliki oleh IT RU IV, karena tidak semua rencana mitigasi dapat diaplikasikan oleh perusahaan. Dokumen ini bisa digunakan sebagai referensi dalam pembuatan strategi BCP yang akan dibuat dalam penelitian ini.

6. **Dokumen PQA (*Pertamina Quality Assesment)* 2014**
   Dokumen PQA (*Pertamina Quality Assesment)* 2014 merupakan sebuah dokumen yang berisi profil organisasi, penjelasan terkait kepemimpinan dan keberlanjutan bisnis, bagaimana Pertamina mencapai operasional ekselen, tenaga kerja, pelanggan, hingga hasil kinerja Pertamina RU IV. Informasi spesifik yang digunakan adalah informasi terkait gambaran proses bisnis secara general yang ada di Pertamina RU IV, yang menjadi dasar dalam melakukan analisis BIA.

7. **Dokumen CMDB (*Configuration Management Database*) IT RU IV versi 1.0**
   Dokumen CMDB berisi daftar seluruh software yang ada dan dibuat oleh IT RU IV. Dokumen ini mendukung dan saling melengkapi dokumen aset TI agar hasil analisisnya bisa lebih lengkap dan lebih mendalam.

8. **Kuisioner BIA 2015**
   Kuisoner BIA berisikan daftar pertanyaan dan jawaban dari masing-masing responden ketika wawancara ke seluruh fungsi di RU IV. Walaupun hasilnya sudah ada dalam dokumen BIA, namun dokumen ini bisa dijadikan penunjang apabila peneliti membutuhkan analisa lebih untuk beberapa fungsi, serta mewasapadai jikalau terjadi kesalahan ketika menginterpretasi hasilnya ke dokumen BIA.

9. **Rencana Pengembangan TI 2016**
   Dokumen ini berisi rencana pengembangan TI untuk tahun 2016. Dokumen ini mendukung dalam proses penentuan strategi mitigasi yang paling tepat, yang dapat diaplikasikan pada PT. Pertamina RU IV.

5.2 Elemen Dokumen BCP PT. Pertamina RU IV

Dalam menentukan elemen atau bagian apa saja yang termuat dalam dokumen BCP PT. Pertamina RU IV, peneliti menggunakan acuan standar ISO 22301:2012 terkait *business continuity management systems* (BCMS) dan ISO 27031:2011 tentang *business continuity in ICT*, serta acuan penelitian terdahulu mengenai *business continuity plan* (BCP). Berikut akan dijelaskan rekomendasi elemen untuk dokumen prosedur dari masing-masing standar atau *best practice* yang digunakan:

5.2.1 ISO 22301:2012

Dalam *best practice* ISO 22301:2012 bab 8.4.4 mengenai *business continuity plan*, dijelaskan bahwa organisasi harus menyediakan sebuah prosedur terdokumentasi sebagai panduan dalam menghadapi gangguan atau insiden yang bisa mengancam keberlangsungan bisnis dalam kurun waktu yang telah disepakati. Dokumen BCP menurut ISO 22301:2012 harus mengandung hal-hal sebagai berikut:

Tabel 5.2 Elemen BCP menurut ISO 22301 (Sumber: ISO 22301)

Elemen BCP menurut ISO 22301:2012	
1	Tujuan dan ruang lingkup
2	Pembagian peran, tanggung jawab dan wewenang
3	Kriteria dalam aktivasi rencana
4	Proses dalam aktivasi rencana
5	Alur komunikasi
6	Kebutuhan sumber daya
7	Rincian untuk mengelola konsekuensi langsung dari insiden
8	Tindakan yang diambil organisasi untuk melanjutkan atau memperbaiki aktivitas kritikal
9	Rincian bagaimana media organisasi akan merespon insiden
10	Alur informasi dan proses terdokumentasi

5.2.2 ISO 27031:2011

Dalam ISO 27031:2011 bab 7.4.2 menjabarkan terkait apa yang harus ada dalam sebuah dokumen rencana keberlangsungan bisnis berbasis TI. Sebuah organisasi dapat memiliki satu atau lebih dokumen yang mencakup seluruh rencana kegiatan pemulihan layanan TI. Dokumen BCP menurut ISO 27031:2011 harus mencakup hal-hal sebagai berikut:

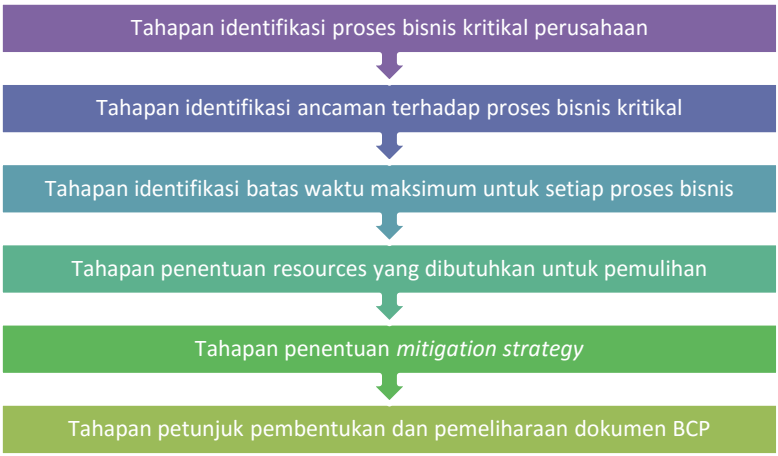
Tabel 5.3 Elemen BCP menurut ISO 27031 (Sumber: ISO 27031)

Elemen BCP menurut ISO 27031:2011	
1	Tujuan dan ruang lingkup
2	Pembagian peran dan tanggung jawab
3	Kriteria aktivasi rencana

Elemen BCP menurut ISO 27031:2011	
4	Pemilik dan pengeloa rencana respon dokumentasi dan pemulihan TI
5	Daftar kontak

5.2.3 Model Kerangka Kerangka BCP oleh Kartini Slamet

Salah satu penelitian sebelumnya yang dapat digunakan sebagai referensi dalam penelitian ini adalah hasil penelitian dari Kartini Slamet [31], dengan judul Thesis "Pembentukan Kerangka Kerja Business Continuity Plan pada Bank Ritel X". Penelitian ini menghasilkan serangkaian tahapan penting dalam penyusunan dokumen BCP. Tahapan tersebut antara lain adalah:



Gambar 5.1 Elemen BCP menurut Kartini Slamet (Sumber: Kartini, 2004)

5.3 Hambatan Pengumpulan Data

Dalam melakukan penelitian tugas akhir ini terdapat beberapa hambatan dan rintangan yang terjadi sehingga menghambat jalannya penelitian. Beberapa hambatan dan rintangan tersebut antara lain adalah sebagai berikut:

1. Proses pengumpulan data yang memakan waktu cukup lama sebelum peneliti bisa sampai ke tahapan pembuatan BCP. Pengumpulan data dalam tahapan analisis risiko memakan waktu yang cukup panjang karena harus melalui tahapan analisis aset TI dan memahami kembali dokumen analisis dampak bisnis.
2. Jarak antara kampus dengan lokasi pengambilan data yang terlampau jauh menyebabkan proses bimbingan dengan pembimbing 2 serta pengumpulan data menjadi lebih lama.

Walaupun terdapat beberapa hambatan dan rintangan, namun penelitian ini tetap dapat berjalan dengan lancar berkat bantuan dari pihak PT. Pertamina RU IV terutama pada bagian IT Area RU IV yang terlibat dan membantu jalannya penelitian. Pihak IT RU IV juga sangat terbuka dalam memberikan data-data yang diperlukan serta memberikan respon yang cepat dan bersedia meluangkan waktu untuk melakukan wawancara dan konsultasi jika diperlukan.

BAB VI
HASIL DAN PEMBAHASAN

Bab ini menjelaskan mengenai hasil dan pembahasan yang didapatkan dari pengerjaan tugas akhir agar dapat menjawab rumusan masalah. Hal-hal yang termuat dalam bab ini adalah penyampaian hasil dan pembahasan mengenai: identifikasi risiko, penilaian risiko, dan penyusunan strategi BCP.

6.1 Elemen Dokumen BCP PT. Pertamina RU IV

Elemen dokumen BCP PT. Pertamina RU IV mengacu pada elemen dokumen prosedur yang terdapat pada standar ISO 22301:2012 terkait *business continuity management systems* (BCMS) dan ISO 27031:2011 tentang *business continuity in ICT*, serta acuan penelitian terdahulu mengenai *business continuity plan* (BCP).

6.1.1 Analisis Rekomendasi Elemen dari *Best Practice*

Tahapan pertama dalam menentukan elemen dokumen BCP PT. Pertamina RU IV adalah melakukan analisis tiap elemen yang ada dalam rekomendasi ISO 22301, ISO 27031 dan penelitian Kartini Slamet. Tujuan dari analisis ini adalah untuk mengetahui dengan jelas maksud dari tiap elemen dari rekomendasi *best practice*. Hasil analisis disajikan dalam **tabel 6.1 Analisis Elemen Dokumen BCP Rekomendasi *Best Practice*.**

Tabel 6.1 Analisis Elemen Dokumen BCP Rekomendasi *Best Practice*

Acuan	Konten	Keterangan
ISO 22301	Tujuan dan ruang lingkup	Poin tujuan mendeskripsikan tujuan pembuatan dokumen BCP, sedangkan pendefinisian ruang lingkup ditujukan untuk membatasi hal-hal apa saja yang tercakup dalam dokumen BCP.

Acuan	Konten	Keterangan
	Pembagian peran, tanggung jawab dan wewenang	Poin ini menjelaskan tentang peran, tanggung jawab, dan wewenang masing-masing anggota organisasi dalam struktur komite BCP.
	Kriteria dalam aktivasi rencana	Poin ini menjelaskan secara detail dalam kriteria bencana seperti apa manajemen harus memulai prosedur yang ada dalam dokumen BCP.
	Proses dalam aktivasi rencana	Poin ini berisikan memberikan panduan kepada pihak-pihak yang terlibat terkait bagaimana proses dalam menjalankan rencana yang telah dituliskan dalam dokumen BCP.
	Alur komunikasi	Poin ini menjelaskan alur komunikasi antar komite BCP saat terjadinya bencana.
	Kebutuhan sumber daya	Poin ini mendefinisikan kebutuhan minimal yang harus dipenuhi oleh perusahaan untuk melanjutkan operasional bisnis yang terganggu.
	Rincian untuk mengelola konsekuensi langsung dari insiden	Poin ini berisi panduan untuk mengelola konsekuensi langsung dari insiden yang mengganggu operasional bisnis perusahaan dan erat kaitannya dengan DRP.
	Tindakan yang diambil organisasi untuk melanjutkan atau memperbaiki aktivitas kritikal	Poin ini menjelaskan mengenai tindakan atau startegi yang diambil oleh organisasi untuk mempertahankan keberlangsungan proses bisnis kritikal.

Acuan	Konten	Keterangan
	Rincian bagaimana media organisasi akan merespon insiden	Poin ini menjelaskan terkait bagaimana media organisasi akan merespon insiden. Berhubungan erat dengan *press conference* pada publik,
	Alur informasi dan proses terdokumentasi	Poin ini berisikan tentang informasi terkait pada siapa saja dokumen BCP ini didistribusikan. Selain itu juga memberikan informasi terkait histori perubahan yang dilakukan pada dokumen.
ISO 27031	Tujuan dan ruang lingkup	Poin tujuan mendeskripsikan tujuan pembuatan dokumen BCP, sedangkan pendefinisian ruang lingkup ditujukan untuk membatasi hal-hal apa saja yang tercakup dalam dokumen BCP.
	Pembagian peran dan tanggung jawab	Poin ini menjelaskan tentang peran, tanggung jawab, dan wewenang masing-masing anggota organisasi dalam struktur komite BCP.
	Kriteria aktivasi rencana	Poin ini menjelaskan secara detail dalam kriteria bencana seperti apa manajemen harus memulai prosedur yang ada dalam dokumen BCP.
	Pemilik dan pengeloa rencana respon dokumentasi dan pemulihan TI	Poin ini berisikan tentang informasi terkait pada siapa saja dokumen BCP ini didistribusikan. Selain itu juga memberikan informasi terkait histori perubahan yang dilakukan pada dokumen.
	Daftar kontak	Poin ini berisi daftar nomer telfon yang bisa dihubungi

Acuan	Konten	Keterangan
		beserta alternatifnya dari anggota komite BCP.
Penelitian Kartini Slamet	Identifikasi proses bisnis kritikal perusahaan	Poin ini berisi identifikasi proses bisnis kritikal perusahaan dilakukan dengan mengukur tingkat kerugian finansial dan operasional yang ditanggung oleh perusahaan jika proses bisnis tersebut berhenti berjalan.
	Identifikasi ancaman terhadap proses bisnis kritikal	Poin ini menjelaskan terkait apa-apa saja yang bisa mengganggu keberlangsungan proses bisnis kritikal.
	Identifikasi batas waktu maksimum untuk setiap proses bisnis	Poin ini menjelaskan terkait batas waktu maksimum yang dapat ditoleransi oleh perusahaan jika layanan TI berhenti beroperasi. Dalam dokumen BCP, didefinisikan dalam nilai RTO.
	Tahap penentuan *resources* yang dibutuhkan untuk pemulihan	Poin ini mendefinisikan kebutuhan minimal yang harus dipenuhi oleh perusahaan untuk melanjutkan operasional bisnis yang terganggu.
	Tahap penentuan *mitigation strategy*	Poin ini menjelaskan mengenai tindakan atau startegi yang diambil oleh organisasi untuk meminimalisir dan mempertahankan keberlangsungan proses bisnis kritikal.

6.1.2 Justifikasi Pemilihan Elemen Dokumen BCP PT. Pertamina RU IV

Setelah dilakukan analisis per elemen rekomendasi *best practice* maka dilanjutkan dengan memberikan justifikasi apakah elemen tersebut harus atau tidak dalam dokumen BCP PT. Pertamina RU IV. Pemberian justifikasi didasarkan pada beberapa referensi terkait elemen dokumen BCP dan hasil pemikiran subjektif peneliti. Berikut merupakan justifikasi terkait pemilihan elemen yang ada pada dokumen BCP PT. Pertamina RU IV:

Tabel 6.2 Justifikasi Pemilihan Elemen Dokumen BCP PT. Pertamina RU IV (Sumber: Peneliti)

Acuan	Konten	Kesesuaian	Justifikasi
ISO 22301	Tujuan dan ruang lingkup	Sesuai	Elemen ini harus ada dalam dokumen BCP Pertamina RU IV agar anggota organisasi dapat memahami maksud pembuatan dokumen BCP, dan pendefinisian ruang lingkup harus ada dalam dokumen BCP Pertamina RU IV untuk membatasi hal-hal apa saja yang tercakup dalam dokumen BCP sehingga pembahasan menjadi lebih fokus karena pembatasan ruang lingkup sudah dideskripsikan dengan jelas [38].
	Pembagian peran, tanggung jawab dan wewenang	Sesuai	Elemen harus ada dalam dokumen BCP agar anggota komite BCP mengerti peran, tanggung jawab, dan wewenang masing-masing angota

Acuan	Konten	Kesesuaian	Justifikasi
			sehingga diharapkan rencana dapat dijalankan dengan baik [20].
	Kriteria dalam aktivasi rencana	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina RU IV untuk mendeskripsikan dengan jelas pada komite BCP terkait kapan rencana yang dituliskan dalam dokumen BCP dijalankan [7].
	Proses dalam aktivasi rencana	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina agar komite BCP paham terkait bagaimana proses dalam menjalankan rencana yang telah dituliskan dalam dokumen BCP [20].
	Alur komunikasi	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina karena berfungsi sebagai panduan dalam proses komunikasi antar pihak-pihak yang terlibat dalam menjalankan rencana BCP [38].
	Kebutuhan sumber daya	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina agar tim BCP dapat mempersiapkan sumber daya yang dibutuhkan oleh perusahaan jika terjadi gangguan pada proses bisnis kritikal [39].

Acuan	Konten	Kesesuaian	Justifikasi
	Rincian untuk mengelola konsekuensi langsung dari insiden	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina karena berfungsi sebagai panduan untuk mengelola dampak langsung dari insiden sehingga meminimalisir dampak yang ditimbulkan [38].
	Tindakan yang diambil organisasi untuk melanjutkan atau memperbaiki aktivitas kritikal	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina untuk memberikan gambaran pada manajemen terkait apa yang harus dilakukan untuk meminimalisir kemungkinan kejadian ancaman atau risiko yang telah dijelaskan pada tahap sebelumnya [38].
	Rincian bagaimana media organisasi akan merespon insiden	Tidak sesuai	Elemen ini tidak harus ada dalam dokumen BCP PT. Pertamina RU IV karena berhubungan erat dengan *press conference* pada publik yang ditangani oleh fungsi General Manager sehingga tidak masuk ke dalam cakupan penelitian ini [40].
	Alur informasi dan proses terdokumentasi	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina karena berfungsi untuk memberikan informasi pada siapa saja dokumen BCP ini didistribusikan, serta memberikan informasi terkait histori perubahan yang dilakukan pada dokumen. Hal ini dikarenakan dokumen ini

Acuan	Konten	Kesesuaian	Justifikasi
			mengandung banyak informasi *confidential* terkait perusahaan maka tidak semua pihak dapat mengakses dokumen BCP, serta harus terdapat informasi yang jelas terkait pada siapa saja dokumen ini didistribusikan [38].
ISO 27031	Tujuan dan ruang lingkup	Sesuai	Elemen ini harus ada dalam dokumen BCP Pertamina RU IV agar anggota organisasi dapat memahami maksud pembuatan dokumen BCP, dan pendefinisian ruang lingkup harus ada dalam dokumen BCP Pertamina RU IV untuk membatasi hal-hal apa saja yang tercakup dalam dokumen BCP sehingga pembahasan menjadi lebih fokus karena pembatasan ruang lingkup sudah dideskripsikan dengan jelas [38].
	Pembagian peran dan tanggung jawab	Sesuai	Elemen harus ada dalam dokumen BCP agar anggota komite BCP mengerti peran, tanggung jawab, dan wewenang masing-masing angota sehingga diharapkan rencana dapat dijalankan dengan baik [20].
	Kriteria aktivasi rencana	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina RU IV untuk mendeskripsikan dengan jelas pada komite BCP terkait kapan

Acuan	Konten	Kesesuaian	Justifikasi
			rencana yang dituliskan dalam dokumen BCP dijalankan [40].
	Pemilik dan pengeloa rencana respon dokumentasi dan pemulihan TI	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina karena berfungsi untuk memberikan informasi pada siapa saja dokumen BCP ini didistribusikan, serta memberikan informasi terkait histori perubahan yang dilakukan pada dokumen. Hal ini dikarenakan dokumen ini mengandung banyak informasi *confidential* terkait perusahaan maka tidak semua pihak dapat mengakses dokumen BCP, serta harus terdapat informasi yang jelas terkait pada siapa saja dokumen ini didistribusikan [40].
	Daftar kontak	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina RU IV untuk mempermudah proses komunikasi koordinasi disaat terjadinya insiden [38].
Penelitian Kartini Slamet	Identifikasi proses bisnis kritikal perusahaan	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina RU IV karena memuat hasil identifikasi proses bisnis kritikal dengan mengukur tingkat kerugian finansial dan operasional yang ditanggung oleh perusahaan jika proses bisnis tersebut berhenti berjalan.

Acuan	Konten	Kesesuaian	Justifikasi
			Penilaian ini penting dilakukan untuk memastikan bahwa proses bisnis mana yang harus tetap dijaga keberlangsungannya. Proses ini masuk ke dalam tahap analisis dampak bisnis [38].
	Identifikasi ancaman terhadap proses bisnis kritikal	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina RU IV karena memuat hasil identifikasi ancaman atau risiko pada proses bisnis kritikal PT. Pertamina RU IV. Dengan mengetahui ancaman/risiko, maka dapat disusun rencana mitigasi untuk meminimalisir kemungkinan kejadian atau dampak dari risiko tersebut [38].
	Identifikasi batas waktu maksimum untuk setiap proses bisnis	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina RU IV untuk mengetahui sejauh apa perusahaan dapat mentoleransi gangguan pada proses bisnis kritikal. Semakin kecil nilai batas waktu maksimum, maka proses bisnis tersebut akan makin dikategorikan sebagai proses bisnis kritikal. Tahapan ini merupakan bagian dari tahapan penentuan proses bisnis kritikal [38].

Acuan	Konten	Kesesuaian	Justifikasi
	Tahap penentuan *resources* yang dibutuhkan untuk pemulihan	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina agar tim BCP dapat mempersiapkan sumber daya yang dibutuhkan oleh perusahaan jika terjadi gangguan pada proses bisnis kritikal [39].
	Tahap penentuan *mitigation strategy*	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina untuk memberikan gambaran pada manajemen terkait apa yang harus dilakukan untuk meminimalisir kemungkinan kejadian ancaman atau risiko yang telah dijelaskan pada tahap sebelumnya [38] [39].
	Tahap petunjuk pembentukan dan pemeliharaan dokumen BCP	Sesuai	Elemen ini harus ada dalam dokumen BCP PT. Pertamina karena berfungsi untuk memberikan informasi pada siapa saja dokumen BCP ini didistribusikan, serta memberikan informasi terkait histori perubahan yang dilakukan pada dokumen. Hal ini dikarenakan dokumen ini mengandung banyak informasi *confidential* terkait perusahaan maka tidak semua pihak dapat mengakses dokumen BCP, serta harus terdapat informasi yang jelas terkait pada siapa saja dokumen ini didistribusikan [7].

Setelah dilakukan justifikasi maka didapatkan elemen-elemen yang sesuai untuk dokumen BCP PT. Pertamina RU IV. Analisis dilanjutkan dengan melakukan pengelompokan *(mapping)* elemen sejenis ke dalam satu kategori yang sama. Dalam melakukan *mapping*, justifikasi didasarkan pada kesamaan konten dari elemen-elemen tersebut. Elemen yang sejenis dan sesuai untuk dokumen BCP PT. Pertamina RU IV akan dikelompokkan pada kategori yang sama dan membentuk elemen baru untuk dokumen BCP PT. Pertamina RU IV. Berikut merupakan elemen yang ada dalam dokumen BCP PT. Pertamina RU IV:

Tabel 6.3. Elemen Dokumen BCP PT. Pertamina (Sumber: Peneliti)

Acuan		Justifikasi	Elemen Dokumen BCP PT. Pertamina RU IV
ISO 22301	Alur informasi dan proses terdokumentasi	Ketiga elemen ini dimasukkan ke dalam satu kategori karena sama-sama mendefinisikan terkait pada siapa saja dokumen BCP ini didistribusikan, juga memberikan informasi terkait histori perubahan yang dilakukan pada dokumen.	Halaman kontrol dokumen
ISO 27031	Pemilik dan pengeloa rencana respon dokumentasi dan pemulihan TI		
Penelitian Kartini Slamet	Tahap petunjuk pembentukan dan pemeliharaan dokumen BCP		
ISO 22301	Tujuan dan ruang lingkup	Kedua elemen ini dimasukkan ke dalam satu kategori karena sama-sama mendefinisikan tujuan pembuatan dokumen BCP, dan mendefinisikan ruang	Tujuan Ruang lingkup
ISO 27031	Tujuan dan ruang lingkup		

		lingkup yang menjadi batasan dalam pembuatan dokumen BCP.	
ISO 22301	Pembagian peran, tanggung jawab dan wewenang	Kedua elemen ini dimasukkan ke dalam satu kategori karena sama-sama menjelaskan tentang peran, tanggung jawab, dan wewenang masing-masing anggota organisasi dalam struktur komite BCP.	Pembagian peran dan tanggung jawab
ISO 27031	Pembagian peran dan tanggung jawab		
ISO 27031	Daftar kontak	Elemen ini dalam dokumen BCP masuk ke dalam kategori tersendiri yaitu daftar kontak yang berisi nomer telfon yang bisa dihubungi dari anggota komite BCP.	Daftar kontak
ISO 22301	Alur komunikasi	Elemen ini dalam dokumen BCP masuk ke dalam kategori tersendiri yaitu *call tree* BCP yang menjelaskan alur komunikasi antar komite BCP saat terjadinya bencana.	*Call Tree BCP*
ISO 22301	Kriteria dalam aktivasi rencana	Ketiga elemen ini dimasukkan ke dalam satu kategori karena sama-sama menjelaskan kriteria bencana seperti apa	Aktivasi Rencana
	Proses dalam aktivasi rencana		

ISO 27031	Kriteria aktivasi rencana	sehingga manajemen harus memulai prosedur yang ada dalam dokumen BCP.	
Penelitian Kartini Slamet	Identifikasi proses bisnis kritikal perusahaan Identifikasi batas waktu maksimum untuk setiap proses bisnis	Elemen ini dalam dokumen BCP masuk ke dalam kategori tersendiri yaitu analisis dampak bisnis karena berisi identifikasi proses bisnis kritikal di PT. Pertamina RU IV.	Analisis dampak bisnis
Penelitian Kartini Slamet	Identifikasi ancaman terhadap proses bisnis kritikal	Elemen ini dalam dokumen BCP masuk ke dalam kategori tersendiri yaitu analisis risiko karena menjelaskan terkait apa-apa saja yang bisa mengganggu keberlangsungan proses bisnis kritikal dilihat dari sisi TI	Analisis risiko
ISO 27031	Rincian untuk mengelola konsekuensi langsung dari insiden Tindakan yang diambil organisasi untuk melanjutkan atau memperbaiki aktivitas kritikal	Kelima elemen ini masuk ke dalam kategori yang sama karena sama-sama menjelaskan mengenai tindakan atau startegi yang diambil oleh organisasi untuk mempertahankan keberlangsungan proses bisnis kritikal.	Strategi BCP dan DRP

ISO 22301	Kebutuhan sumber daya		
Penelitian Kartini Slamet	Tahap penentuan *resources* yang dibutuhkan untuk pemulihan		
	Tahap penentuan *mitigation strategy*		

6.1.3 Pembahasan Elemen Dokumen BCP PT. Pertamina RU IV

Berikut merupakan pembahasan terkait masing-masing poin yang terdapat pada dokumen BCP PT. Pertamina RU IV:

6.1.2.1 Profil Perusahaan

Bagian ini akan menjelaskan mengenai informasi perusahaan yang menjadi studi kasus dalam pembuatan dokumen business continuity plan (BCP). Penjelasan profil perusahaan terkait visi misi, proses bisnis secara general, dan stuktur organisasi perusahaan.

6.1.2.2 Tujuan Pembuatan Dokumen BCP

Pada bagian ini akan dijelaskan mengenai tujuan organisasi dalam melakukan pembuatan dokumen BCP. Tujuan ini nantinya akan menjadi acuan dalam proses pengerjaan BCP. Sehingga harapannya dokumen BCP yang dibuat dapat mendukung proses operasional dan tujuan dari organisasi itu sendiri.

6.1.2.3 Ruang Lingkup

Bagian ini akan menjelaskan batasan atau ruang lingkup dalam penyusunan dokumen BCP. Dalam penyusunan dokumen BCP PT. Pertamina RU IV, tidak semua fungsi terlibat dalam penelitian. Pemilihan fungsi yang terlibat didasarkan pada hasil analisis BIA 2015 dengan mempertimbangkan tingkat kritikalitas proses bisnis yang ada dalam fungsi tersebut. Dengan kata lain, fungsi bisnis dan proses bisnis yang terlibat dalam penelitian ini adalah proses bisnis kritikal, serta menggunakan dan memiliki ketergantungan yang tinggi terhadap teknologi dan informasi dalam melakukan aktivitas didalamnya.

6.1.2.4 Peran dan Tanggung Jawab

Dalam pembentukan BCP, sumber daya manusia (SDM) tentu saja menjadi suatu hal yang penting dan harus diperhatikan. Dengan adanya pembagian peran dan tanggung jawab SDM yang jelas, diharapkan BCP dapat berjalan secara optimal. Maka dari itu, perlu dilakukan pembagian peran dan tanggung jawab untuk masing-masing komite dalam sebuah struktur BCP. Identifikasi usulan struktur BCP ini merupakan adaptasi dari *best practice* yang dikeluarkan oleh ANT (Andalan Nusantara Teknologi), yang kemudian dikonsultasikan dengan pihak PT. Pertamina RU IV.

Anggota komite BCP dipilih dari staff PT. Pertamina RU IV dengan mempertimbangkan pengetahuan dan pengalaman mereka terkait aktivitas, prosedur, serta kesamaan aktivitas BCP dengan *regular job description* mereka. Dalam struktur BCP PT. Pertamina RU IV nantinya juga terdapat struktur tim DRP. Tim DRP sendiri adalah bagian dari tim BCP yang memiliki tanggung jawab spesifik untuk menangani semua gangguan yang berhubungan dengan teknologi informasi dan komunikasi yang ada di PT. Pertamina RU IV.

6.1.2.5 Contact List

Setelah pembagian peran dan tanggung jawab masing-masing anggota tim BCP, hal lain yang tidak kalah penting adalah daftar kontak yang bisa dihubungi ketika bencana terjadi sehingga komunikasi dapat berjalan dengan lancar. Detail kontak berfungsi sebagai panduan dalam menghubungi semua stakeholder ketika bencana atau insiden terjadi. Metode yang digunakan adalah dengan menggunakan *"call tree"* berdampingan dengan *"contact list"*. Terdapat pula *contact person* alternatif yang digunakan ketika *leader* tidak bisa dihubungi.

Daftar kontak ini disesuaikan dengan pembagian peran dan tanggung jawab tim BCP yang telah dibahas dalam sub-bab sebelumnya. Beberapa daftar kontak ditulis dengan inisial sebagai bentuk pengamanan privasi terkait data personal yang dicantumkan disana.

6.1.2.6 Call Tree

Dari daftar kontak yang disusun pada bagian sebelumnya kemudian disusunlah sebuah *call tree* (alur komunikasi). *Call tree* bersama-sama dengan tabel *contact list* dapat mempermudah proses komunikasi dengan tim dan masing-masing anggota tim. Seorang anggota tim direpresentasikan dalam sebuah node di dalam *call tree*, dan akan dinotifikasi oleh anggota lain yang berada pada node yang lebih tinggi, jika keduanya saling terhubung. Untuk setiap node (anggota tim) wajib menunjuk anggota tim yang lain yang dirasa dapat menggantikan posisinya.

6.1.2.7 Aktivasi Rencana

Dalam bagian ini akan dijelaskan kapan saat dimulainya eksekusi rencana BCP. Alur aktivasi rencana dalam penelitian kali ini berasal dari adaptasi *best practice* ANT (Andalan Nusantara Teknologi) yang kemudian dikomunikasikan dengan pihak PT. Pertamina RU IV. Dalam bab ini akan dijelaskan kapan dan poin-

poin penting apa yang harus dipenuhi sebelum tim BCP mulai mendeklarasikan keadaan bencana dan memulai eksekusi rencana.

6.1.2.8 Analisis Dampak Bisnis

Analisis dampak bisnis bertujuan untuk menentukan dan melakukan prioritasi proses operasional bisnis yang paling dianggap kritis pada suatu organisasi. Analisa dampak bisnis juga membantu perusahaan untuk melihat dampak apa yang ditimbulkan jika suatu proses bisnis terganggu, selain itu juga membantu organisasi dalam mengetahui batas waktu toleransi gangguan untuk layanan IT sampai proses bisnis terkait mengalami gangguan sehingga menimbulkan kerugian bagi perusahaan.

Seluruh hasil analisa ini mengacu pada hasil analisis dokumen *business impact analysis* (BIA) tahun 2015 yang dikerjakan oleh peneliti saat menjalani kerja praktek di PT. Pertamina RU IV. Dokumen pendukung lainnya adalah daftar pertanyaan wawancara BIA 2015 dan hasil wawancara BIA 2015. Karena tidak banyak perubahan dari segi proses bisnis, maka dapat disimpulkan bahwa BIA 2015 ini masih *reliable* untuk dijadikan acuan dalam pembuatan dokumen BCP.

6.1.2.9 Analisis Risiko

Setelah melalui tahap analisa dampak bisnis yang menghasilkan proses-proses bisnis yang bersifat kritikal, maka dilanjutkan dengan melakukan analisis risiko pada proses-proses bisnis yang bersifat kritikal. Dalam tahapan analisis risiko pada penelitian ini hanya dibatasi pada risiko teknologi informasi (TI).

6.1.2.10 Strategi BCP

Strategi BCP akan ditentukan berdasarkan hasil analisis yang telah dilakukan pada tahapan analisis dampak bisnis dan analisis risiko. Strategi BCP ini dibuat dengan tujuan untuk menjaga keberlangsungan dari proses bisnis yang diprioritaskan oleh organisasi, dan juga sebagai bentuk pengelolaan mitigasi dari

risiko. Selain strategi BCP, nantinya akan terdapat strategi DRP yang berfokus untuk menangani gangguan yang berhubungan dengan TI yang ada dalam organisasi. Dalam penentuan strategi akan dilihat berdasarkan risiko dan penyebab risiko.

Strategi BCP disusun dengan menggunakan masukan risiko TI yang bernilai *very high* (RPN>200) dan *high* (200>RPN>120) dengan asumsi bahwa jika risiko ini benar-benar terjadi akan mengganggu aktivitas yang ada pada proses bisnis kritikal di PT. Pertamina RU IV Cilacap.

6.2 Identifikasi Risiko

6.2.1 Identifikasi Penyebab Potensial

Penyebab potensial merupakan penyebab dari timbulnya risiko yang terjadi dan didapatkan dari identifikasi kerentanan dan ancaman dari aset TI yang digunakan dalam proses bisnis kritikal di PT. Pertamina RU IV. Identifikasi penyebab potensial akan dibatasi pada aset TI yang digunakan dalam proses bisnis kritikal hasil dari BIA 2015. Proses bisnis kritikal hasil BIA 2015 adalah sebagai berikut:

Tabel 6.4 Proses Bisnis Kritikal BIA 2015 (Sumber: BIA 2015)

Proses Bisnis	Sub Proses Bisnis	Fungsional Bisnis
Perencanaan proses pengolahan	Perencanaan proses pengolahan	RPO
	Pengadaan bahan baku	Procurement
	Quality control	Production II
	Shipping	Marine
Pengolahan dan produksi BBM, non-BBM dan Petrokimia	Produksi BBM	Production I
	Produksi non-BBM	Production II
Distribusi produk BBM,	Perencanaan	RPO
	Shipping	Marine

non-BBM dan Petrokimia	*Piping* dan penimbunan	Production I
Pemeliharaan dan pengendalian peralatan kilang	Pemeliharaan rutin harian dan insidentil	ME
	Pemeliharaan rutin tahunan dan 4 tahun sekali	TA
Pengelolaan *health safety enviroment*	*Leader and control*	HSE
	Pengaman area minyak di kapal dan lepas laut	Marine
	Penanganan K3	PHC

Berikut merupakan **contoh pembahasan** dari kerentanan, ancaman, dan penyebab potensial aset TI yang ada pada proses bisnis perencanaan proses pengolahan. Untuk analisis penyebab potensial pada proses bisnis lainnya dapat dilihat pada buku produk pada **subbab 10.1.1 Identifikasi Penyebab Potensial**.

6.2.1.1 Penyebab Potensial Proses Perencanaan Proses Pengolahan

Dalam menentukan penyebab potensial, terlebih dahulu melakukan analisis terkait kerentanan dan ancaman untuk masing-masing aset yang digunakan dalam proses bisnis terkait. Penentuan kerentanan, ancaman, dan penyebab potensial didasarkan pada **hasil observasi, wawancara, dan penilaian subjektif peneliti.** Berikut ini merupakan identifikasi penyebab potensial dari proses bisnis perencanaan proses pengolahan.

Tabel 6.5 Penyebab Potensial Perencanaan Proses Pengolahan (Sumber: Peneliti)

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial
Software	– LIMS – Saprodu – SIMOPS	Adanya celah keamanan pada sistem	Serangan baik dari dalam	Pertahanan sistem tidak cukup kuat untuk

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial
	– Daftar Telfon – mySAP – P2P *(procure to pay)* – E-Corr – Material Catalogue – Monitoring data purchasing – Laporan SS – Tank Vision – Absensi fingerprint		maupun luar perusahaan	mencegah serangan luar
		Aplikasi berhenti berkerja (hang)	Beban request terlalu besar	Sistem tidak bisa menerima semua request
		Kurangnya pembaharuan versi sistem	Terdapat bug dan error	Adanya bug dan error bawaan dari sistem
		Adanya kesalahan dari aplikasi		
		Anti-virus tidak update	Virus worm, trojan, dan jenis virus lain yang tidak terdeteksi	Antivirus tidak dalam versi update terbaru
		Penyebaran virus secara tidak sengaja oleh karyawan		
		Adanya celah keamanan pada firewall	Adanya serangan dari pihak luar	Serangan dari sumber yang tidak diketahui
		Kurangnya kesadaran untuk selalu logout setelah menggunakan aplikasi	Manipulasi data	Penyalahgunaan hak akses oleh orang yang tidak bertanggungjawab
		Penggunaan aplikasi bergantung pada koneksi internet	Jaringan internet kurang stabil	Kecepatan loading aplikasi bergantung pada kecepatan internet

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial
Hardware	– Telfon – *Handy Talkie* – Modem – Jaringan – Telfon meja – Intercom – PC – Kamera – CCTV – AP	Belum diterapkannya *cable management* yang baik	Konsleting atau hubungan pendek arus listrik	Terjadinya konsleting atau hubungan pendek arus listrik
		Tidak semua sudut kantor dipasang trails	Pencurian hardware	Kurangnya pengamanan fisik pada hardware
		Hak akses bisa dipinjam		
		Sistem CCTV di ruangan kurang baik		
		Kurangnya SOP untuk pengguna yang masuk ke dalam ruangan	Hardware terkena air	Pengguna yang membawa minuman ke ruangan kantor
		Aliran udara di PC yang kurang baik	Kerusakan pada sistem pendingin gedung	*Over heat*
		Umur hardware yang sudah tua dan usang	Belum adanya pembaharuan hardware	Durabilitas fisik hardware yang rendah
		Kerentanan alam dan lokasi	Bencana alam	Terjadinya bencana alam
Jaringan	Kabel LAN dan WAN	Kurangnya pengamanan khusus pada fisik kabel	Pencurian	Sistem kemanan kabel yang masih kurang baik

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial
		Komponen kabel yang rentan terputus	Kabel terputus	Tikus yang menggigit kabel
	Internet	Jaringan tidak memenuhi standar konfigurasi	Potensi downtime yang tinggi	Tidak dilengkapi dnegan jalur ring/backup
		Jaringan eksisting sudah tidak memadai mendukung operasi kilang	Monitoring availabilitas LAN sulit	Topologi LAN masih full star, dengan luasan area yang besar
			Dapat mengganggu operasional kilang karena jaringan data di kilang dimanfaatkan untuk banyak layanan (fire alarm, radio trunking, APN, CCTV, komputer, ATG, juga DCS)	Pemeliharaan di area kilang tidak mudah (hazardous area banyak dan luas)
		Umur instalasi yang sudah tua	Tidak ada cadangan untuk FO eksisting	FO eksisting di area 70 akan segera dibongkar karena issue sosial

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial
				(mengganggu jalur nelayan)
Data	– Monitoring kegiatan laboratorium – Surat ijin penyaluran/ pemompaan /penyerahan – Pembayaran Pengadaan barang/ jasa – Kode dan nama material yang digunakan – Pergerakan tangki RU IV	Kesalahan sistem database	Data corrupt	Data tidak bisa diakses
		Adanya celah keamanan	Manipulasi data	Hacker dan cracker
		Kontrolling yang kurang teratur	Kegagalan backup data	Kapasitas penyimpanan overload
			Data termodifikasi oleh virus	Antivirus tidak update
		Konfigurasi firewall yang kurang baik	Pencurian data	Unauthorized access yang masuk ke dalam database
		Sistem keamanan database belum baik		
		Ketidaksempurnaan dalam clean disk policy	Penyusupan secara fisik	Unauthorized access yang masuk ke dalam database
Sumber Daya Manusia	– Manager – Asisten manager – karyawan	Kurangnya kesadaran pentingnya menjaga aset	Adanya kepentingan tertentu yang tidak bertanggung jawab	Tidak ada SOP untuk pengelolaan aset
		Belum diterapkan prosedur access	Penyalahgunaan hak akses	Unathourized access yang masuk ke dalam sistem

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial
		management yang baik		
		Pengawasan kurang maksimal	*Social engineering*	Hak akses yang disalahgunakan
		Rasa memiliki pegawai yang rendah		

6.2.2 Identifikasi Risiko

Penentuan risiko dibuat berdasarkan analisis penyebab potensial yang dianggap dapat menyebabkan kemungkinan risiko terjadi. Proses penentuan risiko terbatas pada pengetahuan dan penilaian subjektif peneliti yang hasilnya akan divalidasi oleh pihak perusahaan. Sama dengan proses sebelumnya, identifikasi risiko akan diolah berdasarkan penyebab potensial per proses bisnis hasil dari BIA 2015.

Berikut merupakan **contoh pembahasan** dari identifikasi risiko aset TI yang ada pada proses bisnis perencanaan proses pengolahan. Untuk analisis risiko pada proses bisnis lainnya dapat dilihat pada buku produk pada **subbab 10.1.2 Identifikasi Risiko.**

6.2.2.1 Identifikasi Risiko Proses Perencanaan Proses Pengolahan

Berikut ini merupakan daftar risiko yang telah disusun dari proses bisnis perencanaan proses pengolahan:

Tabel 6.6 Identifikasi Risiko Perencanaan Proses Pengolahan (Sumber: Peneliti)

Kategori	Nama Aset	Penyebab Potensial	ID Risiko	Risiko
Software	– LIMS	Pertahanan sistem tidak cukup kuat	S.01.01	*Cyber threat*

Kategori	Nama Aset	Penyebab Potensial	ID Risiko	Risiko
	– Saprodu – SIMOPS – Daftar Telfon – mySAP – P2P *(procure to pay)* – E-Corr – Material Catalogue – Monitoring data purchasing – Laporan SS – Tank Vision – Absensi fingerprint	untuk mencegah serangan dari luar		
		Antivirus tidak dalam versi update terbaru		
		Serangan dari sumber yang tidak diketahui		
		Sistem tidak bisa menerima semua request	S.01.02	Kegagalan aplikasi
		Adanya bug dan error bawaan dari sistem		
		Kecepatan loading aplikasi bergantung pada kecepatan internet	S.01.03	*Loading* aplikasi lambat
		Penyalahgunaan hak akses oleh orang yang tidak bertanggungjawab	S.01.04	Penyalahgunaan hak akses
Hardware	– Telfon – *Handy Talkie* – Modem – Jaringan – Telfon meja – Intercom – PC – Kamera – CCTV – AP	Terjadinya konsleting atau huungan pendek arus listrik	H.01.01	Kebakaran
		Kurangnya pengamanan fisik pada hardware	H.01.02	Pencurian hardware
		Pengguna membawa minuman ke ruangan kantor (zat cair)	H.01.03	Kerusakan hardware
		Over heat		

Kategori	Nama Aset	Penyebab Potensial	ID Risiko	Risiko
		Durabilitas fisik hardware yang rendah		
		Terjadinya bencana alam		
Jaringan	– Kabel LAN dan WAN	Sistem kemanan kabel yang masih kurang baik	J.01.01	Kehilangan kabel LAN dan WAN
		Tikus yang menggigit kabel	J.01.02	Kerusakan fisik kabel LAN dan WAN
	– Internet	Topologi LAN masih full star, dengan luasan area yang besar	J.01.03	Lambatnya akses jaringan
		Tidak dilengkapi dengan jalur ring/backup	J.01.04	Jaringan mati
		Pemeliharaan di area kilang tidak mudah (hazardous area banyak dan luas)		
		FO eksisting di area 70 akan segera dibongkar karena isu sosial (mengganggu jalur nelayan)		
Data	– Monitoring kegiatan laboratorium – Surat ijin penyaluran/	Data tidak bisa diakses	D.01.01	Kehilangan data
		Kapasitas penyimpanan overload		
		Antivirus tidak update		

Kategori	Nama Aset	Penyebab Potensial	ID Risiko	Risiko
	pemompaan/ penyerahan – Pembayaran Pengadaan barang/ jasa – Kode dan nama material yang digunakan – Pergerakan tangki RU IV	Hacker dan cracker	D.01.02	Informasi rahasia tersebar luas
		Unauthorized access yang masuk ke dalam database		
Sumber Daya Manusia	– Manager – Asisten manager – karyawan	Tidak ada SOP untuk pengelolaan aset	P.01.01	Kesalahan pengelolaan aset
		Unathourized access yang masuk ke dalam sistem	P.01.02	Penyebaran data dan informasi rahasia
		Hak akses yang disalahgunakan		

6.2.3 *Risk Register*

Risk register adalah sebuah tabel yang berisi daftar potensi kejadian-kejadian risiko yang telah diidentifikasi beserta dengan kerentanan, ancaman, penyebab dan dampak dari setiap risiko jika benar-benar terjadi. Berikut merupakan hasil dari *risk register* dari proses bisnis perencanaan proses pengolahan yang telah diidentifikasikan sebelumnya. Penjelasan mengenai tiap komponen yang ada pada tabel *risk register* akan dijelaskan sebagai berikut:

- **Kerentanan *(vulnerability)*** adalah suatu kelemahan atau faktor internal yang dapat meningkatkan kemungkinan atau likelihood terjadinya suatu ancaman
- **Ancaman *(threat)*** adalah suatu aksi dan non-aksi yang timbul sebagai bentuk negatif atau situasi yang tidak diinginkan. Ancaman berasal dari faktor eksternal atau lingkungan luar
- **Penyebab potensial *(potential causes)*** adalah penyebab dari timbulnya risiko yang terjadi dan didapatkan dari identifikasi kerentanan dan ancaman
- **Risiko *(risk)*** merupakan kombinasi dari probabilitas dan ketidakpastian dengan menghasilkan konsekuensi yang positif atau negatif yang bisa berdampak pada tujuan dan punya banyak penyebab
- **Dampak *(impact)*** adalah dampak yang ditimbulkan akibat terjadinya risiko

Berikut merupakan **contoh** *risk register* dari proses bisnis perencanaan proses pengolahan. Untuk melihat risk *register* selengkapnya dapat dilihat pada buku produk **subbab 10.1.3 Risk Register.**

6.2.3.1 *Risk Register* Proses Perencanaan Proses Pengolahan

Berikut ini merupakan *risk register* yang telah disusun dari proses bisnis perencanaan proses pengolahan:

Tabel 6.7 *Risk Register* Perencanaan Proses Pengolahan (Sumber: Peneliti)

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
Software	– LIMS – Saprodu – SIMOPS – Daftar Telfon – mySAP – P2P *(procure to pay)* – E-Corr – Material Catalogue – Monitoring data purchasing	Adanya celah keamanan pada sistem	Serangan baik dari dalam maupun luar perusahaan	Pertahanan sistem tidak cukup kuat untuk mencegah serangan luar	S.01.01	*Cyber threat*	Hal ini akan menimbulkan layanan tidak bisa berjalan sebagaimana mestinya, yang pada akhirnya akan mengganggu aktivitas operasional. Selain itu juga akan menimbulkan complain dari pengguna dan menurunkan citra positif IT RU IV.
		Anti-virus tidak update	Virus worm, trojan, dan jenis virus lain yang tidak terdeteksi	Antivirus tidak dalam versi update terbaru			
		Penyebaran virus secara tidak sengaja oleh karyawan					

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
	– Laporan SS – Tank Vision – Absensi fingerprint	Adanya celah keamanan pada firewall	Adanya serangan dari pihak luar	Serangan dari sumber yang tidak diketahui			
		Aplikasi berhenti berkerja (hang)	Beban request terlalu besar	Sistem tidak bisa menerima semua request	S.01.02	Kegagalan Aplikasi	Loading aplikasi menjadi sangat lambat hingga dampak terburuk aplikasi tidak dapat digunakan. Hal ini akan mengganggu aktivitas bisnis karena proses yang biasanya dilakukan secara terautomasi harus dilakukan secara manual. Hal ini juga akan berdampak pada citra IT RU IV
		Kurangnya pembaharuan versi sistem	Terdapat bug dan error	Adanya bug dan error bawaan dari sistem			
		Adanya kesalahan dari aplikasi					
		Penggunaan aplikasi bergantung	Jaringan internet kurang stabil	Kecepatan loading aplikasi bergantung	S.01.03	Loading aplikasi lambat	Hal ini akan memperlambat aktivitas bisnis. Selain itu juga menimbulkan

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
		pada koneksi internet		pada kecepatan internet			complain dari user serta menurunkan citra IT RU IV.
		Kurangnya kesadaran untuk selalu logout setelah menggunakan aplikasi	Manipulasi data	Penyalahgunaan hak akses oleh orang yang tidak bertanggungjawab	S.01.04	Penyalahgunaan hak akses	Hal ini berdampak pada banyak hal, dari mulai tersebarnya informasi rahasia perusahaan hingga manipulasi data yang bisa diakses melalui aplikasi sehingga kebenaran data menjadi diragukan.
Hardware	– Telfon – *Handy Talkie* – Modem – Jaringan – Telfon meja – Intercom – PC	Belum diterapkannya *cable management* yang baik	Konsleting atau hubungan pendek arus listrik	Terjadinya konsleting atau hubungan pendek arus listrik	H.01.01	Kebakaran	Kebakaran akan berdampak pada rusaknya hardware dan lokasi kantor. Hal ini tentu saja akan menghambat proses bisnis dan menimbulkan kerugian finansial bagi

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
	– Kamera – CCTV – AP						perusahaan. Selain itu juga akan merusak citra perusahaan di mata masyarakat.
		Tidak semua sudut kantor dipasang trails	Pencurian hardware	Kurangnya pengamanan fisik pada hardware	H.01.02	Pencurian hardware	Hilangnya hardware akan merugikan perusahaan secara finansial, serta mengganggu aktivitas bisnis perusahaan.
		Hak akses bisa dipinjam					
		Sistem CCTV di ruangan kurang baik					
		Kurangnya SOP untuk pengguna yang masuk ke dalam ruangan	Hardware terkena air	Pengguna yang membawa minuman ke ruangan kantor	H.01.03	Kerusakan hardware	Rusaknya hardware akan mengganggu aktivitas bisnis perusahaan dan menimbulkan complain dari user.

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
		Aliran udara di PC yang kurang baik	Kerusakan pada sistem pendingin gedung	*Over heat*			Hal ini akan berdampak pada turunnya citra IT RU IV.
		Umur hardware yang sudah tua dan usang	Belum adanya pembaharuan hardware	Durabilitas fisik hardware yang rendah			
		Kerentanan alam dan lokasi	Bencana alam	Terjadinya bencana alam			
Jaringan	Kabel LAN dan WAN	Kurangnya pengamanan khusus pada fisik kabel	Pencurian	Sistem kemanan kabel yang masih kurang baik	J.01.01	Kehilangan kabel LAN dan WAN	Terganggunya kabel LAN dan WAN secara otomatis akan mengganggu aktivitas bisnis karena hampir semua aplikasi yang digunakan bergantung pada koneksi jaringan.
		Komponen kabel yang rentan terputus	Kabel terputus	Tikus yang menggigit kabel	J.01.02	Kerusakan fisik kabel LAN dan WAN	

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
	Internet	Jaringan eksisting sudah tidak memadai mendukung operasi kilang	Monitoring availabilitas LAN sulit	Topologi LAN masih full star, dengan luasan area yang besar	J.01.03	Lambatnya akses jaringan	Akses jaringan yang lambat akan memperlambat loadingnya aplikasi sehingga mengganggu aktivitas bisnis karena hampir semua aplikasi yang digunakan bergantung pada koneksi jaringan inetrnet
		Jaringan tidak memenuhi standar konfigurasi	Potensi downtime yang tinggi	Tidak dilengkapi dnegan jalur ring/backup	J.01.04	Jaringan mati	Jaringan mati akan berdampak pada hampir seluruh aspek proses bisnis yang ada di RU IV. Jaringan internet bisa dikatakan merupakan hal yang utama karena hampir semua aktivitas bisnis didukung oleh peran
			Dapat mengganggu operasional kilang karena jaringan data	Pemeliharaan di area kilang tidak mudah (hazardous			

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
			di kilang dimanfaatkan untuk banyak layanan (fire alarm, radio trunking, APN, CCTV, komputer, ATG, juga DCS)	area banyak dan luas)			aplikasi yang terhubung pada internet. Hal ini tentu juga akan menimbulkan complain dari user dan merusak citra IT RU IV.
		Umur instalasi yang sudah tua	Tidak ada cadangan untuk FO eksisting	FO eksisting di area 70 akan segera dibongkar karena issue sosial (menggangg u jalur nelayan)			

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
Data	– Monitoring kegiatan laboratorium – Surat ijin penyaluran/ pemompaan/ penyerahan – Pembayaran Pengadaan barang/ jasa – Kode dan nama material yang digunakan – Pergerakan tangki RU IV	Kesalahan sistem database	Data corrupt	Data tidak bisa diakses	D.01.01	Kehilangan data	Kehilangan data tentu saja merugikan perusahaan serta mengganggu operasional bisnis perusahaan. Selain itu juga akan menimbulkan dampak pada sistem aplikasi yang ada di RU IV.
		Kontrolling yang kurang teratur	Kegagalan backup data	Kapasitas penyimpanan overload			
			Data termodifikasi oleh virus	Antivirus tidak update			
		Adanya celah keamanan	Manipulasi data	Hacker dan cracker	D.01.02	Informasi rahasia tersebar luas	Informasi rahasia perusahan yang terserbar luas akan merugikan karena merusak citra baik RU IV. Selain itu juga menurunkan kepercayaan masyarakat terhadap.
		Konfigurasi firewall yang kurang baik	Pencurian data	Unauthorized access yang masuk ke dalam database			
		Sistem keamanan database belum baik					
		Ketidaksempurnaan dalam	Penyusupan secara fisik	Unauthorized access			

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
		clean disk policy		yang masuk ke dalam database			
Sumber Daya Manusia	– Manager – Asisten manager – karyawan	Kurangnya kesadaran pentingnya menjaga aset	Adanya kepentingan tertentu yang tidak bertanggung jawab	Tidak ada SOP untuk pengelolaan aset	P.01.01	Kesalahan pengelolaan aset	Kesalahan pengelolaan aset akan berdampak pada usia aset. Aset yang tidak dikelola dengan baik akan memperpendek umur aset serta merugikan perusahaan dalam bidang finansial
		Belum diterapkan prosedur access management yang baik	Penyalahgunaan hak akses	Unathourized access yang masuk ke dalam sistem	P.01.02	Penyebaran data dan informasi rahasia	Informasi rahasia perusahan yang terserbar luas akan merugikan karena merusak citra baik RU IV. Selain itu juga menurunkan kepercayaan masyarakat terhadap.
		Pengawasan kurang maksimal	Social engineering	Hak akses yang			

Kategori	Nama Aset	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	Dampak
		Rasa memiliki pegawai yang rendah		disalahgunakan			

6.2.4 Penilaian Risiko

Setelah melakukan identifikasi risiko, maka tahap selanjutnya adalah melakukan penilaian risiko untuk mengukur nilai risiko yang dihasilkan dengan mempertimbangkan kerentanan, penyebab, dan dampaknya. Proses penilaian didasarkan pada hasil obserasi, wawancara, dan penilaian subjektif dari peneliti. Output dari tahap ini adalah nilai RPN *(risk priority number)* untuk masing-masing risiko dari tiap proses bisnis kritikal yang ada di PT. Pertamina RU IV.

Dalam proses penilaian risiko menggunakan metode FMEA, dengan menggunakan tiga komponen penilaian, antara lain adalah *severity* (keparahan), *occurrence* (kemungkinan terjadi), serta *detection* (deteksi). Ketiga nilai ini digunakan untuk menghitung nilai RPN *(risk priority number)* untuk menghasilkan prioritasi risiko. Parameter dari level *severity, occurance dan detection* dapat dilihat pada **Bab II Tinjauan Pustaka** pada **subbab 2.2.4 Metode FMEA**.

Pada bab ini akan dipaparkan contoh penilaian risiko pada proses bisnsi perencanaan proses pengolahan. Untuk hasil analisis pada proses bisnis lainnya dapat dilihat pada buku produk subbab **10.1.4 Penilaian Risiko**.

6.2.4.1 Penilaian Risiko Proses Perencanaan Proses Pengolahan

Berikut ini merupakan penilaian risiko yang telah disusun dari proses bisnis perencanaan proses pengolahan:

Tabel 6.8 Penilaian Risiko Perencanaan Proses Pengolahan (Sumber: Peneliti)

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
Software	Adanya celah keamanan pada sistem	Serangan baik dari dalam maupun luar perusahaan	Pertahanan sistem tidak cukup kuat untuk mencegah serangan luar	S.01.01	*Cyber threat*	5	*Cyber threat* akan menyebabkan penurunan kinerja dan mengakibatkan kerugian bagi perusahaan.	2	*Cyber threat* hampir tidak pernah terjadi. Hal ini dikarenakan perusahaan sudah melakukan prosedur pengamanan yang baik.	3	Perusahaan sudah menerapkan metode deteksi yang baik. Selain itu proses monitoring juga dilakukan setiap hari sehingga memperbesar peluang	30
	Anti-virus tidak update	Virus worm, trojan, dan jenis virus lain yang tidak terdeteksi	Antivirus tidak dalam versi update terbaru									
	Penyebaran virus secara tidak sengaja oleh karyawan											

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
	Adanya celah keamanan pada firewall	Adanya serangan dari pihak luar	Serangan dari sumber yang tidak diketahui								deteksi dini jika terjadi *cyber threat.*	
	Aplikasi berhenti berkerja (hang)	Beban request terlalu besar	Sistem tidak bisa menerima semua request	S.01.02	Kegagalan Aplikasi	4	Kegagalan aplikasi pada proses bisnis ini tidak terlalu terlihat dampaknya. Hal ini dikarenakan aktivitasnya bisa di cover dengan	4	Kegagalan aplikasi jarang terjadi. Dan jika terjadi sekalipun teknisi programmer akan dengan sigap memperbaiki hingga aplikasi dapat digunakan kembali	6	Metode deteksi memiliki efektivitas rendah. Hal ini dikarenakan tidak adanya dokumentasi pengembangan aplikasi sehingga waktu	96
	Kurangnya pembaharuan versi sistem	Terdapat bug dan error	Adanya bug dan error bawaan dari sistem									
	Adanya kesalahan dari aplikasi											

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
							mengguna kan cara manual				memperbai ki memakan waktu yang cukup lama	
	Penggunaan aplikasi bergantung pada koneksi internet	Jaringan internet kurang stabil	Kecepatan loading aplikasi bergantung pada kecepatan internet	S.01. 03	Loading aplikasi lambat	3	Loading aplikasi yang lambat akan berdampak pada penurunan kinerja dan mengakiba tkan kerugian bagi perusahaan	7	Kejadian ini sering kali terjadi karena penggunaan aplikasi bergantung pada kecepatan internet, seringkali *traffic*nya penuh sehingga	5	Metode deteksi yang diterapkan bisa dibilang belum maksimal karena tidak adanya rencana kontigensi ketika	105

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
									menyebabkan aksesnya lambat		jaringan sangat lambat	
	Kurangnya kesadaran untuk selalu logout setelah menggunakan aplikasi	Manipulasi data	Penyalahgunaan hak akses oleh orang yang tidak bertanggungjawab	S.01.04	Penyalahgunaan hak akses	4	Jika ini terjadi, maka perusahaan tentu akan menanggung kerugian dan menggangu proses bisnis	2	Kejadian ini hampir tidak pernah terjadi karena tiap anggota sudah mengetahui peran dan tanggung jawabnya masing-masing	5	Telah diterapkan pengamanan sedemikian rupa sehingga hanya orang yang memiliki hak akseslah yang bisa membuka aplikasi.	40
Hardware	Belum diterapkannya *cable*	Konsleting atau hubungan	Terjadinya konsleting atau	H.01.01	Kebakaran	7	Kebakaran, baik kecil maupun	2	Kebakaran pernah terjadi dalam	2	Kebakaran merupakan musuh	28

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
	management yang baik	pendek arus listrik	hubungan pendek arus listrik				besar akan berdampak bagi keberlangsungan bisnis perusahaan. Apalagi jika kejadiannya di dalam kilang.		kilang RU IV. Namun hal itu sangat jarang terjadi dan kemungkinannya kecil karena sudah banyak kontrol yang diterapkan untuk mengantisipasi hal tersebut		utama dalam bisnis di RU IV. Banyak kontrol yang sudah diterapkan, antara lain alarm kebakaran, pendeteksi perubahan suhu, hingga pemadam kebakaran milik Pertamina sendiri	

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
	Tidak semua sudut kantor dipasang trails Hak akses bisa dipinjam Sistem CCTV di ruangan kurang baik	Pencurian hardware	Kurangnya pengamanan fisik pada hardware	H.01.02	Pencurian hardware	5	Pencurian hardware akan menimbulkan kerugian secara finansial bagi perusahaan. Selain ituu efek lainnya adalah menurunkan kinerja karyawan dan menggangu proses bisnis	3	Pencurian di Pertamina pernah terjadi beberapa kali, terutama pada lokasi *head office* karena pada malam hari security fokus untuk mengamankan area kilang	5	Kontrol yang diterapkan memiliki efektifitas rata-rata. Hal ini dikarenakan tidak semua tempat dipasang trails, CCTV sering mati, dan penjagaan security yang tidak bisa menjangka	75

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
											u semua area.	
	Kurangnya SOP untuk pengguna yang masuk ke dalam ruangan	Hardware terkena air	Pengguna yang membawa minuman ke ruangan kantor	H.01.03	Kerusakan hardware	3	Kerusakan hardware akan menggangu proses bisnis yang ada di PT. Pertamina. Namun dampak yang dirasakan tidak besar karena teknisi akan sigap memperbai	6	Frekuensi kejadian kerusakan hardware bisa dikatakan cukup sering terjadi.	3	Metode deteksi yang diterapkan sudah cukup efektif untuk mengatasi masalah kerusakan hardware	54
	Aliran udara di PC yang kurang baik	Kerusakan pada sistem pendingin gedung	*Over heat*									
	Umur hardware yang sudah tua dan usang	Belum adanya pembaharuan hardware	Durabilitas fisik hardware yang rendah									

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
	Kerentanan alam dan lokasi	Bencana alam	Terjadinya bencana alam				ki atau mengganti dengan hardware baru sementara yang rusak sedang diperbaiki.					
Jaringan	Kurangnya pengamanan khusus pada fisik kabel	Pencurian	Sistem kemanan kabel yang masih kurang baik	J.01.01	Kehilangan kabel LAN dan WAN	7	Kabel LAN dan WAN merupakan salah satu komponen jaringan yang penting dan mempengaruhi	2	Kehilangan kabel LAN dan WAN hampir tidak pernah terjadi di Pertamina	2	Kegagalan ini sangat mudah diketahui karena dapat dilihat langsung dan sangat mudah dikendalikan dengan	28

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
							keberlangsungan aplikasi yang ada di perusahaan				memberikan pengamanan khusus berlapis.	
	Komponen kabel yang rentan terputus	Kabel terputus	Tikus yang menggigit kabel	J.01.02	Kerusakan fisik kabel LAN dan WAN	7	Kabel LAN dan WAN merupakan salah satu komponen jaringan yang penting dan mempengaruhi keberlangsungan aplikasi	4	Kerusakan fisik pada kabel LAN dan WAN pernah beberapa kali terjadi dikarenakan hewan pengerat	5	Kegagalan membutuhkan upaya deteksi dan pengendalian yang ekstra karena melibatkan faktor eksternal dan membutuhkan perlindung	140

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
							yang ada di perusahaan				an khusus untuk kabel serta perbaikan kondisi lingkungan kabel.	
	Jaringan eksisting sudah tidak memadai mendukung operasi kilang	Monitoring availabilitas LAN sulit	Topologi LAN masih full star, dengan luasan area yang besar	J.01.03	Lambatnya akses jaringan	5	Akses jaringan yang lambat akan menyebabkan penurunan kinerja dan merugikan perusahaan.	10	Kejadian ini hampir terjadi setiap hari pada PT. Pertamina RU IV	4	Lambatnya akses jaringan dapat diketahui dan dikendalikan dengan kontrol pembagian beban kerja server	200

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
	Jaringan tidak memenuhi standar konfigurasi	Potensi downtime yang tinggi	Tidak dilengkapi dnegan jalur ring/backup	J.01.04	Jaringan mati	10	Kejadian ini akan berdampak besar bagi keberlangusngan bisnis di RU IV. Selain itu juga akan menibulkan komplain pelanggan dan merusak citra IT RU IV.	2	Kejadian ini belum pernah terjadi di PT. Pertamina RU IV	2	Kejadian ini dapat dicegah dan dideteksi dengan kontroliing secara teratur	40
		Dapat menggangu operasional kilang karena jaringan data di kilang dimanfaatkan untuk banyak layanan (fire alarm, radio trunking,	Pemeliharaan di area kilang tidak mudah (hazardous area banyak dan luas)									

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
		APN, CCTV, komputer, ATG, juga DCS)										
	Umur instalasi yang sudah tua	Tidak ada cadangan untuk FO eksisting	FO eksisting di area 70 akan segera dibongkar karena issue sosial (menggangg u jalur nelayan)									
Data	Kesalahan sistem database	Data corrupt	Data tidak bisa diakses	D.01.01	Kehilangan data	8	Data merupakan salah satu aset terpenting bagi	2	Kehilangan data hampir tidak pernah terjadi. Jika hal ini terjadipun,	5	Kehilangan data dapat dideteksi dan dikendalik	80
	Kontrolling yang kurang teratur	Kegagalan backup data	Kapasitas penyimpanan overload									

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
		Data termodifikasi oleh virus	Antivirus tidak update				perusahaan. Kehilangan data akan menyebabkan operasional bisnis perusahaan terganggu hingga yang paling parah dapat menghentikan kegiatan operasional		IT RU IV telah melakukan tindakan antisipasi berupa backup harian data yang tersimpan dalam server dan dapat dilakukan restore sewaktu-waktu jika benar-benar dibutuhkan.		an dengan pengamanan khusus yang baik terhadap data	

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
							perusahaan.					
	Adanya celah keamanan	Manipulasi data	Hacker dan cracker	D.01.02	Informasi rahasia tersebar luas	7	Informasi rahasia yang tersebar luas tentu saja akan merugikan perusahaan. Namun dalam proses bisnis ini, data yang disimpan bisa dikatakan tidak confidential sehingga	2	Data dan informasi telah disimpan dengan pengamanan sedemikian rupa sehingga penyebaran terkait informasi rahasia belum pernah terjadi hingga saat ini.	4	Telah diterapkan pengamanan sedemikian rupa sehingga data dan informasi tetap terjaga kerahasiaannya. Analisis log data juga bisa digunakan untuk mendeteksi	56
	Konfigurasi firewall yang kurang baik	Pencurian data	Unauthorized access yang masuk ke dalam database									
	Sistem keamanan database belum baik											
	Ketidaksempurnaan dalam clean disk policy	Penyusupan secara fisik	Unauthorized access yang masuk ke dalam database									

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
							dampaknya tidak egitu berpengaruh untuk perusahaan				penyebaran data.	
Sumber Daya Manusia	Kurangnya kesadaran pentingnya menjaga aset	Adanya kepentingan tertentu yang tidak bertanggung jawab	Tidak ada SOP untuk pengelolaan aset	P.01.01	Kesalahan pengelolaan aset	4	Kesalahan pengeolaan aset akan berdampak pada berkurangnya umur hardware atau memperlambat proses bisnis jika berkaitan dengan	3	Aset IT yang ada di RU IV secara garis besar sudah dikelola dengan baik. Hal ini diketahui dari adanya jadwal maintenance teratur untuk tiap aset, serta	3	Deteksi kerusakan pada aset sudah cukup tinggi. Hal ini dibuktikan jika terdapat aset yang rusak atau tidak bisa digunakan, maka	36

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
							software dan data.		pengamanan yang cukup memadai.		teknisi sudah siap untuk membantu hingga aset dapat digunakan kembali sehingga proses bisnis tidak begitu lama terganggu.	
	Belum diterapkan prosedur access management yang baik	Penyalahgunaan hak akses	Unathourized access yang masuk ke dalam sistem	P.01.02	Penyebaran data dan informasi rahasia	7	Penyebaran data dan informasi rahasia tentu saja akan	2	Kejadian penyebaran informasi rahasia sangat jarang dan	4	Penyebaran data dan informasi rahasia dapat dideteksi	56

Kategori	Kerentanan	Ancaman	Penyebab Potensial	ID Risiko	Risiko	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
	Pengawasan kurang maksimal						berdampak buruk bagi perusahaan. Namun dalam proses bisnis ini informasi yang tersedia tidak begitu confidential sehingga dampaknya tidak begitu terasa bagi perusahaan.		hampir tidak pernah terjadi di Pertamina. Hal ini juga didukung oleh pengamanan seperti *access door* dan login ketika harus menggunakan aplikasi sehingga meminimalisir kemungkinan kejadian.		dan dikendalikan dengan prosedural maupun perjanjian tertentu (contoh: *access door* dan login menggunakan username dan password)	
	Rasa memiliki pegawai yang rendah	*Social engineering*	Hak akses yang disalahgunakan									

6.2.5 Prioritasi Risiko

Dari proses penilaian risiko menggunakan metode FMEA maka didapatkan risiko dengan masing-masing *score assessment* dari yang paling tinggi hingga yang paling rendah. Nilai RPN *(risk priority number)* akan dikelompokkan menjadi prioritas risiko *very high, high, medium, low* dan *very low*. Berikut merupakan tabel prioritasi risiko dari masing-masing proses bisnis kritikal:

6.2.5.1 Prioritasi Risiko (Perencanaan Proses Pengolahan)

Berikut merupakan tabel prioritasi risiko untuk proses perencanaan proses pengolahan:

Tabel 6.9 Prioritasi Risiko Perencanaan Proses Pengolahan (Sumber: Peneliti)

No	ID Risiko	Risiko	RPN	Level Risiko
1	J.01.03	Lambatnya akses jaringan	200	Very High
2	J.01.02	Kerusakan fisik kabel LAN dan WAN	140	High
3	S.01.03	Loading aplikasi lambat	105	Medium
4	S.01.02	Kegagalan aplikasi	96	Medium
5	D.01.01	Kehilangan data	80	Medium
6	H.01.02	Pencurian hardware	75	Low
7	D.01.02	Informasi rahasia tersebar luas	56	Low
8	P.01.02	Penyebaran data dan informasi rahasia	56	Low
9	H.01.03	Kerusakan hardware	54	Low
10	J.01.04	Jaringan mati	40	Low
11	S.01.04	Penyalahgunaan hak akses	40	Low
12	P.01.01	Kesalahan pengelolaan aset	36	Low
13	S.01.01	Cyber Threat	30	Low
14	H.01.01	Kebakaran	28	Low

15	J.01.01	Kehilangan kabel LAN dan WAN	28	Low

6.2.5.2 Prioritasi Risiko (Pengolahan dan Produksi BBM, Non-BBM dan Petrokimia)

Berikut merupakan tabel prioritasi risiko untuk proses pengolahan dan produksi BBM, non-BBM dan Petrokimia:

Tabel 6.10 Prioritasi Risiko Pengolahan dan Produksi BBM, non BBM dan Petrokimia (Sumber: Peneliti)

No	ID Risiko	Risiko	RPN	Level Risiko
1	J.02.03	Lambatnya akses jaringan	240	Very High
2	J.02.02	Kerusakan fisik kabel LAN dan WAN	160	High
3	S.02.02	Kegagalan aplikasi	144	High
4	D.02.02	Informasi rahasia tersebar luas	144	High
5	S.02.03	Loading aplikasi lambat	105	Medium
6	D.02.01	Kehilangan data	80	Medium
7	H.02.02	Pencurian hardware	75	Low
8	P.02.02	Penyebaran data dan informasi rahasia	72	Low
9	H.02.03	Kerusakan hardware	54	Low
10	J.02.04	Jaringan mati	40	Low
11	H.02.01	Kebakaran	40	Low
12	S.02.04	Penyalahgunaan hak akses	40	Low
13	P.02.01	Kesalahan pengelolaan aset	36	Low
14	J.02.01	Kehilangan kabel LAN dan WAN	32	Low
15	S.02.01	Cyber Threat	30	Low

6.2.5.3 Prioritasi Risiko (Distribusi Produk BBM, non-BBM dan Petrokimia)

Berikut merupakan tabel prioritasi risiko untuk proses distribusi produk BBM, non-BBM dan Petrokimia:

Tabel 6.11 Prioritasi Risiko Distribusi Produk BBM, non-BBM dan Petrokimia (Sumber: Peneliti)

No	ID Risiko	Risiko	RPN	Level Risiko
1	J.03.03	Lambatnya akses jaringan	240	Very High
2	J.03.02	Kerusakan fisik kabel LAN dan WAN	160	High
3	S.03.02	Kegagalan aplikasi	144	High
4	D.03.02	Informasi rahasia tersebar luas	144	High
5	S.03.03	Loading aplikasi lambat	105	Medium
6	H.03.02	Pencurian hardware	90	Medium
7	D.03.01	Kehilangan data	80	Medium
8	P.03.02	Penyebaran data dan informasi rahasia	72	Low
9	H.03.03	Kerusakan hardware	54	Low
10	J.03.04	Jaringan mati	40	Low
11	H.03.01	Kebakaran	40	Low
12	S.03.04	Penyalahgunaan hak akses	40	Low
13	P.03.01	Kesalahan pengelolaan aset	36	Low
14	J.03.01	Kehilangan kabel LAN dan WAN	32	Low
15	S.03.01	Cyber Threat	30	Low

6.2.5.4 Prioritasi Risiko (Pemeliharaan dan Pengendalian Peralatan Kilang)

Berikut merupakan tabel prioritasi risiko untuk proses pemeliharaan dan pengendalian peralatan kilang:

Tabel 6.12 Prioritasi Risiko Pemeliharaan dan Pengendalian Peralatan Kilang (Sumber: Peneliti)

No	ID Risiko	Risiko	RPN	Level Risiko
1	J.04.03	Lambatnya akses jaringan	240	Very High
2	J.04.02	Kerusakan fisik kabel LAN dan WAN	160	High
3	S.04.03	Kegagalan aplikasi	144	High
4	D.04.02	Informasi rahasia tersebar luas	144	High
5	S.04.04	Loading aplikasi lambat	105	Medium
6	H.04.03	Kerusakan hardware	90	Medium
7	D.04.01	Kehilangan data	80	Medium
8	H.04.02	Pencurian hardware	75	Low
9	P.04.02	Penyebaran data dan informasi rahasia	72	Low
10	J.04.04	Jaringan mati	40	Low
11	H.04.01	Kebakaran	40	Low
12	S.04.05	Penyalahgunaan hak akses	40	Low
13	P.04.01	Kesalahan pengelolaan aset	36	Low
14	J.04.01	Kehilangan kabel LAN dan WAN	32	Low
15	S.04.02	Cyber Threat	30	Low
16	S.04.01	Aplikasi tidak bisa digunakan	30	Low

6.2.5.5 Prioritasi Risiko (Pengelolaan *Health Safety Enviroment*)

Berikut merupakan tabel prioritasi risiko untuk proses pengelolaan *health safety environment:*

Tabel 6.13 Prioritasi Risiko Pengelolaan *Health Safety Enviroment* (Sumber: Peneliti)

No	ID Risiko	Risiko	RPN	Level Risiko
1	J.05.03	Lambatnya akses jaringan	200	Very High

2	J.05.02	Kerusakan fisik kabel LAN dan WAN	140	High
3	S.05.03	Loading aplikasi lambat	105	Medium
4	S.05.02	Kegagalan aplikasi	96	Medium
5	D.05.01	Kehilangan data	80	Medium
6	H.05.02	Pencurian hardware	60	Low
7	D.05.02	Informasi rahasia tersebar luas	56	Low
8	P.05.02	Penyebaran data dan informasi rahasia	56	Low
9	H.05.03	Kerusakan hardware	54	Low
10	J.05.04	Jaringan mati	40	Low
11	S.05.04	Penyalahgunaan hak akses	40	Low
12	P.05.01	Kesalahan pengelolaan aset	36	Low
13	S.05.01	Cyber Threat	30	Low
14	H.05.01	Kebakaran	28	Low
15	J.05.01	Kehilangan kabel LAN dan WAN	28	Low

6.3 Penyusunan Strategi BCP

Strategi BCP akan ditentukan berdasarkan hasil analisis yang telah dilakukan pada tahapan analisis dampak bisnis dan analisis risiko. Strategi BCP ini dibuat dengan tujuan untuk menjaga keberlangsungan dari proses bisnis yang diprioritaskan oleh organisasi. Selain strategi BCP, nantinya akan terdapat strategi DRP yang dibatasi hanya pada pemilihan metode pencadangan *(backup)* dan pemulihan *(restore)* untuk aplikasi non-ERP di PT. Pertamina RU IV.

Strategi BCP disusun dengan menggunakan masukan risiko TI yang bernilai *very high* (RPN≥200) dan *high* (RPN: 120-199) dengan asumsi bahwa jika risiko ini benar-benar terjadi akan mengganggu aktivitas yang ada pada proses bisnis kritikal di PT. Pertamina RU IV Cilacap. Menurut Padmavathy [38] dalam penyusunan sebuah strategi BCP, dibagi menjadi beberapa bagian, antara lain:

- **Strategi Pencegahan *(Prevention)***
  Tujuan dari strategi ini adalah untuk mengurangi kemungkinan terjadinya bencana/gangguan.
- **Strategi Tanggapan *(Response)***
  Strategi ini adalah perusahaan ketika bencana terjadi untuk mencegah kerusakan lebih lanjut, menilai tingkat kerusakan, serta menyediakan jalur komunikasi darurat untuk memulihkan operasional perusahaan dalam jangka waktu yang telah ditentukan sebelumnya.
- **Strategi Pemulihan *(Recovery)***
  Strategi pemulihan meliputi apa yang akan dilakukan perusahaan untuk memulai kembali proses bisnis yang terkena bencana, termasuk penentuan lokasi alternative untuk menjaga layanan TI agar tetap dapat digunakan oleh user.

Strategi yang disusun pada tugas akhir ini terbatas pada strategi pencegahan, tanggapan dan pemulihan dengan mengacu

pada *best practice* ISO 27002, *bandwith management* dari Cisco, dan *high availability* dari Microsoft. Pembuatan prosedur dan kebijakan terbatas pada pemberian rekomendasi sesuai dengan strategi yang diberikan.

Terdapat empat risiko TI yang menjadi dasar dalam pembuatan strategi BCP yang merupakan hasil dari analisis risiko pada tahap sebelumnya, antara lain adalah:

1. Lambatnya akses jaringan
2. Kerusakan fisik kabel LAN
3. Informasi rahasia tersebar luas
4. Kegagalan aplikasi

Strategi BCP untuk masing-masing risiko akan dipaparkan sebagai berikut:

6.3.1 Lambatnya Akses Jaringan

Tabel 6.14 Strategi Lambatnya Akses Internet (Sumber: Peneliti)

PERTAMINA	Risiko	: Lambatnya Akses Jaringan
	Penyebab	: Topologi LAN masih full star, dengan luasan area yang besar
Dampak	:	1. Perencanaan Proses Pengolahan 2. Pengolahan dan Produksi BBM, non-BBM dan Petrokimia 3. Distribusi Produk BBM, non-BBM dan Petrokimia 4. Pemeliharaan dan Pengendalian Peralatan Kilang 5. Pengeolaan *Health Safety Enviroment*
Strategi Pencegahan *(Prevention)*		
Strategi		**Keterangan**
Pemberlakuan kebijakan penggunaan internet dalam lingkungan kantor		Kebijakan ini bertujuan untuk mengatur penggunaan internet di masing-masing fungsi terkait tingkat kritikalitasnya. Salah satu contoh kebijakan terkait penggunaan internet adalah membagi jatah internet perfungsi dengan meninjau tingkat kritikalitas dan kebutuhannya. Kebijakan ini

	bisa didukung dengan dukungan dari IT seperti contohnya memblokir situs-situs yang tidak berhubungan dengan pekerjaan *(social media, youtube)* sehingga penggunaan *bandwith* dapat ditekan.

Menurut *best practice bandwith management* dari Cisco, langkah mitigasi yang direkomendasikan:

Penambahan bandwith bukanlah suatu solusi utama karena terbentur dengan terbatasnya budget. Berikut merupakan beberapa rekomendasi solusi yang ditawarkan oleh CISCO:

1. *Propagation delay*
   Salah satu solusi untuk mengatasi lambatnya jaringan internet adalah dengan mengurangi jarak yang harus ditempuh oleh data. Jarak yang semakin dekat antara *sites* dengan data center akan mempersingkat jarak yang ditempuh oleh data sehingga mempercepat akses jaringan. Namun hal ini sulit dilakukan karena pertimbangan keamanan dsb.
2. Pengolahan dan serial keterlambatan *(processing and serialization delay)*
   Setiap data yang melewati router atau switch akan memperlambat jalannya data karena data akan melewati proses penerimaan, proses, hingga kemudian dikirim kembali. Cara untuk mengatasi hal ini adalah dengan menggunakan Metro-Ethernet, dimana teknologi ini mendukung hardware-assisted forwarding, yang akan mengurangi *latency*. Cara lainnya adalah dengan menggunakan *cut-trough switching*, yang akan mengurangi dampak serialization-related delay pada switch. Dengan menggunakan *cut-trough switching*, data akan langsung diteruskan ke server tanpa melalui proses pembentukan paket data pada switch.
3. Mengecilkan paket *(smaller packets)*
   Untuk mempercepat proses pengiriman data, paket data yang dikirimkan akan *compress*, kemudian di *decompress* ketika sampai di tempat tujuan. Dewasa ini telah ditemukan sebuah algoritma yang memakan waktu yang lebih kecil dalam proses decompress, serta memakai tidak memakai usability CPU yang besar dan tetap menggunakan ukuran data yang rasional.
4. Antrian keterlambatan *(queuing delay)*
   Ketika paket yang datang pada router lebih cepat dari kecepatan paket meninggalkan router, maka akan terjadi antrian paket data. hal inilah yang menyebabkan jaringan menjadi lambat. Untuk menangai hal ini,

CISCO menawarkan solusi dengan menggunakan metode QoS, salah satunya adalah *Low-Latency Queuing* (LLQ).

5. Arsitektur server/OS *(server/OS architecture)*
   Jaringan yang optimal harus didukung oleh komponen infrastuktur yang memadai. Contohnya CPU, harddisk, memori dan OS *(operating systems)*
6. Keamanan dan kepatuhan
   Untuk mempercepat waktu pemorsesan data harus mempunyai sebanyak mungkin fitur keamanan yang diproses dalam satu wkatu yang bersamaan. Seperti contohnya, kebijakan keamanan yang diterapkan pada *firewall*, *intrusion detection*, perlindungan peralatan, enkripsi, *load balancers*, *traffic monitors*, dsb. Salah satu contoh solusinya adalah dengan menerapkan DMZ *(dimilitary zone)*, dimana per fungsi dibuat DMZ-nya sendiri-sendiri, dengan menerapkan kebijakan yang berbeda-beda antara satu dengan yang lain sehingga memudahkan proses monitoring dan pembedaan perlakuan tiap fungsi.

Strategi Tanggapan *(Response)*

Strategi	Keterangan
Pemindahan proses dari automasi ke proses manual	Jika terjadi gangguan pada akses jaringan yang menyebabkan jaringan mati total, maka akan dilakukan pemindahan proses dari terautomasi menjadi manual selama sistem dipulihkan. Proses pemindahan ini dapat memberikan tindakan langsung untuk menjaga operasional perusahaan.
Identifikasi penyebab gangguan	Saat menerima laporan terkait gangguan pada akses internet, maka langkah yang diambil oleh IT RU IV adalah melakukan identifikasi terkait penyebab gangguan. Tugas ini akan dilakukan oleh seluruh anggota *disaster recovery team* yang diketuai oleh *network officer* selaku penanggung jawab jaringan yang ada di RU IV.
Memperbaiki kesalahan sistem	Melakukan perbaikan terhadap gangguan jaringan sesuai dengan hasil identifikasi penyebab gangguan.

Penyelamatan data dan informasi	Penyelamatan data dilakukan oleh *data center officer* dengan tujuan untuk mencegah dampak lebih luas dari gangguan jaringan.
Restorasi data	Jika gangguan tidak bisa diatasi dalam jangka waktu maksimal yang telah disepakati, maka IT RU IV harus melakukan restorasi data dan menyediakan support layanan jaringan untuk mendukung berjalannya proses bisnis kritikal pada kondisi darurat.
Strategi Pemulihan *(Recovery)*	
Strategi	**Keterangan**
Sinkronisasi data	Sinkronisasi data bertujuan untuk menyamakan data yang disimpan dalam server selama kinerja sistem digantikan dengan manual. Sinkronisasi data dilakukan dengan bantuan personel IT yang disebar pada fungsi-fungsi yang terkena dampak gangguan.
Melakukan evaluasi terkait penyebab gangguan	Evaluasi penyebab gangguan bertujuan untuk mencegah kejadian serupa terulang kembali dan sebagai upaya peningkatan kinerja dari IT RU IV.
Melakukan evaluasi prosedur penanganan gangguan	Evaluasi terkait prosedur penanganan gangguan dan dokumentasi insiden yang dilakukan oleh tim DRP untuk memaksimalkan proses penanganan jika bencana serupa terulang kembali.

Menurut Susan [3], tidak ada satupun strategi dari *best practice* yang dapat tepat diaplikasikan pada perusahaan, namun harus disesuaikan dengan keadaan finansial, operasional, dan tujuan manajemen risiko masing-masing perusahaan. Oleh karena itu, hasil rekomendasi mitigasi dari *best practice* diatas akan dianalisis dengan mempertimbangkan biaya, kapabilitas, dan kebutuhan perusahaan sehingga menghasilkan strategi BCP untuk risiko lambatnya akses jaringan yang dapat diaplikasikan di PT. Pertamina RU IV. Justifikasi yang diberikan didasarkan pada rencana pengembangan TI RU IV 2016 dan justifikasi subjektif dari peneliti.

Tabel 6.15 Pemilihan Strategi Mitigasi Risiko Lambatnya Akses Jaringan (Sumber: Peneliti)

PERTAMINA	**Pemilihan Strategi Mitigasi**		
Kategori	Opsi Mitigasi	Biaya, Kapabilitas, dan Kebutuhan	Mitigasi Risiko
Akses Jaringan	*Propagation delay*	Biaya relatif besar karena harus memindahkan data center, pertimbangan lain adalah data center tidak bisa diletakkan dekat dengan kilang (tempat proses bisnis kritikal) karena faktor keamanan, efektifitas cukup tinggi [38]	Dengan mempertimbangkan biaya yang dikeluarkan dan tingkat efektifitas, maka solusi potensial untuk risiko lambatnya akses jaringan adalah: **1.Mengecilkan paket data *(risk limitation)*** Strategi ini bisa diterapkan karena membutuhkan biaya yang relatif kecil dengan efektifitas yang cukup tinggi. ***2.Queuing delay (risk limitation)*** Strategi ini bisa diterapkan karena membutuhkan biaya yang relatif kecil dengan efektifitas yang cukup tinggi.
	Processing and serialization delay	Biaya relatif besar karena harus didukung oleh hardware Metro-Ethernet, namun tingkat efektifitas cukup tinggi [34]	
	Mengecilkan paket data	Biaya relatif murah karena hanya menerapkan	

		algoritma tertentu dalam coding router, tingkat efektifitas cukup tinggi [34]	**3.Arsitektur server/OS *(risk limitation)*** Infrastruktur yang ada di Pertamina dapat dikatakan sudah memadai sehingga secara tidak langsung Pertamina telah menerapkan strategi ini. **4.Keamanan dan kepatuhan *(risk limitation)*** Strategi pembuatan *dimilitary zone* dapat menjadi pilihan karena IT dapat membagi wewenang tiap fungsi pada jaringan. Strategi ini juga relatif murah karena hanya mengubah pengaturan *(coding)* dalam router dan menghasilkan dampak yang cukup signifikan.
	Queuing delay	Biaya relatif murah karena hanya mengubah pengaturan (coding) pada router, tingkat efektifitas cukup tinggi [39]	
	Arsitektur server/OS	Biaya moderate karena perusahaan harus memilih infrastruktur mana yang bisa mendukung jaringan, tingkat efektifitas tidak dapat dipastikan	
	Keamanan dan kepatuhan	Biaya relatif murah karena hanya mengubah pengaturan *(coding)* pada router, tingkat efektifitas cukup tinggi [40]	

6.3.2 Kerusakan Fisik Kabel LAN dan WAN

Tabel 6.16 Strategi Kerusakan Fisik Kabel LAN dan WAN (Sumber: Peneliti)

PERTAMINA	Risiko	: Kerusakan Fisik Kabel LAN dan WAN
	Penyebab	: 1. Kurangnya pengamanan fisik pada kabel LAN dan WAN 2. Komponen kabel yang rentan terputus
Dampak	:	1. Perencanaan Proses Pengolahan 2. Pengolahan dan Produksi BBM, non-BBM dan Petrokimia 3. Distribusi Produk BBM, non-BBM dan Petrokimia 4. Pemeliharaan dan Pengendalian Peralatan Kilang 5. Pengeolaan *Health Safety Enviroment*
Strategi Pencegahan *(Prevention)*		
Strategi		**Keterangan**
Penyusunan prosedur pengkabelan dan peralatan listrik		Ditujukan untuk sebagai pedoman perusahaan terkait pemasangan, perlindungan, serta permasalahan terkait kelistrikan, jaringan LAN, dan jaringan WAN.
Menurut ISO 27002:2011, langkah mitigasi yang direkomendasikan: *Control Objective*: **9.2.3 [Pengamanan Kabel]** Kabel daya dan telekomunikasi yang menyalurkan data atau mendukung layanan informasi harus dilindungi dari gangguan atau kerusakan		
Implementation Guadiance: 1. Kabel daya dan telekomunikasi yang berkaitan dengan fasilitas penyaluran informasi harus diletakkan di bawah tanah jika memungkinkan, atau diberikan proteksi alternatif lain yang sebanding. 2. Untuk sistem kritikal, sebaiknya diterapkan kontrol lebih lanjut, termasuk diantaranya: – Instalasi saluran lapis baja dan mengunci ruangan atau kotak pada *termination points.* – Penggunaan routing alternatif dan/atau media transmisi untuk menyediakan pengamanan yang sesuai		

– Penggunaan kabel serat optic – Penggunaan perisai elektromaknetik untuk melindungi kabel – Insiasi inspeksi teknis dan pemeriksaan fisik untuk mencari perangkat tidak sah yang melekat pada kabel – Akses pada panel patch dan ruangan kabel dikontrol dengan baik	
Pemberlakuan prosedur backup data secara rutin pada proses bisnis kritikal	Hal ini dilakukan sebagai langkah preventif jika tiba-tiba kabel atau jaringan mengalami gangguan secara tiba-tiba.
Melakukan monitoring secara berkala	Monitoring ditujukan untuk mengetahui kondisi terkini dari kabel LAN secara berkala. Jika terjadi kerusakan atau pelanggaran, maka petugas bisa langsung mengambil tindakan sehingga kerugian perusahaan dapat diminimalisir. Penerapan strategi ini didukung oleh dokumen lain, yaitu: 1. Prosedur monitoring dan evaluasi kondisi fisik kabel LAN dan WAN
Strategi Tanggapan *(Response)*	
Pemindahan proses dari automasi ke proses manual	Jika terjadi gangguan pada kabel LAN dan WAN secara otomatis akan mengganggu akses user ke jaringan. Yang harus dilakukan pertama kali adalah memindahkan proses dari terautomasi menjadi manual selama sistem dipulihkan pada proses bisnis yang terkena dampak.
Identifikasi penyebab gangguan	Tugas ini akan dilakukan oleh seluruh anggota *disaster recovery team* yang diketuai oleh *network officer* selaku penanggung jawab jaringan yang ada di RU IV.
Memperbaiki penyebab gangguan	Melakukan perbaikan pada sumber gangguan kerusakan kabel sesuai dengan hasil identifikasi penyebab gangguan.
Strategi Pemulihan *(Recovery)*	
Sinkronisasi data	Sinkronisasi data bertujuan untuk menyamakan data yang disimpan dalam server selama kinerja sistem digantikan dengan manual. Sinkronisasi

	data dilakukan dengan bantuan personel IT yang disebar pada fungsi-fungsi yang terkena dampak gangguan.
Melakukan evaluasi terkait penyebab gangguan	Evaluasi penyebab gangguan bertujuan untuk mencegah kejadian serupa terulang kembali dan sebagai upaya peningkatan kinerja dari IT RU IV.
Melakukan evaluasi prosedur penanganan gangguan	Evaluasi terkait prosedur penanganan gangguan dan dokumentasi insiden yang dilakukan oleh tim DRP untuk memaksimalkan proses penanganan jika bencana serupa terulang kembali.

Menurut Susan [3], tidak ada satupun strategi dari *best practice* yang dapat tepat diaplikasikan pada perusahaan, namun harus disesuaikan dengan keadaan finansial, operasional, dan tujuan manajemen risiko masing-masing perusahaan. Oleh karena itu, hasil rekomendasi mitigasi dari *best practice* akan dianalisis dengan mempertimbangkan biaya, kapabilitas, dan kebutuhan perusahaan sehingga menghasilkan strategi BCP untuk risiko kerusakan fisik kabel LAN dan WAN yang dapat diaplikasikan di PT. Pertamina RU IV. Justifikasi yang diberikan didasarkan pada rencana pengembangan TI RU IV 2016 dan justifikasi subjektif dari peneliti.

Tabel 6.17 Pemilihan Strategi Mitigasi Risiko Kerusakan Fisik Kabel LAN dan WAN (Sumber: Peneliti)

PERTAMINA	**Pemilihan Strategi Mitigasi**		
Kategori	Opsi Mitigasi	Biaya, Kapabilitas, dan Kebutuhan	Mitigasi Risiko
Kerusakan fisik kabel LAN dan WAN	Pengamanan kabel	Biaya bervariasi, dari murah hingga mahal. Cukup efektif untuk mitigasi risiko	Dengan mempertimbangkan biaya yang dikeluarkan dan tingkat efektifitas, maka solusi

		kerusakan fisik kabel LAN dan WAN yang disebabkan oleh komponen kabel yang rentan putus	potensial untuk risiko kerusakan fisik kabel LAN dan WAN adalah: **1.Menerapkan *cable management (risk limitation)*** Bentuk pengamanan kabel yang mungkin diterapkan pada PT. Pertamina RU IV adalah merapikan jalannya kabel dan menjepit kabel pada dinding sehingga lebih rapi dan mengurangi risiko kabel tertarik secara tidak sengaja.

6.3.3 Informasi Rahasia Tersebar Luas

Tabel 6.18 Strategi Informasi Rahasia Tersebar Luas (Sumber: Peneliti)

PERTAMINA	Risiko	: Informasi Rahasia Tersebar Luas
	Penyebab	: 1. *Hacker* dan *cracker* 2. *Unauthorized access* yang masuk ke dalam database
Dampak	:	1.Perencanaan Proses Pengolahan 3.Distribusi Produk BBM, non-BBM dan Petrokimia 4.Pemeliharaan dan Pengendalian Peralatan Kilang

Strategi Pencegahan *(Prevention)*	
Strategi	**Keterangan**
Pemberlakuan kebijakan dan prosedur penggunaan jaringan internet	Bertujuan untuk memberikan pedoman dan panduan bagi civitas organisasi terhadap penggunaan jaringan internet dan hak akses tiap user
Memberikan pelatihan dan sosialisasi terkait keamanan data	Sosialisasi ini bertujuan untuk meningkatkan kesadaran seluruh karyawan terkait pentingnya keamanan data, the power of data, apa yang bisa dilakukan untuk menjaga data. Dalam memaksimalkan pengamanan data, dapat pula dibarengi dengan penerapan beberapa prosedur untuk mendukung hal tersebut. Antara lain adalah: 1. Prosedur pengamanan fisik ruang server 2. Prosedur akses ruang server 3. Prosedur hak akses sistem 4. Prosedur manajemen password
Pengujian tingkat keamanan secara periodik	Strategi ini bertujuan untuk mengetahui sebaik mana kontrol keamanana jaringan yang telah diterapkan organisasi. Hasil dari pengujian ini digunakan sebagai bahan evaluasi untuk perbiaikan.

Menurut ISO 27002:2011, langkah mitigasi yang harus dilakukan:

Control Objective:

11.4.1 [Kebijakan Penggunaan Layanan Jaringan]

User hanya diberikan akses pada jaringan spesifik, dimana mereka memang diijinkan untuk menggunakannya.

Implementation Guadiance:

Kebijakan harus dibuat dengan berfokus pada penggunaan jaringan dan layanan jaringan. Kebijakan ini mencakup antara lain:

a. Jaringan dan layanan jaringan yang boleh diakses
b. Prosedur otorisasi untuk menentukan siapa yang diperbolehkan untuk mengakses jaringan dan layanan jaringan
c. Kontrol manajemen dan prosedur untuk melindungi akses pada koneksi jaringan dan layanan jaringan

Cara yang digunakan untuk mengakses jaringan dan layanan jaringan

Control Objective:

11.4.2 [Autentifikasi User untuk Koneksi Eksternal]

Metode autentifikasi yang memadai harus digunakan untuk mengontrol akses dari user jarak jauh
Implementation Guadiance: 1. Autentifikasi untuk user jarak jauh bisa dicapai dengan menggunakan, contohnya, teknik kriptografi, token hardware, atau dengan mengerapkan protokol balasan *(response protocol)*. Kemungkinan implementasi tersebut dapat diterapkan untuk solusi *virtual private network* (VPN). 2. Prosedur dan kontrol *dial-back*, contohnya dengan menggunakan modem *dial-back*, dapat digunakan untuk melindungi koneksi yang tidak terauthentifikasi pada fasilitas pengiriman informasi yang digunakan oleh organisasi. Kontrol autentifikasi tambahan harus diimplementasikan untuk mengontrol akses pada jaringan *wireless*. Dalam sebagian kasus, penanganan spesial perlu dilakukan dengan mempertimbangkan kemungkinan tidak terdeteksinya intersepsi atau gangguan pada traffic jaringan.
Control Objective: **11.4.3 [Identifikasi Peralatan dalam Jaringan]** Identifikasi peralatan otomatis harus dipertimbangkan untuk membuktikan lokasi spesifik dan peralatan yang digunakan untuk mengakses jaringan.
Implementation Guadiance: 1. Identifikasi peralatan dapat digunakan jika dirasa penting untuk kasus jika jalur komunikasi hanya bisa diakses dari lokasi dan peralatan yang spesifik. Implementasinya bisa menggunakan *identifier* yang diletakkan pada peralatan yang bisa digunakan untuk mengindikasikan apakah peralatan ini diijinkan atau tidak untuk mengakses jaringan. *Identifier* harus bisa dengan jelas mengindikasikan jaringan mana yang boleh diakses. Dan jika terdapat lebih dari satu jaringan yang ada, dan terutama jika jaringan ini memiliki tingkat sensitivitas yang berbeda, maka perlu dipertimbangkan untuk memberikan perlindungan fisik peralatan untuk menjaga keamanan *identifier*.
Control Objective: **11.4.4 [Diagnosa Jarak Jauh dan Perlindungan Konfigurasi Port]** Akses fisik dan logis untuk diagnosa dan konfigurasi port harus dikontrol
Implementation Guadiance:

1. Kontrol potensial untuk akses ke diagnosa dan konfigurasi port termasuk penggunaan *key lock* dan prosedur pendukung untuk mengontrol akses fisik ke dalam port. Contoh prosedur pendukung adalah memastikan bahwa diagnosa dan konfigurasi port hanya dapat diakses melalui pengaturan antara manager TI dan personil hardware/software.

Port, layanan, dan fasilitas serupa yang terpasang pada fasilitas komputer atau jaringan, yang tidak khusus diperlukan untuk fungsi bisnis harus dinonaktifkan atau dihapus.

Control Objective:

11.4.5 [Pemisahan dalam Jaringan]

Kelompok layanan informasi, user dan sistem informasi harus dipisahkan dalam jaringan

Salah satu metode untuk mengontrol keamanan pada jaringan yang luas adalah membaginya berdasarkan domain logikal, contohnya, domain internal dan eksternal organisasi. Terdapat beberapa cara yang dapat dilakukan, antara lain:

1. Penerapan *security perimeter* untuk melindungi domain internal dan eksternal organisasi. *Security perimeter* dapat diimplementasikan dengan menginstal pintu gerbang aman *(secure gateway)* diantara dua jaringan untuk dapat terhubung pada kontrol akses dan alur informasi diantara dua domain.
2. Metode lain yang dapat diterapkan adalah dengan menggunakan fungsionalitas perangkat jaringan *(network device functionality)*, sebagai contoh IP switching.
3. Cara lainnya adalah mengontrol alur data dengan menggunakan kemampuan *routing* atau *switching*, seperti contohnya *access control list*.

Kriteria dalam pemisahan jaringan menjadi domain-domain tertentu harus didasarkan pada kebijakan kontrol akses dan kebutuhan akses, dan juga mempertimbangkan biaya relative dan dampak pada kinerja perusahaan.

Control Objective:

11.4.7 [Kontrol *Routing* Jaringan]

Kontrol *routing* harus diimplementasikan pada jaringan untuk memastikan bahwa koneksi komputer dan arus informasi tidak melanggar kebijakan pengendalian akses dari aplikasi bisnis.

Implementation Guadiance:

Kontrol routing harus didasarkan pada sumber positif dan menerapkan mekanisme pengecekan alamat tujuan.

Security gateway dapat digunakan untuk validasi sumber dan alamat tujuan pada kontrol poin jaringan internal atau eksternal jika proxy dan/atau teknologi perubahan alamat jaringan digunakan. implementers harus memahami kelebihan dan kekurangan dari mekanisme yang diterapkan.	
Strategi Tanggapan *(Response)*	
Strategi	**Keterangan**
Identifikasi pelaporan	Melakukan identifikasi saat terdapat pelaporan atau terdeteksi gangguan untuk mengetahui penyebab gangguan sehingga dapat segera diambil tindakan penyelesaian.
Pengamanan aset TI terutama pada data confidential	Melakukan upaya backup atau pembatasan hak akses pada aset TI yang mengandung data confidential.
Menutup celah keamanan yang terbuka	Hal ini harus dilakukan dengan cepat untuk menghindari dampak yang semakin parah.
Strategi Pemulihan *(Recovery)*	
Strategi	**Keterangan**
Penindakan pelaku	Pelaku diserahkan pada pihak berwajib agar menimbulkan efek jera dan sebagai pelajaran bagi civitas lain yang ada di PT. Pertamina RU IV.
Evaluasi manajemen password dan pengelolaan hak akses	Evaluasi ini diperlukan untuk mereview kembali tingkat efektivitas prosedur yang telah dijalankan terkait dengan risiko ini. Peninjauan ulang dilakukan agar dapat dilakukan perbaikan prosedur sehingga kejadian serupa tidak akan terjadi kembali di masa depan. Penerapan strategi ini didukung oleh dokumen lain, yaitu: 1. Prosedur pemantauan dan evaluasi pengelolaan hak akses
Evaluasi tingkat keamanan data pada sistem	Evaluasi ini bertujuan untuk melihat celah kerentanan dari sistem keamanan yang diterapkan oleh organisasi. Hasil dari evaluasi ini akan menjadi bahan perbaikan sistem keamanan kedepannya.

	Penerapan strategi ini didukung oleh dokumen lain, yaitu: 1. Prosedur pemantauan dan evaluasi keamanan informasi
Perbaikan prosedur manajemen password dan pengeloaan hak akses	Strategi perbaikan prosedur ini dilakukan dengan melihat hasil evaluasi prosedur yang telah dijalankan. Nantinya perbaikan diharapkan dapat meningkatkan keefektifan prosedur dalam meminimalisir risiko ini.
Perbaikan terhadap keamanan data pada sistem organisasi	Hal ini dilakukan setelah melihat hasil evaluasi tingkat keamanan data pada sistem. Langkah ini diambil sesegera mungkin untuk mencegah terjadinya kembali risiko yang sama, serta meminimalisir kerugian.
Pengujian dan monitoring hasil perbaikan	Melakukan pengujian dan monitoring hasil perbaikan agar kejadian serupa tidak terulang kembali.

Menurut Susan [3], tidak ada satupun strategi dari *best practice* yang dapat tepat diaplikasikan pada perusahaan, namun harus disesuaikan dengan keadaan finansial, operasional, dan tujuan manajemen risiko masing-masing perusahaan. Oleh karena itu, hasil rekomendasi mitigasi *best practice* diatas akan dianalisis dengan mempertimbangkan biaya, kapabilitas, dan kebutuhan perusahaan sehingga menghasilkan strategi BCP untuk risiko informasi rahasia tersebar luas yang dapat diaplikasikan di PT. Pertamina RU IV. Justifikasi yang diberikan didasarkan pada rencana pengembangan TI RU IV 2016 dan justifikasi subjektif dari peneliti.

Tabel 6.19 Pemilihan Strategi Mitigasi Risiko Informasi Rahasia Tersebar Luas (Sumber: Peneliti)

PERTAMINA	**Pemilihan Strategi Mitigasi**		
Kategori	Opsi Mitigasi	Biaya, Kapabilitas, dan Kebutuhan	Mitigasi Risiko

Informasi rahasia tersebar luas	Kebijakan penggunaan layanan jaringan	Biaya relatif murah, perlu adanya sosialisasi, tingkat efektifitas bergantung pada kerjasama antar *stakeholder*.	Dengan mempertimbangkan biaya yang dikeluarkan dan tingkat efektifitas, maka solusi potensial untuk risiko informasi rahasia tersebar luas antara lain: **1.Kebijakan penggunaan layanan jaringan *(risk limitation)*** Dalam memaksimalkan pengamanan data, dapat pula dibarengi dengan penerapan beberapa prosedur untuk mendukung hal tersebut. Antara lain adalah: – Prosedur pengamanan fisik ruang server – Prosedur akses ruang server – Prosedur hak akses sistem – Prosedur manajemen password
	Autentifikasi user untuk koneksi eksternal	Biaya relatif murah, tingkat efektifitas relatif tinggi karena user eksternal tidak bisa terhubung.	
	Identifikasi peralatan dalam jaringan	Biaya relatif mahal karena diperlukan identifier yang ditempatkan pada tiap perangkat sebagai tanda pengenal, namun tingkat efektifitas relatif tinggi [41]	
	Diagnosa jarak jauh dan perlindungan konfigurasi port	Biaya relatif mahal namun Pertamina telah menerapkan startegi perlindungan port. Tingkat efektifitas cukup tinggi	

		untuk mencegah orang yang tidak berkepentingan mengubah konfigurasi	**2.Autentifikasi user untuk koneksi eksternal *(risk limitation)*** Proses autentifikasi dilakukan dengan cara memasang proxy, dimana user yang hendak masuk ke dalam jaringan harus memasukkan id dan password yang hanya dimiliki oleh karyawan internal. **3.Perlindungan konfigurasi port *(risk limitation)*** Strategi ini telah diterapkan oleh Pertamina dalam bentuk pengamanan ruang server dengan menggunakan kartu akses. Namun dalam pelaksanaannya masih belum maksimal karena akses bisa dipinjam antar
	Pemisahan dalam jaringan	Biaya relatif mahal karena dibutuhkan hardware pendukung dalam penerapan strategi ini. Tingkat efektifitas cukup tinggi untuk meningkatkan keamanan jaringan	
	Kontrol routing jaringan	Biaya relatif murah karena hanya penambahkan pengaturan (koding) pada perangkat, tingkat efektifitas cukup tinggi untuk mencegah jaringan terhubung pada sumber yang tidak dikenal	

			karyawan. Untuk peningkatan bisa dengan menggunakan *finger print* dan *acess log* yang di review secara rutin. **4.Kontrol routing jaringan *(risk limitation)*** Strategi ini bisa diterapkan karena tidak membutuhkan biaya yang besar namun tingkat efektifitas yang ditimbulkan cukup tinggi.

6.3.4 Kegagalan Aplikasi

Tabel 6.20 Strategi Kegagalan Aplikasi (Sumber: Peneliti)

PERTAMINA	Risiko	: Kegagalan Aplikasi
	Penyebab	: 1. Sistem tidak bisa menerima semua request 2. Adanya bug dan error bawaan dari sistem
Dampak	:	2. Pengolahan dan Produksi BBM, non-BBM dan Petrokimia 3. Distribusi Produk BBM, non-BBM dan Petrokimia 4. Pemeliharaan dan Pengendalian Peralatan Kilang
Strategi Pencegahan *(Prevention)*		
Strategi		**Keterangan**

Meningkatkan kualifikasi pengembang aplikasi	Pengembang aplikasi yang berpengalaman akan memperbesar kemungkinan menghasilkan aplikasi dalam kualitas yang bagus. Pertamina bisa mensyaratkan portofolio atau pengalaman kerja minimal 2 tahun bagi pengembang aplikasi. Penerapan strategi ini didukung oleh dokumen lain, yaitu: 1. Prosedur seleksi pengembang aplikasi
Memberikan pelatihan terkait pembangunan aplikasi	Pelatihan ini akan diikuti oleh developer, baik karyawan baru maupun lama. Tujuan dari pelatihan ini adalah untuk memberikan wawasan tambahan bagi pengembang aplikasi mengenai bagaimana cara mengembangkan aplikasi dengan *high availability*. Pengisi materi bisa dari internal atau eksternal perusahan.
Membuat *disaster recovery plan* (DRP)	Strategi *disaster recovery plan* (DRP) akan menjadi panduan bagi perusahaan dalam menghadapi gangguan yang berkaitan dengan teknologi informasi.
Adanya pendokumentasian sistem	Dokumen *Software Requiremet Spesification* (SKPL) menjadikan pembuatan sistem terdokumentasi dengan baik, sehingga menghindari kesalahan dalam pembangunan sistem.
Menurut ISO 27002:2011, langkah mitigasi yang harus dilakukan: *Control Objective*: **9.2.4 [Perawatan Peralatan]** Peralatan harus dikelola secara baik untuk memastikan *availability* dan *integrity*-nya.	
Implementation Guadiance: a. Harus dilakukan tindakan maintenance berdasarkan rekomendasi interval dan spesifikasi dari pemasok aset b. Hanya staff yang diizinkan yang dapat melakukan perbaikan dan servis peralatan c. Penerapan kontrol harus dilakukan untuk memastikan bahwa maintenance aset dilakukan tepat waktu dan dengan menggunakan prosedur yang tepat.	
Menurut *best practice best availability* dari Microsoft, langkah mitigasi yang harus dilakukan:	

Berikut merupakan rekomendasi *best practice* dari Microsoft selaku perusahaan yang mengembangkan bahasa pemograman ASP terkait *high-availability* aplikasi:

1. Menggunakan *clustering*
   Clustering adalah teknologi kunci yang digunakan untuk menyediakan aplikasi dengan high availability karena memberikan layanan *failover instant* ketika aplikasi mengalami kegagalan.
2. Menggunakan *network load balancing*
   Network load balancing (NLB) mendukung *high availability* aplikasi dengan cara secara otomatis mendeteksi kegagalan server dan mengalihkan *traffic* klien ke server lain yang sedang berkerja dalam waktu kurang dari sepuluh detik. Dengan menerapkan NLB akan mendapatkan dua keuntungan, yaitu *high availability* dengan support minimal, dan *incremental scability* dengan penambahan kapasitas yang mudah.
3. Menyediakan *help desk* untuk mengurangi downtime
   Help desk bertanggung jawab untuk mengumpulkan informasi permasalahan, menentukan penyebab permasalahan, dan mencari solusi sementara. Menguji prosedur *help desk* dapat membantu meminimalisir waktu yang dibutuhkan dalam menangani kegagalan aplikasi.
4. Menguji *recovery plan*
   Menguji DRP dengan memasukkan berbagai situasi yang mungkin terjadi akan meminimalisir kerugian. Dengan rencana yang dan eksekusi yang matang, akan meminimalisir kerugian yang akan diterima perusahaan.
5. Memilih infrastruktur yang baik
   Infrastuktur yang baik akan mendukung jalannya aplikasi sehingga kemungkinan kegagalan aplikasi bisa diminimalisir. Beberapa jenis hardware yang dapat mempengaruhi kinerja aplikasi antara lain adalah:
   - Hardware
   - Software
   - Memori
   - *Physical data storage*
   - Database
   - Network

- Environment
- Front-end servers
- Back-end servers

6. Menggunakan data backup
   Salah satu cara untuk melakukan maintain integritas data adalah dengan melakukan full data backup. Cara ini dapat dikembangkan lagi dengan menggabungkan backup dengan aplikasi transaction log.
7. Melakukan review pada seluruh rencana keamanan
   Untuk aplikasi yang bersifat kritikal, penting untuk menjaga keamanan komunikasi antara aplikasi, user, dan web partner bisnis. Keamanan dari aplikasi web mencakup beberapa hal:
   - Pengamanan front-end server dari unathourized access
   - Pengamanan privasi data dan integritas server
   - Pengamanan dari intruisi, contohnya *denial service attack*
8. Pelatihan advokat dan sertifikasi

Staff ekspert adalah salah satu part penting dalam *availability engineering*. Staff ekspert akan membantu organisasi dalam membuat desain dan *coding* yang lebih baik sehingga mengurangi kemungkinan kegagalan aplikasi.

Dari sudut pandang infrastruktur, langkah mitigasi yang harus dilakukan:

Jika dipandang dari sudut pandang infastruktur, hal yang bisa dilakukan untuk meminimalisir kemungkinan kegagalan aplikasi adalah dengan menerapkan *Virtual Dedicated Server*. VDS adalah sebuah teknologi server side tentang sistem operasi dan perangkat lunak yang memungkinkan sebuah mesin dengan kapasitas besar dibagi ke dalam beberapa mesin virtual. Hal ini juga bisa menekan budget untuk pengadaan server serta dapat dikatakan cukup efektif, karena jika terjadi kerusakan pada suatu server akan secara otomatis akan diganti pada server lain yang standby sehingga risiko kegagalan aplikasi yang disebabkan oleh faktor infrastruktur bisa diminimalisir.

Strategi Tanggapan *(Response)*

Strategi	Keterangan
Melakukan *restore* backup database	Saat terjadi insiden kehilangan data, hal pertama yang harus dilakukan adalah melakukan restore data backup yang disimpan dalam server

	cadangan. Prosedur ini diatur dalam *disaster recovery plan.*
Mengaktifkan strategi DRP	Dalam strategi pengamanan aset SI/TI terdapat strategi DRP, yaitu terkait dengan pembuatan panduan manajemen insiden. Manajemen insiden dibuat untuk memastikan bahwa pemulihan gangguan dapat berjalan.
Strategi Pemulihan *(Recovery)*	
Strategi	**Keterangan**
Sinkronisasi data	Sinkronisasi data bertujuan untuk menyamakan data yang disimpan dalam server selama kinerja sistem digantikan dengan manual. Sinkronisasi data dilakukan dengan bantuan personel IT yang disebar pada fungsi-fungsi yang terkena dampak gangguan.
Melakukan evaluasi terkait penyebab gangguan	Evaluasi penyebab gangguan bertujuan untuk mencegah kejadian serupa terulang kembali dan sebagai upaya peningkatan kinerja dari IT RU IV.
Melakukan evaluasi prosedur penanganan gangguan	Evaluasi terkait prosedur penanganan gangguan dan dokumentasi insiden yang dilakukan oleh tim DRP untuk memaksimalkan proses penanganan jika bencana serupa terulang kembali.

Menurut Susan [3], tidak ada satupun strategi dari *best practice* yang dapat tepat diaplikasikan pada perusahaan, namun harus disesuaikan dengan keadaan finansial, operasional, dan tujuan manajemen risiko masing-masing perusahaan. Oleh karena itu, hasil rekomendasi mitigasi *best practice* akan dianalisis dengan mempertimbangkan biaya, kapabilitas, dan kebutuhan perusahaan sehingga menghasilkan strategi BCP untuk risiko kegagalan aplikasi yang dapat diaplikasikan di PT. Pertamina RU IV. Justifikasi yang diberikan didasarkan pada rencana pengembangan TI RU IV 2016 dan justifikasi subjektif dari peneliti.

Tabel 6.21 Pemilihan Strategi Mitigasi Risiko Kegagalan Aplikasi (Sumber: Peneliti)

PERTAMINA	**Pemilihan Strategi Mitigasi**		
Kategori	Opsi Mitigasi	Biaya, Kapabilitas, dan Kebutuhan	Mitigasi Risiko
Kegagalan aplikasi	Perawatan peralatan	Biaya moderat, meminimalisir kemungkinan terjadinya risiko dari faktor hardware	Dengan mempertimbangkan biaya yang dikeluarkan dan tingkat efektifitas, maka solusi potensial untuk risiko kegagalan aplikasi adalah: **1.Perawatan peralatan *(risk limitation)*** Dalam IT RU IV terdapat tim khusus yang memiliki *jobdesc* maintenance rutin atau pemeliharaan aset TI sehingga aset TI selalu dalam keadaan baik. ***2.Help desk (risk limitation)*** IT RU IV memiliki help desk yang berfungsi sebagai garda depan jika
	Clustering	Biaya moderat, zero downtime, bisa memenuhi MTD, efektifitas cukup tinggi karena seluruh prosesor dapat melakukan fungsi yang sama sehingga kegagalan dari sebuah prosesor tidak akan menghentikan sistem [42]	
	Network load balancing	Biaya untuk software relatif murah, kapabilitas tidak bisa ditentukan karena performanya	

		sangat bergantung pada hardware dan infrastruktur [43]	user mengalami masalah yang berhubungan dengan layanan TI. Harapannya, permasalahan TI sehari-hari yang bersifat minor dapat terselesaikan dengan bantuan help desk. **3.Menggunakan teknologi backup data *(risk limitation)*** IT RU IV telah menerapkan beberapa strategi pencadangan *(backup)* dan pemulihan *(restore)* yang disesuaikan dengan kebutuhan masing-masing aplikasi. Detail strategi backup yang digunakan dapat dilihat pada bab **6.3.1 Strategi DRP.** ***4.Virtual dedicated server (risk limitation)***
	Help desk	Biaya relatif murah, bertugas sebagai garda depan dalam mengatasi permasalahan TI sehari-hari	
	Menguji *recovery plan*	Biaya relatif mahal karena untuk menguji recovery plan berarti harus menghentikan layanan IT, baik secara parsial maupun seluruhnya, dan melibatkan fungsi bisnis lain yang terkait.	
	Memilih infrastruktur yang baik	Pemilihan infrastruktur terbentur oleh budget belanja departemen sehingga IT tidak bisa leluasa menentukan infrastruktur	

		apa yang digunakan	VDS merupakan salah satu solusi yang menjanjikan zero downtime. Pemilihan strategi ini sejalan dengan rencana tindak lanjut mitigasi risiko tahun 2015 dan 2016 PT. Pertamina RU IV.
	Menggunakan *data backup*	Biaya relatif mahal, memenuhi MTD, menekan waktu *recovery* data	
	Review rencana keamanan	Biaya relatif murah dan efektif digunakan untuk evaluasi sejauh mana upaya mitigasi yang telah diterapkan	
	Pelatihan advokat dan sertifikasi	Biaya relatif mahal, dampak tidak bisa dirasakan langsung oleh perusahaan	
	Virtual dedicated server	Biaya relatif mahal, zero downtime, memenuhi MTD	

6.3.1 Strategi DRP

Strategi DRP adalah rencana pemulihan layanan IT pasca terjadinya bencana atau gangguan untuk menekan risiko kerugian perusahaan ke tingkat yang dapat diterima oleh manajemen. Strategi DRP fokus kepada penggunaan teknologi, proses dan sumber daya manusia yang bertujuan untuk memenuhi service level objective yang diwujudkan dalam bentuk kesepakatan nilai

RTO dan RPO masing-masing aplikasi pada saat terjadinya bencana [3]. Dalam strategi DRP yang dibuat dalam penelitian tugas akhir ini dibatasi pada strategi pencadangan *(backup)* dan strategi pemulihan *(restore)* pada layanan aplikasi non-ERP yang ada di PT. Pertamina RU IV.

6.3.1.1 Posisi RTO dan RPO Maksimum Layanan Aplikasi

Sebelum menentukan strategi pencadangan dan pemulihan layanan TI, terlebih dahulu harus didefinisikan kebutuhan pemulihan masing-masing layanan. Proses penentuan kebutuhan pemulihan mengacu pada nilai RTO dan RPO masing-masing layanan yang telah didefinisikan sebelumnya pada dokumen BIA. Berikut merupakan **contoh** daftar RTO dan RPO maksimum layanan aplikasi dan non aplikasi yang ada di PT. Pertamina RU IV Cilacap. Untuk daftar nilai RTO dan RPO seluruh layanan aplikasi dan non-aplikasi lainnya dapat dilihat di buku produk pada bab **11.2.1.1 Posisi RTO dan RPO Maksimum Layanan Aplikasi.**

Berikut merupakan contoh nilai RTO dan RPO maksimum layanan aplikasi dan non aplikasi berdasarkan analisa yang dimunculkan pada dokumen BIA:

Tabel 6.22 Posisi RTO dan RPO Maksimum Layanan Aplikasi (Sumber: BIA 2015)

No	Aplikasi Bisnis	Fungsi Bisnis User	Proses Bisnis	Lokasi Penyimpanan	RPO	RPO Maks
1	LIMS	RPO	Perencanaan Proses Pengolahan	Data Center	1 hari	< 1 jam
		Production II	Pengolahan dan Produksi BBM dan Non-BBM	Data Center	< 1 jam	
		Engineering Development	Evaluasi dan Rekomendasi Teknologi	Data Center	1 hari	
2	MySAP	All	All	Kantor Pusat	< 1 jam	< 1 Jam
3	P2P	All	Perencanaan Proses Pengolahan	Kantor Pusat	< 1 jam	< 1 Jam

No	Aplikasi Bisnis	Fungsi Bisnis User	Proses Bisnis	Lokasi Penyimpanan	RPO	RPO Maks
			Distribusi Produk BBM, NBBM dan Petrokimia	Kantor Pusat	< 1 jam	
4	MMHM (Material Master Hydro Movement)	Marine	Perencanaan Proses Pengolahan	Kantor Pusat	1 hari	1 hari
			Distribusi Produk BBM, NBBM, dan Petrokimia	Kantor Pusat	1 hari	
5	Monitoring Data Purchasing	Procurement	Perencanaan Proses Pengolahan	Data Center	4 jam	4 jam
			Pengelolaan Kontrak Pengadaan Barang	Data Center	4 jam	
			Pengadaan Bahan Baku Non Hydro	Data Center	4 jam	
6	ROAS	Production 1	Distribusi Produk BBM, NBBM, dan Petrokimia	Data Center	< 1 jam	< 1 jam
		OPI	Pengawasan dan Pengembangan Lintas Fungsi	Kantor Pusat	< 1 jam	
		RPO	Perencanaan Proses Pengolahan	Data Center	< 1 jam	
		FInance	Pencatatan Transaksi Keuangan Arus Minyak	Data Center	< 1 jam	
7	Material Catalog	Procurement	Perencanaan Proses Pengolahan	Data Center	1 hari	1 hari
			Pengadaan Bahan Baku Non Hydro	Data Center	1 hari	
8	Web Reliability	Reliability	Pembuatan Program Maintenance Kilang	Data Center	1 bulan	1 bulan
9	Web MPS	ME	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	7 hari	< 1 Jam
		MPS	Pembuatan Program Maintenance Kilang	Data Center	< 1 jam	
10	Engineering Drawing	ME	Pemeliharaan dan Pengendalian Peralatan Kilang	Data Center	7 hari	1 hari
		Eng&Dev	Pengembangan Teknologi	Data Center	1 hari	

6.2.1.2 Rekomendasi Strategi Mitigasi dan Penanggulangan Layanan Aplikasi Minimum

Rekomendasi strategi mitigasi dan penanggulangan layanan aplikasi minimum mengacu pada matriks rekomendasi penanganan bencana di IT RU IV. Matriks ini akan menjadi acuan dalam menentukan strategi pencangan dan pemulihan minimum masing-masing aplikasi dengan mempertimbangkan nilai RTO dan RPO masing-masing aplikasi.

Contoh cara penentuan strategi pencadangan dan pemulihan adalah sebagai berikut: Jika suatu layanan x memiliki nilai RTO dalam kategori *high* dan memiliki nilai RPO < 1 jam, menurut matriks rekomendasi penanganan bencana di IT RU IV, rekomendasi strategi pencadangan minimum untuk aplikasi tersebut adalah *mirroring*. Sedangkan strategi pemulihan untuk aplikasi tersebut adalah dengan menggunakan metode *electronic vaulting (active-active)*

Tabel 6.23 Matriks Rekomendasi Strategi Pencadangan dan Pemulihan (Sumber: Pertamina RU IV)

		RTO (Recovery Time Objective)		
		High	Medium	Low
RPO (Recovery Point Objective)	< 1 Jam	*Electronic Vaulting (Active - Active)*	*Electronic Vaulting (Active - Standby)*	*Offsite Vaulting*
		Mirroring	Incremental Backup – Scheduled	Normal Backup – Daily
	1 - 24 Jam	*Electronic Vaulting (Active – Active)*	*Electronic Vaulting (Active - Standby)*	*Offsite Vaulting*
		Incremental Backup – Scheduled	Incremental Backup - Scheduled	Normal Backup – Daily
	> 24 Jam	*Electronic Vaulting (Active – Active)*	*Electronic Vaulting (Active - Standby)*	*Offsite Vaulting*
		Normal Backup – Daily	Normal Backup - Daily	Normal Backup – Daily

Dibawah ini merupakan **contoh** daftar rekomendasi startegi pencadangan dan pemulihan layanan IT berdasarkan hasil kesimpulan RTO dan RPO dengan mengacu pada matriks

rekomendasi strategi pemulihan. Untuk daftar selengkapnya bisa dilihat pada **buku produk** pada **bab 11.2.1.2 Rekomendasi Strategi Mitigasi dan Penanggulangan Layanan Aplikasi Minimum.**

Tabel 6.24 Rekomendasi Strategi Mitigasi dan Penanggulangan Layanan Aplikasi Minimum (Sumber: Peneliti)

No	Aplikasi Bisnis	Proses Bisnis	RTO Level	RPO Maks	Strategi Pencadangan	Strategi Pemulihan
1	LIMS	Perencanaan Proses Pengolahan Pengolahan dan Produksi BBM dan Non-BBM Evaluasi dan Rekomendasi Teknologi	High	< 1 jam	Mirroring	Electronic Vaulting (Active-Active)
2	MySAP	All	High	< 1 Jam	Dilakukan tim DCOC Kantor Pusat	Dilakukan tim DCOC Kantor Pusat
3	P2P	Perencanaan Proses Pengolahan Distribusi Produk BBM, NBBM dan Petrokimia	High	< 1 Jam	Dilakukan tim DCOC Kantor Pusat	Dilakukan tim DCOC Kantor Pusat
4	MMHM (Material Master Hydro Movement)	Perencanaan Proses Pengolahan Distribusi Produk BBM, NBBM, dan Petrokimia	High	1 hari	Dilakukan tim DCOC Kantor Pusat	Dilakukan tim DCOC Kantor Pusat
5	Monitoring Data Purchasing	Perencanaan Proses Pengolahan Pengelolaan Kontrak Pengadaan Barang Pengadaan Bahan Baku Non Hydro	High	4 jam	Incremental Backup - Scheduled	Electronic Vaulting (Active-Active)
6	ROAS	Distribusi Produk BBM, NBBM, dan Petrokimia Pengawasan dan Pengembangan Lintas Fungsi Perencanaan Proses Pengolahan	High	< 1 jam	Mirroring	Electronic Vaulting (Active-Active)

No	Aplikasi Bisnis	Proses Bisnis	RTO Level	RPO Maks	Strategi Pencadangan	Strategi Pemulihan
		Pencatatan Transaksi Keuangan Arus Minyak				
7	Material Catalog	Perencanaan Proses Pengolahan	High	1 hari	Incremental Backup - Scheduled	Electronic Vaulting (Active-Active)
		Pengadaan Bahan Baku Non Hydro				
8	Web Reliability	Pembuatan Program Maintenance Kilang	Low	1 bulan	Normal Backup - Daily	Offsite Vaulting
9	Web MPS	Pemeliharaan dan Pengendalian Peralatan Kilang	Low	< 1 Jam	Normal Backup - Daily	Offsite Vaulting
		Pembuatan Program Maintenance Kilang				
10	Engineering Drawing	Pemeliharaan dan Pengendalian Peralatan Kilang	Medium	1 hari	Incremental Backup - Scheduled	Electronic Valuting (Active-Standby)
		Pengembangan Teknologi				

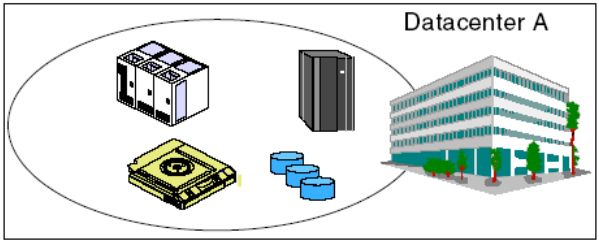
Berikut ini akan dijelaskan masing-masing opsi pencadangan yang terdapat pada tugas akhir ini:

1. ***Daily Backup***
   Daily backup berarti menyalin semua file yang dipilih yang telah dimodifikasi pada hari yang sama dengan jadwal backup. File-file yang telah di-backup tidak ditandai (dengan kata lain, atribut arsip tidak dihapus).
2. ***Incremental Backup***
   Incremental backup hanya mencadangkan file yang telah dibuat atau berubah sejak backup terakhir. Tipe backup ini akan menandai file yang telah di-backup (dengan kata lain, atribut arsip dihapus).
3. ***Normal Backup***
   Normal backup mencadangkan semua file yang dipilih dan menandai setiap file yang telah di-backup (dengan

kata lain, atribut arsip dihapus). Dengan menggunakan metode ini kita hanya perlu salinan terbaru dari file cadangan atau tape untuk mengembalikan semua file. Biasanya metode ini digunakan saat pertama kali membuat satu set backup.

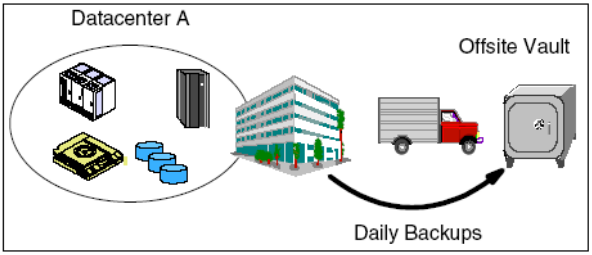
Sedangkan untuk strategi pemulihan terdapat beberapa opsi, yang akan dijelaskan sebagai berikut:

1. **Tier 0 – *Do nothing, no offsite data***
   Pada strategi pencadangan ini tidak ada perlakuan khusus dan tidak ada pencadangan di off-site area. Digunakan untuk layanan TI pada proses bisnis yang tidak kritikal.



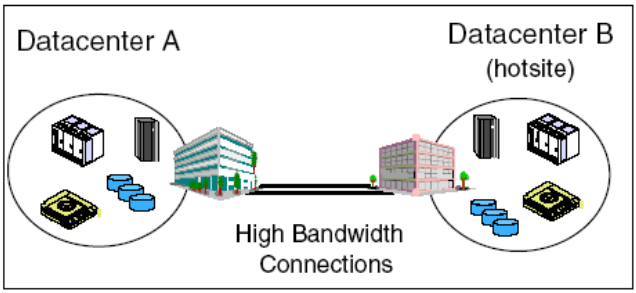
Gambar 6.1 Tier 0 - *No Offsite Data* (Sumber: Pertamina)

2. **Tier 1 – *Offsite Vaulting***
   Menggunakan strategi pencadangan yang diletakkan di luar area operasional (misalnya di luar kota). Metode ini cocok digunakan untuk layanan IT yang digunakan di proses bisnis yang butuh pencadangan namun tidak harus segera.



Gambar 6.2 Tier 1 - *Offsite Vaulting* (Sumber: Pertamina)

3. **Tier 2 – *Electronic Vaulting***
   Menggunakan strategi pencadangan dengan perangkat cadangan di lokasi lain. Metode ini cocok untuk layanan IT yang digunakan di proses bisnis yang butuh pencadangan dan ketika *downtime* harus segera aktif kembali.



Gambar 6.3 Tier 2 - *Electronic Vaulting* (Sumber: Pertamina)

Tingkat ini meliputi kemampuan untuk fasilitas *offsite*, rencana pemulihan, *electronic vaulting*, pusat data kedua. Pada tingkat ini data yang dicadangkan selalu dalam keadaan terkini. Kedua lokasi, antara lokasi utama dan *mirrorsite* melakukan sinkronisasi data cadangan dengan menggunakan koneksi *high bandwidth*.

Electronic Vaulting ini terbagi menjadi 2 jenis, antara lain:

a. Active-Standby

Metode ini berarti perangkat terdapat di 2 lokasi, namun apabila terjadi bencana aktivasinya harus secara manual.

b. Active-Active
Metode ini berarti perangkat terdapat di 2 lokasi dan aktif, apabila terjadi bencana secara otomatis failover ke server backup.

LAMPIRAN A

Lampiran dokumen konfirmasi kesesuaian hasil analisis risiko PT. Pertamina RU IV.

SURAT KONFIRMASI
Kesesuaian Hasil Analisis Risiko untuk PT. Pertamina RU IV

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama : Ulvi Rahma Isnaini
NRP : 5212100017
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

Dengan ini menyatakan permohonan konfrimasi atas kesesuaian hasil analisis risiko TI untuk PT. Pertamina RU IV. Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis risiko TI yang dibuat secara khusus, sesuai dengan kebutuhan dalam pembuatan dokumen BCP untuk PT. Pertamina RU IV.

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

PERSETUJUAN KONFIRMASI
Cilacap, 13 Juni 2016

Mengetahui,

Dito Anggodo Prihastomo, S.T.

Peneliti,

Ulvi Rahma Isnaini

Halaman ini sengaja dikosongkan

LAMPIRAN B

Lampiran dokumen konfirmasi kesesuaian dokumen BCP PT. Pertamina RU IV.

SURAT KONFIRMASI
Kesesuaian Dokumen *Business Continuity Plan* (BCP)
untuk PT. Pertamina RU IV

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama	: Ulvi Rahma Isnaini
NRP	: 5212100017
Pekerjaan	: Mahasiswa Sistem Informasi Institut Teknologi Sepuluh Nopember

Dengan ini menyatakan permohonan konfrimasi atas kesesuaian dokumen *business continuity plan* (BCP) PT. Pertamina RU IV. Konfirmasi ini dilakukan sebagai langkah untuk melakukan validasi bahwa dokumen *business continuity plan* (BCP) yang dibuat dapat diterima oleh perusahaan.

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

PERSETUJUAN KONFIRMASI
Cilacap, 13 Juni 2016

Mengetahui,	Peneliti,
Dito Anggodo Prihastomo, S.T.	Ulvi Rahma Isnaini

Halaman ini sengaja dikosongkan

LAMPIRAN C

Lampiran Interview Protokol Analisis Risiko

Informasi Narasumber	
Narasumber	Dito Anggodo Prihastomo
Jabatan	Assistant Data Center Operation and Automation
Tanggal	17 Februari 2016
Lokasi	Head Office PT. Pertamina RU IV
Topik	Identifikasi aset TI, identifikasi risiko TI apa saja yang mungkin terjadi, kebutuhan keamanan, dan kontrol keamanan TI apa yang telah diterapkan.

Kategori Pertanyaan	**No**	**Pertanyaan**	**Jawaban**
Tujuan : Untuk mengetahui kondisi umum fungsi IT di PT. Pertamina RU IV			
Kondisi Umum Fungsi TI	1	Bagaimana pembagian umum untuk fungsi TI?	Fungsi TI di Pertamina RU IV merupakan fungsi CSS (*corporate shared service)*, dimana artinya, divisi TI mendapat perintah langsung dari Pertamina pusat. Jadi untuk instruksi dan pertanggungjawabannya langsung ke Pertamina pusat yang ada di Jakarta.
	2	Fungsi TI dibagi menjadi berapa sub-fungsi?	Ada 3 pembagian dari fungsi TI, antara lain IT RU IV yang berada di head office, Business Operation and Technology dan Business Support and Infrastructure
	3	Apa sub-divisi tempat Bapak serta apa tupoksinya?	Saya ada pada sub-divisi IT RU IV. Disini saya bertanggung jawab untuk

			operasional data center, serta pengembangan aplikasi. Jadi secara garis besar tupoksi saya adalah mengurus operasional data center (maintenance, backup, restore), juga bertanggung jawab untuk pengembangan aplikasi baik yang digunakan untuk internal maupun eksternal. Untuk masalah pengembangan aplikasi kami dibantu oleh tenaga outsource programmer. Ohya, dalam sub-divisi ini juga terdapat held desk yang membantu user ketika mengalami gangguan. Seperti contohnya, gagal login aplikasi, email tidak bisa dibuka, dsb.
Tujuan: Untuk menggali informasi terkait aset kritis teknologi dan sistem informasi yang diterapkan perusahaan.			
Aset TI	1	Bagaimana proses umum penerapan teknologi informasi di organisasi?	Proses teknologi informasi pada Pertamina bisa dikatakan sudah menyeluruh. Hampir seluruh proses bisnis dalam perusahaan ini sudah terdapat campur tangan TI walaupun mungkin terdapat beberapa proses bisnis yang menggunakan TI hanya sebagai supporting (bukan yang utama)
	2	Apa saja fungsional organisasi yang	Seperti yang saya bilang sebelumnya, hampir seluruh

		mendukung penggunaan teknologi dan sistem informasi?	fungsi bisnis di Pertamina sudah menerapkan TI untuk mendukung berjalannya proses bisnis dalam fungsi mereka. Namun yang bergantung tinggi pada availabilitas TI adalah proses bisnis utama yang ada di Pertamina, seperti yang tercantum dalam dokumen BIA itu.
	3	Aset TI apa saja yang digunakan dalam proses bisnis kritikal tersebut?	Secara garis besar yang mereka (fungsi bisnis kritikal) gunakan adalah layanan TI yang berupa aplikasi dan komunikasi. Contoh aplikasi yang digunakan untuk proses pengolahan adalah GLS/SAMK, Tank Vision, LIMS, PIMS, mySAP, e-Corr dsb. Untuk layanan komunikasi yang digunakan adalah HT, telfon, atau kadang e-confrence jika berhubungan dengan pihak luar. Untuk masalah hardware yang sering mereka gunakan standard ya, PC, laptop dsb. Untuk lebih jelasnya bisa dilihat pada dokumen BIA atau kuisioner BIA yang dulu itu, *vi*.
	4	Aset teknologi kritis apa sajakah yang dapat memberikan ancaman pada proses bisnis kritikal?	Aset teknologi kritis antara lain server, komunikasi jaringan, ketersediaan aplikasi, karena user sering kali mengeluhkan terkait

			akses jaringan yang lambat ataupun aplikasi yang berjalan lambat, nah hal ini dikarenakan aplikasi tersebut sebagian besar bergantung pada koneksi jaringan. Jadi ya.. sebenernya semuanya terhubung dan poin utamanya adalah di jaringan.
	5	Komponen vital pendukung apa saja yang termasuk aset TI	Untuk Pertamina sendiri dibagi menjadi software, hardware, jaringan, data/information, people dan intagible. Yang masuk dalam komponen intagible adalah citra perusahaan, kepercayaan user, dsb
Tujuan: Untuk menggali informasi mengenai identifikasi ancaman, kerentanan, dan risiko aset teknologi dan informasi			
Risiko TI	1	Menurut Bapak, risiko TI apa saja yang mungkin terjadi?	Kalo menurut pada bidang yang aku pegang, di head office sini belum ada cable management yang baik. Seperti yang bisa dilihat, kabel disini berserakan di lantai dan belum diatur dengan standar-standar kabel yang baik. Padahal kalo sampe konsleting kan bahaya, dekat dengan kilang sehingga bisa memicu kebakaran yang lebih besar
	2	Jika terkait server gitu apa nggak ada risikonya Pak?	Tentu saja ada, hanya saja proses pengamanan untuk server disini sudah cukup baik. Pertamina baru saja

			menggunakan teknologi virtual server sehingga kemungkinan untuk server down bisa diminimalisir
	3	Wah bagus ya Pak jika pengamanan servernya sudah terjamin. Berarti untuk proses backup dan restore juga sudah diterapkan Pak?	Sudah diterapkan dari dulu. Data yang tersimpan dalam server di backup sehari sekali tiap tengah malam sehingga tidak mengganggu operasional kantor pada jam kerja. Dan hal ini sudah dilakukan secara teratur.
Tujuan: Untuk menggali informasi terkait praktik keamanan yang telah diterapkan serta kelemahan perusahaan.			
Kontrol Keamanan yang Diterapkan	1	Musuh utama untuk unit kilang kan api ya Pak, untuk mengantisipasinya apa yang sudah dilakukan?	Wah iya benar sekali. Api merupakan musuh utama dalam unit pengolahan. Untuk mengantisipasi, hal yang dilakukan adalah dengan memasang alat pemadam di hampir seluruh sudut kantor, juga Pertamina RU IV memiliki pemadam kebakaran sendiri jika tiba-tiba terjadi kebakaran yang lebih besar. Selain itu untuk masuk ke kilang sendiri kan tiap orang tidak boleh membawa handphone atau sejenisnya, dan ini benar-benar diperiksa oleh petugas keamanan kami.
	2	Apakah terdapat SOP terkait keamanan teknologi informasi?	Sudah ada SOP terkait proses TI dan juga keamanan TI namun belum mencakup semuanya

			sehingga masih tergolong general.
	3	Apa saja kelemahan teknis untuk aset TI yang ada pada organisasi?	Kelemahan teknis yang dimiliki oleh organisasi antara lain adalah belum adanya prosedur teknis dan detail untuk keamanan proses TI.

LAMPIRAN D

Lampiran Interview Protokol Analisis Risiko

Informasi Narasumber	
Narasumber	Satrio Wahyu Pratomo
Jabatan	Junior Assistant Computer Development and Creative Technology
Tanggal	18 Februari 2016
Lokasi	Head Office PT. Pertamina RU IV
Topik	Identifikasi risiko TI

Kategori Pertanyaan	**No**	**Pertanyaan**	**Jawaban**
Tujuan: Untuk menggali informasi terkait kondisi umum sub fungsi Business Operation and Technology			
Kondisi Umum Organisasi	1	Apa sub-divisi tempat Bapak serta apa tupoksinya?	Saya ada pada sub-divisi Business Operation and Technology. Disini tugas pokok fungsi saya meliputi pengelolan aset TI dan bantuan dalam menangani permasalahan operasional TI. Dalam sub divisi ini terdapat beberapa karyawan outsource yang secara spesifik ditugaskan untuk menangani atau membantu user ketika terjadi permasalahan. Sebagai contohnya ketika tinta printer habis, atau bantuan lain terkait operasional TI maka kami siap membantu.
Tujuan: Untuk menggali informasi mengenai identifikasi ancaman, kerentanan, dan risiko aset teknologi dan informasi			

Risiko TI	1	Menurut Bapak, risiko TI apa saja yang mungkin terjadi pada divisi Bapak?	Kalo menurut pada bidang yang aku pegang, ada beberapa risiko potensial yang remeh namun sering terjadi ya, diantaranya: – Permasalahan lisence. Karena kantor ini gak hanya diisi orang TI yang ngerti pentingnya lisence ya, jadi ada sebagian orang yang suka nginstall aplikasi yang nggak resmi ke PC kantor, nah tentu saja hal ini merugikan perusahaan ya. – Masalah akses data. disini kan seluruh pegawai punya email pertamina. Nah, mereka yang punya email itu secara nggak langsung punya akses buat ngubah data ke database. Ini sebenernya gak aman ya, karena kan jadi membuka celah buat modifikasi data dsb kan – Virus. Nah hal ini kayanya kelihatan sepele banget tapi ini pernah ngerepotin kita. Pernah suatu waktu itu ke infeksi sampe mindahin seluruh data laptop – Yang ini masalah data. kan sering terjadi

			perpindahan hardware dari sini ke sini, nah satu hal yang sering kelupaan adalah memusnahkan data pada device lama yang ditinggalkan. Hal ini kelihatan sepele namun bisa jadi besar kalo data tersebut disalahgunakan oleh pihak yang gak bertanggung jawab.
	2	Wah banyak juga ya Pak, selain hal yang telah disebutkan apa terdapat risiko yang lain?	Tentu saja ada, contohnya seperti laptop disini sering hilang. Serius lho, laptop kantor disini sering hilang. Selain itu mungkin risiko-risiko kecil sih, kaya contohnya sparepart printer yang sering rusak, tinta. Kalo dari scanner mungkin roll up nya yang sering rusak, LCD, headphone gitu sering rusak.
	3	Jika terjadi kerusakan gitu tindakan yang dilakukan orang TI seperti apa Pak?	Ya kalo terjadi kerusakan gitu biasanya laporan sama kita, dan kita langsung ngirim orang ke divisi tersebut. Lalu dilihat kerusakannya, kalo bisa diperbaiki langsung ya langsung diperbaiki, kalo sparepartnya rusak ya langsung dicari sparepart cadangan. Alhamdulilah di TI sendiri cadangan sparepart sudah mencukupi ya, jadi kalo ada kerusakan gitu cepet penanganannya.

Halaman ini sengaja dikosongkan

LAMPIRAN E

Lampiran Interview Protokol Analisis Risiko

Informasi Narasumber	
Narasumber	Indri Setyowati
Jabatan	Assisstant Fixed and Mobile Communication
Tanggal	19 Februari 2016
Lokasi	Gedung Telekomunikasi dan Jaringan PT. Pertamina RU IV
Topik	Risiko TI

Kategori Pertanyaan	**No**	**Pertanyaan**	**Jawaban**
Tujuan: Untuk menggali informasi terkait kondisi umum sub-fungsi Business Support and Infrastructure			
Konisi Umum Sub-Fungsi	1	Apa sub-fungsi tempat Ibu serta apa tupoksinya?	Saya ada pada sub-fungsi Business Support and Infrastructure. Disini fokus pekerjaan kami lebih kepada jaringan dan komunikasi. Kami memiliki pemancar dan repeater yang digunakan untuk keberlangsungan operasional HT. selain itu juga terdapat beberapa operator telpon yang secara spesifik membantu menghubungan user yang ingin berbicara dengan fungsi lain ketika mereka tidak mengetahui nomor telfon fungsi tersebut. Tidak hanya jaringan yang ada dalam kantor, namun kami juga bertanggung jawab

			untuk jaringan yang ada dalam kilang sehingga sebagian besar memang kami bekerja di lapangan, bukan dalam kantor.
Tujuan: Untuk menggali informasi mengenai identifikasi ancaman, kerentanan, dan risiko aset teknologi dan informasi			
Risiko TI	1	Menurut Ibu, risiko TI apa saja yang mungkin terjadi pada divisi Ibu?	Kalo menurut pada divisi saya, sebenarnya tidak banyak risiko TI yang akan mempengaruhi proses bisnis kritikal ya, karena pada divisi telekomunikasi tidak berhubungan langsung dengan aplikasi atau server untuk penyimpanan data. Beberapa risiko yang mungkin terjadi paling-paling hanya proses manajemen aset yang belum dilakukan secara maksimal sih. Jadi misal terjadi kerusakan atau tracking kehilangan aset itu susah dilakukan, ya karena gimana mau tracking, orang data asetnya apa aja itu gak update. Kalo masalah virus atau pengubahan data gitu bisa dibilang jarang terjadi ya, ya karena memang fokus bidang divisi ini tidak ke arah situ.
	2	Oh begitu ya Bu, selain hal yang telah disebutkan apa terdapat risiko yang lain?	Oh iya ada, yaitu layanan radio atau HT. disini karena daerah kilang, jadi orang yang mau masuk ke kilang tidak boleh membawa HP,

			jadi komunikasi utama yang digunakan ya HT itu. HT selain digunakan pada kilang, juga digunakan untuk operasional kantor. Keberadaan HT memang dilengkapi dengan adanya telfon, intercom, dsb. namun keberadaaan HT tidak bisa disampingkan. Ya.. bisa dibilang ini merupakan aset TI penting dalam menunjang proses operasional kilang dan berpengaruh besar pada keberlangsungan proses bisnis kritikal menurut saya.
	3	Jika terjadi kerusakan gitu tindakan yang dilakukan orang TI seperti apa Bu?	Ya kalo terjadi kerusakan gitu biasanya laporan sama kita, dan kita langsung ngirim orang ke divisi tersebut. Lalu dilihat kerusakannya, kalo bisa diperbaiki langsung ya langsung diperbaiki, kalo sparepartnya rusak ya langsung dicari sparepart cadangan. Alhamdulilah di TI sendiri cadangan sparepart sudah mencukupi ya, jadi kalo ada kerusakan gitu cepet penanganannya.

Halaman ini sengaja dikosongkan

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini akan merangkum hasil akhir dari pembuatan tugas akhir menjadi sebuah kesimpulan dan dilengkapi dengan saran untuk perbaikan ataupun saran untuk penelitian selanjutnya.

7.1 Kesimpulan

1. Penelitian ini telah menghasilkan elemen dokumen BCP PT. Pertamina RU IV yang mengacu pada ISO 22301, ISO 27031, dan penelitian Kartini Slamet, yang terdiri dari:
   - Halaman kontrol dokumen
   - Tujuan
   - Ruang lingkup
   - Pembagian peran dan tanggung jawab
   - Daftar kontak
   - Call tree BCP
   - Aktivasi rencana
   - Analisis dampak bisnis
   - Analisis risiko
   - Strategi BCP dan DRP
2. Penelitian ini telah menghasilkan analisis risiko beserta penilaiannya untuk risiko teknologi informasi pada proses bisnis kritikal (memiliki dampak OPS/FIN>3) pada PT. Pertamina RU IV sesuai dengan ISO 31000 dan FMEA. Dari hasil analisis tersebut, didapatkan kesimpulan sebagai berikut:
   - Terdapat satu risiko dengan level *very high* pada semua proses bisnis kritikal yaitu **lambatnya akses jaringan** yang dikarenakan oleh faktor topologi jaringan dan ukuran bandwith.
   - Terdapat tiga risiko dengan level *high* yaitu risiko pertama, **kerusakan fisik kabel LAN dan WAN** yang berdampak pada semua proses bisnis kritikal. Risiko kedua adalah **informasi rahasia tersebar**

luas yang berdampak pada proses bisnis pengolahan dan produksi BBM, non-BBM dan Petrokimia, distribusi produk BBM, non-BBM dan Petrokimia, serta pemeliharaan dan pengendalian peralatan kilang. Risiko ketiga adalah **kegagalan aplikasi** yang berdampak pada proses bisnis pengolahan dan produksi BBM, non-BBM dan Petrokimia, distribusi produk BBM, non-BBM dan Petrokimia, serta pemeliharaan dan pengendalian peralatan kilang.

3. Dari hasil penyusunan strategi BCP menunjukkan bahwa IT RU IV perlu mengimplementasikan beberapa strategi untuk mendukung keberlanjutan proses bisnis kritikal di PT. Pertamina RU IV yang meliputi strategi pencegahan *(prevention)* yang diwujudkan dalam bentuk mitigasi risiko, strategi tanggapan *(response)*, strategi pemulihan *(recovery)*, dan strategi DRP.

7.2 Saran

Adapun saran yang dapat disampaikan untuk penelitian selanjutnya adalah melanjutkan strategi yang disampaikan dalam penelitian ini hingga pada tahap pembuatan prosedur, kebijakan, hingga simulasi sehingga dokumen BCP yang dibuat benar-benar dapat diimplementasikan untuk menjaga keberlangsungan bisnis di PT. Pertamina Refinery Unit IV.

DAFTAR PUSTAKA

[1] Pertamina, "Pertamina Company Profile," Pertamina, 2012. [Online]. Available: http://www.pertamina.com/company-profile/visi-dan-misi/. [Accessed 6 01 2015].

[2] I. R. IV, Business Impact Analysis, Cilacap: Pertamina, 2015.

[3] S. Snedaker, in *Business Continuity and Disaster Recovery for IT Professional*, USA, Elsevier, 2014.

[4] Sidorova, 2008.

[5] M. Niemimaa and J. Jarvelainen, "IT Service Continuity : Achieving Embeddedness Through Planning," International Conference on Availability, Reliability and Security, Findland, 2013.

[6] G. Prastisukma, Kerangka Kerja BCP di PDAM Surabaya, Surabaya: Jurusan Sistem Informasi, 2015.

[7] ISO, "ISO 22301:2012," USA, 2012.

[8] W. Heins, "A Study of Corporate Risk," 2011.

[9] PMBOK, 2013. [Online]. Available: https://www.pmiwdc.org/sites/default/files/presentations/201310/PMIW_LocalCommunity_WashingtonCircle_PresentationSlides_2013-09.pdf. [Accessed 06 12 2015].

[10] B.-C. Bjork, "Information Technology in Construction : Domain Definition and Research Issues," *International Journal of Computer Integrated Design and Construction, SETO, London*, vol. 1, pp. 1-16, 1999.

[11] J. O. George Marakas, Introduction to Information Systems 15th Edition, New York: McGraw-Hill/Irwin, 2010.

[12] ISO, "ISO 31000:2009," *Risk Management-Principles and Guidelines*, 2009.

[13] A. Alisia, in *Kerangka BCP untuk Bank Surya Yudha Banjarnegara*, Surabaya, Jurusan Sistem Informasi, 2014.

[14] ISACA, "ISACA Glossary," 2012. [Online]. Available: http://www.isaca.org/Pages/Glossary.aspx?tid=1536&char=I. [Accessed 6 12 2015].

[15] ISO, "ISO 31000 Risk Management-Principles and Guidelines," ISO, 2009.

[16] Gygi, DeCarlo and Williams, 2005.

[17] I. R. I. Pertamina, "Draft Business Impact Analysis," RU IV, Cilacap, 2015.

[18] Pertamina, "Business Impact Analysis 2014," Pertamina, Cilacap, 2014.

[19] ISO, "ISO 22301:2012," Switzerland, ISO, 2012.

[20] P. R. G. Ltd., "Plain English ISO 22301:2012 : Business Continuity Definitions," 23 06 2014. [Online]. Available: http://www.praxiom.com/iso-22301-definitions.htm#3.5_Business_continuity_management_system_(BCMS). [Accessed 13 11 2015].

[21] ISO, "ISO 22301," USA, 2012.

[22] L. S. d. Souza, "BCP Guide," 29 12 2011. [Online]. Available: https://id.scribd.com/doc/76709264/BCP-Guide#scribd. [Accessed 09 03 2016].

[23] S. H. C. Wan, "Adoption of Business Continuity Planning Processes in IT Service Management," p. 1, 2008.

[24] F. Zhao, "Governments Business Continuity Plan for Records in the Electronic Age," p. 1, 2010.

[25] U. Solihudin, R. M.Samik-Ibrahim, J. Moningka and A. M. Wibowo, "Business Continuity and Disaster Recovery Plan," in *Proteksi dan Teknik Keamanan Sistem Informasi*, Jakarta, Magister Teknologi Informasi Universitas Indonesia, 2005, p. 5.

[26] Wiboonrat, An Empirical IT Contigency Planning Model for Disaster Recovery Strategy Selection, Bangkok, Thailand: IEEE, 2008.

[27] Naseer, Modiri and Ghorbani, The Requirement Needs and Impact of Business Continuity Plan on Security Strategies, Iran: IEEE, 2010.

[28] Caroline, "DRP Share Issue and Underwriting," 24 11 2008. [Online]. Available: http://www.asx.com.au/asxpdf/20080514/pdf/3193yyp21yznjz.pdf. [Accessed 06 12 2015].

[29] Pertamina, "Disaster Recovery Plan 2014," Pertamina, Cilacap, 2014.

[30] ISO, "ISO/IEC 27031 Business Continuity in ICT," ISO, 2011.

[31] K. Slamet, "Pembentukan Kerangka Kerja Business Continuity Plan pada Bank Ritel X," 2004.

[32] ISO, "ISO/IEC 27002 Information Security Management Systems," ISO, 2005.

[33] "Cisco System," Wikipedia, 2014. [Online]. Available: https://id.wikipedia.org/wiki/Cisco_Systems. [Accessed 20 05 2016].

[34] Cisco, "Design Best Practices for Latency Optimization," 2015. [Online]. [Accessed 30 05 2016].

[35] "Microsoft Indonesia," Wikipedia, 20 03 2016. [Online]. Available: https://id.wikipedia.org/wiki/Microsoft. [Accessed 05 07 2016].

[36] Microsoft, "Availability Overview," Microsoft, 2015. [Online]. Available: https://msdn.microsoft.com/en-us/library/aa291543(v=vs.71).aspx. [Accessed 13 06 2016].

[37] Y. K. Robert, Case Study Research: Design and Method (Applied Social Reseacrh Methods), 2009.

[38] E. 152A, "Propagation Delay, Circuit Timing & Adder Design," 2012. [Online]. Available: http://www.ece.ucsb.edu/Faculty/Johnson/ECE152A/L4%20-%20Propagation%20Delay,%20Circuit%20Timing%20&%20Adder%20Design.pdf. [Accessed 10 07 2016].

[39] Cisco, "Low Latency Queueing," Cisco, [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fslllq26.html. [Accessed 10 07 2016].

[40] Cisco, "IACS Network Security and the Demilitarized Zone," 2015. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter6.pdf. [Accessed 10 07 2016].

[41] Aboba, "The Network Access Identifier," 2005. [Online]. Available: https://www.ietf.org/rfc/rfc4282.txt. [Accessed 10 07 2016].

[42] U. Gunadarma, "Clustering," 2015. [Online]. Available: https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiY34ysnejNAhVGt48KHQeiCrkQFggaMAA&url=http%3A%2F%2Famutiara.staff.gunadarma.ac.id%2FDownloads%2Ffiles%2F267%2FClustering.pdf&usg=AFQjCNFkvyb9GPXjvvqrJ567IiLOLIXxXA. [Accessed 10 07 2016].

[43] C. H. Indonesia, "Mengenal Tipe Load Balancing beserta Perbandingannya," Cloud Hosting Indonesia, 2015. [Online]. Available: https://idcloudhost.com/mengenal-tipe-load-balancing-beserta-perbandingannya/. [Accessed 09 07 2016].

[44] F. O. o. I. Security, BSI Standard 100-4, Germany: Godesberger , 2009.

BIODATA PENULIS

Penulis adalah mahasiswa S1 Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember Surabaya yang dilahirkan di Sidoarjo, 15 Januari 1994. Penulis menempuh pendidikan di SD Muhammadiyah 1 Taman, SMP Negeri 1 Taman, SMA Negeri 1 Sidoarjo, dan melanjutkan ke ITS dengan mengambil jurusan Sistem Informasi dengan fokus bidang manajemen sistem informasi. Selain aktif dalam bidang akademis dan pernah menjadi asisten dosen mata kuliah matematika diskrit, penulis juga aktif dalam organisasi kemahasiswaan, baik di dalam maupun di luar kampus. Beberapa organisasi pernah menjadi ladang untuk menimba ilmu dan pengalaman bagi penulis, antara lain adalah HMSI sebagai staff departemen riset dan teknologi (2013/2014), serta bendahara umum 1 (2014/2015), BEM Fakultas Teknologi Informasi ITS sebagai staff departemen sosial masyarakat (2013/2014), BEM ITS sebagai staff magang pada departemen media informasi, *volunteer* AISINDO *(Association for Information System Indonesia)* dari tahun 2013 hingga 2016. Penulis juga tercatat sebagai penerima beasiswa PPA (Peningkatan Prestasi Akademik) dari Direktorat Perguruan Tinggi pada 2 periode, serta beasiswa GenBI (generasi baru Bank Indonesia) dari Bank Indonesia. Penulis yang memiliki hobi mendaki gunung dan menggemari buku *self-help* ini juga pernah menjalani kerja praktek di PT. Pertamina Refinery Unit IV Cilacap dan pernah menjadi karyawan kontrak di Bank Indonesia Surabaya sebagai petugas entri data. Untuk keperluan akademik, penulis dapat dihubungi di ulvirahmaa@gmail.com