TUGAS AKHIR – KS 141501

PERANCANGAN BUSINESS CONTINUITY PLAN BERBASIS RISIKO PADA SUB DIREKTORAT PENGEMBANGAN SISTEM INFORMASI, DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI.

Caesar Fajriansah
NRP 5213 100 179

Dosen Pembimbing 1:
Dr. Apol Pribadi, S.T, M.T

Dosen Pembimbing 2:
Anisah Herdiyanti, S.Kom., M.Sc.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS 141501

DEVELOPING RISK BASED BUSINESS CONTINUITY PLAN ON SUB DIRECTORATE INFORMATION SYSTEM DEVELOPMENT, DIRECTORATE OF INFORMATION SYSTEMS AND TECHNOLOGY DEVELOPMENT

Caesar Fajriansah
NRP 5213100179

Supervisor 1 :
Dr. Apol Pribadi S.T, M.T

Supervisor 2 :
Anisah Herdiyanti, S.Kom., M.Sc.

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Institute of Technology Sepuluh Nopember
Surabaya 2017

LEMBAR PENGESAHAN

PERANCANGAN BUSINESS CONTINUITY PLAN BERBASIS RISIKO PADA SUB DIREKTORAT PENGEMBANGAN SISTEM INFORMASI, DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI.

TUGAS AKHIR

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

Oleh:

Caesar Fajriansah
5213 100 179

Surabaya, Januari 2017

KETUA
JURUSAN SISTEM INFORMASI

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

PERANCANGAN BUSINESS CONTINUITY PLAN BERBASIS RISIKO PADA SUB DIREKTORAT PENGEMBANGAN SISTEM INFORMASI, DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI.

TUGAS AKHIR

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

Oleh :

Caesar Fajriansah

5213 100 179

Disetujui Tim Penguji : Tanggal Ujian : 16 Januari 2017
Periode Wisuda: Maret 2017

Dr. Apol Pribadi, S.T, M.T **(Pembimbing 1)**

Anisah Herdiyanti, S.Kom., M.Sc. **(Pembimbing 2)**

Sholiq, S.T, M.Kom, MSA **(Penguji 1)**

Eko Wahyu Tyas, S.Kom., MBA **(Penguji 2)**

PERANCANGAN BUSINESS CONTINUITY PLAN BERBASIS RISIKO PADA SUB DIREKTORAT PENGEMBANGAN SISTEM INFORMASI, DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI.

Nama Mahasiswa : CAESAR FAJRIANSAH
NRP : 5213 100 179
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing 1: Dr. Apol Pribadi S.T, M.T
Dosen Pembimbing 2: Anisah Herdiyanti, S.Kom., M.Sc.

ABSTRAK

Setiap organisasi memiliki proses bisnis yang harus dijaga keberlangsungannya, untuk dapat menjaga kelangsungan bisnis dari gangguan yang disebabkan oleh risiko organisasi, diperlukan sebuah perencanaan yang berisikan prosedur dan strategi yang dapat mengurangi risiko tersebut. Penelitian ini bertujuan untuk menyusun sebuah kerangka Perencanaan Keberlangsungan Bisnis (Business Continuity Plan) yang sesuai dengan kebutuhan perusahaan terkait keberlanjutan bisnis untuk menjaga kelangsungan proses bisnis pada organisasi. Studi kasus pada penelitian ini adalah DPTSI, organisasi yang bergerak pada bidang pengembangan teknologi dan menggunakan teknologi informasi untuk mendukung jalannya operasional proses bisnis dan sebagai pendukung layanan teknologi informasi yang dimilikinya. Untuk dapat menjaga keberlangsungan bisnis pada suatu organisasi, dibutuhkan sebuah perencanaan yang dapat mengidentifikasikan risiko terjadinya bencana kemudian memberikan prosedur dan strategi untuk dapat mengurangi atau meminimalisir risiko tersebut. Perencanaan inilah yang disebut dengan Business Continuity Plan (BCP). Usulan Business Continuity Plan pada DPTSI difokuskan kepada kemampuan perusahaan untuk memitigasi resiko dan insiden

yang mungkin akan menimpa DPTSI dan juga untuk membantu mengambil tindakan saat terjadi ancaman dan bencana.

Direktorat Pengembangan Teknologi dan Sistem Informasi yang merupakan suatu organisasi yang bergerak dibidang pengembangan dan pusat layanan sistem informasi di ITS. DPTSI sebagai pusat pengembangan SI/TI di ITS memiliki tugas melaksanakan, mengkoordinasi, memonitor dan mengevaluasi kegiatan penelitian dan pengembangan teknologi dan sistem informasi. DPTSI menggunakan teknologi informasi untuk media utama untuk menjalankan operasional proses bisnis sekaligus mendukung layanan teknologi informasi yang dimilikinya.

Metode penelitian ini menggunakan BCP pendekatan berbasis risiko. Penyusunan kerangka dilakukan dengan melakukan formulasi antara kebutuhan dan tujuan perusahaan terkait keberlanjutan bisnis dalam melakukan formulasi kerangka kerja BCP serta melakukan analisis risiko serta analisis dampak bisnis. Formulasi kerangka kerja BCP dilakukan dengan melihat kebutuhan dan keinginan organisasi mengenai keberlangsungan bisnis dan menyeseuaikannya dengan standar kerangka kerja BCP yang digunakan sebagai acuan, yaitu ISO 22301:2012. Rancangan dokumen BCP dihasilkan dengan meninjau hasil penilaian risiko dan penilaian dampak bisnis yang disesuaikan dengan hasil formulasi kerangka kerja BCP. Sehingga nantinya didapatkan dokumen BCP yang sesuai dengan kebutuhan dan keinginan organisasi.

Kata Kunci*: risiko, business continuity plan, keberlangsungan bisnis, strategi keberlangsungan bisnis*

DEVELOPING RISK BASED BUSINESS CONTINUITY PLAN ON SUB DIRECTORATE INFORMATION SYSTEM DEVELOPMENT, DIRECTORATE OF INFORMATION SYSTEMS AND TECHNOLOGY DEVELOPMENT

Name	**: CAESAR FAJRIANSAH**
NRP	**: 5213 100 179**
Department	**: Information Systems FTIF -ITS**
Supervisor 1	**: Dr. Apol Pribadi S.T, M.T**
Supervisor 2	**: Anisah Herdiyanti, S.Kom., M.Sc.**

ABSTRACT

Every organization has a business process that must be maintained sustainably, in order to maintain business continuity of the distortion caused by the risk organization, needed a plan that contains procedures and strategies that can reduce the risk. This study aims to develop a framework of Business Continuity Planning (Business Continuity Plan) that fits the needs of companies related to the business continuity to keep the continuity of business processes in the organization. The case study in this research is DPTSI, an organization that focuses on the technology development and use of information technology to support business processes and operational activities to support its information technology services. To be able to maintain business continuity in an organization, needed a plan to identify the risks of a disaster then provide procedures and strategies to reduce or minimize the risk. Planning is called the Business Continuity Plan (BCP). Proposed Business Continuity Plan in DPTSI focused on the company's ability to mitigate risks and incidents that might befall DPTSI and also to help take action as it happens threats and disasters.

Direktorat Pengembangan Teknologi dan Sistem Informasi is an organization that is engaged in the development and service center information systems at ITS. DPTSI as a center for the development of the IS / IT in the ITS has a task to carry out,

coordinate, monitor and evaluate the activities of research and development of technology and information systems. DPTSI use of information technology for the mainstream media to run the operational business processes as well as support its information technology services.

This research method using BCP risk-based approach. The preparation of the framework done by the formulation of the needs and objectives related companies doing business sustainability in the formulation of the framework of the BCP and perform risk analysis and business impact analysis. BCP formulation frameworks is done by looking at the needs and desires of the organization's business continuity and menyeseuaikannya with BCP standard framework that is used as reference, namely ISO 22301: 2012. BCP draft document produced by reviewing the results of the risk assessment and business impact assessments were adjusted on the BCP formulation frameworks. So later BCP documents obtained in accordance with the needs and desires of the organization

Keywords: risk, business continuity plan, business continuity, business continuity strategy

KATA PENGANTAR

Syukur Alhamdulillah dipanjatkan oleh peneliti atas segala petunjuk, pertolongan, kasih sayang, dan kekuatan yang diberikan oleh Allah SWT. Hanya karena ridho-Nya, peneliti dapat menyelesaikan laporan Tugas Akhir, dengan judul **PERANCANGAN BUSINESS CONTINUITY PLAN BERBASIS RISIKO PADA SUB DIREKTORAT PENGEMBANGAN SISTEM INFORMASI, DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI.**

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

- Orang tua penulis yang senantiasa mendoakan dan mendukung, dan kakak yang selalu mendorong penulis untuk segera menyelesaikan tugas akhir ini.
- Ibu Anny Yuniarti, S.Kom., M.Comp.Sc selaku Ketua Sub Direktorat Pengembangan Sistem Informasi DPTSI ITS, Bapak Royyana M Ijtihadie, S.Kom.,M.Kom.,Ph.D Ketua Sub Direktorat Infrastruktur dan Keamanan Teknologi Informasi yang telah menjadi narasumber untuk kebutuhan penelitian mahasiswa.
- Bapak Dr. Apol Pribadi S.T, M.T dan Ibu Anisah Herdiyanti, S.Kom., M.Sc., selaku dosen pembimbing yang yang telah meluangkan waktu untuk membimbing dan mendukung dalam penyelesaian tugas akhir ini.
- Ibu Erma Suryani, S.T., M.T., Ph.D., selaku dosen wali yang senantiasa memberikan pengarahan selama penulis menempuh masa perkuliahan dan pengerjaan tugas akhir ini
- Pak Hermono, selaku admin laboratoriun MSI yang membantu penulis dalam hal administrasi penyelesaian tugas akhir.

- Teman – teman Lab MSI, Beltranis, All We Can Eat, yang telah memberikan semangat dalam menyelesaikan penelitian ini.
- Chitra Utami Putri, yang selalu memberikan dukungan dan masukan dari awal perkuliahan sampai dengan pengerjaan tugas akhir ini.
- Serta pihak lain yang telah mendukung dan membantu dalam kelancaran penyelesaian tugas akhir ini.

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

Surabaya, Januari 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

Bab ini menjelaskan beberapa hal mendasar pada penulisan tugas akhir ini. Hal –hal tersebut meliputi latar belakang, rumusan permasalahan, batasan masalah, tujuan, dan manfaat, sistematika penulisan dan relevansi dari tugas akhir.

1.1 Latar Belakang

Institut Teknologi Sepuluh Nopember merupakan salah satu Perguruan Tinggi Negeri yang telah lama berkecimpung dalam bidang teknologi informasi yang senantiasa mengedepankan layanan dalam memberikan kemudahan mendapatkan informasi terkait akademik yang diperlukan dengan menerapkan pemanfataan teknologi informasi berupa layanan sistem informasi online yang dikelola oleh Lembaga Pengembangan Teknologi Sistem Informasi (LPTSI) ITS [1]. LPTSI memiliki 3 jenis layanan, salah satu diantaranya adalah Sub Direktorat Pengembangan Sistem Informasi. Dimana peran dan fungsi dari Pusat Sub Direktorat Pengembangan Sistem Informasi ini adalah mengembangkan dan memaintain sistem informasi yang ada pada institut. Pengembangan sistem informasi tersebut tidak lepas dari permasalahan yang sering terjadi sehingga mengakibatkan terganggunya operasional proses bisnis.

Salah satu tantangan organisasi pendidikan adalah bagaimana dapat menghadapi ancaman, salah satunya bencana alam. Kondisi letak geografi Indonesia sangat berpotensi sekaligus rawan bencana seperti letusan gunung berapi, gempa bumi, tsunami, banjir dan tanah longsor. Data menunjukkan bahwa Indonesia merupakan salah satu negara yang memiliki tingkat kegempaan yang tinggi di dunia, lebih dari 10 kali lipat tingkat kegempaan di Amerika Serikat [2].

Saat suatu organisasi mulai mengimplementasikan teknologi informasi, maka pada saat itu juga suatu organisasi akan memiliki berbagai macam risiko yang timbul dari ancaman dan gangguan.

Oleh karena itu, perusahaan harus mulai melakukan manajemen risiko [3]. Manajemen risiko dapat membantu perusahaan untuk mengurangi atau meminimalisasi terjadinya risiko atau dampak dari risiko tersebut. Untuk dapat memiliki manajemen risiko yang baik, maka perusahaan membutuhkan perencanaan keberlangsungan bisnis atau *business continuity plan* (BCP) yang baik pula. BCP dapat menjadi sebuah jaminan untuk perusahaan agar dapat menghadapi risiko-risiko yang muncul. BCP memiliki fokus utama terhadap: bagaimana menjamin kontinuitas dari bisnis ketika kehilangan akses terhadap manusia, fasilitas, sistem informasi, layanan dan sumber daya [4].

Business Continuity Plan (BCP) adalah sebuah rencana yang diambil suatu perusahaan untuk mempertahankan keberlangsungan bisnisnya, BCP merupakan hal yang sangat penting dalam proses bisnis, namun jarang menjadi prioritas karena alasan memerlukan biaya yang mahal dan sulit penerapannya. Pembuatan *Business Continuity Plan* ini merupakan upaya untuk mencegah gangguan terhadap aktivitas bisnis normal [5]. BCP dirancang untuk melindungi proses bisnis yang kritis dari kegagalan akibat dari bencana, yang dapat mengakibatkan hilangnya kemampuan perusahaan dalam melakukan proses bisnis secara normal. BCP merupakan suatu strategi untuk memperkecil efek gangguan dan untuk memungkinkan proses bisnis terus berlangsung.

Penyusunan kerangka dimulai dengan inisiasi awal yang dilanjutkan dengan penilaian risiko-risiko yang berpotensi terjadi pada organisasi, dari penilaian tersebut dapat dilakukan analisa dampak (*business impact analysis*) dari risiko tersebut. Setelah melakukan pembuatan BIA dilanjutkan dengan pembuatan strategi mitigasi yang dapat meminimalisir, menghindari atau mentransfer risiko tersebut, setelah strategi mitigasi didapatkan selanjutnya adalah membangun BCP dilakukan dengan melakukan formulasi antara kebutuhan dan tujuan perusahaan terkait keberlanjutan bisnis dengan sintesis kerangka BCP yang digunakan sebagai

acuan yaitu, kajian panduan kerangka kerja ISO 22301:2012, dan kajian empiris.

Manajemen risiko merupakan pengelolaan risiko yang terjadi pada organisasi yang dilakukan untuk meminimalisasi risiko TI yang mungkin muncul dan dapat memberikan dampak buruk bagi perusahaan [6]. Pada konteks penelitian ini manajemen risiko dilakukan untuk Departemen Teknologi Informasi. Dalam pelaksanaan manajemen risiko, perlu adanya sebuah perencanaan keberlanjutan bisnis perusahaan atau yang biasa disebut dengan *Business Continuity Planning* (BCP).

Sub Direktorat Pengembangan Sistem Informasi merupakan salah satu layanan yang ada pada LPTSI, suatu lembaga dibawah ITS yang bergerak sebagai pusat layanan sistem informasi di ITS. LPTSI sebagai pusat pengembangan SI/TI di ITS memiliki tugas melaksanakan, mengkoordinasi, memonitor dan mengevaluasi kegiatan penelitian dan pengembangan teknologi dan sistem informasi. Sub Direktorat Pengembangan Sistem Informasi memiliki tugas pokok fungsi yaitu menyediakan dan mengelola aplikasi sistem informasi berbasis web untuk mengoptimalkan e-layanan. Sebagai salah satu layanan yang vital pada LPTSI, Sub Direktorat Pengembangan Sistem Informasi belum pernah melakukan analisis risiko ataupun mempunyai dokumen yang mengatur respon saat terjadi gangguan pada organisasi. Besarnya aset TI yang dimiliki oleh LPTSI dapat berpotensi terkena risiko bencana yang dapat menghentikan proses bisnisnya.

Walaupun telah memiliki aset teknologi informasi yang berjalan, Sub Direktorat Pengembangan Sistem Informasi belum memiliki manajemen risiko teknologi informasi maupun perencanaan keberlangsungan bisnis atau business continuity plan (BCP) untuk teknologi informasi di organisasi. Padahal banyak gangguan, ancaman bahkan bencana yang dapat muncul dan merugikan organisasi dalam segi biaya maupun waktu bahkan bisa melumpuhkan proses bisnis organisasi. Sub Direktorat Pengembangan Sistem Informasi membutuhkan sebuah business continuity plan (BCP) berbasis profil risiko untuk membantu

bagian TI organisasi agar dapat merespon terhadap risiko yang muncul dan untuk menjaga berjalannya operasional bisninsya. Setiap organisasi memiliki kebutuhan yang berbeda-beda, sehingga BCP antara satu organisasi dengan yang lain akan berbeda – beda pula. Kerangka BCP yang dibuat harus sesuai dengan kebutuhan dan juga kondisi kekinian organisasi untuk memudahkan organisasi dalam menjaga keberlanjutan proses bisnisnya.

Penelitian ini diharapkan dapat menunjukkan bahwa implementasi BCP di sebuah perusahaan merupakan sesuatu hal yang unik, di mana setiap implementasi tersebut harus disesuaikan dengan kebutuhan perusahaan. Pendekatan yang digunakan dalam pembuatan *Business Continuity Plan* mengharuskan perusahaan untuk aktif melakukan manajemen risiko perusahaan dan peningkatan secara terus-menerus (*continuous improvement*), mengingat kebutuhan perusahaan yang dapat berubah sesuai dengan perkembangan teknologi informasi dan regulasi pemerintah yang berlaku. *Business Continuity Plan* memiliki 2 arah dalam implementasinya, yaitu maju yang berfokus kepada keberlangsungan bisnis ke depannya dan mundur yaitu berfokus pada manajemen risiko yang terdapat di perusahaan. Penerapan *Business Continuity Plan* ini dapat mengalami kegagalan jika penerapannya hanya menggunakan satu arah.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, maka rumusan permasalahan yang menjadi fokus dan akan diselesaikan dalam Tugas Akhir ini antara lain:

1. Apa hasil penilaian risiko teknologi informasi pada Sub Direktorat Pengembangan Sistem Informasi?
2. Apa hasil analisis dampak bisnis dan pengaruh pada aset informasi di Sub Direktorat Pengembangan Sistem Informasi jika risiko teknologi informasi yang telah ditentukan terjadi?

3. Bagaimana hasil rancangan Business Continuity Plan berbasis risiko yang sesuai dengan kebutuhan Sub Direktorat Pengembangan Sistem Informasi?

1.3 Batasan Masalah

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

1. Penelitian ini dilakukan pada salah satu layanan di DPTSI yaitu Sub Direktorat Pengembangan Sistem Informasi.
2. Risiko yang di analisis pada penelitian ini hanya risiko dari Sub Direktorat Pengembangan Sistem Informasi
3. Metode yang digunakan untuk penelitian adalah wawancara dan observasi dengan menggunakan referensi OCTAVE dan FMEA untuk manajemen risiko, ISO 22317:2015
4. Proses pengerjaan BCP fokus pada proses bisnis kritis dan risiko TI yang bernilai tinggi dan sangat tinggi pada Sub Direktorat Pengembangan Sistem Informasi.

1.4 Tujuan

Berdasarkan rumusan masalah di atas, maka tugas akhir ini memiliki tujuan sebagai berikut:

1. Menghasilkan rancangan *Business Continuity Plan* yang sesuai dengan kebutuhan dari Sub Direktorat Pengembangan Sistem Informasi
2. Menghasilkan *Business Continuity Plan* berbasis risiko pada Sub Direktorat Pengembangan Sistem Informasi.
3. Menghasilkan penilaian risiko Sub Direktorat Pengembangan Sistem Informasi sesuai dengan ISO 22317:2015.
4. Menghasilkan penilaian dampak bisnis pada teknologi informasi pada Sub Direktorat Pengembangan Sistem Informasi.

1.5 Manfaat

Manfaat yang diharapkan dapat diperoleh dari tugas akhir ini adalah:

1. Sub Direktorat Pengembangan Sistem Informasi dapat memiliki rancangan kerja *Business Continuity Plan* berbasis risiko
2. Sub Direktorat Pengembangan Sistem Informasi mengetahui penilaian risiko yang muncul pada layanan Teknologi Informasi.
3. Sub Direktorat Pengembangan Sistem Informasi mendapatkan acuan kerangka kerja *Business Continuity Plan* (BCP) yang dapat memfasilitasi LPTSI disesuaikan dengan kebutuhan.
4. Sub Direktorat Pengembangan Sistem Informasi dapat mengetahui faktor kritis dari analisa dampak bisnis yang ada pada bagian Teknologi Informasi.

1.6 Relevansi Tugas Akhir

Tugas akhir ini berkaitan dengan mata kuliah Manajemen Risiko Teknologi Informasi, Manajemen Proyek Teknologi Informasi, Pengukuran Kinerja dan Evaluasi Teknologi Informasi dan Perencanaan Keberlangsungan Bisnis.

1.7. Sistematika Penulisan

Sistematika penulisan tugas akhir ini dibagi menjadi tujuh bab, yakni:

BAB I PENDAHULUAN

Bab ini berisi pendahuluan yang menjelaskan latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat, relevansi dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Definisi dan penjelasan pustaka yang dijadikan referensi dalam pembuatan tugas akhir ini akan dijelaskan pada bab dua. Teori yang dipaparkan di antaranya mengenai Tata Kelola TI, SOP, BAI03 COBIT 5, manajemen perubahan ITIL v3, serta konsep-konsep lain yang berkaitan dengan pembuatan tugas akhir.

BAB III METODOLOGI
Bab ini menggambarkan uraian dan urutan pekerjaan yang akan dilakukan dalam penyusunan tugas akhir ini.

BAB IV PERANCANGAN
Bab ini menjelaskan perancangan perangkat yang dilakukan oleh penulis untuk mengumpulkan data kondisi kekinian.

BAB V IMPLEMENTASI
Bab ini menjelaskan hasil yang didapatkan dari proses pengumpulan data, yakni meliputi kondisi kekinian, kondisi yang diharapkan dari pihak organisasi, dan apa saja hambatan yang dihadapi ketika mengumpulkan data.

BAB VI HASIL DAN PEMBAHASAN
Bab ini berisi tentang bagaimana kesenjangan yang terjadi antara kondisi kekinian dan kondisi ideal, kemudian menjelaskan bagaimana proses pembuatan dokumen SOP, serta proses verifikasi dan validasi SOP dilakukan untuk dapat melihat apakah SOP yang telah dibuat dapat diterapkan atau tidak.

BAB VII PENUTUP
Bab ini berisi tentang simpulan dari keseluruhan tugas akhir dan saran maupun rekomendasi terhadap penelitian tugas akhir ini untuk perbaikan ataupun penelitian lanjutan yang memiliki kesamaan dengan topik yang diangkat.

“Halaman ini sengaja dikosongkan

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya

Bab ini akan menjelaskan mengenai penelitian sebelumnya dan dasar teori yang dijadikan acuan atau landasan dalam pengerjaan tugas akhir ini. Landasan teori akan memberikan gambaran secara umum dari landasan penjabaran tugas akhir ini. Penelitian yang dijadikan acuan dalam pengerjaan tugas akhir ini disajikan pada tabel berikut:

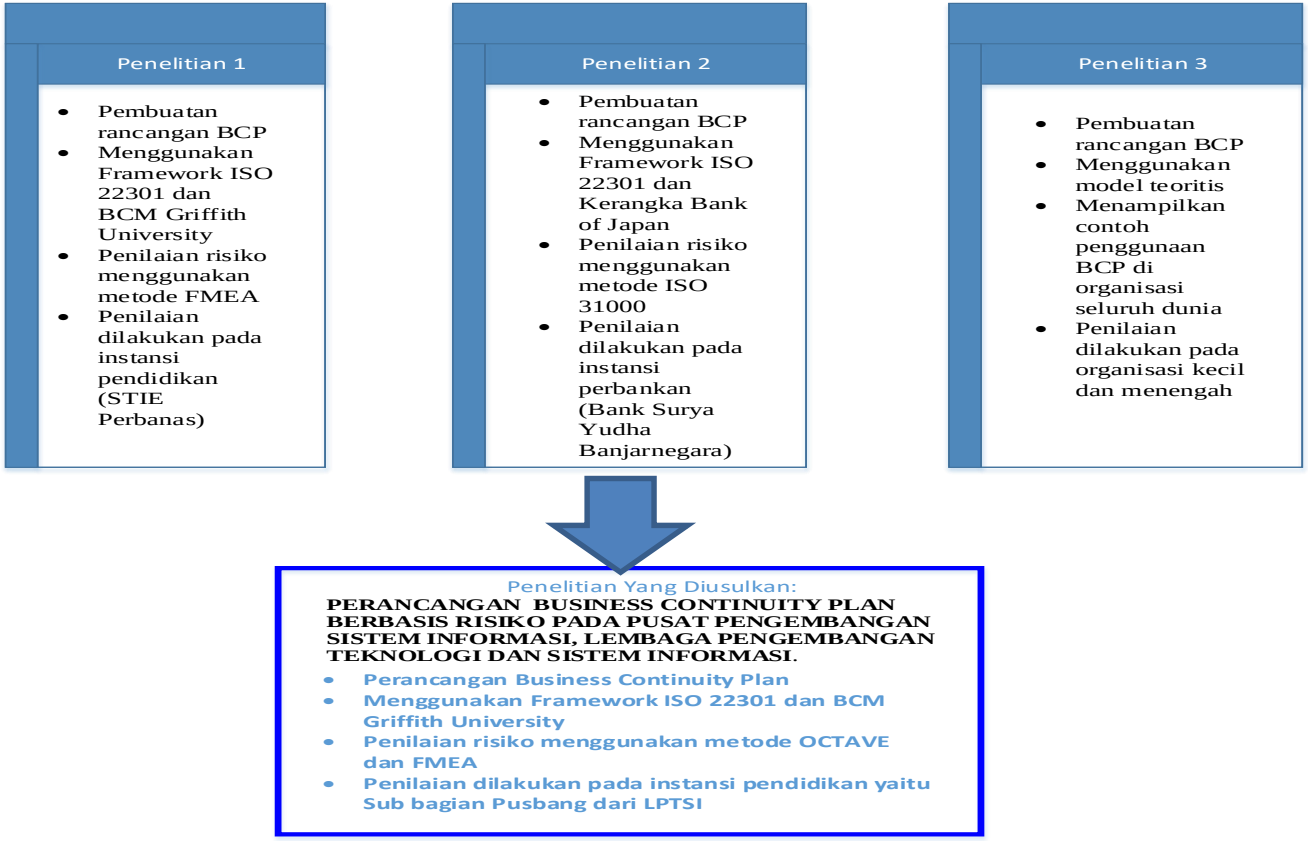
Tabel 2.1 Penelitian Sebelumnya

Judul Paper	Perancangan *Business Continuity Plan* Untuk Teknologi Informasi Pada Studi Kasus STIE Perbanas
Penulis, Tahun	Sabrina Leviana Putri, 2015
Deskripsi Umum Penelitian	Penelitian ini menghasilkan suatu kerangka kerja *business continuity planning* (BCP) berbasis risiko yang sesuai dengan kebutuhan perusahaan yang mengacu dengan kerangka ker ISO 22301:2012 dan ISO 22317:2015
Keterkaitan Penelitian	Penelitian ini memberi pandangan terhadap implementasi *business continuity planning* (BCP) khususnya pada perguruan tinggi atau organisasi pendidikan dimana sesuai dengan studi kasus pada tugas akhir penulis.

Judul Paper	*Business Continuity Plan* pada Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjernegara
Penulis, Tahun	Anindita Alisia Amanda, 2014
Deskripsi Umum Penelitian	Penelitian ini menghasilkan suatu kerangka kerja *business continuity planning* (BCP) berbasis risiko yang sesuai dengan kebutuhan perusahaan yang mengacu

	dengan kerangka ker ISO 22301:2012 dan ISO 22317:2015. Terdapat pula langkah-langkah pembuatan kerangka kerja BCP yang dijelaskan secara terstruktur.
Keterkaitan Penelitian	Penelitian ini merupakan suatu bahan referensi pembuatan kerangka kerja *business continuity planning* (BCP) berbasis risiko dan bagaimana menbuat suatu BCP yang benar sesuai dengan kebutuhan dan tujuan suatu organisasi

Judul Paper	*The Definitive Handbook of Business Continuity Management*
Penulis, Tahun	Andrew Hiles, 2007
Deskripsi Umum Penelitian	Penelitian ini menghasilkan suatu pendekatan implementasi BCP dengan menggunakan model teoritis juga menampilkan contoh penggunaan BCP di organisasi seluruh dunia.
Keterkaitan Penelitian	Penelitian ini merupakan suatu bahan referensi pembuatan kerangka kerja *business continuity planning* (BCP), langkah-langkah yang diberikan pada penelitian ini dapat dijadikan landasan implementasi BCP di organisasi kecil dan menengah.


Penelitian 1
Pembuatan rancangan BCP
Menggunakan Framework ISO 22301 dan BCM Griffith University
Penilaian risiko menggunakan metode FMEA
Penilaian dilakukan pada instansi pendidikan (STIE Perbanas)
Penelitian 2
Pembuatan rancangan BCP
Menggunakan Framework ISO 22301 dan Kerangka Bank of Japan
Penilaian risiko menggunakan metode ISO 31000
Penilaian dilakukan pada instansi perbankan (Bank Surya Yudha Banjarnegara)
Penelitian 3
Pembuatan rancangan BCP
Menggunakan model teoritis
Menampilkan contoh penggunaan BCP di organisasi seluruh dunia
Penilaian dilakukan pada organisasi kecil dan menengah
Penelitian Yang Diusulkan:
PERANCANGAN BUSINESS CONTINUITY PLAN BERBASIS RISIKO PADA PUSAT PENGEMBANGAN SISTEM INFORMASI, LEMBAGA PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI.
Perancangan Business Continuity Plan
Menggunakan Framework ISO 22301 dan BCM Griffith University
Penilaian risiko menggunakan metode OCTAVE dan FMEA
Penilaian dilakukan pada instansi pendidikan yaitu Sub bagian Pusbang dari LPTSI

2.2 Risiko

Risiko adalah ancaman terhadap kehidupan, properti atau keuntungan finansial akibat bahaya yang terjadi [7]. Menurut sudut pandang hasil atau output, risiko adalah "sebuah hasil atau output yang tidak dapat diprediksikan dengan pasti, yang tidak disukai karena akan menjadi kontra produktif". Sedangkan untuk sudut pandang proses, risiko adalah "faktor-faktor yang dapat mempengaruhi pencapaian tujuan, sehingga terjadi konsekuensi yang tidak diinginkan".Secara umum risiko dikaitkan dengan kemungkinan (probabilitas) terjadinya peristiwa diluar yang diharapkan [8].

Menurut ISO 31000:2009, risiko adalah *effect of uncertainty on objectives*, atau dapat dikatakan bahwa risiko adalah efek yang muncul akibat adanya ketidakpastian dalam tujuan. Tujuan – tujuan ini bisa juga ditujukan untuk tujuanperusahaan maupun organisasi [9].Sesuatu yang tidak pasti (*uncertainty*) dapat berakibat menguntungkan atau merugikan. Ketidakpastian yang menimbulkan kemungkinan menguntungkan dikenal dengan istilah peluang (*opportunity*), sedangkan ketidakpastian yang menimbulkan akibat yang merugikan dikenal dengan istilah risiko. Bentuk – bentuk risiko [10]:

1. Risiko Murni
   Bentuk risiko yang kalau terjadi akan Menimbulkan kerugian atau tidak menimbulkan kerugian. Contoh: Risiko Kebakaran, Risiko Kecelakaan.
2. Risiko Spekulatif
   Risikoyang jika terjadi dapat menimbulkan kerugian atau menimbulkan kerugian atau mendatangkan keuntungan. Contoh: Risiko Produksi, Risiko Moneter (Kurs Valuta Asing).
3. Risiko Fundamental (Mendasar)
   Risiko yang kalau terjadi dampak kerugiannya bisa sangat luas atau bersifat catastrophic. Contoh: Risiko Perang, Gempa Bumi dan Polusi Udara.
4. Risiko Khusus

Risiko yang jika terjadi, dampak kerugiannya Bersifat lokal tidak menyeluruh atau non *catastrophic*. Contoh: Risiko Kebakaran, Risiko Kecelakaan, Pencurian.

2.3 Manajemen Risiko

Menurut Peraturan Menteri Keuangan Nomor 191/PMK.09/2008, definisi manajemen risiko adalah pendekatan sistematis untuk menentukan tindakan terbaik dalam kondisi ketidakpastian.

Menurut International Organization for Standardization (ISO) melalui Dokumen ISO 31000: 2009 – *Risk Management Principles and Guidelines,* manajemen risiko adalah aktivitas terkoordinasi yang dilakukan untuk mengarahkan dan mengelola organisasi dalam rangka menangani risiko [9]. Sedangkan menurut AS/NZS 4360 Risk Management Standard, 1999, manajemen risiko adalah budaya, proses, dan struktur yang diarahkan menuju pengelolaan potensi ancaman maupun kesempatan secara efektif .

Oleh karena itu, dapat disimpulkan bahwa manajemen risiko adalah sebuah aktivitas atau proses pengelolaan risiko pada sebuah perusahaan atau organisasi yang bertujuan untuk menentukan tindakan terbaik dalam meminimalisir suatu kerugian atau dampak yang disebabkan apabila risiko terjadi.

2.4 Risiko Teknologi Informasi

Risiko teknologi informasi merupakan risiko-risiko yang berhubungan dengan teknologi informasi, dikarenakan pentingnya suatu teknologi informasi pada suatau perusahaan, maka risiko teknologi informasi memberikan dampak yang cukup signifikan bagi perusahaan. Risiko dapat terjadi diantaranya pada penerapan TI. Risiko tersebut dapat berupa ancaman terhadap aset TI seperti data, software, dan hardware; ancaman terhadap layanan-layanan yang disediakan TI, proses bisnis organisasi, dan organisasi secara keseluruhan [6]. Berikut ini merupakan risiko teknologi informasi berdasarkan enam komponen sistem informasi:

Tabel 2.2 Ancaman Komponen Sistem Informasi (Sumber: Peneliti)

Komponen	Ancaman
People	Sabotase, *hacking, cracking, human error*
Procedure	Kesalahan dalam melakukan sebuah prosedur
Hardware	Pencurian *hardware,* kerusakan *hardware, hardware* mati
Software	*Virus, bug, worm, trojan,*
Data	Kehilangan data, penyalahgunaan data, pencurian data
Network	Terputusnya kabel internet, *firewall* terkena hack

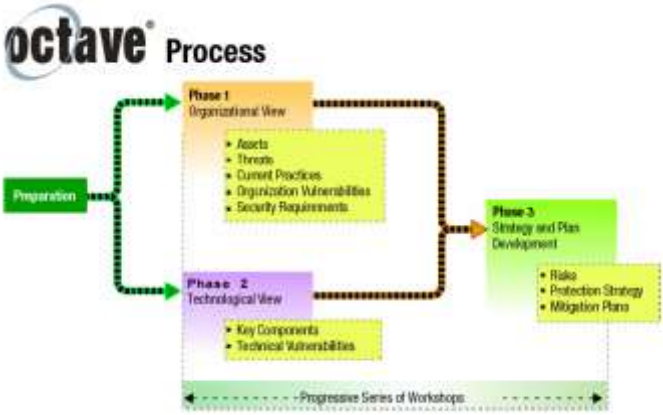
2.5 Manajemen Risiko Teknologi Informasi

Manajemen risiko teknologi informasi adalah suatu pengelolaan/manajemen dari risiko-risiko terkait teknologi informasi pada sebuah organisasi atau perusahaan tertentu yang memiliki tujuan untuk meminimalisasi risiko yang muncul dengan solusi yang berhubungan dengan aspek teknologi informasi.Manajemen risiko teknologi informasi merupakan suatu subset dari keseluruhan manajemen risiko bisnis [11].
Manajemen risiko Teknologi Informasi (TI) adalah kemampuan organisasi dalam mengurangi risiko-risiko TI yang mungkin akan menghambat pencapaian tujuan organisasi terkait dengan pemanfaatan TI itu sendiri.

2.6 OCTAVE

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) adalah suatu penilaian strategi berbasis risiko dan teknik perencanaan untuk keamanan. OCTAVE merupakan suatu proses untuk mengidentifikasi pengetahuan beberapa pihak mengenai praktek yang terjadi dari segi proses keamanan organisasi serta melihat kondisi praktek keamanan yang telah berjalan di organisasi [12].
OCTAVE adalah sebuah pendekatan terhadap evaluasi risiko keamanan informasi yang komprehensif, sistematik, terarah, dan dilakukan sendiri. Pendekatannya disusun dalam satu set kriteria yang mendefinisikan elemen esensial dari evaluasi risiko keamanan informasi. Kriteria OCTAVE memerlukan eveluasi yang harus dilakukan oleh sebuah tim interdisipliner

yang terdiri dari personil teknologi informasi dan bisnis organisasi. Anggota tim bekerjasama untuk membuat keputusan berdasarkan risiko terhadap aset informasi kritis organisasi [13].



Gambar 2.1 Proses OCTAVE [13]

Gambar 2.2 Proses OCTAVE (2) (Sumber: OCTAVE)

Pendekatan OCTAVE menggunakan tiga tahapan, yaitu membangun proses profil ancaman berdasarkan aset yang ada (*Build Asset-Based Threat Profiles*), melakukan identifikasi

kerentanan dari infrasruktur (*Develop Security Strategy and Plans*), dan mengembangkan rencana dan strategi keamanan (*Develop Security Strategy and Plans*). Berikut ini penjelasan tentang tahapan-tahapan tersebut:

1. **Tahap Persiapan**
   Dalam tahapan ini kegiatan persiapan yang harus dilakukan adalah penyusunan jadwal, membentuk tim analisis, meminta dukungan dan menyiapkan logistic.
2. **Fase 1 : Build Asset-Based Threat Profile**
   Tahapan ini melakukan identifikasi aset TI yang bersifat kritis dengan mengumpulkan informasi-informasi terkait aset TI tersebut. Dalam tahapan ini juga mengklasifikasikan aset apa saja yang menjadi prioritas pada organisasi. Tahap ini memiliki empat proses, yaitu:
   - **Proses 1 : Identify Senior Management Knowledge**
     Melakukan identifikasi pengetahuan dari senior management seperti mengidentifikasi aset kritis, mendeskripsikan aset yang vulnerable, mendefinisikan kebutuhan kemanan untuk setiap aset.
   - **Proses 2 : Identify Operational Area Knowledge**
     Melakukan penggalian informasi dari pengetahuan dari bagian operational tentang aset-aset kritis dan stratego perlindungan dari risiko.
   - **Proses 3 : Identify Staff Knowledge**
     Melakukan penggalian informasi dari pengetahuan yang dimiliki oleh para pegawai di organisasi.
   - **Proses 4 : Create Threat Profiles**
     Setelah mendapatkan semua informasi dari berbagai sumber, lalu membuat profil ancaman terhadap aset kritis.

   ▪ **Fase 2 : Identify Infrastructure Vulnerabilities**
   Tahapan ini melakukan identifikasi terhadap kerentanan dari infrastruktur yang ada di sebuah organisasi. Informasi yang telah diperoleh dari tahapan pertama akan diolah. Selain itu, juga melibatkan pegawai lainnya untuk membantu mengidentifikasi kerentanan infrastruktur apa saja yang ada. Tahap ini memiliki dua proses, yaitu:

- **Proses 5 : identify Key Components**
  Melakukan identifikasi dari key component infrastruktur yang diuji kerentanannya terhadap risiko yang mungkin akan terjadi dan mengancam aset kritis.
- **Proses 6 : Evaluate Selected Components**
  Melakukan evaluasi terhadap komponen infrastruktur yang dipilih untuk setiap aset kritis.

▪ **Fase 3 : Develop Security Strategy and Plans**

Tahapan ini telah dilakukan identifikasi risiko yang berhubungan dengan aset kritis organisasi, kemudian barulah membuat rencana mitigasi untuk risiko tersebut. Tahapan ini juga membangun strategi bagi organisasi untuk perlindungan. Tahap ini memiliki dua proses, yaitu:

- **Proses 7 : Conduct Risk Analysis**
  Setelah menganalisis informasi yang telah diperoleh dari proses-proses sebelumnya, kemudian dilakukan identifikasi pengaruh dari setiap ancaman, membuat kriteria evaluasi, dan mengevaluasi dampak dari ancaman tersebut.
- **Proses 8 : Develop Protection Strategy**
  Proses terakhir dari OCTAVE yang melakukan pengembangan strategi untuk perlindungan terhadap risiko-risiko, melakukan perencanaan mitigasi dari risiko tersebut.

Dari gambaran proses tiga fase tersebut, dapat diketahui output atau luaran dari setiap fase, yaitu:

Fase	Luaran
Fase 1	▪ Aset Kritis ▪ Kebutuhan keamanan untuk aset kritis ▪ Ancaman pada aset kritis ▪ Praktik keamanan saat ini ▪ Kerentanan organisasi saat ini
Fase 2	▪ Komponen utama

	▪ Kerentanan teknologi saat ini
Fase 3	▪ Risiko aset kritis ▪ Pengukutan risiko ▪ Strategi perlindungan ▪ Perencanaan mitigasi risiko

Tabel 2.3 Output setiap fase OCTAVE

2.7 Metode Failure Mode and Effect Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) merupakan analisa teknik yang bila dilakukan dengan tepat dan waktu yang tepat akan memberikan nilai yang besar dalam membantu proses pembuatan keputusan dari engineeri selama perancangan dan pengembangan [14]. FMEA merupakan metode sistematis yang digunakan untuk melakukan identfikasi akibat atau konsekuensi dari potensi kegagalam sistem atau proses, serta mengurangi peluang terjadinya kegagalan. FMEA adalah salah satu alat yang dapat diandalkan untuk mengurangi kerugian yang terjadi akibat kegagalan tersebut.FMEA adalah salah satu alat yang dapat diandalkan untuk mengurangi kerugian yang terjadi akibat kegagalan tersebut. Langkah langkah dari FMEA adalah sebagai berikut :

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

Tujuan dari FMEA adalah:

- Mengetahui kegagalan yang berpotensi
- Memprediksi dan mengevaluasi pengaruh dari kegagalan pada sistem yang ada
- Menunjukkan prioritas terhadap perbaikan suatu proses
- Mengidentifikasi dan membangun tindakan untuk mencegah atau mengurangi kesempatan terjadinya kegagalan
- Dokumentasi proses secara keseluruhan

Risiko-risiko yang sudah diidentifikasi pada tahap sebelumnya akan dinilai berdasarkan metode FMEA (Failure Mode Effect Analysis) dengan mengukur tingkat severity number, occurence number, dan detection number yang nantinya akan menghasilkan Risk Probability Number (RPN).

2.7.1 Penentuan Nilai Dampak (Severity: S)

Severity number merupakan penilaian terhadap pengaruh buruk yang dirasakan akibat kegagalan potensial. Severity number mengukur tingkat keparahan dari risiko yang terjadi. Pengukuran Severity atau nilai dampak dilihat dari seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek-aspek penting dalam organisasi. Terdapat tiga aspek yang akan dijabarkan yaitu aspek jadwal, aspek biaya dan aspek teknis. Pada tabel 4 dibawah, terdapat penjelasan nilai deteksi dan kemampuan metode deteksi terhadap risiko.

Tabel 2.4 Nilai Dampak (Sumber:FMEA)

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

2.7.2 Penentuan Nilai Kemungkinan (Occurence: O)

Occurence merupakaan pengukuran terhadap tingkat kemungkinan frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat menghasilkan kegagalan. Occurence membantu dalam pengukuran probabilitas penyebab kemungkinan terjadinya risiko akan menghasilkan kegagalan yang akan berdampak sesuatu. Pada tabel 5 dibawah, terdapat penjelasan nilai kemungkinan dan kemungkinan terjadinya risiko.

Tabel 2.5 Nilai Kemungkinan (Sumber: FMEA)

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

2.7.3 Penentuan Nilai Deteksi (Detection: D)

Nilai deteksi atau detection merupakan suatu nilai pengukuran terhadap kemampuan mengendalikan atau mengontrol kegagalan yang dapat terjadi. Pada tabel 6 dibawah, terdapat penjelasan nilai deteksi dan kemampuan metode deteksi terhadap risiko.

Tabel 2.6 Nilai Deteksi (Sumber: FMEA)

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

Hampir Pasti	Metode deteksi hampir pasti dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	1

2.7.4 Penentuan Level Risiko (*Risk Priority Number*)

Risk Priority Number (RPN) merupakan produk matematis dari keseriusan effects (Severity), kemungkinan terjadinya cause akan menimbulkan kegagalan yang berhubungan dengan effects (occurrence), dan kemampuan untuk mendeteksi kegagalan sebelum terjadi pada pelanggan (detection). RPN dapat ditunjukkan dengan persamaan sebagai berikut:

RPN = Severity x Occurence x Detection

Dari hasil RPN, maka dapat diketahui tingkat risiko tersebut. Tingkat risiko berdasarkan FMEA adalah sebagai berikut:

Tabel 2.7 Level Risiko (Sumber: FMEA)

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

Skala RPN dari setiap risiko akan digunakan sebagai penentu level risiko, yang berguna untuk menilai risiko manakah yang bernilai paling tinggi. Perusahaan perlu melakukan antisipasi, mitigasi dan strategi terhadap risiko yang memiliki tingkatan paling tinggi, untuk menjaga keberlangsungan operasional bisnis saat gangguan tersebut terjadi

2.8 Kerangka Kerja ISO 22301:2012

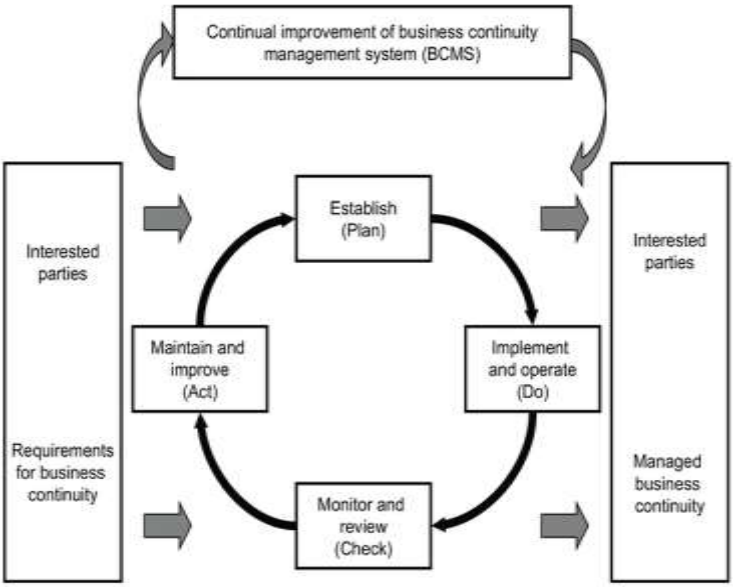
ISO (the International Organization for Standardization) adalah sebuah badan yang mengatur standar nasional di seluruh dunia. ISO 22301:2012 merupakan suatu produk dari ISO berupa standar internasional yangdibuat untuk mengatur dan mengelola sistem pengelolaan keberlangsungan bisnis atau *Business Continuity Management Systems* (BCMS) yang efektif. ISO 22301:2012 menspesifikasikan kebutuhan untuk merencanakan, membangun, mengimplementasikan, mengoperasikan, memantau, melakukan review, menjaga dan secara terus menerus meningkatkan suatu sistem manajemen yang terdokumentasi untuk melindungi, mengurangi kemungkinan terjadi, mempersiapkan, menanggapi dan pulih dari gangguan yang timbul [15].

ISO 22301:2012 dibuat sebagai mengembangan dari British Standard BS 259999-2:2007 dan standar yang digunakan pada wilayah lain. Standar ini dibuat untuk menjaga bisnis dari potensi gangguan yang dapat terjadi. Gangguan ini dapat berupa cuaca ekstrim, kebakaran, banjir, bencana alam, pencurian dan lain sebagainya. Standar ini dibuat agar manajemen dapat melakukan identifikasi ancaman yang relevan dan memiliki dampak yang besar pada proses bisnis yang kritis, selain itu juga dapat melakukan perencanaan sehingga membantu bisnis untuk tidak stagnan atau diam ditempat.

Alasan penggunaan standar ini pada kerangka BCP adalah, peneliti meyakini bahwa standar ini merupakan standar yang komperhensif dan diakui secara internasional. Selain itu, ISO (International Standard Organization) menjadi sumber dari penggunaan standar di seluruh dunia, dan standar ini selalu berkembang dan bersifat dinamis sesuai dengan kebutuhan dan kondisi pasar.Dari keunggulan-keunggulan tersebut ditetapkan bahwa penelitian akan menggunakan kerangka kerja ISO 22301:2012, karena standar ini dikenal relevan dan komprehensif dengan topik penelitian.

Standar internasional ini mengaplikasikan model siklus “Plan-Do-Check-Act” (PDCA) untuk melakukan tahapan pada kerangka kerja business continuity management systems (BCMS). Hal ini dilakukan untuk menjaga konsistensi standar

dengan standar manajemen sistem lainnya seperti ISO 9001 quality management systems, ISO 14001 enviromental management systems, ISO/IEC 27001 Information security management systems dan lain sebagainya. Model ini diharapkan dapat mendukung konsistensi dan integrasi implementasi dan operasi dengan sistem manajemen lainnya yang terkait. Berikut adalah siklus PDCA yang digunakan pada proses BCMS di ISO 22301:2012 [15].



Gambar 2.3 Proses PDCA pada ISO 22301:2012

Penjelasan dari model tersebut adalah sebagai berikut.

1. **Plan (Establish)**
   Membuat kebijakan keberlanjutan bisnis (business continuity), objektif, target, kontrol, proses dan prosedur yang relevan untuk meningkatkan keberlanjutan bisnis, dalam rangka penyelarasan dengan kebijakan dan tujuan organisasi atau perusahaan.
2. **Do (Implement and Operate)**

Mengimplementasi dan mengoperasikan kebijakan keberlanjutan bisnis (business continuity), kontrol, proses dan prosedur.

3. **Check (Monitor and Review)**
   Memantau dan meninjau performa yang bertentangan dengan kebijakan dan tujuan keberlanjutan bisnis (business continuity), melaporkan hasil ke manajemen untuk peninjauan dan menetapkan serta mengesahkan tindakan untuk memperbaiki dan meningkatkan performa.
4. **Act (Maintain and Improve)**
   Memelihara dan meningkatan BCMS dengan mengambil perbaikan tindakan, berdasarkan hasil dari peninjauan pengelolaan. Tindakan ini juga melingkupi penilaian ulang ruang lingkup BCMS dan kebijakan serta tujuan dari keberlanjutan bisnis (business continuity).

Pada model PDCA tersebut, terdapat beberapa masukkan (input) sebelum model PDCA tersebut dijalankan, yaitu *interested parties* atau pihak yang bersangkutan dan juga *requirement for business continuity* atau kebutuhan untuk keberlanjutan bisnis. Kedua input tadi dibutuhkan untuk menjalankan proses yang ada pada model tersebut, yaitu perencanaan-pengerjaan-pemeriksaan-tindakan (plan-do-check-act). Selain masukkan, terdapat pula keluaran (output) pada siklus tersebut, interested parties atau pihak yang bersangkutan masih menjadi keluaran dari model ini, yang membedakan input dan outputnya adalah terdapat *managed business continuity* atau keberlangsungan bisnis yang telah terkelola.

Selanjutnya, dalam proses yang ada pada model PDCA tersebut, terdapat suatu siklus peningkatan berkelanjutan (continual improvement) yang diharapkan dapat menyempurnakan proses, yaitu melakukan perbaikan-perbaikan pada hal-hal yang belum sesuai dengan standar yang telah ditetapkan. Sehingga pada akhirnya, dapat mengeluarkan hasil yang baik bagi para pihak yang bersangkutan serta dapat mengelola keberlanjutan bisnis di perusahaan atau organisasi tersebut.

ISO 22301:2012 terdiri dari 10 Klausa yang digunakan terkait sistem pengelolaan keberlangsungan bisnis (BCMS). Klausa 1, 2 dan 3 tidak berhubungan secara langsung dengan model PDCA. Klausa 1 menjelaskan mengenai ruang lingkup dokumen, klausa 2 menjelaskan mengenai referensi yang dijelaskan pada dokumen dan klausa 3 menjelaskan mengenai definisi dan istilah terkait yang digunakan pada dokumen. Klausa yang berkaitan dengan model PDCA adalah klausa 4, 5, 6, 7, 8, 9 dan 10 berikut penjelasan dari masing masing klausa.

Tabel 2.8 Klausa Kerangka Kerja (Sumber: ISO 22301:2015)

Fase	Klausa	Keterangan Klausa
Plan	4	Klausa 4 mengenalkan kebutuhan yang diperlukan dalam membuat konteks BCMS, juga menjelaskan mengenai kebutuhan pihak ketiga dan ruang lingkup yang akan digunakan sesuai dengan kebutuhan organisasi.
	5	Klausa 5 menjelaskan kebutuhan spesifik mengenai peran dari pihak *top management* atau manajemen tertinggi di organisasi dalam BCMS, juga termasuk megenai bagaimana manajemen dapat membuat kebijakan terkait dengan BCMS.
	6	Klausa 6 menjelaskan mengenai kebutuhan mengenai bagaimana membangun tujuan strategis dan pedoman untuk keseluruhan BCMS.
	7	Klausa 7 berisi tentang bagian-bagian yang mendukung operasional BCMS yang berkaitan tentang pembuatan kompetensi dan komunikasi dengan pihak-pihak terkait serta pendokumentasian terkait seluruh informasi dalam BCMS.
Do	8	Klausa 8 menjelaskan kebutuhan keberlanjutan bisnis, menentukan bagaimana pertanggungjawaban atas apa yang terjadi (sumber daya), serta

		mengembangkan prosedur-prosedur yang digunakan untuk mengelola kerusakan atau gangguan yang terjadi pada organisasi. Dalam klausa ini juga menjelaskan beberapa proses penting yang terkait dengan penyusunan BCMS sebagai berikut : • Perencanaan dan kontrol operasional. • BIA (Business Impact Analysis) dan Penilaian risiko (Risk Assessment). • Strategi keberlanjutan bisnis. • Penyusunan dan implementasi prosedur keberlanjutan bisnis.
Check	9	Klausa 9 menjelaskan tentang kebutuhan yang digunakan untuk mengukur performa pengelolaan bisnis keberlanjutan (Business Continuity Management), kesesuaian BCMS yang ada dengan standar internasional, ekspektasi atau keinginan pihak manajemen serta mengumpulkan *feedback* dari manajemen terkait ekspektasi yang ditetapkan.
Act	10	Klausa 10 menjelaskan tentang tindakan yang dilakukan atas ketidaksesuaian BCMS dengan hal-hal yang telah ditetapkan. Dengan melakukan tindakan yang dapat berupa perbaikan, ataupun peningkatan yang berkelanjutan (*continual improvement*).

2.9 ISO 22317: 2015

ISO 22317:2015 merupakan suatu standar internasional yang digunakan untuk melakukan analisis dampak bisnis dengan mengidentifikasi bagaimana BIA dapat sesuai dengan keseluruhan program keberlangsungan bisnis atau sistem manajemen keberlangsungan bisnis. ISO 22317 :2015 adalah spesifikasi teknis internasional yang merekomendasikan

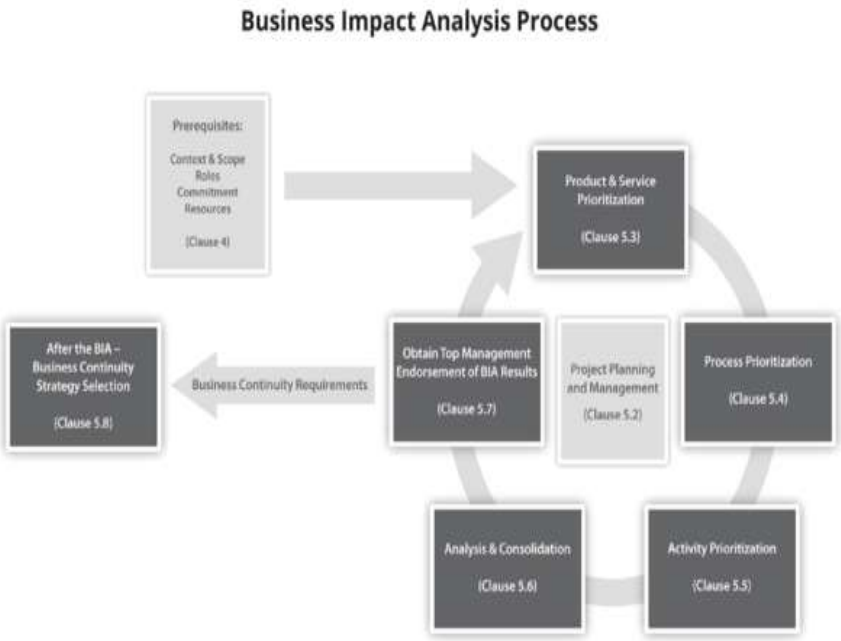
mengenai panduan dan langkah yang diperlukan suatu organisasi dalam membangun, mengimplementasi dan menjaga dokumentasi dan formalitas dari proses analisis dampak bisnis (*business impact analysis*). ISO 22317:2015 ini dapat diterapkan pada semua tipe, jenis dan sifat organisasi [16].

Tujuan dari penggunaan ISO 22317:2015 ini adalah sebagai berikut:

- Menyediakan dasar untuk pemahaman, pengembangan, pengiplementasian, peninjauan, penjagaan dan peningkatan terus menerus dari efektivitas proses analisis dampak bisnis pada organisasi
- Menyediakan panduan untuk perencanaan, pengerjaan dan pelaporan analisis dampak bisnis.
- Membantu organisasi untuk menjalankan analisis dampak bisnis dengan cara yang sesuai dengan praktik yang baik
- Membantu membuat koordinasi antara analisis dampak bisnis dengan program BCM.

Menurut ISO 22317:2015, BIA merupakan suatu siklus yang membutuhkan masukan (*input*) dan menghasilkan keluaran (*output*). Siklus ini bersifat layaknya sebuah proyek, memiliki waktu mulai dan selesai yang telah didefinisikan di awal. Manajemen proyek digunakan agar organisasi bisa melakukan koordinasi sumber daya dan juga kerangka waktu. Masukan dari siklus BIA adalah cakupan dan konteks yang telah ditentukan, peran dan tanggung jawab yang telah ditentukan di dikomunikasikan, adanya komitmen dari pimpinan dan adanya alokasi sumber daya yang cukup. Sedangkan keluaran dari siklus BIA merupakan kebutuhan untuk keberlangsungan bisnis yang akan digunakan untuk proses pemilihan strategi keberlangsungan bisnis dalam proses business continuity management systems (BCMS). Selain itu tujuan dari BIA adalah untuk melakukan prioritisasi terhadap berbagai komponen organisasi sehingga produk atau layanan dapat melanjutnkan prosesnya sesuai dengan yang telah ditentukan

dan tingkat kepuasan dari pihak terkait setelah terjadinya insiden.



Gambar 2.4 Proses Pembuatan Business Impact Analysis pada 22317:2015

2.10 Business Impact Analysis

Menurut Franklin Fletcher, BIA merupakan dasar dari program bisnis kontinuitas (*business continuity program*). Tujuanya adalah untuk mengukur dampak yang disebabkan oleh hilangnya layanan. BIA mengidentifikasi layanan yang paling penting bagi organisasi sehingga dapat memberikan masukan penting bagi strategi. Analisis itu mengidentifikasi :

1) Jenis kerusakan (bencana/gangguan)
2) Bagaimana kerusakan bisa meningkat
3) Kompetensi, fasilitas dan layanan yang dibutuhkan untuk melanjutkan proses yang penting

4) Perkiraan penentuan jangka waktu proses pemulihan

Menurut Internation Standards Organization ISO 22301:2012, BIA adalah suatu proses penilaian dari dampak yang terjadi pada aktivitas aktivitas yang mendukung produk maupun layanan dari suatu organisasi atau perusahaan [15]. Proses yang ada dalam BIA itu sendiri adalah sebagai berikut : mengidentifikasi aktivitas, melakukan penilaian dampak, membuat prioritasi dan mengidentifikasi adanya ketergantungan antar sumber daya yang ada.
Organisasi perlu menyusun, mengimplementasi dan memelihara proses evaluasi yang formal dan terdokumentasi untuk menentukan prioritas pemulihan dan keberlanjutan, tujuan serta target. Pada proses pembuatan BIA, juga terdapat proses penilaian dampak dari gangguan yang terjadi pada aktivitas atau proses bisnis di organisasi. BIA terdiri dari beberapa hal berikut ini [15]:

- Mengidentifikasi aktivitas yang mendukung produk dan jasa di organisasi.
- Menilai dampak ketika sistem tidak dapat berjalan pada aktivitas tersebut.
- Mengatur dan menentukan waktu maksimal organisasi tersebut dapat bertahan tanpa sistem pada saat terjadinya gangguan.
- Mengidentifikasikan ketergantungan sistem terhadap sumber daya pada aktivitas tersebut, termasuk pemasok, mitra kerja dari luar organisasi serta pihak lain yang bersangkutan dengan organisasi.

2.10.1 Proses dan Tahapan Business Impact Analysis (BIA) berdasarkan ISO 22317:2015

Proses pembuatan *Business Impact Analysis* (BIA) yang terdapat pada ISO 22317:2015 termasuk pada Klausa 5. Proses dan tahapan tersebut adalah sebagai berikut:

5.1 Pengantar
5.2 Manajemen dan Perencanaan Proyek

5.3 Prioritisasi Layanan dan Produk
5.4 Prioritisasi Proses
5.5 Prioritisasi Aktivitas
5.6 Analisa dan Konsolidasi
5.7 Mendapatkan Dukungan Manajemen terhadap Hasil BIA
5.8 Langkah Selanjutnya – pemilihan strategi keberlangsungan bisnis

Pada penelitian ini fase yang digunakan dalam pembuatan BIA sesuai dengan ISO 22317 adalah fase prioritasi layanan dan produk, prioritisasi proses, prioritisasi aktivitas, analisa dan konsolidasi dan mendapatkan dukungan manajemen terhadap hasil BIA. Fase inilah yang akan tercakup dalam kerangka kerja BCP yang sesuai dengan kebutuhan perusahaan studi kasus.

2.11 Business Continuity Planning

Business Continuity Plan (BCP) adalah sebuah rencana yang diambil suatu perusahaan untuk mempertahankan keberlangsungan bisnisnya, BCP merupakan hal yang sangat penting dalam proses bisnis, namun jarang menjadi prioritas karena alasan memerlukan biaya yang mahal dan sulit penerapannya. Pembuatan *Business Continuity Plan* ini merupakan upaya untuk mencegah gangguan terhadap aktivitas bisnis normal. [5]

Business continuity plan (BCP) didefinisikan sebagai dokumen berisi prosedur yang bertujuan untuk menjadi panduan perusahaan dalam merespon, melindungi, melanjutkan dan mengembalikan (respond, recover, resume, restore) proses bisnis perusahaan ke level yang telah didefinisikan sebelumnya setelah terjadi gangguan [15].

Menurut Andrew Hiles, *Business continuity planning* (BCP) adalah suatu proses identifikasi dan proteksi terhadap proses bisnis kritis dan sumber daya yang dibutuhkan dalam menjaga proses bisnis agar tetap berada pada level yang dapat diterima, menjaga semua sumber daya dan mempersiapkan prosedur untuk memastikan keberlangsungan suatu organisasi pada saat dimana bisnis terkena gangguan [17].

2.12 Disaster Recovery Planning

Disaster Recovery Plan (DRP) adalah suatu perencanaan yang didesain untuk mengembalikan atau melakukan *recovering* operasionalitas dari suatu sistem, aplikasi atau fasilitas komputer pada suatu tempat alternatif lain setelah terjadi bencana. Pembuatan DRP terlebih dahulu membutuhkan analisis bisnis proses dan kebutuhan perusahaan yang nantinya bertujuan sebagai pencegahan dampak saat keadaan darurat [18]

Pengertian lain terhadap DRP disampaikan oleh National Institute of Standard and Technology (NIST), bahwa DRP merupakan suatu perencanaan yang berfokus pada sistem informasi yang telah didesain untuk melakukan pemulihan sistem kondisi pengganti atau alternatif setelah muncul adanya gangguan.

Disaster Recovery Plan (DRP) merupakan suatu bagian dari keberlangsungan bisnis atau business continuity yang berfokus pada bagaimana menangani dampak dari suatu kejadian. DRP berisi langkah langkah dalam tahap perencanaan yang dapat diimplementasikan untuk menghentikan dampak dari suatu krisis yang tidak pernah direncanakan sebelumnya [11]. *Disaster Recovery Planning* (DRP) dan *Business Continuity Planning* (BCP) membahas mengenai perencanaan untuk keadaan darurat yang mengancam kelangsungan bisnis dan meneruskan bisnis tersebut walaupun terjadi bencana. Tujuan dari BCP dan DRP adalah menjaga bisnis tetap beroperasi meskipun ada gangguan dan menyelamatkan sistem informasi dari dampak bencana lebih lanjut.

Disaster Recovery Planning (DRP) sangat penting bagi perusahaan agar operasional perusahaan dapat tetap berjalan meskipun terjadi bencana. Apabila operasional perusahaan terhambat, maka perusahaan pun akan mengalami kerugian.

2.13 Hubungan BCP Dengan DRP

BCP dan DRP ditujukan untk memenuhi kebutuhan bisnis dalam menghadapi gangguan-gangguan terhadap operasi perusahaan. *Business Continuity Plan* dan *Disaster Recovery Plan* adalah meliputi persiapan, pengujian dan pemutakhiran tindakan-tindakan yang diperlukan untuk melindungi proses bisnis vital (*critical*) terhadap dampak dari kegagalan jaringan dan sistem utama.

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. 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 [5].

National Institute of Standards and Technology (NIST) mengeluarkan sebuah pedoman perencanaan peristiwa yang mungkin terjadi untuk bagian sistem informasi ada pemerintah pusat Amerika Serikat (Contingency Planning Guide for Federal Information Systems). Dalam dokumen tersebut dijelaskan mengenai perencanaan-perencanaan yang dapat digunakan ketika muncul peristiwa yang mengganggu keberlangsungan sebuah proses pada perusahaan atau organisasi yang bersangkutan. Pedoman ini menjelaskan mengenai fokus dari masing-masing perencanaan, termasuk tentang BCP dan DRP. Berikut ini adalah perbedaan antara BCP dengan DRP menurut NIST.

Tabel 2.9 Perbedaan BCP dan DRP (Sumber: NIST)

Perencanaan	Tujuan	Ruang Lingkup	Waktu Pelaksanaan	Fokus
Business Continuity Plan (BCP)	Menyediakan prosedur untuk mempertaha	Dibuat untuk satu unit proses bisnis saja atau	Dilaksanakan setelah dan selama	Berfokus pada proses bisnis yang berjalan di

	nkan proses operasional bisnis dari gangguan yang bersifat signifikan	seluruh unit bisnis di perusahaan/ organisasi	terjadinya gangguan	suatu organisasi/ perusahaan
Disaster Recovery Plan (DRP)	Menyediakan prosedur untuk melakukan relokasi operasional ke lokasi alternatif	Dibuat untuk mengatasi sistem informasi yang mengalami gangguan dan membutuhkan relokasi tempat	Dilaksanakan setelah terjadinya gangguan	Berfokus pada sistem informasi yang di implementasikan suatu organisasi/ perusahaan

Banyak yang masih tidak dapat membedakan antara BCP dengan DRP, masyarakat masih menganggap bahwa kedua hal tersebut adalah hal yang sama. Dilihat dari tahapannya, kedua hal ini jelas memiliki perbedaan yang signifikan. Berikut adalah perbedaan antara BCP dan DRP menurut Usep Solehudin [5]:

Tahapan dari Business Continuity Planning:

- Project Initiation
- Risk Assessment
- Business Impact Analysis
- Mitigation Strategy Development
- Plan Development
- Training,Testing, Auditing
- Plan Maintenance

Sementara tahapan dari Disaster Recovery Planning adalah sebagai berikut:

1. *Risk Assessment*
2. *Priority Assessment*
3. *Recovery Assesment*
4. *Plan Documentation*

BCP memiliki cakupan yang lebih luas yaitu untuk merencanakan keberlangsungan bisnis. DRP sendiri merupakan suatu perencanaan yang mendukung BCP untuk memulihkan proses bisnis dari gangguan yang terjadi. BCP harus dikoordinasikan dengan pemilik sistem informasi sehinggga terjadi kesinambungan antara ekspektasi BCP dengan kapabilitas sistem informasi. Berikut merupakan penjelasan dari tahapan-tahapan pada penjelasan diatas [11]:

1. Project Intiation
   Fase awal dari pembuatan perencanaan adalah Project Initiation, tahapan awal ini sangat penting karena pada tahap ini dilakukan penentuan titik awal dan akhir dari pembuatan perencanaan BCP/DRP, tujuan, kebutuhan, target-target serta perencanaan awal dari proyek.

2. Risk Assessment
   Pada fase ini dilakukan penggalian data mengenai risiko-risiko yang berpotensi terjadi pada suatu organisasi. Dilakukan juga penilaian dari risiko-risiko yang telah ditemukan pada sebelumna, risiko ini sendiri dapat berupa risiko yang ukurannya kecil hingga yang besar seperti bencana alam.

3. Business Impact Analysis
   Dari hasil risiko yang telah dianalisa pada proses sebelumnya, akan dilakukan analisis terhadap dampak yang harus dihadapi suatu organisasi apabila risiko itu terjadi. BIA mengidentifikasi layanan yang paling penting bagi organisasi sehingga dapat memberikan masukan penting bagi strategi perusahaan demi kelancaran proses bisnis organisasi.

4. Mitigation Strategy Development
   Pada fase ini dilakukan pengambilan langkah-langkah untuk mengurangi efek atau akibat dari risiko yang terjadi. Mitigasi risiko adalah proses umum yang digunakan dalam manajemen risiko bisnis tradisional, terdapat aspek unik untuk mitigasi risiko yang berkaitan dengan BCP dan DRP. Tahap Mitigation Strategy Development pengembangan strategi mitigasi

kelangsungan bisnis dan proyek pemulihan bencana rencana, adalah tahap dimana dilakukan pengembangan strategi untuk menerima, menghindari, mengurangi, atau mentransfer risiko yang berkaitan dengan gangguan bisnis potensial.

5. BC/DR Plan Development
   Mulai membangun perencanaan business continuity/disaster recovery dimulai dengan membuat outline metodologi perencanaan yang akan digunakan. Keluaran dari proses ini adalah rancangan dokumen BCP yang sesuai dengan standar dan best practice serta kebutuhan organisasi.

6. Training, Testing, Auditinya BC/DR Plan
   Memberikan informasi dan melakukan pelatihan kepada karyawan organisasi atau perusahaan terkait bagaimana melakukan implementasi dari perencanaan. Serta melakukan pengujian dan audit dari perencanaan yang telah dibuat.

7. BC/DR Plan Maintenance
   Menjaga kevalidan BCP/DRP dengan melakukan peninjauan kembali dan memperbarui perencanaan apabila ada proses bisnis yang berubah.

Berikut adalah tahapan Disaster Recovery Planning [5]:

1. *Risk Assessment*
   Risk Assessment adakah proses identifikasi ancaman-ancaman yang mungkin terjadi, baik yang berasal dari dalam, maupun dari luar. Bencana yang dianalisa termasuk bencana alam, bencana kegagalan teknis, maupun ancaman-ancaman faktormanusia. Risk Assessment berperan penting untuk keberlangsungan pembangunan keseluruhan Disaster Recovery Planning karena dapat dianggap sebagai landasan awal yang akan mempengaruhi tahapan-tahapan selanjutnya. Risk Assessment biasanya diikuti dengan Impact Analysis, dimana kemungkinan-kemungkinan bencana yang sudah teridentifikasi kemudian dianalisis dampaknya.

2. *Priority Assessment*
   Saat suatu bencana terjadi dan mengganggu berbagai macam proses bisnis dan operasi, sangatlah penting untuk memiliki urutan prioritas proses yang jelas. Proses yang dianggap paling vital untuk keberlangsungan sistem nantinya akan mendapatkan alokasi perhatian paling besar untuk dipulihkan kembali sebelum proses-proses lainnya. Dengan demikian tujuan dari pembangunan Disaster Recovery Plan, yaitu untuk memastikan sistem dapat berfungsi sebaik mungkin secepat mungkin setelah gangguan suatu bencana, dapat terlaksana. Priority Assessment untuk proses biasanya sangat relatif terhadap waktu dan tempat terjadinya suatu bencana. Penentuan prioritas pada tahap ini sangat krusial dan berkaitan dengan eksekusi Disaster Recovery Plan di lapangan nantinya bila terjadi bencana, tahapan ini harus dilakukan dengan hati-hati dan melalui berbagai macam pertimbangan yang matang

3. *Recovery Strategy Selection*
   Pemilihan strategi pemulihan haruslah dipertimbangkan dengan seksama. Strategi pemulihan yang baik harus memenuhi beberapa kriteria, yaitu:
   - Strategi pemulihan harus memenuhi key requirement yang sudah didefinisikan di tahap sebelumnya.
   - Strategi pemulihan harus cost effective berbanding dengan risiko dan prioritasnya
   - Strategi pemulihan harus dapat diterapkan dengan kondisi yang terdapat sekarang dan memungkinkan untuk ditingkatkan jika teknologi atau bisnis yang terkait berkembang di masa depan. Strategi pemulihan yang sudah dirancang kemudian harus dituangkan ke dalam Disaster Recovery Plan yang terdokumentasi secara baik sehingga dapat dengan mudah dilaksanakan jika suatu saat terjadi bencana.

4. *Plan Documenting*
   Hasil analisa dan rancangan strategi yang sudah dihasilkan dari tahapan-tahapan sebelumnya harus didokumentasikan dengan

baik, sehingga saat kembali terjadi bencana di masa depan, dan sumber daya manusia atau karyawan yang bekerja pada organisasi tersebut dapat mengikuti dokumen DRP yang sebelumnya telah di dokumentasikan. Karena itu Disaster Recovery Plan haruslah didokumentasikan dengan terstruktur sehingga mudah dipahami saat dibutuhkan. Tersedia berbagai macam standar untuk mendokumentasikan sebuah Disaster Recovery Plan. Toolkit dan pedoman-pedoman penyusunan dokumen Disaster Recovery Plan pun banyak tersedia.

2.14 Kerangka Kerja Business Continuity Management Griffith University

Griffith University adalah salah satu universitas penelitian yang berada pada Queensland, Australia. Universitas yang berdiri sejak 1971 ini menawarkan lebih dari 300 gelar sarjana, pascasarjana dan penelitian di berbagai bidang sebagai berikut: humaniora, pendidikan, hukum, bisnis, sains, musik, seni rupa, dan kesehatan.

Griffith University mempublikasikan standar yang telah dirancang mengenai kerangka kerja keberlangsungan bisnis yang difokuskan untuk universitas atau organisasi pendidikan. Kerangka kerja BCM ini juga diimplementasikan pada Griffith University dan telah disetujui oleh dewan universitas, untuk mengikuti perkembangan dan kesesuaian dengan teknologi terbaru, akan dilakukan review setiap 5 tahun sekali terhadap kerangka kerja ini [19]. Dalam implementasinya, penyusunan kerangka ini mengacu kepada beberapa standar internasional seperti:

- AS/NZS 5050:2010 *Business Continuity – Managing disruption-related risk*
- ISO 22301 *Societal Security – Business Continuity Management Systems*

Alasan mengapa peneliti menggunakan kerangka kerja BCP Griffith University sebagai kerangka acuan untuk penelitian ini adalah karena standar ini menggunakan studi kasus organisasi pendidikan yang dimana relevan dengan studi kasus pada

penelitian ini yaitu LPTSI yang juga merupakan salah satu organisasi pendidikan. Kerangka kerja Griffith University ini dapat menjadi salah satu acuan dikarenakan studi kasus sejenis yang diharapkan dapat membantu penelitian ini. BCP merupakan suatu perencanaan yang bersifat unik yang mana akan berbeda untuk masing-masing organisasi. Untuk itu selain standar utama, maka diperlukan standar BCP yang memang dikhususkan untuk pembuatan kerangka kerja BCP untuk organisasi pendidikan sehingga nantinya hasil penelitian akan lebih relevan dan sesuai dengan kebutuhan organisasi.

2.14.1 Definisi BCP Menurut Griffith University

BCP merupakan suatu fungsi dalam program keberlangsungan bisnis, pada BCP dilakukan identifikasi terhadap bencana dan kerentanan dari universitas atau organisasi dan merupakan sebuah proses kontinyu atau terus menerus, BCP memperkirakan terjadinya bencana, potensi konsekuensi terhadap tujuan dan keberhasilan strategi, keefektifan kontrol yang berlaku dan strategi untuk meningkatkan kinerja dan efisiensi. BCP juga mempertimbangkan risiko yang terjadi saat suatu lokasi kerja, staff, aset atau proses yang tidak tersedia atau tidak dapat berfungsi.

Menurut Griffith University berikut adalah alasan mengapa BCP perlu untuk diimplementasikan pada universitas atau organisasi pendidikan :

- Agar memiliki perencanaan terhadap kapabilitas keberlangsungan bisnis akan membuat organisasi dapat lebih bertindak proaktif yang mana dapat meningkatkan citra universitas pada pelajar, pekerja dan pihak lain yang terkait secara internal maupun eksternal
- Agar organisasi mendapatkan pemahaman lebih baik mengenai inter-relasi antara proses inti mengajar universitas dan bagian penelitian, dukungan bisnis/layanan administratif, sumber daya dan semua proses kritis yang dibutuhkan untuk memastikan kelangsungan hidup masing-masing dari itu semua dan juga depedensi organisasi kepada pihak ketiga.

2.14.2 Konsep Kunci Dari BCP

Pada proses BCP terdapat beberapa konsep kunci yang penting agar proses perencanaan dapat berjalan dengan baik dan menghasilkan keluaran yang optimal. Konsep kunci dari proses BCP adalah sebagai berikut :

- Memahami proses bisnis (*Understand the business*)
  Untuk dapat mengembangkan BCP maka dibutuhkan pemahaman menyeluruh terhadap proses bisnis yang dibutuhkan. Hal ini termasuk mendefinisikan misi organisasi dan objektif yang memiliki target waktu, mengidentifikasi keluaran dan masukan dari proses kritis dan ketergantungan fungsi, memprioritisasi proses dan kebutuhan sumber daya dan menentukan pemasok eksternal dan kontrak perjanjian organisasi.

- Penilaian Risiko (*Assess the risks*)
  Penilaian risiko merupakan suatu aktivitas utama dalam membuat sebuah BCP. Identifikasi, analisis dan evaluasi risiko adalah langkah awal yang penting untuk dilakukan agar mendapatkan pemahaman mengenai probabilitas, dampak dan masalah terkait lainnya dari suatu gangguan atau ancaman.
- Mempersiapkan BCP (*Prepare a business continuity plan*)
  Keluaran utama pada proses business continuity (BC) atau keberlangsungan bisnis adalah suatu BCP. BCP sendiri akan didefinisikan diawal, dilakukan pengujian dan disetujui oleh manajemen. BCP akan dieksekusi sebagai respon saat terjadi suatu gangguan pada bisnis
- Pengujian Perencanaan (*Test the plan*)
  Saat terjadinya suatu gangguan pada bisnis, maka staf yang terkait harus mengetahui apa yang harus dilakukan. Staf yang memiliki peran dan tanggung jawab dalam BCP harus secara teratur mempraktekkan

peran mereka untuk melakukan pengetesan terhadap BCP. Hal ini dilakukan agar dapat memiliki pemahaman mengenai apakah BCP dapat dipraktekkan, menvalidasi kekiniannya, mengkonfirmasi kompetensinya dan melakukan pengujian terhadap asumsi mereka mengenai akses terhadap sumber daya.

2.14.3 Tujuan Utama BCP

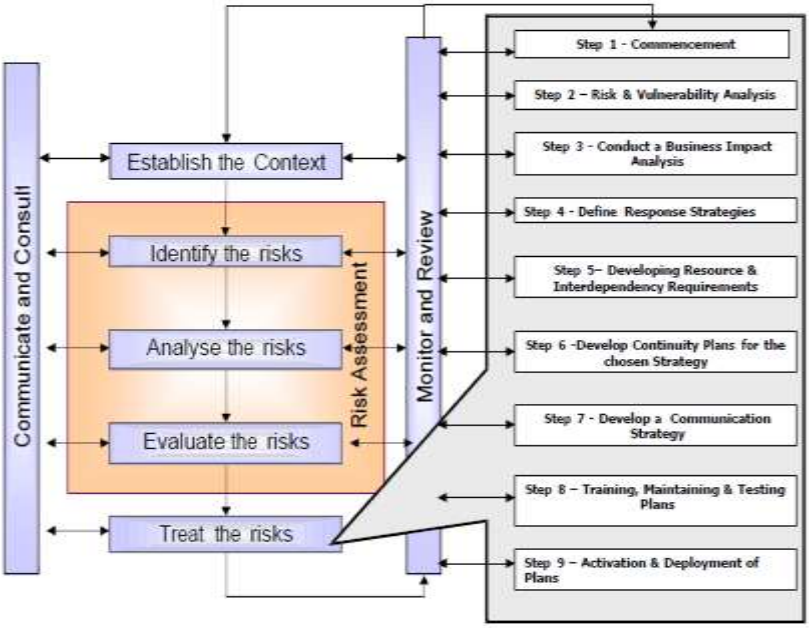
Selain memperkirakan terjadinya bencana dan potensi konsekuensi bisnis, berikut adalah tujuan utama dari BCP yang dijabarkan oleh Griffith University :

1. Mendokumentasikan bisnis proses yang kritis perlu untuk tetap berlangsung
2. Mendokumentasikan sumber daya yang dibutuhkan untuk mendukung proses – proses kritis
3. Mendokumentasikan lama waktu proses binis dapat berhenti sebelum terjadi risiko yang membayarakan atau kerugiaan pada tujuan
4. Mendokumentasikan tahapan waktu pemulihan (recovery time) dan titik data yang dapat digunakan untuk memulihkan fungsi bisnis
5. Dapat mengetahui garis besar perencanaan untuk melakukan akomodasi alternatif
6. Mendokumentasikan catatan penting dan detail penyimpanan untuk mendukung keberlanjutan bisnis
7. Membuat rantai komando, tanggung jawab personel dan personel pengganti
8. Mendokumentasikan notifikasi dan eskalasi dari prosedur

2.14.4 Metodologi Kerangka Kerja BCP Griffith University

Kerangka kerja BCP yang digunakan oleh Griffith University adalah BCP berbasis risiko yang bertujuan untuk meningkatkan pemahaman organisasi mengenai risiko yang terjadi akibat gangguan, perencanaan keberlangsungan, respon manajemen, meningkatkan kewaspadaan staf dan kompetensi untuk bekerja saat terjadi gangguan hingga fungsi sepenuhnya pulih atau

mode operasi baru telah diimplementasi. Berikut adalah metodologi yang digunakan oleh Griffith University.



Gambar 2.5 Kerangka Kerja BCP Griffith University (Sumber: Griffith University)

Berikut adalah penjelasan dari kerangka kerja BCP Griffith Univevrsity:

Tahap 1: Permulaan

Pada tahap pertama ini terdapat aktivitas konfirmasi komitmen manajemen terhadap proses penggunaan kerangka kerja BCP

Tahap 2 : Analisis Risiko dan Kerentanan

Padatahap kedua dilakukan analisis risiko dan juga kerentanan dari risiko-risiko tersebut sehngga dibutuhkan beberapa pemahaman mengenai fungsi utama universitas, proses-proses yang kritis, aset, penjelasan tentang kontribusi dari aset dan kerentanan dari suatu aset. Untuk melakukan analisis

kerentanan risiko, berikut adalah hal – hal yang perlu dilakukan oleh senior manajemen :

- Mengidentifikasi ancaman atau bencana pada keberlangsungan dan proses dari fungsi bisnis utama, sistem, informasi, sumber daya manusia, aset, partner outsource dan sumber daya lain yang mendukung atau didukung olehnya
- Menganalisa kemungkinan dan konsukuensi atau dampak dari gagngguan dan melakukan pengukuran berdasarkan yang telah ada pada kerangka kerja manajemen risiko secara sistematis
- Melakukan evaluasi terhadap gangguan berdasarkan risiko manakah yang perlu untuk ditindak lanjuti
- Mengidentifikasi tindakan yang akan dilakukan sesuai dengan tujuan keberlangsungan bisnis dan risiko universitas.

Tahap 3 : Melakukan Analisis Dampak Bisnis

Analisis dampak bisnis atau business impact analysis (BIA) merupakan suatu proses untuk mengukur tingkat kerugiaan atau kerusakan suatu operasi sepanjang waktu apabila terdapat aset yang tidak tersedia untuk mendukung proses bisnis kritis dan juga efek yang didapat untuk fungsi bisnis. Pada bagian ini dibutuhkan pemahaman mengenai fungsi utama universitas, operasi yang berjalan, proses bisnis, tingkat ekspektasi kustomer untuk dapat melakukan analisa dampak dari suatu gangguan dan dapat menentukan proses mana yang kritis untuk keberlangsungan bisnis.

BIA bertujuan untuk membangun pemahaman mengenai gangguan atau permaslaahan yang membutuhkan tindak lanjut dan memiliki kemungkinan dapat membutuhkan kapabilitas manajemen yang lebih. BIA mengidentifikasikan operasional (qualitative) dan finansial (quantitative) dari suatu gangguan dan membuat dasar pengembangan untuk keberlangsungan dan strategi pemulihan yang nantinya dapat dilakukan saat

diperlukan untuk mengembalikan operasional dalam jangka waktu yang dibutuhkan.
Keluaran dari tahap 2 dan tahap 3 sebaiknya di konsolidasi sehingga kemungkinan terjadinya gangguan dapat diasosiasikan dengan dampak secara keseluruhan dan juga mitigasi risiko. Hal ini dapat disimpan untuk dijaadikan risk register universitas.

Tahap 4 : Mendefinisikan Respon Strategi
Penentuan dan pemilihan strategi akan dilakukan berdasarkan output dari BIA dan dibuat berdasarkan maksimal penghentian perkejaan yang dapat diterima atau maximum accetable outage (MAO) yang diidentifikasi untuk masing masing proses kritis.
Respon strategi akan diinformasikan oleh jangka waktu yang disetujui untuk pemulihan dari proses kritis *(Recovery Time Objectives* – RTO). RTO adalah target waktu untuk suatu proses kritis dalam melanjutnya operasinya sebelum melebihi MAO atau mempengaruhi objektif. Dalam memilih respon strategi berikut adalah hal – hal yang perlu diperhatikan :

1. Tipe-tipe bencana yang dapat terjadi
2. Prosedur alternatif untuk dapat melanjutkan keseluruhan proses atau melanjutkan ke level minimal yang dapat diterima hingga pemulihan dapat dilakukan
3. Kemampuan untuk melakukan pengolahan manual dan biaya yang terkait
4. Penggunaan asuransi
5. Perencanaan dengan pihak ketiga, mitra bisnis dan ketergantungannya, bantuan dari sektor lain
6. Siklus bisnis dan periode puncak dari bisnis (*peak periods*)
7. Kapabilitas sumber daya internal, rantai pasok kritis dan pengelolaan vendor
8. Aksesibilitas data
9. Pilihan untuk tidak melakukan apa-apa ditentukan dari berapa kerugian yang dapat ditanggung oleh bisnis

Tahap 5 : Mengembangkan Sumber Daya & Interdependensi antar Kebutuhan

BCP akan mengindikasi kebutuhan sumber daya untuk mendukung proses kritis dan menetapkan dimana sumber daya akan saling digunakan. Berikut adalah tipe sumber daya yang termasuk didalamnya:

1. Sumber daya manusia
2. Data dan Informasi
3. Bangunan, lingkungan kerja dan keperluan terkait
4. Fasilitas, alat dan barang yang dapat dihabiskan (consumables)
5. Sistem teknologi informasi dan komunikasi (ICT)
6. Logistik dan transport
7. Keuangan
8. Partner, perencanaan dengan pihak ketiga dan pemasok

Tahap 6 : Mengembangkan Perencanaan Keberlangsungan Bisnis

Pada tahap ke enam ini dilakukan pengembangan perencanaan keberlangsungan bisnis (BCP) yang terdiri dari:

Tahap 7 : Mengembangkan Strategi Komunikasi

Bagian utama untuk mengelola adanya gangguan adalah untuk mengembangkan komunikasi yang jelas dan efektif serta strategi konsultasi. Strategi harus dilakukan dengan cara yang merefleksikan besarnya dampak bisnis. Untuk membangun strategi komunikasi, berikut adalah prosedur yang harus dibangun, diimplementasi dan dikelola oleh senior manajemen.

1. Proses kritis yang akan dilanjutkan atau dilakukan pemulihan
2. Peran dan tanggung jawab yang telah ditentukan serta kontak mengenai orang atau tim yang memiliki kewenangan pada saat dan setelah terjadinya gangguan
3. Proses permohonan dan peningkatan respon
4. Sumber daya yang dibutuhkan untuk mendukung respon
5. Strategi komunikasi
6. Hubungan saling ketergantungan antara detail

7. Detail dari pemasok atau vendor penting dan perencanaan alternatif
8. Daftar catatan yang relevan dan penting, tempat penyimpanan dan detail akses
9. Strategi untuk mengelalo kerugian atau terjadinya gangguan pada orang, properti, platform dan provider (atau kombinasi diantaranya)

Tahap 8 : Pelatihan, Pemeliharaan dan Pengujian Perencanaan

Terdapat 3 metode untuk menguji dan memastikan bahwa BCP dapat berjalan dengan baik dan dapat bertahan dari berbagai gangguan yaitu:

Pelatihan

Tahapan ini bertujuan untuk memastikan bahwa BCP yang telah dikembangkan dan didokumentasikan dapat memungkinkan unit bisnis yang kritis untuk dapat bertahan dari gangguan. Melakukan edukasi dan pelatihan merupakan komponen penting dalam perencanaan, respon dan operasi pemulihan. Berikut adalah beberapa model pelatihan yang perlu dilakukan.

1. Perencanaan dewan universitas dan tim terkait/perencanaan harian
2. Orientasi Pegawai
3. Pelatihan manajemen risiko
4. Pelatihan spesifik pada keberlangsungan bisnis (Business Continuity)
5. Pengujian evakuasai darurat

Pada penelitian, nantinya pelatihan yang akan dirancang adalah pelatihan dengan bentuk pelatihan spesifik terhadap keberlangsungan bisnis. Pelatihan ini nantinya diharapkan dapat memberikan pengetahuan kepada pegawai maupun personel yang terlibat dalam perencanaan untuk melakukan pemulihan maupun pencegahan gangguan.

Pengujiaan

Sebagai indikator kesuksesan, maka setiap BCP harus dilakukan pengujian dan dievaluasi pada secara teratur, hasil akan didokumentasi dan perbaikan akan diimplemntasi. Hal ini adalah untuk memastikan bahwa BCP tetap relevan, terkini dan efektif. Respon dan tindakan pemulihan akan dilatih dalam kondisi simulasi untuk melihat asumsi asumsi atas strategi dan perencanaan serta melatih orang yang memiliki peran dan tanggung jawab pada BCP. Berikut adalah beberapa bentuk pengujian BCP yang dapat dilakukan.

1. *Call tree Test*

Melakukan pengujian terhadap daftar nomor yang ada di kontak dan pengetahuan mengenai peran masing masing individu.

2. *Desk Check Test*

Melakukan review dari dokumen BCP

3. *Walk through Test*

Merencanakan peserta untuk melakukan wallkthrough terhadap perencanaan prosedur sebagai respon dari suatu skenario untuk menvalidasi pengetahuan peran yang dimiliki dan mengkonfirmasi kelayakan perencanaan terhadap tujuan bisnis dan lingkungan.

Pada penelitian, nantinya pengujian yang akan dirancang adalah pengujian dengan bentuk walk through test. Rancangan skenario walk through test akan dibuat untuk dapat melihat kesesuaian prosedur yang ada dengan situasi proses bisnis yang berlangsung.

Pemeliharaan

Penjadwalan untuk pemeliharaan BCP yang telah berjalan harus dibangun dan dilaporkan sebagai bagian dari proses jaminan kualitas (*quality assurance*). Senior manajemen akan bertanggung jawab untuk memastikan bahwa pemeliharaaan akan mempertimbangkan biaya, kompleksitas dan risiko serta menfasilitas pada interval yang ditetapkan setelah terjadinya gangguan.

Tahap 9 : Aktivasi dan Pelaksanaan Perencanaan

Saat suatu peritiwa bencana atau gangguan terjadi, hal ini menyebabkan aktivasi prosedur BCP. Maka senior manajemen dan beberapa personil utama akan yang terlibat akan mengumpulkan informasi dengan melakukan wawancara setelah kejadian selesai serta merekam hasil observasi dan rekomendasi untuk menginformasikan perencanaan dari tindakan selanjutnya

2.15 Direktorat Pengembangan Teknologi dan Sistem Informasi (LPTSI)

LPTSI dibentuk pada tahun 1982 dengan nama awal yaitu UPT Pusat Komputer. UPT Pusat Komputer dilengkapi dengan Honeywell Bull Mini 6 System yang merupakan salah satu sistem komputer yang cukup baik. Pada periode tersebut mulai berkembang generasi PC yang pertama yang membuat Puskom pada akhirnya mentransformasi teknologi computer mini ke teknologi PC pada tahun 1988. [1]

Pada awal tahun 1982an UPT Pusat Komputer banyak mendukung staf peneliti ITS dalam melakukan penelitian yang membutuhkan computer untuk melakukan baik data prosessing maupun menyelesaikan persamaan matematik. Mulai tahun 1992 UPT Puskom dipercaya untuk melakukan pemprosesan data test untuk masuk perguruan tinggi negeri di wilayah Indonesia

Sejak tahun 1999 UPT Pusat Komputer dimandatkan untuk mengelola ITS-net yaitu jaringan baik intranet maupun internet untuk ITS secara keseluruhan. Dengan adanya tugas tersebut maka semua data dan informasi di ITS bisa di hubungan secara menyeluruh.

Pada status yang baru 2003 UPT Pusat Komputer berfungsi sebagai unit pelaksana teknis dibidang pengelolahan data yang berada di bawah dan bertanggungjawab langsung kepada Rektor dan sehari-hari pembinaannya dilakukan oleh Pembantu Rektor I, dengan tugas mengumpulkan, mengolah, menyajikan, dan menyimpan data dan informasi serta memberikan layanan untuk program-program pendidikan, penelitian, dan

pengabdian kepada masyarakat. Dengan terbitnya SK Rektor nomor 2769.1/K03/OT/2006 tanggal 8 Juni 2006 merubah nama UPT Pusat Komputer (PUSKOM) menjadi ITS-ICT Services (ITS-Information and Comunication Technology Services) Permendikbud No.49 tahun 2011 tentang Statuta ITS dan Peraturan Rektor ITS No.03 tahun 2012 tentang OTK ITS, merubah nama ITS-ICT Services dan sekaligus menggabungkan bagian Sistem Informasi dari BAPSI, menjadi Badan Teknologi dan Sistem Informasi yang mempunyai fungsi mengelola, mengkoordinasikan, mengendalikan serta mengembangkan teknologi dan sistem informasi secara terpadu sesuai peraturan perundang-undangan.
BTSI berubah nama menjadi LPTSI (Lembaga Pengembangan Teknologi Sistem Infromasi) berdasarkan Permendikbud No. 86, Tahun 2013 tentang OTK ITS. LPTSI mempunyai tugas melaksanakan, mengkoordinasi, memonitor dan mengevaluasi kegiatan penelitian dan pengembangan teknologi dan sistem informasi.

2.15.1 Sub Direktorat Pengembangan Sistem Informasi

Sub Direktorat Pengembangan Sistem Informasi merupakan salah satu layanan yang ada pada LPTSI, suatu lembaga dibawah ITS yang bergerak sebagai pusat layanan sistem informasi di ITS. LPTSI sebagai pusat pengembangan SI/TI di ITS memiliki tugas melaksanakan, mengkoordinasi, memonitor dan mengevaluasi kegiatan penelitian dan pengembangan teknologi dan sistem informasi. Sub Direktorat Pengembangan Sistem Informasi memiliki tugas pokok fungsi yaitu menyediakan dan mengelola aplikasi sistem informasi berbasis web untuk mengoptimalkan e-layanan.
Capaian yang dicapai Sub Direktorat Pengembangan Sistem Informasi Tahun 2012-2015 antara lain: inventarisasi asset sistem informasi yang dimiliki ITS dan pengalihan pengelolaan beberapa SIM yang dikembangkan pihak ketiga ke LPTSI, pengembangan sistem baru, implementasi sistem yang telah dikembangkan, penyempurnaan dan pengembangan beberapa sistem yang telah ada [20].

Rincian capaian dari masing-masing capaian dijelaskan sebagai berikut.

1. Inventarisasi aset SIM yang dimiliki ITS
2. Pengembangan SIM baru
3. Pengembangan SIM yang ada sebelumnya
4. Penerapan/Implementasi SIM yang dibangun

Capaian Sub Direktorat Pengembangan Sistem Informasi sampai tahun 2015 adalah

1. Saat ini telah ada 52 sistem informasi yang mendukung proses bisnis di ITS
2. Sejumlah 19 sistem informasi telah terintegrasi ke Integra

Jumlah pengelola sistem informasi yang ada di di ITS

1. 16 sistem informasi (31%) dikelola oleh pegawai tetap LPTSI
2. 22 sistem informasi (425) dikelola oleh tenaga harian lepas (THL) atau pegawai kontrak di LPTSI
3. 14 sistem informasi (27%) dikelola oleh unit selain LPTSI

Walaupun telah memiliki aset teknologi informasi yang berjalan, Sub Direktorat Pengembangan Sistem Informasi belum memiliki manajemen risiko teknologi informasi maupun perencanaan keberlangsungan bisnis atau business continuity plan (BCP) untuk teknologi informasi di organisasi. Padahal banyak gangguan, ancaman bahkan bencana yang dapat muncul dan merugikan organisasi dalam segi biaya maupun waktu bahkan bisa melumpuhkan proses bisnis organisasi. Sub Direktorat Pengembangan Sistem Informasi membutuhkan sebuah business continuity plan (BCP) berbasis profil risiko untuk membantu bagian TI organisasi agar dapat merespon terhadap risiko yang muncul dan untuk menjaga berjalannya operasional bisninsya. Setiap organisasi memiliki kebutuhan yang berbeda-beda, sehingga BCP antara satu organisasi dengan yang lain akan berbeda – beda pula. Kerangka BCP yang dibuat harus sesuai dengan kebutuhan dan juga kondisi

kekinian organisasi untuk memudahkan organisasi dalam menjaga keberlanjutan proses bisnisnya.

2.16 Penentuan Strategi BCP

Pada penelitian ini pembuatan strategi BCP dilakukan dengan menggunakan referensi dari Standar Cisco dan Standard Operating Procedure Incident Handling Database yang dibuat oleh Indonesia Government Computer Security Incident Response Team (Gov-CSIRT).

2.16.1 Cisco

Cisco merupakan sebuah perusahaan yang bergerak pada pembuatan hardware dan software yang berhubungan dengan jaringan komputer, selain itu Cisco juga menyediakan sebuah edukasi yang ditujukan kepada sumber daya manusia TI untuk dapat mengoperasikan, mengimplementasi, dan menjaga keamanan dari perangkat TI [21]. Untuk dapat memberikan informasi kepada SDM TI serta pengguna TI untuk menjaga keamanan dari infrastruktur TI, Cisco membuat sebuah panduan untuk penanganan insiden keamanan terkait TI. Insiden pada keamanan data mungkin bisa disebabkan karena beberapa hal seperti pencurian, pembobolan, dan manipulasi data. Semua gangguan tersebut harus ditangani sesuai dengan prosedur yang sesuai standar.

Rekomendasi strategi yang diambil dari strategi Cisco adalah untuk risiko manipulasi data oleh *hacker* pada strategi saat terjadi gangguan. Strategi yang diambil dari Cisco adalah mengidentifikasi kerusakan yang terjadi, proses restore data, pemulihan terhadap metode akses, dan menonaktifkan sistem.

2.16.2 Indonesia Government Computer Security Incident Response Team

Government Computer Security Insident Respon Team merupakan suatu team yang dibentuk Badan Pengkajian dan Penerapan Teknologi, Kementrian Riset, Teknologi, dan Pendidikan Tinggi, dalam rangka melakukan respon atas

berbagai permasalahan dalam bidang Teknologi Informasi, terutama dalam menangani masalah keamanannya [21]. Gov-CSIRT merupakan tim koordinasi teknis terkait insiden jaringan internet dengan ruang lingkup terbatas untuk kalangan tertutup yang dibangun oleh institusi pemerintahan.

Gov-CSIRT mengeluarkan dokumen *standard operating procedure* yang berkaitan tentang *incident management*. Dokumen tersebut berisikan tahapan untuk membantu organisasi memahami tentang penanganan suatu insiden yang terjadi pada data-data yang dimiliki oleh organisasi. Prosedur ini menetapka suatu proses untuk penanganan insiden keamanan data. Insiden pada keamanan data mungkin bisa disebabkan karena beberapa hal seperti pencurian, pembobolan, dan manipulasi data. Semua gangguan tersebut harus ditangani sesuai dengan prosedur yang sesuai standar [23].

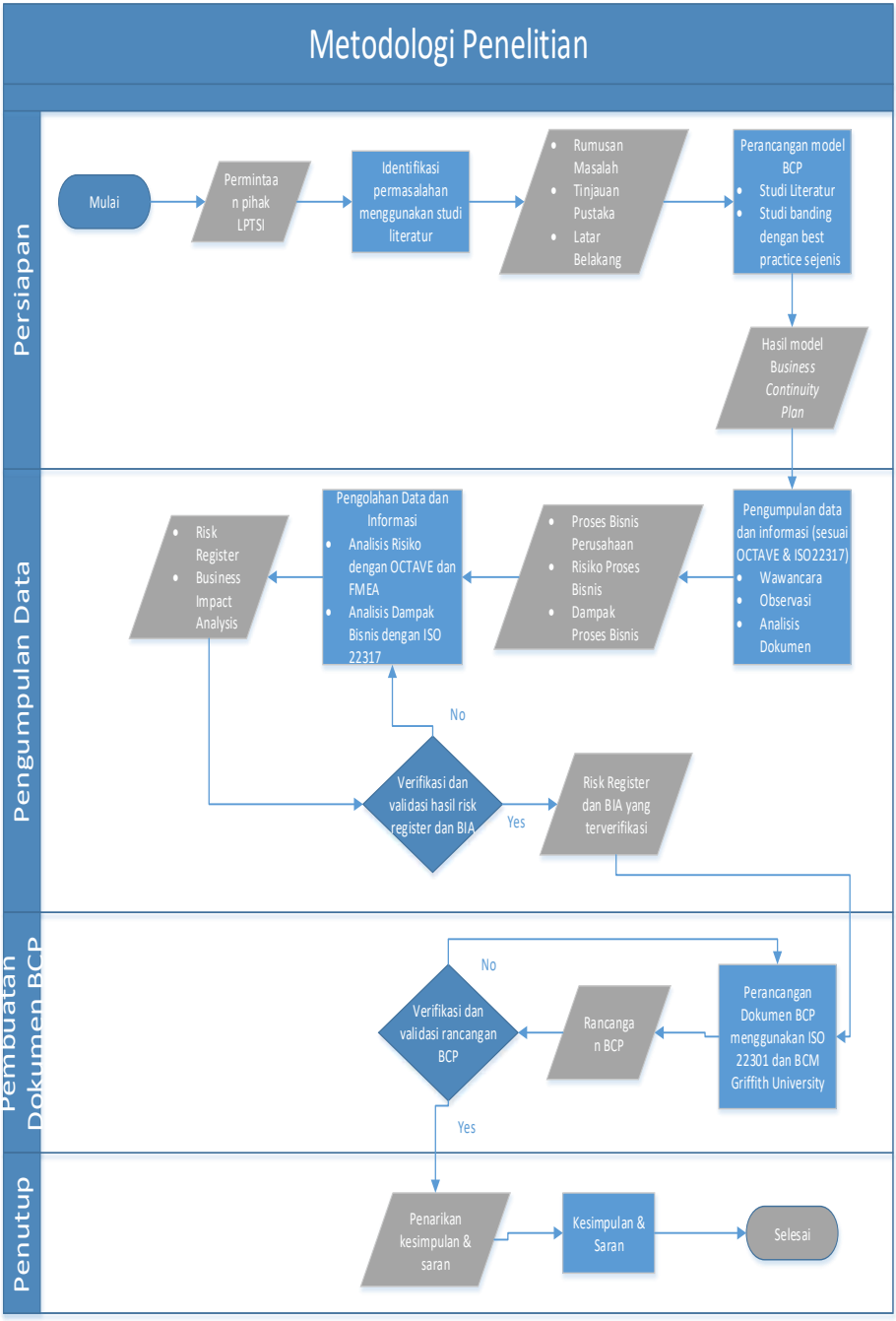
Rekomendasi strategi yang diambil dari strategi Gov-CSIRT adalah untuk risiko server tidak beroperasi dan manipulasi data Strategi yang diambil dari GOC-CSIRT adalah untuk strategi preventif, saat terjadi gangguan, dan korektif untuk risiko server tidak beroperasi, lalu strategi preventif dan korektif untuk risiko manipulasi data.

"Halaman ini sengaja dikosongkan"

BAB III
METODOLOGI PENELITIAN

Bab ini menggambarkan metodologi yang akan digunakan selama penelitian, termasuk tahapan yang dilakukan dalam penyusunan kerangka *Business Continuity Plan* (BCP).

Tabel 3.1 Metodologi Penelitian (Sumber: Peneliti, 2016)


Metodologi Penelitian
Persiapan
Mulai
Permintaan pihak LPTSI
Identifikasi permasalahan menggunakan studi literatur
Rumusan Masalah
Tinjauan Pustaka
Latar Belakang
Perancangan model BCP
Studi Literatur
Studi banding dengan best practice sejenis
Hasil model Business Continuity Plan
Pengumpulan Data
Pengumpulan data dan informasi (sesuai OCTAVE & ISO22317)
Wawancara
Observasi
Analisis Dokumen
Proses Bisnis Perusahaan
Risiko Proses Bisnis
Dampak Proses Bisnis
Pengolahan Data dan Informasi
Analisis Risiko dengan OCTAVE dan FMEA
Analisis Dampak Bisnis dengan ISO 22317
Risk Register
Business Impact Analysis
No
Verifikasi dan validasi hasil risk register dan BIA
Yes
Risk Register dan BIA yang terverifikasi
Pembuatan Dokumen BCP
Perancangan Dokumen BCP menggunakan ISO 22301 dan BCM Griffith University
Rancangan BCP
No
Verifikasi dan validasi rancangan BCP
Yes
Penutup
Penarikan kesimpulan & saran
Kesimpulan & Saran
Selesai

3.1 Identifikasi Permasalahan

Tahap Identifikasi merupakan langkah awal untuk memulai penyusunan tugas akhir ini. Masukkan dari permasalahan yang terdapat pada penelitian ini datang dari permintaan manajemen perusahaan, mengenai pentingnya manajemen risiko pada departemen teknologi informasi perusahaan serta implementasi BCP (*Business Continuity Plan*) bagi Direktorat Pengembangan Sistem Informasi.
Proses identifikasi permasalahan ini didukung dengan adanya studi literatur yang dilakukan untuk memperkuat data dan sebagai referensi untuk memberikan aspek integritas pada penelitian ini. Tahapan ini akan menghasilkan rumusan permasalahan serta latar belakang penelitian yang dijadikan sebagai bahan dasar untuk memulai penelitian ini.

3.2 Perancangan Model BCP

Berdasarkan rumusan masalah dan literatur yang ada, proses selanjutnya adalah perancangan model BCP berdasarkan studi literatur dan studi banding dengan standar serta best practices yang ada, untuk menghasilkan model BCP terbaik yang sesuai dengan kebutuhan Sub Direktorat Pengembangan Sistem Informasi. Standar yang digunakan adalah berdasarkan ISO 22301:2012 dan best practices yang digunakan adalah berdasarkan penerapan BCP pada organisasi pendidikan lainnya.

3.3 Pengumpulan Data

Terdapat beberapa metode pada tahap pengumpulan data, tahap ini diantaranya dilakukan dengan cara wawancara, observasi peneliti serta analisis dokumen perusahaan. Pada tahap ini akan dilakukan proses verifikasi kepada pihak perusahan untuk dapat memastikan kebenaran pada data dan informasi yang didapat serta dapat dipertanggung jawabkan.

3.3.1 Wawancara

Tahap wawancara akan dilakukan kepada narasumber terkait yang memiliki pengetahuan tentang teknologi informasi yang ada pada Sub Direktorat Pengembangan Sistem Informasi. Wawancara akan dilakukan untuk dapat melakukan pengumpulan data dan informasi yang dibutuhkan pada penelitian ini. Pada metode wawancara akan digali informasi mengenai proses bisnis, kondisi organisasi, risiko proses bisnis dan dampak proses bisnis. Proses pengumpulan data disesuaikan dengan standar acuan yang terkait, yaitu OCTAVE dan ISO 22317.

3.3.2 Observasi Peneliti

Tahap observasi dilakukan pada saat peneliti mengumpulkan data untuk menganalisis risiko. Di mana, pada tahapan identifikasi risiko, diperlukan pengamatan untuk bisa mengidentifikasikan dengan tepat, risiko teknologi informasi yang mungkin muncul pada perusahaan tersebut. Pengamatan juga dilakukan terhadap kinerja dan aktivitas yang ada pada Sub Direktorat Pengembangan Sistem Informasi untuk menggali informasi mengenai risiko proses bisnis agar dapat menentukan BCP yang sesuai untuk kebutuhan.

3.3.3 Analisis Dokumen Perusahaan

Pada tahap ini peneliti akan mempelajari beberapa dokumen yang dimiliki perusahan agar dapat melakukan analisis yang lebih akurat. Dokumen seperti prosedur, kebijakan dan laporan tahunan ini dapat menjadi bahan peneliti untuk dapat memperdalam pengetahuan mengenai lingkungan organisasi serta proses bisnis. Hasil analisis dokumen tersebut nantinya akan dihasilkan data proses bisnis organisasi, dampak dari masing masing aktivtas proses bisnis serta ancaman yang terjadi pada proses binis.

3.4 Pengolahan Data

Berdasarkan informasi proses bisnis, dampak dan risiko dalam proses bisnis perusahaan, maka proses selanjutnya adalah mengolah data dan informasi yang telah dimiliki. Terdapat dua

bagian dalam proses ini yaitu melakukan analisis dampak bisnis dan analisis risiko.

3.4.1 Analisis Dampak Bisnis dengan ISO 22317:2015

Pada tahapan ini akan dilakukan identifikasi dari proses bisnis organisasi dan dampak yang akan didapatkan perusahaan apabila terjadi gangguan pada aktivitas proses bisnis tersebut. Analisis ini akan dilakukan dengan menggunakan acuan ISO 22317:2015. Analisis dampak bisnis akan dilihat dari layanan dan produk, proses dan aktivitas yang berjalan pada organisasi. Sehingga proses ini akan menghasilkan prioritisasi proses bisnis yang paling kritis dan penting bagi organisasi.

ISO 22317 :2015 adalah spesifikasi teknis internasional yang merekomendasikan mengenai panduan dan langkah yang diperlukan suatu organisasi dalam membangun, mengimplementasi dan menjaga dokumentasi dan formalitas dari proses analisis dampak bisnis (business impact analysis). ISO 22317:2015 ini dapat diterapkan pada semua tipe, jenis dan sifat organisasi [16].

Keluaran dari proses ini akan menghasilkan tabel Business Impact Analysis (BIA) yang akan digunakan untuk tahapan perancangan BCP.

3.4.2 Analisis Risiko dengan FMEA

Setelah dilakukan proses identifikasi risiko, maka akan dilanjutkan dengan melakukan penilaian terhadap risiko-risiko yang ada. Penilaian ini nantinya akan menggunakan metode (*Failure Mode and Effect Analysis*) dengan melakukan perhitungan nilai dampak (*severity*), nilai kemungkinan (*occurence*) dan nilai deteksi (*detection*). Perhitungan ini akan diberikan untuk setiap risiko SI/TI yang telah diidentifikasi. Setelah itu perhitungan nilai prioritas risiko atau risk priority number dilakukan dengan melakukan perkalian terhadap dampak, kemungkinan dan deteksi (kecenderungan x dampak x deteksi). Dari hasil penilaian tersebut akan terbentuk grafik yang menggambarkan urutan skor dari prioritas risiko. Pada BCP yang akan dirancang, risiko yang digunakan untuk

penyelesaian masalah hanyalah risiko IT yang berada pada nilai high atau yang menjadi prioritas dari manajemen.
Keluaran dari proses ini akan menghasilkan tabel risk register yang akan digunakan untuk tahapan perancangan BCP.

3.4.3 Verifikasi

Tahapan verifikasi dilakukan dengan meninjau kesesuaian risk register dan business impact analysis dengan standar dan best practice yang akan digunakan. Tahapan ini adalah suatu kontrol yang dilakukan untuk memastikan bahwa hasil telah sesuai dengan standar yang digunakan.

3.4.4 Validasi

Tahapan validasi merupakan tahapan yang memastikan bahwa hasil keluaran dari proses pengolahan data dan informasi yaitu risk register dan BIA telah sesuai dan diterima oleh organisasi. Validasi dilakukan dengan melakukan konfirmasi risk register dan BIA kepada Sub Direktorat Pengembangan Sistem Informasi. Hasil yang diharapkan nantinya adalah risk register dan business impact analysis telah sesuai dengan kebutuhan organisasi.

3.5 Rancangan Dokumen BCP

Perancangan BCP pada LPTSI dilakukan dengan menerapkan model BCP yang telah diformulasikan dari standar ISO dan best practice untuk dijadikan sebuah kerangka yang nantinya akan dapat diimplementasikan perusahaan. Proses perancangan ini memiliki masukan yaitu tabel risk register dan juga business impact analysis. Dari kedua masukan tersebut akan dirancang dokumen BCP yang dibuat menggunakan acuan standar ISO 22301 dan juga Kerangka Kerja BCM Griffith University, penelitian menggunakan proses plan-do-check-act sesuai dengan acuan ISO 22301 yang masing-masing fasenya diisi sesuai dengan ketentuan pada ISO 22301 sendiri dan juga Kerangka Kerja BCM Grifffith University. Proses dimulai dari melakukan penentuan tujuan, ruang lingkup serta sumber daya manusia dalam perusahaan.

3.5.1 Verifikasi BCP

Tahap verifikasi BCP dilakukan dengan melihat BCP yang telah dibuat dan dilihat kesesuaian rancangan BCP dengan standar dan best practice yang akan digunakan dan juga dengan analisis risiko dan business impact analysis yang telah dilakukan.

3.6 Validasi BCP

Pada tahap validasi dokumen BCP diberikan kepada perusahaan sebagai bentuk persetujuan bahwa hasil dari penelitian dapat diterima dan diimplementasikan. Validasi dilakukan dengan melakukan konfirmasi mengenai hasil rancangan BCP kepada kepala organisasi dan juga bagian teknologi informasi. Dalam proses validasi ini juga dilakukan pengujian BCP untuk memastikan kesesuaiannya. Proses validasi ini adalah proses yang krusial karena merupakan bentuk persetujuan dari manajemen organisasi bahwa rancangan BCP telah menjawab kebutuhan organisasi.

Setelah rancangan BCP divalidasi maka proses akan berlanjut ke dokumentasi BCP dan penarikan kesimpulan. Namun, jika menurut organisasi hasil rancangan BCP belum valid maka akan kembali dilakukan ke tahap perancangan BCP hingga BCP sesuai dengan kebutuhan perusahaan.

3.7 Dokumentasi BCP dan Penarikan Kesimpulan

Tahapan akhir dalam penelitian ini adalah melakukan dokumentasi tugas akhir yaitu pembuatan dokumentasi dan penarikan kesimpulan BCP. Pendokumentasian tugas akhir adalah hal yang sangat penting, karena dengan adanya pendokumentasian yang rapi dan jelas, akan dapat dijadikan acuan yang baik bagi perusahaan. Selain itu, pendokumentasian tugas akhir dilakukan untuk memudahkan peneliti dalam memeriksa kekurangan atau hal-hal yang belum sesuai dengan tujuan penyusunan tugas akhir

“Halaman ini sengaja dikosongkan”

BAB IV
PERANCANGAN

4.1 Fungsional Bisnis yang Terlibat dalam Penlitian

Pada Subdirektorat Pengembangan Sistem Informasi terdapat 3 fungsional bisnis yang berada dibawah ketua dari Subdirektorat itu sendiri, yaitu bagian Developer, Analyst, dan Dokumentasi. Alasan peneliti memilih 3 fungsional tersebut adalah berdasarkan hasil wawancara dengan Ketua Subdirektorat, terdapat 4 fungsional yang menjalankan proses bisnis utama dari Subdir. Selain itu 3 fungsional bisnis ini juga telah memiliki ketergantungan pada sistem informasi dan teknologi informasi untuk menjalankan proses bisnisnya. Berikut adalah penjelasan dari fungsional bisnis yang terkait dalam pembuatan BCP di penelitian ini:

1. **Developer**

   Developer merupakan bagian yang melakukan seluruh aktvitas yang berkaitan dengan kode untuk pembuatan sistem informasi di Subdirektorat Pengembangan Sistem Informasi. Developer melakukan pengembangan SIM baru yang sesuai dengan kebutuhan ITS serta melakukan penambahan fitur dari SIM yang ada untuk meningkatkan optimalitas.

2. **Analyst**

   Analyst bertugas untuk mengevaluasi kegiatan-kegiatan proses bisnis perusahaan untuk mengidentifikaso dampak dari kegiatan tersebut. Analyst membantu dalam mempersiapkan segala kebutuhan yang digunakan untuk pembentukan SIM.

3. **Dokumentasi**

   Dokumentasi merupakan bagian yang melakukan pencatatan tentang segala aktivitas dan sistem informasi dalam Sub Direktorat.

4.2 Proses Bisnis yang Terlibat dalam Penelitian

Dari ketiga fungsional bisnis yang terdapat pada Sub Direktorat Pengembangan Sistem Informasi, akan dijelaskan lebih lanjut mengenai proses bisnis dari masing masing fungsional yang terkait dengan tujuan dari organisasi. Proses-proses berikut merupakan proses yang dianggap penting bagi keberlangsungan proses bisnis organisasi. Berikut merupakan proses bisnis terkait sistem dari ketiga fungsional bisnis yang ada.

Tabel 4.1 Proses Bisnis Terkait Fungsional Bisnis

Fungsional Bisnis	Proses Bisnis Terkait Sistem
Developer	Menyediakan aplikasi sistem informasi berbasis web
	Mengelola aplikasi sistem informasi berbasis web
	Melakukan pengujian program atau modul sistem informasi
	Memaksimalkan kinerja aplikasi sistem informasi
	Menyelesaikan keluhan terkait sistem informasi di ITS
Analyst	Menganalisis proses bisnis organisasi
	Memaksimalkan kinerja aplikasi sistem informasi
Dokumentasi	Menyediakan aplikasi sistem informasi berbasis web
	Memaksimalkan kinerja aplikasi sistem informasi
	Melakukan dokumentasi keluhan terkait sistem informasi di ITS

4.3 Persiapan Pengumpulan Data

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

4.3.1 Wawancara

Proses wawancara akan dilakukan pada dua layanan yang terdapat pada LPTSI yaitu Sub Direktorat Pengembangan Sistem Informasi dan Pusat Infrastruktur dan Keamanan Teknologi Informasi. Diharapkan setelah melakukan wawancara akan didapatkan informasi terkait risiko TI yang dihadapi oleh perusahaan.

Tabel 4.2 Ketentuan Wawancara

Nama Proses	**Pengumpulan Data dan Informasi**
Teknik	*Interview*/Wawancara Teknik wawancara akan dilakukan dengan metode tanya jawab langsung dengan narasumber. Wawancara akan dilakukan secara terstruktur, dimana peneliti telah menyiapkan pertanyaanpertanyaan yang dibutuhkan terlebih dahulu.
Objek	Kondisi kekinian organisasi, proses bisnis organisasi, aset TI, risiko proses bisnis dan dampak terhadap proses bisnis kritis.
Kebutuhan Proses	- Interview Protocol - Laptop - Alat perekam
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

1. Jumlah dan Tujuan Wawancara

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

Tabel 4.3 Jumlah dan Tujuan Wawancara

Wawancara Ke-	Narasumber	Tujuan Wawancara
1	Anny Yuniarti, S.Kom.,M.Comp.Sc	Wawancara dilakakukan untuk mengetahui kondisi kekinian, proses bisnis, serta informasi mengenai penerapan teknologi infromasi dari Sub Direktorat Pengembangan Sistem Informasi.
2	Royyana M Ijtihadie, S.Kom.,M.Kom.,Ph.D	Pada wawancara ini akan digali lebih dalam lagi mengenai aset serta risiko TI yang terdapat pada DPTSI. Dilakukan juga identifikasi aset TI, kebutuhan keamanan, keamanan TI yang telah diterapkan, kelemahan risiko identifikasi ancaman dan risiko serta dampak terhadap proses bisnis kritis apabila terkena gangguan.
3	Cahya Purnama Dani, A.Md.	Dilakukan identifikasi aset TI, kebutuhan keamanan, keamanan TI yang telah diterapkan, identifikasi ancaman dan risiko, kelemahan organisasi serta dampak terhadap proses bisnis kritis apabila terkena gangguan.

2. Profil Narasumber Wawancara

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

Tabel 4.4 Profil Narasumber

Nama	Jabatan
Anny Yuniarti, S.Kom.,M.Comp.Sc	Ketua SubDirektorat Pengembangan Sistem Informasi
Royyana M Ijtihadie, S.Kom.,M.Kom.,Ph.D	Ketua SubDirektorat Infastruktur dan Keamanan Teknologi Informasi

3. Daftar Pertanyaan Wawancara (*Interview Protocol*)
Berikut merupakan daftar pertanyaan yang tercantum pada *interview protocol*

Tabel 4.5 Daftar Pertanyaan Wawancara

No.	Tujuan Pertanyaan	Standar Acuan Terkait	Detail pertanyaan
1.	Untuk mengetahui proses bisnis dan kondisi kekinian dari Subdir Pengembangan Sistem Informasi.	Tidak ada	• Proses bisnis di Sub Direktorat Pengembangan Sistem Informasi • Fungsional bisnis organisasi
2.	Wawancara dilakukan untuk melakukan identifikasi risiko, hal ini dilakukan dengan melakukan identifikasi aset TI, kebutuhan keamanan, keamanan TI yang telah diterapkan.	**OCTAVE** Fase 1 - *Build Asset-Based Threat Profile*	• Aset TI yang digunakan dalam proses bisnis kritikal • Aset TI kritikal yang dapat memberi ancaman pada organisasi • Kebutuhan keamanan TI dari organisasi • Ancaman yang mungkin terjadi kepada aset TI

			• Praktik keamanan TI yang telah dilakukan oleh organisasi • Kelemahan Organisasi
		OCTAVE Fase 2 - *Identify Infrastructure Vulnerabilities*	• Komponen aset TI yang ada di orgainsasi • Kelemahan teknis aset TI organisasi
3.	Wawancara dilakukan untuk mengidentifikasi layanan TI, proses bisnis TI dan aktivitas TI serta tingkat prioritasnya. Selain itu wawancara ini juga bertujuan untuk dapat mengetahui toleransi waktu dan dampak yang terjadi apabila adanya gangguan pada proses bisnis.	**ISO 22317** Klausa 5.3 – Prioritisasi produk dan layanan	• Layanan TI organisasi • Tingkat prioritas pada layanan TI
		ISO 22317 Klausa 5.4 – Prioritisasi Proses	• Proses bisnis yang ada pada fungsional organisasi • Prioritisasi proses bisnis
		ISO 22317 Klausa 5.5 - Prioritisasi Aktivitas	• Aktivitas yang terdapat pada proses bisnis • Prioritisasi terhadap aktivitas
		ISO 22317 Klausa 5.6 Analisis dan Konsolidasi	• Dampak yang terjadi akibat gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis)

			• Waktu yang ditoleransi organisasi terkait gangguan • Respon organisasi terhadap proses bisnis kritis bila terjadi gangguan?

4.4 Pengolahan Data dan Informasi

Proses selanjutnya setelah melakukan pengumpulan data adalah pengolahan data dan informasi. Di dalam proses ini terdapat dua analisis utama yang dilakukan, yaitu analisis risiko dan analisis dampak bisnis.

4.4.1 Analisis Risiko

Pada penelitian ini menggunakan OCTAVE dan metode Failure Modes and Effects Analysis (FMEA) untuk mengidentifikasi serta menilai risiko. Nantinya beberapa fase yang akan dilakukan untuk melakukan penilaian risiko tersebut adalah

1. Identifikasi Risiko

Dalam melakukan identifikasi risiko, metode yang digunakan dalam penelitian adalah metode OCTAVE. Metode Octave sendiri nantinya dibagi menjadi beberapa tahapan antara lain adalah :

Fase 1 – Membangun profil ancaman berbasis risiko

Pada tahapan ini akan dikumpulkan informasi dari pihak senior management dan pihak operasional untuk dapat menentukan aset kritis, kebutuhan keamanan, ancaman dan kelemahan maupun kelebihan dari kondisi kekinian organisasi.

Output dari fase ini nantinya adalah tabel aset kritis, tabel kebutuhan keamanan untuk aset kritis, tabel
ancaman untuk aset kritis, tabel praktik keamanan yang telah diterapkan dan tabel kerentanan dari kondisi kekinian organisasi.

Fase 2 – Mengidentifikasi Kelemahan Infrastruktur

Pada tahapan ini akan dilakukan evaluasi terhadap komponen – komponen utama yang mendukung aset kritis untuk dapat melihat kerentanan dari sisi teknologi yang ada.
Output dari fase ini nantinya adalah tabel komponen utama dan tabel kerentanan teknologi.

Fase 3 – Membangun Perencanaan dan Strategi Keamanan

Pada tahapan in iakan dilakukan evaluasi terhadap risiko risiko pada aset kritis serta melakukan penilaian terhadap masing masing risiko tersebut.
Output dari fase ini nantinya adalah tabel risiko dari aset kritis dan tabel pengukuran risiko
Penilaian risiko pada penelitian menggunakan metode FMEA, FMEA merupakan metode sistematis yang digunakan untuk melakukan identfikasi akibat atau konsekuensi dari potensi kegagalam sistem atau proses, serta mengurangi peluang terjadinya kegagalan. Proses dalam analisis ini melibatkan perhitungan nilai dari *Severity* (dampak), *Occurence* (kemungkinan) dan *Detection* (deteksi).
Severity number merupakan penilaian terhadap pengaruh buruk yang dirasakan akibat kegagalan potensial. Severity number mengukur tingkat keparahan dari risiko yang terjadi. Pengukuran Severity atau nilai dampak dilihat dari seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek-aspek penting dalam organisasi.

Tabel 4.6 Ranking Severity

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

Occurence merupakaan pengukuran terhadap tingkat kemungkinan frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat menghasilkan kegagalan. Occurence membantu dalam pengukuran probabilitas penyebab kemungkinan terjadinya risiko akan menghasilkan kegagalan yang akan berdampak sesuatu.

Tabel 4.7 Ranking Occurence

Kemungkinan Kegagalan	Kemungkinan Terjadi	Ranking
Very High: Kegagalan hampir/tidak dapat dihindari	Lebih dari satu kali tiap harinya	10

Very High: Kegagalan selalu terjadi	Satu kali setiap 3-4 hari	9
High: Kegagalan terjadi berulang kali	Satu kali dalam seminggu	8
High: Kegagalan sering terjadi	Satu kali dalam sebulan	7
Moderately High : Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan	6
Moderate : Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan	5
Moderate Low : Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relative kecil	Satu kali dalam 1-3 tahun	3
Very Low: Kegagalan terjadi relative kecil dan sangat jarang	Satu kali dalam 3 - 6 tahun	2
Remote: Kegagalan tidak pernah terjadi	Satu kali dalam 6 - 50 tahun	1

Sementara itu *Detection* atau nilai deteksi merupakan suatu nilai pengukuran terhadap kemampuan mengendalikan atau mengontrol kegagalan yang dapat terjadi. Nilai deteksi ini akan mencerminkan kemampuan dari organinsasi untuk dapat mendeteksi risiko dan melakukan kontrol terhadap gangguan tersebut.

Tabel 4.8 Ranking Detection

Deteksi	Kriteria Deteksi	Ranking
Hampir tidak mungkin	Tidak ada metode penanganan	10

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

Dari hasil perhitungan dari nilai Severity (dampak), Occurence (kemungkinan) dan Detection (dampak) maka akan didapatkan hasil penilaian risiko dengan nilai yang paling tinggi. *Risk Priority Number* (RPN) merupakan produk matematis dari ketiga perhitungan tersebut. RPN dapat ditunjukkan dengan persamaan sebagai berikut:

RPN = Severity x Occurence x Detection

Dari hasil RPN, maka dapat diketahui tingkat risiko tersebut. Tingkat risiko berdasarkan FMEA adalah sebagai berikut:

Tabel 4.9 Level Risiko (Sumber: FMEA)

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

Skala RPN (*Risk Priority Number*) dari setiap risiko akan digunakan sebagai penentu level risiko, yang berguna untuk menilai risiko manakah yang bernilai paling tinggi. RPN tersebut akan dikategorikan berdasarkan level risiko di Skala RPN. Organisasi perlu melakukan antisipasi, mitigasi dan strategi terhadap risiko yang memiliki tingkatan paling tinggi, untuk menjaga keberlangsungan operasional bisnis saat gangguan tersebut terjadi.

4.4.2 Analisis Dampak Bisnis

Setelah melakukan analisis risiko, dilanjutkan dengan analisis dampak bisnis. Analisis dampak bisnis dilakukan untuk mengetahui dampak yang dihasilkan dari risiko yang telah dianalisis sebelumnya, pada tahap ini juga dilakukan prioritasi yang dilakukan pada layanan, proses bisnis dan aktivitas TI. Berikut ini adalah langkah-langkah untuk melakukan analisis dampak bisnis yang mengacu pada ISO 22317 :

1. Prioritisasi Layanan TI

Tahap pertama dari analisis dampak bisnis adalah dengan melakukan prioritisasi layanan dan proses bisnis TI yang ada pada organisasi. Hasil dari prioritisasi akan dikategorikan menjadi beberapa tingkat seperti tabel dibawah ini:

Tabel 4.10 Kategori Prioritas Layanan TI

Tingkat Prioritas	Keterangan
Sangat Kritis	Layanan TI memiliki dampak yang sangat besar apabila terjadi ancaman.
Kritis	Layanan TI memiliki dampak yang tidak terlalu besar apabila terjadi ancaman
Minor	Layanan TI tidak memiliki dampak atau dampaknya hampir tidak terasa saat terjadi ancaman

2. Prioritisasi Proses Bisnis dan Aktivitas TI

Setelah layanan TI akan dilakukan juga prioritisasi terkait proses bisnis TI. Aktivitas ini merupakan aktivitas yang terdapat pada proses bisnis yang telah diidentifikasi sebelumnya. Hasil dari prioritisasi akan dikategorikan menjadi beberapa tingkat seperti tabel dibawah ini:

Tabel 4.11 Kategori Prioritas Layanan TI

Tingkat Prioritas	Keterangan
Sangat Kritis	Proses Bisnis TI memiliki dampak yang sangat besar apabila terjadi ancaman.
Kritis	Proses Bisnis TI memiliki dampak yang tidak terlalu besar apabila terjadi ancaman
Minor	Proses Bisnis TI tidak memiliki dampak atau dampaknya hampir tidak terasa saat terjadi ancaman

3. Analisis Waktu Pemulihan

Setelah melakukan prioritisasi maka selanjutnya akan akan dilakukan identifikasi waktu pemulihan. Waktu pemulihan ini nantinya dianalisis menjadi tiga yaitu Maximum Tolerable Downtime (MTD) dan Recovery Time Objective (RTO). Berikut merupakan penjelasan untuk masing masing waktu pemulihan :

- **Maximum Tolerable Downtime (MTD)** merupakan jumlah waktu maksimal yang dapat ditoleransi oleh perusahaan terhadap kegagalan proses bisnis
- **Recovery Time Objective (RTO)** adalah jumlah waktu lumpuh maksimal untuk seluruh sumber daya sistem yang ada, sebelum terjadi dampak lain kepada sumber daya lainnya. Jika waktu penanggulangan gangguan atau bencana melebihi RTO dapat menyebabkan dampak yang lebih besar bagi organisasi.

4. Analisis Dampak Gangguan

Tahap selanjutnya adalah melakukan analisis dampak gangguan yang bertujuan untuk mengetahui dampak yang terjadi pada suatu proses bisnis. Dampak ini dibagi menjadi tiga aspek, yaitu aspek finansial, aspek reputasi dan juga aspek target teknis. Hasil dari prioritisasi akan dikategorikan menjadi beberapa tingkat seperti tabel dibawah ini:

Tabel 4.12 Kategori Dampak Gangguan

Tingkat Prioritas	Keterangan
Finansial	Jumlah persentase biaya ekstra yang harus dikeluarkan perusahaan, bisa dalam bentuk biaya pinalti, biaya tambahan atau profit yang hilang.
Reputasi	Berupa opini negatif dari media atau masyarakat yang mana dapat membuat perusahaan kehilangan pelanggan yang potensial
Target Teknis	Dampak berupa persentase (%) ketidaktercapaian target atau tujuan dari perusahaan akibat ancaman tersebut.

4.5 Penentuan Strategi BCP

Setelah dilakukan analisis risiko dan dampak bisnis organisasi dapat dilakukan penentuan strategi BCP. Pada penelitian ini strategi BCP dikategorikan menjadi 4 jenis, yaitu strategi preventif, strategi DRP, strategi saat terjadi gangguan dan

strategi korektif. Berikut merupakan penjelasan untuk masing masing strategi [3]:

- **Strategi Preventif**
  Strategi preventif merupakan tindakan atau aksi organisasi yang dilakukan untuk dapat mengurangi risiko terjadinya gangguan dan juga mengurangi dampak yang terjadi akibat risiko tersebut. Strategi Preventif dilakukan agar organisasi memiliki kesiapan lebih untuk dapat menghadapi gangguan yang akan terjadi. Diharapkan juga nantinya strategi preventif dapat membantu organisasi dalam menghadapi gangguan yang terjadi sehingga organisasi dapat menyelesaikan gangguan dalam batas toleransi waktu yang telah ditentukan.
- **Strategi Saat Gangguan**
  Strategi sat terjadi gangguan merupakan suatu tindakan atau aksi yang dilakukan organisasi untuk dapat mengatasi gangguan dan mengembalikan proses bisnis agar dapat kembali berjalan dalam kondisi normal. Berbeda dengan strategi DRP, strategi saat gangguan tidak terbatas hanya untuk tim DRP namun untuk keseluruhan komite BCP yang terkait. Fokus utama strategi ini adalah untuk dapat mengembalikan kondisi organisasi ke status normal.
- **Strategi Korektif**
  Strategi Korektif merupakan suatu tindakan atau aksi yang dilakukan organisasi untuk dapat terus menerus memperbaiki kinerja dari perencanaan BCP. Strategi korektif dilakukan saat organisasi melihat adanya ketidaksesuaian atau kurangnya tingkat keefektifan dari perencanaan BCP yang telah disusun. Diharapkan nantinya strategi korektif ini dapat membantu organisasi untuk dapat terus menerus meningkatkan performa dari strategi BCP.

4.6 Rencana Validasi BCP

Tahapan validasi adalah tahapan dimana peneliti memastikan bahwa BCP telah sesuai dengan kebutuhan organisasi. Tahapan ini dilakukan untuk memastikan bahwa BCP yang dibuat sudah benar dan dapat diterima oleh perusahaan, maka dari itu proses validasi dinilai menjadi hal yang sangat penting dalam penelitian ini. Berikut merupakan tabel rencana validasi yang akan diajukan oleh peneliti kepada pihak Pusbang:

Tabel 4.13 Rencana Validasi BCP

No	Nama Validasi	Keterangan
1.	Validasi kesesuaian analisis risiko	Validasi ini bertujuan untuk memastikan kesesuaian analisis risiko dengan kebutuhan organisasi berdasarkan penggalian data yang dilakukan di Sub Direktorat Pengembangan Sistem Informasi
2.	Validasi kesesuaian analisis dampak bisnis	Validasi ini bertujuan untuk memastikan kesesuaian analisis dampak bisnis dengan kebutuhan organisasi berdasarkan penggalian data yang dilakukan di

BAB V
IMPLEMENTASI

Bab ini menjelaskan hasil dari perancangan dan proses pelaksanaan dari penelitan. Selain itu, akan dijabarkan pula mengenai hasil pengumpulan data dan informasi, formulasi BCP, kerangka kerja 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 wawancara dan melakukan analisis dokumen.

5.1.1 Hasil Wawancara

Pengumpulan data menggunakan metode wawancara dilakukan kepada beberapa pihak terkait di Direktorat Pengembangan Teknologi dan Sistem Informasi. Berikut merupakan keterangan dari pelaksanaan tahap pengumpulan data dan Informasi dengan wawancara

Tabel 5.1 Hasil Wawancara

1.	Narasumber:	Anny Yuniarti, S.Kom., M.Comp.Sc
	Jabatan:	Ketua Sub Direktorat Pengembangan Sistem Informasi
	Tanggal:	Jumat, 11 November
	Lokasi:	Direktorat Pengembangan Teknologi dan Sistem Informasi
	Topik:	Kondisi kekinian organisasi, proses bisnis organisasi, identifikasi aset kritis, ancaman dan risiko serta dampak terhadap proses bisnis kritis apabila terkena gangguan.
	Hasil:	Lampiran A
2.	Narasumber:	Royyana M Ijtihadie, S.Kom.,M.Kom.,Ph.D

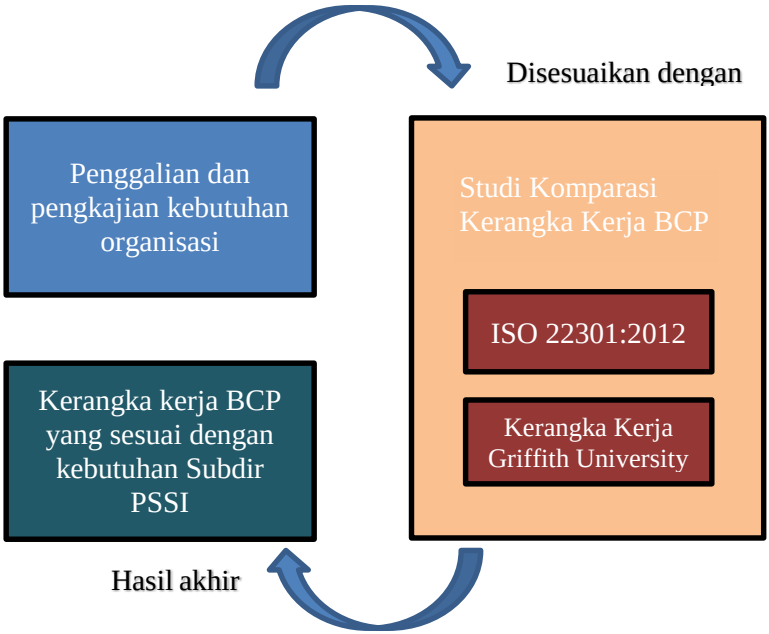
	Jabatan:	Ketua Sub Direktorat Infastruktur dan Keamanan Teknologi Informasi
	Tanggal:	Rabu, 23 November 2016
	Lokasi:	Direktorat Pengembangan Teknologi dan Sistem Informasi
	Topik:	Identifikasi aset kritis, kebutuhan aset kritis, ancaman dan risiko serta dampak terhadap proses bisnis kritis apabila terkena gangguan.
	Hasil:	Lampiran A
3.	Narasumber:	Cahya Purnama Dani, A.Md.
	Jabatan:	Staff Sub Direktorat Infastruktur dan Keamanan Teknologi Informasi
	Tanggal:	Selasa, 17 Januari 2017
	Lokasi:	Perpustakaan Lantai 6
	Topik:	Identifikasi aset kritis, kebutuhan aset kritis, ancaman dan risiko serta dampak terhadap proses bisnis kritis apabila terkena gangguan.
	Hasil:	Lampiran A

5.2 Formulasi Kerangka Kerja *Business Continuity Plan*

Untuk melakukan melakukan formulasi dokumen BCP, peneliti menggunakan pendekatan mundur dimana dilakukan penggalian kebutuhan dan keinginan pihak organisasi terlebih dahulu dari bentuk BCP yang dibuat. BCP ini nantinya akan digali dari keinginan pihak Subdirektorat Pengembangan Sistem Informasi.

Setelah melakukan penggalian kebutuhan dari pihak organisasi untuk kerangka kerja BCP, selanjutnya dilakukan komparasi atau perbandingan terhadap kerangka kerja BCP yang dijadikan acuan dalam penelitian ini. Kerangka kerja BCP yang digunakan sebagai acuan pada penelitian ini adalah Kerangka Kerja BCMS ISO 22301:2012 dan Kerangka Kerja BCM Griffith University. Dengan adanya penggabungan antara studi komparasi kerangka kerja BCP dengan kebutuhan dan

keinginan perusahaan, maka akan dihasilkan sebuah kerangka kerja BCP yang sesuai dengan kebutuhan Subdirektorat Pengembangan Sistem Informasi. Berikut ini adalah skema pendekatan mundur pada penelitian ini.



Gambar 5.1 Formulasi Kerangka Kerja BCP

5.2.1 Penggalian Kebutuhan dan Keinginan Subdirektorat Pengembanan Sistem Informasi

Penggalian kebutuhan dan keinginan perusahaan pada penelitian ini dikhususkan pada kebutuhan perusahaan akan proses keberlanjutan bisnis, khususnya BCP dalam penelitian ini. Penggalian kebutuhan ini dilakukan dengan metode wawancara dengan pimpinan di bagian DPTSI.

Berikut ini adalah hasil dari penggalian kebutuhan perencanaan keberlanjutan bisnis

Tabel 5.2 Kebutuhan Organisasi terkait BCP

No.	Kebutuhan dan Keinginan	Status
1.	BCP yang dibuat harus sesuai dengan tujuan dan fungsi organisasi	Terverifikasi
2.	BCP yang dibuat dapat menangani risiko yang timbul dari teknologi informasi yang dimplementasikan organisasi.	Terverifikasi
3.	BCP yang dibuat harus dapat mengurangi risiko yang timbul dari teknologi informasi yang diimplementasikan organisasi	Terverifikasi
4.	BCP yang dibuat dapat digunakan dalam waktu jangka panjang.	Terverifikasi
5.	BCP yang dibuat bersifat sederhana dan mudah digunakan oleh SDM	Terverifikasi
6.	BCP yang dibuat harus dapat sesuai dengan teknologi informasi yang sudah diimplementasikan.	Terverifikasi
7.	BCP yang dibuat harus sesuai dengan keberlanjutan operasional bisnis perusahaan.	Terverifikasi
8.	BCP yang dibuat dapat diperbaharui dari waktu ke waktu	Terverifikasi
9.	BCP yang dibuat harus dinamis serta dapat mengikuti perkembangan dunia teknologi informasi.	Terverifikasi

5.2.2 Proses Formulasi Kerangka Kerja BCP SubDir PSSI

Metode yang digunakan dalam penyusunan kerangka BCP dalam penelitian ini adalah melakukan penyesuaian dari kerangka BCP yang digunakan sebagai literatur, untuk disesuaikan dengan kebutuhan dan keinginan perusahaan.
Penjelasan mengenai kerangka kerja BCP yang menjadi acuan dalam penelitian ini telah dijelaskan pada BAB II Tinjauan Pustaka Penyesuaian serta analisis dilakukan dengan menggunakan model atau kerangka dari beberapa standar dan kerangka kerja organisasi terkait yaitu ISO 22301:2012 dan kerangka kerja BCP Griffith University. Berikut merupakan hasil analisis dari masing masing kerangka BCP.

5.2.2.1 Kerangka Kerja BCMS ISO 22301:2012

Kerangka Business Continuity Management Systems (BCMS) ISO 22301:2012 merupakan suatu suatu kerangka yang menjelaskan bagaimana organisasi dapat melakukan sistem pengelolaan keberlangsungan bisnis. Kerangka pada ISO 22301:2012 dalam penerapan pengelolaan keberlangsungan bisnis menggunakan model berupa siklus PDCA (Plan-Do-Check-Act). Model PDCA merupakan bentuk model keberlanjutan bisnis yang cukup komprehensif, dikarenakan organisasi dapat terus melakukan peningkatan secara terus-menerus (*Continuous Improvement*). Untuk ISO 22301:2012, pelaksanaan BCP dijabarkan pada klausa 4 hingga kalusa 10. Berikut merupakan pemetaan tiap fasenya.

Kelebihan dari pemakaian kerangka BCP menggunakan ISO 22301:2012 adalah sebuah kerangka yang komprehensif, adanya fase *Check* dan *Act* juga berperan penting untuk menjaga peningkatan terus-menerus (*Continous Improvement*). Kerangka ISO 223013:2012 juga bersifat dinamis sehingga dapat diperbarui jika terjadi perubahan. Kekurangan yang ada pada kerangka ini adalah masih bersifat sangat umum dan tidak mendetail sehingga membutuhkan

kerangka kerja lain untuk membantu mengisi fase-fase yang ada pada kerangka kerja ini.

5.2.2.2 Kerangka Kerja BCM Griffith University

Griffith University membuat suatu kerangka kerja business *continuity management* (BCM) yang dirancang sebagai kerangka kerja keberlangsungan bisnis yang difokuskan untuk universitas atau organisasi pendidikan. Kerangka kerja BCM ini juga diimplementasikan pada Griffith University dan telah disetujui oleh dewan universitas, untuk mengikuti perkembangan dan kesesuaian dengan teknologi terbaru, akan dilakukan review setiap 5 tahun sekali terhadap kerangka kerja ini. Berikut adalah fase-fase dari kerangka kerja BCM Griffith University:

Gambar 5.2 Kerangka Kerja Griffith University

Penggunaan kerangka kerja ini adalah dengan tujuan untuk melengkapi kerangka kerja ISO 22301:2012 yang masih bersifat *general*, kerangka kerja Griffith University dapat digunakan untuk membantu mengisi konten-konten pada fase yang digunakan dari kerangka kerja ISO 22301:2012 yaitu PDCA karena kerangka kerja ini juga bersifat lebih detail dan teknis apabila dibandingkan dengan ISO 22301:2012.

Kekurangan dari kerangka kerja ini adalah memiliki sifat yang mendetail dan condong ke hal teknis, kedua hal ini menjadikan kerangka kerja Griffith Universitu kurang dinamis dan komprehensif. Kerangka kerja ini hanya mencakup fase perencanaan (*plan*), implementasi (*do*) dan pengawasan (*check*), namun tidak mencakup fase tindakan (*act*) yang berguna untuk melakukan peningkatan secara terus menerus

(*continuous improvement*) agar menjaga BCP tetap relevan dengan kondisi dan kebutuhan organisasi. Hal inilah yang membuat kedua kerangka kerja yaitu ISO 22301:2012 dan Griffith University dapat melengkapi satu sama lain. Untuk itu, agar dapat menghasilkan kerangka BCP yang dinamis dan komprehensif, maka peneliti akan menyusun kerangka BCP sesuai dengan hasil gabungan antara kedua standar tersebut, lalu akan disesuaikan dengan kebutuhan dan keinginan organisasi terkait perencanaan keberlangsungan bisnis.

Dari standar-standar yang digunakan untuk membuat kerangka BCP, peneliti menyimpulkan bahwa dari ISO 22301:2012, hal yang diimplementasikan adalah penerapan siklus PDCA, sebagai urutan yang digunakan untuk membuat kerangka BCP yang komprehensif. Sedangkan untuk kerangka kerja Griffith University, peneliti akan mengambil bagian tahapan strategi komunikasi, pengembangan sumber daya dan juga pelatihan dan pengujian

5.2.3 Kesesuaian Kerangka Kerja BCP Subdirektorat Pengembangan Sistem Informasi dengan Kebutuhan Perusahaan

Peneliti melakukan pemetaan terhadap kebutuhan perusahaan dengan sebuah model iteratif manajemen, yang dikenal dengan nama Model PDCA (*Plan-Do-Check-Act*). Alasan pemilihan bentuk model ini adalah, karena bersifat dinamis sehingga dapat diperbarui jika terjadi perubahan, organisasi juga dapat dengan mudah mengembangkan BCP secara terus-menerus untuk mendapatkan performa yang optimal. Hal ini juga berhubungan dengan keinginan organisasi untuk membuat kerangka BCP yang sederhana dan mudah digunakan oleh SDM. Berikut merupakan pemetaaan kerangka kerja BCP dengan kebutuhan dan keinginan organisasi. Kebutuhan dan keinginan organisasi dipetakan sesuai dengan 4 Fase PDCA yaitu perencanaan (*plan*), pengerjaan (*do*), pemeriksaan (*check*) dan juga tindakan (*act*).

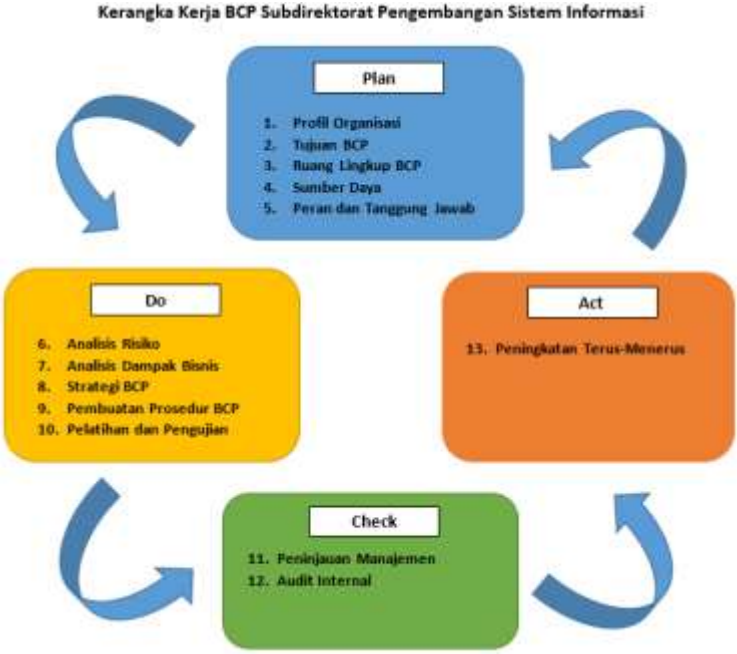
Tabel 5.3 Kesesuaian Kerangka Kerja dengan Kebutuhan Organisasi

Fase.	Kebutuhan Perusahaan	Kerangka BCP
Plan	BCP yang dibuat harus sesuai dengan tujuan dan fungsi organisasi	Profil Organisasi
		Tujuan BCP
		Ruang Lingkup BCP
	BCP yang dibuat harus dapat sesuai dengan teknologi informasi yang sudah diimplementasikan.	Sumber Daya
		Peran dan Tanggung Jawab
Do	BCP yang dibuat harus dapat mengurangi risiko yang timbul dari teknologi informasi yang diimplementasikan organisasi	Analisis Risiko
	BCP yang dibuat dapat menangani risiko yang timbul dari teknologi informasi yang dimplementasikan organisasi.	Analisis Dampak Bisnis
	BCP yang dibuat harus sesuai dengan keberlanjutan operasional bisnis perusahaan.	Strategi BCP
		Pembuatan Prosedur BCP
	BCP yang dibuat bersifat sederhana dan mudah digunakan oleh SDM	Pelatihan dan Pengujian
Check	BCP yang dibuat dapat digunakan dalam waktu jangka panjang.	Peninjauan Manajemen
	BCP yang dibuat dapat diperbaharui dari waktu ke waktu	Audit Internal
Act	BCP yang dibuat harus dinamis serta dapat mengikuti perkembangan dunia teknologi informasi.	Peningkatan terus-menerus (*Continous Improvement*)

Untuk mendapatkan dokumen BCP yang komprehensif dan tepat guna, maka peneliti akan melakukan formulasi antara kebutuhan perusahaan dengan korelasi kedua kerangka kerja BCP yang digunakan dalam penelitian ini.

5.3 Kerangka Kerja Business Continuity Plan Subdirektorat Pengembangan Sistem Informasi

Berdasarkan kebutuhan perusahaan yang telah ditetapkan, serta analisis dari 2 standar kerangka BCP yang digunakan yaitu ISO 22301:2012 dan Griffith University, berikut adalah gambar dari kerangka kerja BCP Subdirektorat Pengembangan Sistem Informasi:



Gambar 5.3 Kerangka Kerja BCP Subdirektorat Pengembangan

Setiap fase dalam kerangka BCP Subdirektorat Pengembangan Sistem Informasi merupakan formulasi kebutuhan perusahaan dan acuan yang digunakan, yaitu ISO 22301:2012 dan Gritffith University. Berikut ini adalah pemetaan setiap fase kerangka BCP dengan acuan yang digunakan:

Tabel 5.4 Pemetaan Kerangka Kerja BCP Sesuai Acuan

Fase	Sub-Fase	Kerangka Acuan
Plan	Profil Organisasi	ISO 22301:2012
	Tujuan BCP	ISO 22301:2012
	Ruang Lingkup BCP	ISO 22301:2012
	Sumber Daya	ISO 22301:2012
	Peran dan Tanggung Jawab	ISO 22301:2012 Griffith University
Do	Analisis Risiko	ISO 22301:2012 Griffith University
	Analisis Dampak Bisnis	ISO 22301:2012 Griffith University
	Strategi BCP	ISO 22301:2012 Griffith University
	Pembuatan Prosedur BCP	ISO 22301:2012 Griffith University
	Pelatihan dan Pengujian	ISO 22301:2012 Griffith University
Check	Peninjauan Manajemen	ISO 22301:2012
	Audit Internal	ISO 22301:2012 Griffith University
Act	Peningkatan terus-menerus (*Continous Improvement*)	ISO 22301:2012

Berdasarkan hasil pemetaan di atas, dapat diamati pada setiap fase di Kerangka BCP terdapat subfase yang mengacu pada kedua standar yang digunakan namun terdapat pula sub-fase yang hanya mengacu pada satu standar kerangka. Hal tersebut

dilakukan agar setiap fase yang ada benar-benar sesuai dengan kebutuhan perusahaan.
Pada penyusunan kerangka BCP dengan menggunakan pendekatan berbasis risiko memerlukan proses peningkatan secara terus-menerus (continuous improvement) dikarenakan adanya kemungkinan perubahan yang terkait dengan proses bisnis yang dipengaruhi oleh perkembangan teknologi informasi, ataupun regulasi organisasi. Oleh karena itu, peran continuous improvement sangat penting dalam pembuatan kerangka BCP ini.

5.4 Hasil Validasi BCP

Tahapan validasi merupakan tahapan penting yang dilakukan untuk memastikan bahwa hasil analisa yang dilakukan sudah benar dan sesuai dengan keadaan perusahaan. Tahapan validasi juga dilakukan sebagai konfirmasi bahwa apa yang dikerjakan oleh peneliti telah sesuai dengan kebutuhan dari Sub Direktorat Pengembangan Sistem Informasi. Proses validasi dilakukan dengan mengajukan surat konfirmasi pada ketua Sub Direktorat Pengembangan Sistem Informasi. Validasi dilakukan untuk dua bagian pada pembuatan BCP yaitu analisis risiko serta analisis dampak bisnis.
Tahap validasi analisis risiko dilakukan setelah menilai tiap risiko per proses bisnis dan melakukan prioritasi risiko sesuai dengan level risiko paling tinggi, proses validasi dilakukan dengan pemeriksaan hasil analisis risiko yang telah dilakukan. Untuk pemeriksaan dari analisis risiko dilakukan oleh pihak-pihak yang berhubungan dengan risiko seperti Ketua Sub Direktorat Infrastruktur serta Staff Infrastruktur, ini dilakukan agar hasil validasi dapat benar-benar sesuai dengan kebutuhan organisasi. Dari hasil analisis risiko yang telah dilakukan, ditemukan 2 risiko yang memiliki tingkat *very high* yaitu server tidak beroperasi dan manipulasi data, setelah dilakukan validasi kepada pihak organisasi ternyata hasil dari analisis risiko memiliki kesesuaian dengan kondisi sebenarnya pada organisasi, hal ini membuktikan bahwa proses validasi telah memastikan bahwa hasil analisa yang dilakukan sudah benar dan sesuai dengan keadaan perusahaan.

Sama seperti analisis risiko, analisis dampak bisnis dilakukan setelah melakukan prioritasi setiap fungsional bisnis dan menganalisa dampak gangguan dari masing-masing proses bisnis. Dari hasil analisis dampak bisnis yang telah dilakukan, didapatkan prioritasi untuk proses bisnis serta aktivitas dari organisasi, analisis dampak gangguan serta strategi BCP yang didapatkan dari proses pengolahan data dampak bisnis yang didapatkan dari wawancara, setelah dilakukan validasi kepada pihak organisasi ternyata hasil dari analisis dampak bisnis memiliki kesesuaian dengan kondisi sebenarnya pada organisasi, hal ini membuktikan bahwa proses validasi telah memastikan bahwa hasil analisa yang dilakukan sudah benar dan sesuai dengan keadaan perusahaan. Untuk hasil validasi dari analisis risiko dapat dilihat pada lampiran G, sementara hasil validasi analisis dampak bisnis dapat dilihat pada lampiran H.

5.5 Hambatan dan Rintangan

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

- Penentuan kerangka kerja sejenis dari dokumen BCP yang cukup lama
- Proses pengumpulan data serta validasi membutuhkan waktu yang cukup lama dikarenakan sulitnya jadwal dari karyawan DPTSI untuk melakukan pertemuan
- Analisis risiko serta analisis dampak bisnis membutuhkan waktu yang lama dikarenakan terdapat beberapa koreksi dari pihak DPTSI.

Walaupun terdapat beberapa hambatan serta rintangan, namun penelitian ini tetap berjalan dengan lancar berkat bantuan dan mudahnya alur komunikasi dengan pihak DPTSI. Pihak DPTSI sangat terbuka dan sangat bersedia untuk membantu penelitian dengan memberikan respon yang cepat dan bersedia meluangkan waktu untuk melakukan wawancara dan validasi.

“Halaman ini sengaja dikosongkan”

BAB VI
HASIL DAN PEMBAHASAN

Bab ini menjelaskan proses penyusunan kerangka BCP di Subdirektorat Pengembangan Sistem Informasi yang dirancang dengan menggunakan formulasi kerangka kerja yang telah dijelaskan pada bab sebelumnya.

6.1 Pembahasan Kerangka Kerja BCP Subdirektorat Pengembangan Sistem Informasi

Pada bagian ini akan dijelaskan mengenai implementasi model BCP untuk menyusun Business Continuity Planning di Subdirektorat Pengembangan Sistem Informasi. Fase yang terdapat pada model BCP adalah Siklus Deming PDCA yaitu Plan, Do, Check, dan Act. Fase-fase ini menunjang peneliti untuk mendapatkan hasil terbaik yang sesuai dengan kebutuhan perusahaan.

6.1.1 Plan (Perencanaan)

Pada fase perencanaan, organisasi diharapkan dapat menyusun BCP sesuai dengan kebutuhan dan tujuan dari organisasi. Dalam fase ini, organisasi akan menentukan kebutuhan terkait profil organisasi, tujuan, ruang lingkup, sumber daya dan peran dan tanggung jawab, yang mendukung proses keberlanjutan bisnis di organisasi.

6.1.1.1 Profil Perusahaan

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) bertugas untuk menyediakan dan mengelola layanan Teknologi Informasi di lingkungan ITS. Terkait peran, DPTSI berperan untuk mendukung aktivitas akademik, penelitian dan pengabdian masyarakat, serta manajerial di lingkungan ITS dalam rangka membantu ITS mencapai visi misinya [1].

DPTSI menurut sejarah, awalnya merupakan sebuah unit yakni UPT Pusat Komputer. Unit ini dibentuk tahun 1982 dilengkapi dengan Honeywell Bull Mini 6 System yang merupakan salah

satu sistem komputer yang cukup baik. Pada periode tersebut mulai berkembang generasi PC yang pertama yang membuat Puskom pada akhirnya mentransformasi teknologi computer mini ke teknologi PC pada tahun 1988.

Pada awal tahun 1982an UPT Pusat Komputer banyak mendukung staf peneliti ITS dalam melakukan penelitian yang membutuhkan computer untuk melakukan baik data prosessing maupun menyelesaikan persamaan matematik. Mulai tahun 1992 UPT Puskom dipercaya untuk melakukan pemprosesan data test untuk masuk perguruan tinggi negeri di wilayah Indonesia Timur dan pengalaman dalam pemprosesan data tersebut dikembangkan untuk juga kerjasama dengan Pemkot/Pemkab di Jawa Timur dalam memproses data untuk test Pegawai Negeri. Semua ini bisa terlaksana dengan baik dengan akurasi yang sangat tinggi (*zero error*) dan dengan keamanan yang sangat ketat (100% *security*).

Sejak tahun 1999 UPT Pusat Komputer dimandatkan untuk mengelola ITS-net yaitu jaringan baik intranet maupun internet untuk ITS secara keseluruhan. Dengan adanya tugas tersebut maka semua data dan informasi di ITS bisa di hubungan secara menyeluruh.

BTSI berubah nama menjadi LPTSI (Lembaga Pengembangan Teknologi Sistem Infromasi) berdasarkan Permendikbud No. 86, Tahun 2013 tentang OTK ITS. LPTSI mempunyai tugas melaksanakan, mengkoordinasi, memonitor dan mengevaluasi kegiatan penelitian dan pengembangan teknologi dan sistem informasi. Pada bulan Oktober 2016, LPTSI berubah nama menjadi DPTSI (Direktorat Pengembangan Teknologi dan Sistem Informasi) [1]

Kebutuhan dan Keinginan Organisasi

Penggalian kebutuhan dan keinginan perusahaan pada penelitian ini dikhususkan pada kebutuhan perusahaan akan proses keberlanjutan bisnis, khususnya BCP dalam penelitian ini. Penggalian kebutuhan ini dilakukan dengan metode sebagai berikut.

1. Wawancara dengan pimpinan di bagian TSI.

2. Penyesuaian dengan Rencana Jangka Panjang Direktorat Penembangan Teknologi dan Sistem Informasi

Berikut ini adalah hasil dari penggalian kebutuhan perencanaan keberlanjutan bisnis

Tabel 6.1 Kebutuhan BCP Organisasi

No.	Kebutuhan dan Keinginan	Status
1.	BCP yang dibuat harus sesuai dengan tujuan dan fungsi organisasi	Terverifikasi
2.	BCP yang dibuat dapat menangani risiko yang timbul dari teknologi informasi yang dimplementasikan organisasi.	Terverifikasi
3.	BCP yang dibuat harus dapat mengurangi risiko yang timbul dari teknologi informasi yang diimplementasikan organisasi	Terverifikasi
4.	BCP yang dibuat dapat digunakan dalam waktu jangka panjang.	Terverifikasi
5.	BCP yang dibuat bersifat sederhana dan mudah digunakan oleh SDM	Terverifikasi
6.	BCP yang dibuat harus dapat sesuai dengan teknologi informasi yang sudah diimplementasikan.	Terverifikasi
7.	BCP yang dibuat harus sesuai dengan keberlanjutan operasional bisnis perusahaan.	Terverifikasi

No.	Kebutuhan dan Keinginan	Status
8.	BCP yang dibuat dapat diperbaharui dari waktu ke waktu	Terverifikasi
9.	BCP yang dibuat harus dinamis serta dapat mengikuti perkembangan dunia teknologi informasi.	Terverifikasi

6.1.1.2 Tujuan BCP

Pada bagian ini akan dijabarkan mengenai tujuan organisasi dalam melakukan pembuatan BCP. Nantinya tujuan ini akan menjadi acuan dalam pengerjain BCP. Sehingga diharapkan rancangan BCP akan mendukung proses bisnis operasional dan tujuan dari organisasi.

Tujuan dari penyusunan BCP ini adalah :

1. Menghasilkan rancangan *Business Continuity Plan* yang sesuai dengan kebutuhan dari Sub Direktorat Pengembangan Sistem Informasi
2. Menghasilkan dokumen BCP yang dapat mendukung proses keberlangsungan bisnis organisasi serta dapat digunakan secara menyeluruh kepada bagian yang menggunakan teknologi informasi.
3. Dapat meminimalisasi risiko teknologi informasi yang terdapat pada organisasi sehingga dapat menghambat operasional bisnis.
4. Dapat meminimalisasi dampak bisnis teknologi informasi yang mengganggu keberlangsungan operasional bisnis organisasi.
5. Meningkatkan kesadaran dari seluruh pegawai DPTSI atas pentingnya pengelolaan risiko dan pengelolaan keberlangsungan bisnis di organisasi.
6. Menjaga keberlangsungan proses bisnis organisasi untuk meningkatkan reputasi organisasi di tingkat institut

6.1.1.3 Ruang Lingkup

Pada penyusunan dokumen BCP pada Sub Direktorat Pengembangan Sistem Informasi DPTSI, ruang lingkup yang dipilih dalam penyusunan adalah beberapa fungsional dan proses bisnis yang terlibat. Fungsional dan proses bisnis yang terdapat dibawah ini adalah yang memiliki ketergantungan terhadap teknologi dan informasi dalam melakukan aktivitasnya.

Fungsional Bisnis dan Proses Bisnis yang Terlibat

Dalam fungsional bisnis yang dimiliki oleh Sub Direktorat Pengembangan Sistem Informasi, terdapat 3 fungsional bisnis yang berada langsung dibawah Ketua Sub Direktorat. Ketiga fungsional ini menggunakan dukungan teknologi informasi dalam proses bisnisnya. Fungsional bisnis yang terkait dengan penelitian ini adalah developer, analyst, dan dokumentasi.

Proses bisnis yang dibahas pada penelitian ini pun tidak semuanya dimasukkan, karena proses bisnis yang dipilih hanyalah proses bisnis yang dianggap paling penting dan memiliki ketergantungan yang besar terhadap layanan teknologi informasi di organisasi. Berikut merupakan penjabaran dari fungsional bisnis dan proses bisnis yang terlibat dalam proses BCP.

Tabel 6.2 Proses Bisnis Terkait Fungsional Organisasi

Fungsional Bisnis	Proses Bisnis Terkait Sistem
Developer	Menyediakan aplikasi sistem informasi berbasis web
	Mengelola aplikasi sistem informasi berbasis web
	Melakukan pengujian program atau modul sistem informasi
	Memaksimalkan kinerja aplikasi sistem informasi
	Menyelesaikan keluhan terkait sistem informasi di ITS
Analyst	Menganalisis proses bisnis organisasi

Fungsional Bisnis	Proses Bisnis Terkait Sistem
	Memaksimalkan kinerja aplikasi sistem informasi
Dokumentasi	Menyediakan aplikasi sistem informasi berbasis web
	Memaksimalkan kinerja aplikasi sistem informasi
	Melakukan dokumentasi keluhan terkait sistem informasi di ITS

6.1.1.4 Sumber Daya

Pada pembuatan dokumen BCP ini perlu dilakukan identifikasi terhadap sumber daya yang terkait dengan perangkat dan infrastruktur yang dipergunakan ketika terjadi gangguan/bencana di perusahaan. Identifikasi perangkat atau infrastruktur ini diharapkan dapat membantu operasional proses bisnis organisasi.

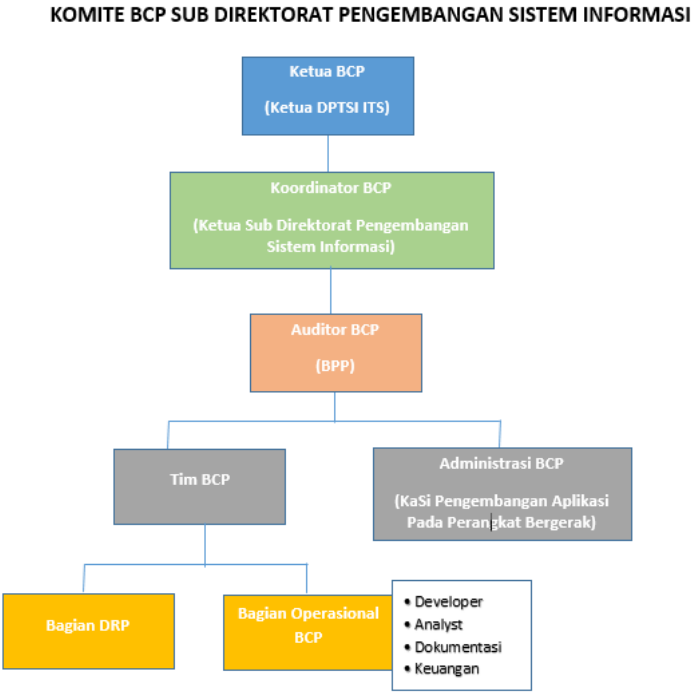
Perangkat keras kritikal yang dibutuhkan untuk melakukan pengelolaan teknologi dan sistem informasi.

- Sistem/CPU AS/400.
- Unit disk/DASD.
- Panel komunikasi dan modem.
- Drive tape dan cartridge.
- Printer.
- Alat komunikasi darurat

6.1.1.5 Peran dan Tanggung Jawab

Sumber Daya Manusia (SDM) menempati peran yang penting dalam penyusunan BCP, karena pada organisasi SDM merupakan orang yang yang bertanggung untuk menyusun serta melaksanakan BCP, jika BCP dilaksanakan secara optimal, maka akan menghasilkan BCP yang optimal pula. Untuk memastikan bahwa SDM yang ada dapat berjalan secara optimal, maka perlu dibuat adanya sebuah komite atau kepanitiaan.

Komite BCP ini juga nantinya akan berhubungan dengan Tim DRP, pada DPTSI tim DRP merupakan bagian dari Sub Direktorat Infrastruktur dan Keamanan Teknologi Informasi. Tim DRP memiliki tanggung jawab untuk menangani semua gangguan pada teknologi informasi di Direktorat Pengembangan Teknologi dan Sistem Informasi.



Gambar 6.1 Komite BCP Sub Direktorat

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

A. Ketua BCP

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

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

C. Auditor BCP
- Melakukan audit internal BCP
- Melakukan evaluasi pelaksanaan BCP
- Memberikan rekomendasi hasil perbaikan berdasarkan evaluasi BCP

D. Tim BCP
- Mengawasi kesesuaian pelaksanaan teknis BCP dengan perencanaan yang telah dibuat
- Memberikan arahan teknis kepada Bagian DRP dan Bagian Operasional BCP

E. Administrasi BCP
- Melakukan dokumentasi pelaksanaan BCP
- Memastikan ketersediaan SDM saat terjadinya gangguan

F. Bagian DRP
- Tim DRP akan diaktivasi untuk mengelola secara efektif adanya kejadian gangguan yang terjadi di kampus
- Melakukan pemulihan aset TI yang terkena gangguan
- Melakukukan backup dan restore data saat terjadi gangguan

G. Bagian Operasional BCP
- Menjalankan proses BCP sesuai dengan arahan teknis dan perencanaan
- Mendukung proses BCP
- Mempersiapkan infrastruktur pendukung BCP

6.1.2 Do (Pengerjaan)

Fase ini organisasi akan melakukan implementasi perencanaan untuk dapat menyusunan perencanaan keberlangsungan bisnis. Dalam fase ini ada beberapa tahapan antara lain adalah analisis risiko, analisis dampak bisnis, penyusungan strategi BCP,

penyusunan prosedur BCP dan juga pelatihan serta pengujian BCP.

6.1.2.1 Analisis Risiko

Tahapan pertama dari Fase Do adalah dengan melakukan analisis risiko. Tahapan analisis risiko pada penelitian ini menggunakan metode OCTAVE untuk identifikasi risiko dan FMEA untuk penilaian risiko.

Identifikasi Risiko dengan OCTAVE.

Analisis Risiko menggunakan OCTAVE dapat membantu dalam mengidentifikasi kemungkinan risiko dan ancaman apa saja yang dapat terjadi dari aset TI yang dimiliki. Tahapan-tahapan dalam metode OCTAVE adalah mengidentifikasi aset kritis, mengidentifikasi kebutuhan keamanan aset kritis, mengidentifikasi ancaman, mengidentifikasi praktik keamanan yang telah dilakukan organisasi, mengidentifikasi komponen utama TI dan mengidentifikasi kerentanan teknologi. Berikut adalah output yang dihasilkan dari masing masing fase OCTAVE.

Tabel 6.3 Identifikasi Risiko Dengan Octave

Fase 1 – *Build asset based profile*	Daftar Aset Kritis
	Daftar Kebutuhan Keamanan Aset Kritis
	Daftar Ancaman Aset Kritis
	Daftar Praktik Keamanan yang Dilakukan Organisasi
	Daftar Kelemahan Organisasi
Fase 2 - *Identify Infrastructure Vulnerabilities*	Dafttar Komponen Utama
	Daftar Kerentanan Teknologi
Fase 3 - *Develop Security Strategy and Plans*	Daftar Risiko untuk Aset Kritis
	Pengukuran Risiko

Fase yang digunakan untuk kebutuhan wawancara adalah Fase 1 dan Fase 2, *output* atau hasil dari wawancara digunakan untuk

membentuk Fase 3. Masing masing tahapan ini didapatkan dari hasil wawancara yang dilampirkan pada Lampiran dan telah dilakukan verifikasi hasil risiko yang dilampirkan pada Lampiran .

Fase 1 – Build Asset Based Profile

Pada fase pertama dari OCTAVE ini akan dilakukan identifikai aset dan ancaman berbasis aset degan menggunakan informasi yang didapat dari senior manajemen dengan melakukan wawancara. Tujuan dari fase ini adalah untuk mendapatkan profil ancaman berbasis aset. Diharapkan analisis ini dapat mengidentifikasi aset mana yang dianggap kritis serta menentukan langkah perlindungan dari aset tersebut. Selain itu organisasi nantinya juga dapat melihat apakah masing masing aset kritis telah memiliki tingkat keamanan sesuai dengn kebutuhanya.
Pada Fase 1 ini terdapat beberapa output yang jika digabungkan akan menghasilkan profil ancaman berbasis aset yang optimal diantaranya adalah tabel aset kritis, tabel kebutuhan keamanan untuk aset kritis, ancaman untuk aset kritis, praktik keamanan yang sekarang dilakukan dan kelemahan organisasi.
Tahapan tersebut memiliki hubungan satu sama lain maka dari itu pengurutan dari tahapannya diurutkan dari tahap awal yaitu tabel aset kritis yang digunaan untuk mengidentifikasi aset kritis TI sampai menentukan kelemahan dari organisasi itu sendiri. Daftar dari aset kritis dibawah disesuaikan dengan komponen dari sistem informasi. Berikut merupakan daftar aset kritis TI organisasi.

Tabel 6.4 Daftar Aset Kritis Organisasi

Daftar Aset Kritis Organisasi	
Hardware	Server
	PC/Laptop
Software	SIM Akademik
	SIM Kepegawaian
	SIM Keuangan

Daftar Aset Kritis Organisasi	
Data	Data Mahasiswa
	Data Transaksi SIM
	Data Keuangan
Network	Core Switch
	Distribution Switch
	Access Switch
People	Pegawai TI
	Pegawai Non-TI

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

Tabel 6.5 Daftar Kebutuhan Keamanan Aset

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset
Hardware	Server	• Server membutuhkan firewall • AC harus terus menyala • Adanya *fire alarm* yang terus menyala • Terdapat sumber listrik cadangan • Sistem operasi untuk server diperbaharui versinya • Suhu dan kelembaban di ruang server harus sesuai dengan batas

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset
		minimal yang ditentukan • Ruangan penyimpanan perangkat aset menggunakan rancangan dan material yang dapat menanggulangi dari bencana
	PC/Laptop	• Adanya sumber listrik cadangan • Adanya pembatasan hak akses berbeda • Terdapat antivirus • Ruangan penyimpanan perangkat aset menggunakan rancangan dan material yang dapat menanggulangi dari bencana
Software	SIM Akademik SIM Kepegawaian SIM Keuangan	• Dapat diakses 24 jam • Terdapat pembatasan hak akses • Terhadap pengamanan data dari SIM

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset
		• Log untuk merekam setiap perubahan yang ada pada SIM • Pembatasan waktu akses pada SIM
Data	Data Mahasiswa Data Transaksi SIM Data Keuangan	• Adanya perbedaan hak akses antar pegawai • Data dapat diakses 24 jam • Terhadap pengamanan data • Prosedur *backup* secara rutin
Network	Core Switch Distribution Switch Access Switch	• Harus tetap menyala 24 jam • Listrik harus tetap menyala 24 jam • Adanya sumber listrik cadangan • Proses inspeksi dan perawatan jaringan

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

Tabel 6.6 Identifikasi Ancaman

Ancaman Dari Lingkungan	
1.	Kebakaran
2.	Gempa Bumi
3.	Banjir
4.	Kerusakan pada Bangunan
5.	Kerusakan oleh hewan

Ancaman Dari Manusia	
6.	Kelalaian Manusia
7.	Pencurian Data
8.	Pembobolan Sistem
9.	Penurunan Komptensi Karyawan
10.	Pemadaman Listrik
Ancaman Dari Infrastruktur	
Hardware	
11.	Server tidak beroperasi
12.	Server *Overheat*
13.	Kerusakan PC/Laptop
14.	Kesalahan Konfigurasi *Hardware*
15.	Pencurian *Hardware*
16.	Kerusakan Pada Sumber Listrik Cadangan
Software	
17.	Virus/Worm
18.	Kesalahan Manajemen Password
19.	Kesalahan Konfigurasi Sistem
20.	Ancaman Keamanan Data dan Pengaturan Data
21.	Data Corrupt
22.	Kesalahan Konfigurasi Sistem
Network	
23.	Gangguan Koneksi Internet
24.	Kerusakan Kabel
25.	Gangguan Pada Jaringan

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

Tabel 6.7 Praktik Keamanan Organisasi

Praktik Keamanan Organisasi	**Pihak Yang Bertanggung Jawab**
Praktik ring backup antar distribution switch	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Memasang Firewall untuk keamanan dan pengaturan data	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Memasang Antivirus untuk keamanan software dan data	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Memasan Spam Filter untuk email yang masuk	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Hak akses yang berbeda untuk setiap karyawan	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Melakukan maintenance pada server, core switch, dan perangkat lainnya	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Melakukan back up data jika diperlukan	Bidang Aplikasi
Terdapat *fire extinguisher* untuk memadamkan api	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Tidak boleh sembarang orang masuk ke ruang server	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Akses keamanan menuju ruang fasilitas aset menggunakan *finger print* untuk menjaga keamanan	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Proses pemeriksaan dan perawatan rutin untuk jaringan	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi

Praktik Keamanan Organisasi	**Pihak Yang Bertanggung Jawab**
Tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi
Pembatasan waktu akses SIM termasuk proses *timeouts* dan otomatis *logout*	Sub Direktorat Infrastruktur Keamanan Teknologi Informasi

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

Tabel 6.8 Daftar Kelemahan Organisasi

Kelemahan Organisasi
Belum terdapat Standar Keamanan untuk SI/TI organisasi
Belum terdapat *Standard of Procedure* terkait praktik keamanan teknologi informasi
Belum adanya BCP untuk organisasi
Belum adanya smoke detector untuk sinyal adanya asap
Maintenance pada aset TI belum dilakukan secara rutin
Back Up data dilakukan hanya jika diperlukan
Belum ada *mirroring database*
Belum terdapat dokumentasi untuk hasil perbaikan gangguan
Belum terdapat evaluasi langkah perbaikan dari gangguan
Belum terdapat prosedur pengamanan dan penggunaan dari aset TI organisasi
Tidak tersedia daftar data/informasi yang harus di-*backup*
Tidak terdapat proses pemeriksaan dan perawatan perangkat PC
Belum terdapat peraturan keamanan untuk ruang penempatan aset TI

Fase 2 - *Identify Infrastructure Vulnerabilities*

Setelah mendapatkan profil bisnis berbasis aset di fase sebelumnya, selanjutnya pada fase 2 akan dilakukan identifiksai kelemahan infrastruktur yang didapatkan dengan menggunakan informasi yang didapat dari senior manajemen di DPTSI. Pada fase ini akan dilakukan evaluasi terhadap komponen utama atau beberapa komponen yang berperan penting untuk berjalannya suatu aset, dari proses identifikasi komponen utama maka akan ditinjau kelemahannya.
Output yang dihasilkan dari fase ini nantinya adalah tabel komponen utama dan tabel kerentanan teknologi.

Tabel 6.9 Komponen Utama Aset

Server	
System of Interest	Server menyimpan semua data-data penting di ITS
Komponen Utama	• Processor • RAM • Kabel • Sistem Operasi • Aliran Listrik
PC/Laptop	
System of Interest	PC yang dimiliki oleh Direktorat Pengembangan Teknologi dan Sistem Informasi
Komponen Utama	• CPU • Monitor, Keyboard dan Mouse • Kabel LAN • Antivirus • Sistem Operasi • Software • Listrik • UPS • Genset • Firewall

Jaringan	
System of Interest	Terdapat core switch yang terdiri atas distribution switch yang digunakan untuk fakultas dan access switch untuk setiap jurusan di ITS.
Komponen Utama	• Kabel • Listrik • Keamanan Jaringan • Switch
Software	
System of Interest	SIM yang dibuat oleh DPTSI contohnya SIM Akademik, SIM Keuangan, dan SIM Kepegawaian.
Komponen Utama	• Firewall • Server • Data • Antivirus
Data	
System of Interest	Data-data yang penting seperti Data Mahasiswa, Data Transaksi SIM, dan Data Keuangan
Komponen Utama	• Database • Server • Listrik • PC • Firewall • Database Administrator (DBA)

Setelah mengetahui komponen utama yang terdapat pada aset kritis, selanjutnya akan dilakukan identifikasi ancaman untuk masing-masing komponen utama aset kritis. Identifikasi ancaman komponen utama bertujuan untuk dapat melihat kerentanan dari teknologi yang ada. Dikarenakan komponen

utama tadi merupakan bagian dari aset, tentunya ancaman yang terdapat pada komponen utama juga akan mengancam aset kritis, maka dari itu hal ini dapat membantu dalam melihat ancaman secara keseluruhan dan mendetail yang dapat mengganggu aset kritis. Berikut merupakan daftar kerentanan teknologi dari masing-masing komponen utama aset kritis TI organisasi.

Tabel 6.10 Komponen Utama dan Kemungkinan Ancaman

Server	
System of Interest	Server menyimpan semua data-data penting di ITS
Komponen Utama	Kemungkinan Ancaman
• Processor • RAM • Kabel • Sistem Operasi • Aliran Listrik	• Kinerja Procesor menurun akibat terlalu banyak akses transaksi • RAM mengalami kekurangan memori akibat terlalu banyak data • Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Genset mati • Keamanan jaringan dapat ditembus • Ruang Server kurang diberi pengamanan • Keamanan server dapat ditembus
PC/Laptop	
System of Interest	PC yang dimiliki oleh Direktorat Pengembangan Teknologi dan Sistem Informasi
Komponen Utama	Kemungkinan Ancaman

• CPU • Monitor, Keyboard dan Mouse • Kabel LAN • Antivirus • Sistem Operasi • Software • Listrik • UPS • Genset • Firewall	• CPU tidak dapat berfungsi karena mengalami kerusakan • Monitor, Keyboard, dan Mouse tidak berfungsi • Kerusakan pada kabel dan konektor jaringan • Antivirus tidak dapat mendeteksi virus • Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Genset dan UPS tidak berfungsi
Jaringan	
System of Interest	Terdapat core switch yang terdiri atas distribution switch yang digunakan untuk fakultas dan access switch untuk setiap jurusan di ITS.
Komponen Utama	Kemungkinan Ancaman
• Kabel • Listrik • Switch • Keamanan Jaringan	• Gangguan atau kerusakan dikarenakan putusnya kabel • Konektor jaringan yang tidak terpasang dengan baik (longgar) • Susunan pengkabelan yang salah • Switch tidak bisa meneruskan *traffic* • Kerusakan kabel rusak karena digigit tikus, • Switch mengalami *hang* dikarenakan terlalu banyaknya arus data • Looping pada switch

Software	
System of Interest	SIM yang dibuat oleh DPTSI contohnya SIM Akademik, SIM Keuangan, dan SIM Kepegawaian.
Komponen Utama	Kemungkinan Ancaman
• Firewall • Server • Data • Antivirus	• Penyalahgunaan sistem untuk hal yang tidak diinginkan • Kesalahan pada konfigurasi software. • Server tidak dapat diakses • Hacking/Cracking
Data	
System of Interest	Data-data yang penting seperti Data Mahasiswa, Data Transaksi SIM, dan Data Keuangan
Komponen Utama	Kemungkinan Ancaman
• Database • Server • Listrik • PC • Firewall • Database Administrator (DBA)	• Pengubahan dan penghapusan data oleh pihak yang tidak berwenang. • Penyalahgunaan data untuk hal yang tidak diinginkan • Server mengalami kerusakan • Pemadaman listrik dari PLN

Fase 3 - Develop Security Strategy and Plans

Pada fase ke 3 akan dilakukan pengembangan rencana dan strategi keamanan untuk melakukan evaluasi risiko dari aset kritis. Fase ini dikerjakan dengan menggunakan output yang didapatkan dari fase 1 dan fase 2. Namun fase ini dibatasi untuk

tidak sampai dalam pengembangan strategi keamanan, oleh karena strategi keamanan nantinya akan dijabarkan pada bagian strategi BCP untuk risiko yang dinilai tinggi. Berikut adalah hasil daftar risiko yang didapatkan dari analisis OCTAVE.

Tabel 6.11 Daftar Risiko dari Analisis OCTAVE

No.	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
			Server tidak beroperasi	Gempa Bumi	1
				Banjir	2
				Kebakaran	3
				Kerusakan pada bangunan	4
				Kelalaian manusia	5
				Pemadaman listrik	6
				Genset dan UPS mati	7
			Kinerja server menurun	Processor memiliki terlalu banyak data	8
				RAM mengalami kelebihan memori	9
				Harddisk penuh	10
			Kerusakan data pada server	Serangan DDOS pada server	11
				Kelalaian Database Administrator	12

No.	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
			Data hilang	Virus	13
				Kelalaian Database Administrator	14
		PC	Kerusakan pada PC	Gempa Bumi	15
				Banjir	16
				Kebakaran	17
				Kerusakan pada bangunan	18
				Kelalaian Manusia	19
				Kerusakan pada monitor, keyboard, atau mouse	20
			PC tidak dapat beroperasi	Pemadaman Listrik	21
				Genset dan UPS mati	22
			PC terkena virus	Antivirus tidak *update*	23
				Virus yang berasal dari email	
2.	Software	• SIM Akademik • SIM Kepeg	SIM mengalami gangguan	Server down	24
				Pemadaman listrik	25
				SIM terkena serangan (*hacking*)	26

No.	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
		awaian • SIM Keuangan		SIM terkena virus	27
3.	Data	• Data Mahasiswa • Data Transaksi SIM • Data Keuangan	Data tidak dapat diakses	Pemadaman listrik	28
				Server mengalami down	29
			Manipulasi data	Terdapat *hacker* yang memanipulasi data	30
				Username dan password diketahui oleh pengguna lain	31
			Data hilang	Terdapat *hacker* yang mencuri data	32
				Kelalaian manusia	33
				Server rusak	34
4.	Jaringan	• Core Switch • Distribution Switch • Access Switch	Switch tidak dapat beroperasi	Beban koneksi melampui kemampuan switch	35
				Kerusakan pada koneksi dan konektor kabel	36
				Pemadaman listrik	37
				Overload	38
		Wifi dan Router	Internet Mati	Wifi rusak	39
				Pemadaman listrik	40
				Genset mati	41

No.	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
			Akses internet lambat	Kesalahan konfigurasi	42
5.	People	Pegawai Non-TI	Penyalahgunaan data organisasi	Penurunan kompetensi karyawan pegawai non TI	43
			Data yang ada tidak valid	Kesalahan dalam input data	44
			Pelanggaran regulasi	Penyalahgunaan akses regulasi	45
		Pegawai TI	Penyalahgunaan data organisasi	Penurunan kompetensi karyawan pegawai TI	46
			Data yang ada tidak valid	Kesalahan dalam input data	47
			Pelanggaran regulasi	Penyalahgunaan akses regulasi	48
		Dosen	Penyalahgunaan data organisasi	Penurunan kompetensi dosen	49
			Data yang ada tidak valid	Kesalahan dalam input data	50
		Mahasiswa	Sharing Password mahasiswa	Manipulasi data	51

Penilaian Risiko dengan FMEA

Setelah selesai melakukan proses identifikasi risiko, tahapan selanjutnya adalah dengan melakukan penilaian risiko berdasarkan FMEA. Penilaian dilakukan dengan memberikan skor dampak, kemungkinan, dan deteksi untuk masing-masin risiko. Untuk skala pemberian skor dapat melihat Bab 4 di bagian Pengolahan Data dan Informasi.
Untuk setiap risikoakan dilakukan perhitungan nilai nilai RPN (risk priority number), RPN digunakan untuk menilai tingkat prioritas dari setiap risiko yang muncul. Skala RPN dapat dilihat pada Bab 4 di bagian Pengolahan Data dan Informasi dan penilaian risiko dapat dilihat pada Lampiran E. Berikut merupakan tabel hasil penilaian risiko.

Tabel 6.12 Hasil Penilaian Risiko

Level Risiko	Risiko	ID Risiko	Penyebab Kegagalan	RPN	Jumlah
Very High	Server tidak beroperasi	4	Kerusakan pada bangunan	200	2
	Manipulasi data	30	Terdapat *hacker* yang memanipulasi data	200	
High	Server tidak beroperasi	7	Genset dan UPS mati	175	6
	SIM mengalami gangguan	24	Server down	144	
	Data tidak dapat diakses	29	Server down	126	
	Data hilang	32	Terdapat *hacker* yang mencuri data	160	
	Manipulasi data	31	Username dan password diketahui oleh pengguna lain	160	

Level Risiko	Risiko	ID Risiko	Penyebab Kegagalan	RPN	Jumlah
	Sharing password mahasiswa	51	Manipulasi data	168	
Medium	Server tidak beroperasi	6	Pemadaman listrik	98	13
	Kinerja server menurun	10	Harddisk penuh	96	
	Kerusakan data pada server	11	Serangan DDOS pada server	84	
	Kerusakan data pada server	12	Kelalaian Database Administrator	112	
	Kinerja server menurun	8	Processor memiliki terlalu banyak data	90	
	Data hilang	14	Kelalaian Database Administrator	84	
	SIM mengalami gangguan	25	Pemadaman listrik	96	
	SIM mengalami gangguan	26	SIM terkena serangan	105	
	Switch tidak dapat beroperasi	35	Beban koneksi melampaui kemampuan *switch*	112	
	Switch tidak dapat beroperasi	36	Kerusakan pada koneksi dan konektor kabel	96	

Level Risiko	Risiko	ID Risiko	Penyebab Kegagalan	RPN	Jumlah
	Switch tidak dapat beroperasi	38	Overload	84	
	Internet mati	39	Wifi rusak	84	
	Internet mati	40	Pemadaman listrik	84	
Low	Server tidak beroperasi	1	Gempa bumi	64	28
	Server tidak beroperasi	2	Banjir	48	
	Server tidak beroperasi	3	Kebakaran	72	
	Server tidak beroperasi	5	Kelalaian manusia	72	
	Kinerja server menurun	9	RAM mengalami kelebihan memori	72	
	Data hilang	14	Virus	42	
	Kerusakan pada PC	15	Gempa Bumi	30	
	Kerusakan pada PC	16	Banjir	30	
	Kerusakan pada PC	17	Kebakaran	50	
	Kerusakan pada PC	18	Kerusakan pada bangunan	45	
	Kerusakan pada PC	19	Kelalaian manusia	60	
	Kerusakan pada PC	20	Kerusakan pada monitor,	60	

Level Risiko	Risiko	ID Risiko	Penyebab Kegagalan	RPN	Jumlah
			keyboard, atau mouse		
	PC tidak beroperasi	21	Pemadaman listrik	63	
	PC tidak beroperasi	22	Genset dan UPS mati	36	
	PC terkena virus	23	Virus yang berasal dari email	40	
	SIM mengalami gangguan	27	SIM terkena virus	56	
	Data hilang	33	Kelalaian manusia	48	
	Switch tidak dapat beroperasi	37	Pemadaman listrik	70	
	Internet mati	41	Genset mati	42	
	Akses internet lambat	42	Kesalahan konfigurasi	72	
	Penyalahgunaan data organisasi	43	Penurunan kompetensi pegawai non TI	60	
	Data yang ada tidak valid	44	Kesalahan dalam input data	50	
	Pelanggaran regulasi	45	Penyalahgunaan akses regulasi	24	
	Penyalahgunaan data organisasi	46	Penurunan kompetensi pegawai non TI	54	

Level Risiko	Risiko	ID Risiko	Penyebab Kegagalan	RPN	Jumlah
	Data yang ada tidak valid	47	Kesalahan dalam input data	40	
	Pelanggaran regulasi	48	Penyalahgunaan akses regulasi	24	
	Penyalahgunaan data organisasi	49	Penurunan kompetensi dosen	36	
	Data yang ada tidak valid	50	Kesalahan dalam input data	45	

6.1.2.2 Analisis Dampak Bisnis

Pada penelitian ini, analisis dampak bisnis digunakan untuk menentukan proses operasional bisnis yang paling kritis, setelah menemukan proses operasional bisnis maka selanjutkanya akan dilakukan prioritisasi proses bisnis yang ada pada organisasi. Selain itu, analisis dampak bisnis juga dapat membantu perusahaan untuk melihat dampak yang ditimbulan terhadap suatu gangguan. Dampak bisnis tersebut dapat membantu organisasi untuk mengetahui batas waktu yang ditoleransi untuk gangguan pada proses bisnis. Pada penelitian ini analisis dampak bisnis dilakukan dengan acuan ISO 22317:2015 – business impact analysis.

Tahapan pada analisis dampak bisnis ini didapatkan dari hasil wawancara yang dilampirkan pada Lampiran A dan telah dilakukan verifikasi hasil analisis bisnis yang dilampirkan pada Lampiran C.

Prioritasi Layanan TI

Tahapan pertama dalam analisis dampak bisnis adalah dengan melakukan identifikasi layanan SI/TI beserta dengan

melakukan prioritisasi tingkat kritis dari tiap layanan. Berikut merupakan prioritisasi tingkat kritis untuk masing masing layanan TI yang dimiliki oleh organisasi.

Tabel 6.13 Prioritasi Layanan TI

Layanan TI	Tingkat Kritis	Keterangan
Pengembangan sistem informasi baru	Sangat Kritis	Pengembangan sistem informasi merupakan layanan TI utama yang terdapat di Sub Direktorat. Jika layanan ini terkena gangguan makan akan berdampak besar pada operasional organisasi
SIM Akademik	Sangat Kritis	SIM Akademik merupakan layanan TI yang berkaitan dengan proses perkuliahan dosen, mahasiswa, dan civitas akademika lain. Jika layanan ini terkena gangguan maka civitas akademika akan kesulitan saat ingin mengakses sistem.
SIM Keuangan	Kritis	SIM Keuangan merupakan layanan TI yang berisikan informasi keuangan seperti program kerja, pendapatan, dan rencana anggaran. Jika layanan ini terkena gangguan makan akan berdampak besar pada operasional organisasi
Melakukan penambahan fitur dari SI yang telah ada	Minor	Penambahanan fitur adalah proses yang dilakukan setelah pembuatan SI selesai dilakukan dan butuh penambahan fitur untuk meningkatkan kinerjanya.

Layanan TI	Tingkat Kritis	Keterangan
		Jika layanan ini terkena gangguan maka SI yang dibuat tidak bersifat dinamis dan tidak *user-friendly*.

Prioritisasi Proses Bisnis dan Aktivitas terkait SI/TI

Identifikasi Fungsional Bisnis yang Terlibat

Pada penelitian ini proses bisnis diidentifikasi dari masing masing fungsional bisnis yang memiliki keterkaitan maupun ketergantungan terhadap layanan TI organisasi. Berikut tabel penjelasan mengenai 4 fungsional bisnis yang terlibat :

Tabel 6.14 Fungsional Bisnis Yang Terlibat

Fungsional Bisnis	Keterangan
Developer	Developer merupakan bagian yang melakukan seluruh aktvitas yang berkaitan dengan kode untuk pembuatan sistem informasi di Subdirektorat Pengembangan Sistem Informasi. Developer melakukan pengembangan SIM baru yang sesuai dengan kebutuhan ITS serta melakukan penambahan fitur dari SIM yang ada untuk meningkatkan optimalitas.
Analyst	Analyst bertugas untuk mengevaluasi kegiatan-kegiatan proses bisnis perusahaan untuk mengidentifikaso dampak dari kegiatan tersebut. Analyst membantu dalam mempersiapkan segala kebutuhan yang digunakan untuk pembentukan SIM.
Dokumentasi	Dokumentasi merupakan bagian yang melakukan pencatatan tentang segala aktivitas dan sistem informasi dalam Sub Direktorat.

Identifikasi Proses Bisnis dan Akativitas TI yang Terlibat
Dari fungsional bisnis yang yang telah didefinisikan tersebut, kemudian dilakukan identifikasi kepada proses bisnis beserta aktivitas – aktivitasnya yang memiliki keterkaitan dan ketergantungan dengan layanan TI organisasi. Berikut merupakan contoh pengidentifikasian proses bisnis dan aktivitas terkait layanan TI. Untuk informasi selengkapnya dapat melihat buku produk.

Tabel 6.15 Proses Bisnis dan Aktivitas Layanan TI

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Aktivitas terkait layanan TI
Developer	Menyediakan aplikasi sistem informasi berbasis web	• Merencanakan Pengembangan Aplikasi Sistem Informasi berbasis web • Melaksanakan proses coding pembuatan aplikasi sistem • Memonitor proses pengembangan dan implementasi aplikasi sistem informasi • Memonitor hasil pengembangan aplikasi sistem informasi
	Mengelola aplikasi sistem informasi berbasis web	• Melakukan proses backup dan recovery sistem informasi di ITS • Memonitor proses perawatan sistem informasi di ITS • Mempersiapkan dan mengelola server backup

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Aktivitas terkait layanan TI
	Melakukan pengujian program atau modul sistem informasi	• Menguji basis data & jaringan. • Menguji sistem yang dibuat • Melakukan penilaian dan evaluasi terhadap komponen sistem
	Memaksimalkan kinerja aplikasi sistem informasi	• Menambahkan fitur pada sistem sesuai kebutuhan stakeholder • Integrasi sim yang belum terintegrasi • Meamasang user manual pada sistem informasi
	Menyelesaikan keluhan terkait sistem informasi di ITS	Melakukan perbaikan sistem informasi berdasarkan keluhan
Analyst	Menganalisis proses bisnis organisasi	• Mendokumentasikan proses-proses bisnis yang ada • Melakukan change management • Memonitor pelaksanaan proses-proses bisnis
	Memaksimalkan kinerja aplikasi sistem informasi	• Identifikasi penambahan fitur • Identifikasi dan pengecekan kesesuaian fitur-fitur sistem informasi dengan kebutuhan

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Aktivitas terkait layanan TI
		• Menganalisis kebutuhan stakeholder
Dokumentasi	Menyediakan aplikasi sistem informasi berbasis web	• Membuat dokumentasi program dan database sistem informasi • Membuat laporan kegiatan
	Memaksimalkan kinerja aplikasi sistem informasi	Inventarisasi aplikasi dan sistem informasi
	Melakukan dokumentasi keluhan terkait sistem informasi di ITS	• Mendata keluhan terkait sistem informasi di ITS • Membuat user manual sistem informasi

Melakukan Prioritisasi Proses Bisnis

Selanjutnya melakukan prioritasi proses bisnis untuk dapat mengetahui tingkat kepentingan dari masing-masing proses bisnis yang terkait dengan layanan TI. Berikut merupakan contoh prioritisasi proses bisnis dan aktivitas terkait layanan TI. Untuk informasi selengkapnya dapat melihat buku produk.

Tabel 6.16 Proses Bisnis Yang Terlibat

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Tingkat Kritis	Keterangan
Developer	Menyediakan aplikasi sistem informasi berbasis web	Sangat Kritis	Penyediaan sistem informasi berbasis web merupakan tujuan utama dari Sub Direktorat

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Tingkat Kritis	Keterangan
	Mengelola aplikasi sistem informasi berbasis web	Sangat Kritis	Mengelola komponen-komponen yang mendukung keberlangsungan dari sistem informasi, jika terjadi gangguan maka proses utama tidap dapat dijalankan
	Melakukan pengujian program atau modul sistem informasi	Kritis	Apabila terjadi gangguan maka sistem informasi yang telah dibuat tidak dapat diuji keberhasilannya.
	Memaksimalkan kinerja aplikasi sistem informasi	Kritis	Melakukan penambahan fungsi yang dibutuhkan oleh sistem, jika terjadi masalah tidak akan menggangu proses lain
	Menyelesaikan keluhan terkait sistem informasi di ITS	Kritis	Penyelesaian keluhan dari pengguna, jika terjadi gangguan akan berpengaruh pada kepuasan pengguna
Analyst	Menganalisis proses bisnis organisasi	Kritis	Dilakukan untuk mengevaluasi kegiatan-kegiatan proses bisnis organisasi agar berjalan sesuai keinginan
	Memaksimalkan kinerja aplikasi sistem informasi	Minor	Mengidentifikasi kebutuhan-kebutuhan yang diperlukan untuk memaksimalkan kinerja, jika terjadi masalah tidak menggangu proses lain

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Tingkat Kritis	Keterangan
Dokumentasi	Menyediakan aplikasi sistem informasi berbasis web	Kritis	Melakukan dokumentasi untuk setiap program dan sistem yang dibuat untuk kebutuhan di masa depan, jika terjadi masalah maka tidak akan ada pencatatan hasil penyediaan aplikasi
	Memaksimalkan kinerja aplikasi sistem informasi	Minor	Melakukan penghitungan jumlah sistem yang terdapat di ITS, jika terjadi masalah tidak akan mengganggu proses lainnya
	Melakukan dokumentasi keluhan terkait sistem informasi di ITS	Minor	Mencatat setiap keluhan yang nantinya akan diselesaikan, jika terjadi masalah tidak akan menggangu proses lainnya

Analisis Waktu Pemulihan

Setelah melakukan prioritasi dari masing masing proses bisnis, akan dilakukan identifikasi waktu pemulihan jika terjadi gangguan. Analisis waktu pemulihan dibagi menjadi tiga, yaitu sebagai berikut :

- **Maximum Tolerable Downtime (MTD)**
  MTD adalah jumlah waktu maksimal yang dapat ditoleransi oleh perusahaan terhadap kegagalan proses bisnis.
- **Recovery Time Objective (RTO)**
  RTO adalah jumlah waktu maksimal yang dapat ditoleransi oleh perusahaan untuk melakukan

pemulihan (*recovery*) terhadap proses bisnis setelah terjadinya bencana.

Berikut merupakan contoh hasil analisis waktu pemulihan untuk proses bisnis tertentu:

Tabel 6.17 Analisis Waktu Pemulihan

Fungsional Bisnis	Proses Bisnis	MTD	RTO
Developer	Menyediakan aplikasi sistem informasi berbasis web	≤ 120 jam	≤ 120 jam
	Mengelola aplikasi sistem informasi berbasis web	≤ 24 jam	≤ 12 jam
	Melakukan pengujian program atau modul sistem informasi	≤ 48 jam	≤ 12 jam
	Memaksimalkan kinerja aplikasi sistem informasi	≤ 24 jam	≤ 12 jam
	Menyelesaikan keluhan terkait sistem informasi di ITS	≤ 24 jam	≤ 12 jam
Analyst	Menganalisis proses bisnis organisasi	≤ 48 jam	≤ 12 jam
	Memaksimalkan kinerja aplikasi sistem informasi	≤ 36 jam	≤ 12 jam
Dokumentasi	Menyediakan aplikasi sistem	≤ 48 jam	≤ 24 jam

Fungsional Bisnis	Proses Bisnis	MTD	RTO
	informasi berbasis web		
	Memaksimalkan kinerja aplikasi sistem informasi	≤ 64 jam	≤ 12 jam
	Melakukan dokumentasi keluhan terkait sistem informasi di ITS	≤ 24 jam	≤ 14 jam

Analisis Dampak Gangguan

Pada analisis dampak gangguan dilakukan penilaian dampak dari masing masing proses bisnis apabila terjadi risiko. Dampak yang didapatkan oleh risiko dibagi menjadi tiga kategori, yaitu dampak dari finansial, reputasi dan dari target teknis. Berikut merupakan contoh hasil analisis dampak gangguan terhadap proses bisnis. Untuk informasi selengkapnya dapat melihat lampiran F.

Tabel 6.18 Analisis Dampak Gangguan

Fungsional Bisnis	Proses Bisnis Terkait	Dampak		
		Finansial	Reputasi	Target Proses Bisnis
Developer	Menyediakan aplikasi sistem informasi berbasis web	Menimbulkan kerugian finansial	Berdampak besar pada reputasi organisasi	Mengganggu 25% dari target proses bisnis
	Mengelola aplikasi sistem informasi berbasis web	Menimbulkan kerugian finansial biaya sebanyak <5%	Berdampak besar pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
	Melakukan pengujian program atau modul sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 10% dari target proses bisnis
	Memaksimalkan kinerja aplikasi sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak kecil pada reputasi organisasi	Mengganggu 10% dari target proses bisnis
	Menyelesaikan keluhan	Tidak menimbulka	Berdampak besar	Mengganggu 10% dari

Fungsional Bisnis	Proses Bisnis Terkait	Dampak		
		Finansial	Reputasi	Target Proses Bisnis
	terkait sistem informasi di ITS	n kerugian finansial	pada reputasi organisasi	target proses bisnis

6.1.2.3 Strategi BCP

Selanjutnya adalah pembuatan strategi BCP berdasarkan hasil analisis yang telah dilakukan sebelumnya yaitu analisis risiko dan analisis dampak bisnis. Strategi BCP merupakan salah satu hal yang penting pada dokumen BCP, strategi BCP dibuat untuk menjaga keberlangsungan dari proses bisnis yang penting oleh organisasi serta dapat juga dijadikan sebuah rencana untuk mitigasi dari risiko. Strategi yang dibuat nantinya merupakan strategi preventif, strategi saat terjadi gangguan dan strategi pemulihan.

Risiko yang dijadikan landasan pembuatan strategi BCP adalah risiko yang memiliki nilai RPN *Very High*, yaitu risiko server tidak beroperasi dan manipulasi data. Hal ini dikarenakan risiko ini dinilai merupakan risiko yang memiliki membahayakan proses bisnis organisasi apabila terjadi.

Berikut merupakan contoh strategi preventif untuk risiko server tidak beroperasi.

Tabel 6.19 Strategi Preventif Risiko 1

	Risiko: Server tidak beroperasi
	Penyebab: Kerusakan pada bangunan
Persiapan alat teknologi dengan pengadaan perangkat untuk pencegahan kerusakan pada bangunan	Untuk dapat melakukan pencegahan terhadap kerusakan bangunan, maka perlu dilakukan pengadaan terhadap ketersediaan perangkat untuk mencegah kerusakan seperti alat penangkal petir, alat komunikasi darurat, smoke detector. Diharapkan nantinya perangkat dapat tersedia dan berfungsi dengan baik saat terjadinya bencana.
Monitoring secara rutin kondisi gedung serta perangkat yang telah digunakan di ruang server.	Kerusakan pada bangunan dapat dicegah dengan memeriksa kondisi gedung secara rutin apakah masih memadai dan dapat bertahan jika terjadi gangguan, kondisi yang diperhatikan contohnya adalah letak penempatan server, atap ruang server, dan meja untuk menempatkan server. Begitu juga untuk peralatan keamanan yang sudah digunakan di ruang server harus diperiksa apakah masih dapat berfungsi dengan baik atau tidak
Backup data secara harian	Strategi backup data harian merupakan strategi yang dilakukan untuk mempermudah organisasi apabila terjadi kehilangan data akibat kerusakan server. Diharapkan nantinya strategi ini dapat meminimalisir data yang hilang.

Pelatihan untuk restore data saat server mengalami kerusakan	Saat terjadi kerusakan pada server diharapkan strategi pemulihan sistem operasional dapat dilakukan secepatnya. Untuk dapat menjalani strategi pemulihan dengan baik dibutuhkan pelalatihan restore

Berikut merupakan contoh dari strategi saat terjadi gangguan pada Server tidak beroperasi:

Tabel 6.20 Strategi Saat Terjadi Gangguan Risiko 1

	Risiko: Server tidak beroperasi
	Penyebab: Kerusakan pada bangunan
Pengamanan aset TI	Pada saat terjadi kerusakan maka tim BCP harus melakukan pengamanan terhadap aset TI kritis terlebih dahulu, terutama server utama. Pengamanan aset TI diharapkan dapat memberikan keamanan kepada aset kritis saat terjadi gangguan, diharapkan dengan melakukan hal ini dapat mengurangi dampak bencana terhadap proses bisnis TI.
Mengidentifikasi penyebab terjadinya bencana	Penyebab kerusakan harus diidentifikasi untuk bisa mendapatkan informasi lebih dalam tentang permasalahan. Jika kerusakan terjadi karena kesalahan manusia, organisasi dapat melakukan antisipasi lebih lanjut kepada pihak yang bertanggung jawab dalam kerusakan. Apabila bencana terjadi karena bukan kesalahan

	manusia, maka akan dilakukan langkah perbaikan terhadap kondisi lingkungan dari ruangan server.
Proses *Restore Data*	Pada saat server mengalami kerusakan dan kehilangan data-datanya, harus dilakukan strategi untuk mengembalikan data-data tersebut. Data dapat direstore menggunakan hasil back-up terbaru yang dilakukan. Untuk menghindari kehilangan data-data yang penting maka restore data dilakukan dengan memprioritaskan data kritis dahulu.
Melihat insiden yang pernah ada (Basis Pengetahuan)	Setelah mengidentifikasi penyebab risisko, dilakukan penelusuran dokumen untuk mencari pengetahuan yang berisi insiden yang pernah terjadi di masa lalu. Jika insiden tersebut merupakan pengulangan maka prosedur yang diikuti sebelumnya harus dilakukan dan dianalisis pada setiap langkah untuk mengetahui penyebab terulangnya kejadian dan memastikan apakah langkah-langkah tersebut
Mematikan sistem	Mematikan atau menonaktifkan sistem sementara akan mempermudah tim BCP dalam melakukan penanggulangan dampak bencana.
Melakukan perbaikan server	Proses perbaikan server ini dilakukan oleh tim BCP untuk dapat mengembalikan kondisi server seperti semula, setelah pemulihan selesai ketua BCP akan memutuskan kapan menempatkan sistem kembali serta memantau kinerja dari server setelah terjadi kerusakan

Berikut merupakan contoh strategi korektif untuk risiko Server tidak beroperasi.

Tabel 6.21 Strategi Korektif Risiko 1

	Risiko: Server tidak beroperasi
	Penyebab: Kerusakan pada bangunan
Mendokumentasi hasil insiden	Setelah terjadinya kerusakan diperlukan pembuatan dokumen hasil insiden yang berisikan informasi lengkap tentang insiden yang terjadi sebagai dokumentasi yang berguna di masa depan.
Mengevaluasi hasil dokumentasi insiden	Setelah pembuatan dokumentasi akan dilakukan proses evaluasi yang dilihat dari hasil dokumentasi dari insiden yang terjadi dan penanganan yang dilakukan. Proses evaluasi ini dapat membantu untuk mengetahui tindakan apa yang harus dilakukan jika insiden yang sama kembali terjadi di masa depan.
Peningkatan pertahanan	Setelah mengetahui *root cause* dari kejadian, perlu dilakukan peningkatan pertahanan keamanan agar tidak terjadi permasalahan yang sama di masa depan. Tim penanganan insiden dapat diberikan insiden serupa untuk melatih diri dan organisasi agar dapat memiliki kontrol keamanan baru untuk mengurangi risiko yang sama

Selain risiko Server tidak beroperasi, risiko lain yang memiliki RPN *Very High* adalah manipulasi data. Berikut adalah contoh strategi preventif dari risiko manipulasi data:

Tabel 6.22 Strategi Preventif Risiko 2

	Risiko: Manipulasi Data
	Penyebab: Terdapat *hacker* yang memanipulasi data
Pembentukan tim penanganan insiden	Pembentukan tim penanganan insiden serta membagi peran dan tanggung jawab bagi masing-masing anggota untuk menyiapkan jika gangguan terjadi. Selain itu menentukan metode kordinasi dan komunikasi antara tim dan penanggung jawab.
Backup data secara harian	Strategi backup data harian merupakan strategi yang dilakukan untuk mempermudah organisasi apabila terjadi kehilangan data *existing* akibat *hacker*. Diharapkan nantinya strategi ini dapat meminimalisir data yang hilang.
Monitoring secara rutin kondisi keamanan jaringan pada sistem informasi.	Manipulasi data dapat dicegah dengan melakukan monitoring kondisi perangkat keamanan yang digunakan organisasi secara rutin, kondisi yang diperhatikan contohnya adalah firewall, antivirus, antispyware, dll. Pastikan juga *software* keamanan yang digunakan selalu di *update* secara berkala.
Meninjau celah keamanan secara rutin	Untuk menghindari serangan dari *hacker* dibutuhkan peninjauan celah

	keamanan secara rutin dengan berbagai tools seperti *vulnerability scanner* atau *security audit*
Membuat pembagian tugas dan tanggung jawab bagi tiap SDM untuk melakukan kegiatan penanganan gangguan.	Perlu dilakukan pembagian tugas dan tanggung jawab yang jelas agar saat terjadi gangguan, SDM dapat melakukan penanganan dengan cepat. Pembagian tugas dan tanggung jawab juga dapat memudahkan dalam proses penanganan gangguan.

Berikut merupaka contoh dari strategi saat terjadi gangguan pada manipulasi data:

Tabel 6.23 Strategi Saat Terjadi Gangguan Risiko 2

	Risiko: Manipulasi Data
	Penyebab: Terdapat *hacker* yang memanipulasi data
Mengidentifikasi kerusakan yang terjadi	Saat terjadi gangguan langkah pertama yang harus diperiksa adalah dengan melihat sebesar apa manipulasi yang dilakukan oleh *hacker*, disini tim BCP melihat data apa saja yang diubah oleh *hacker*, selain itu mengidentifikasi darimana *hacker* dapat mendapat celah untuk masuk ke dalam sistem.
Proses *Restore Data*	Pada saat mengalami kehilangan data-data, harus dilakukan strategi untuk mengembalikan data-data tersebut. Data dapat direstore menggunakan hasil back-up terbaru yang dilakukan. Untuk menghindari kehilangan data-data yang penting maka restore data

	dilakukan dengan memprioritaskan data kritis dahulu.
Menonaktifkan sistem	Mematikan atau menonaktifkan sistem sementara untuk mencegah *hacker* untuk melakukan manipulasi lebih jauh lagi, menonaktifkan sistem juga dapat mempermudah tim BCP dalam melakukan penanggulangan dampak bencana.
Pemulihan terhadap metode akses	Pemulihan terhadap metode akses dapat dilakukan dengan mengganti password yang telah dimanipulasi, password-password tersebut harus diubah mengikuti mekanisme yang telah diberikan atau menjadikannya seperti keadaan *default.*

Berikut merupakan contoh strategi korektif untuk risiko Server tidak beroperasi.

Tabel 6.24 Strategi Korektif Risiko 2

	Risiko: Manipulasi Data
	Penyebab: Terdapat *hacker* yang memanipulasi data
Peningkatan pertahanan pada keamanan data	Setelah mengetahui *root cause* dari kejadian, perlu dilakukan peningkatan pertahanan keamanan contohnya pada aturan akses pada database server, sistem otentikasi dan otorisasi, dan perbaikan *password*
Mendokumentasi hasil insiden	Setelah terjadinya kerusakan diperlukan pembuatan dokumen hasil insiden yang berisikan informasi

	lengkap tentang insiden yang terjadi sebagai dokumentasi yang berguna di masa depan.
Membuat evaluasi dan rekomendasi hasil dokumentasi insiden	Setelah pembuatan dokumentasi akan dilakukan proses evaluasi yang dilihat dari hasil dokumentasi dari insiden yang terjadi dan penanganan yang dilakukan. Proses evaluasi ini dapat membantu untuk mengetahui tindakan apa yang harus dilakukan jika insiden yang sama kembali terjadi di masa depan.
Pembuatan basis pengetahuan baru	Pembuatan dokumen pengetahuan baru yang berisikan teknik serangan yang dapat terjadi serta kelemahan-kelemahan apa saja yang dimiliki oleh web server.
Melakukan perbaikan dan pembaharuan terhadap keamanan dari hasil insiden	Terjadinya manipulasi oleh *hacker* berarti terdapat celah pada sistem. Setelah ditemukan kelemahan dari sistem yang dapat menimbulkan serangan, maka diperlukan adanya strategi perbaikan dan pembaharuan seperti *code scanning* pemasangan *Network* IPS/IDS

6.1.2.4 Pelatihan dan Pengujian

Tahapan pelatihan dilakukan untuk dapat memberikan pengetahuan dan pemahaman kepada keseluruhan karyawan terhadap strategi perencanaan keberlangsungan bisnis maupun prosedur keberlangsungan bisnis yang berlaku. Tahapan pelatihan ini nantinya dibataskan pada penyusunan gambaran umum modul, dikarenakan nantinya pelatihan akan dijadwalkan dan dilakukan oleh pihak organisasi. Gambaran umum modul pelatihan ini nantinya akan dibuat sesuai dengan

strategi BCP yang telah ada. Berikut merupakan contoh modul pelatihan BCP, selangkapnya dapat melihat lampiran D.

Tabel 6.25 Skenario Pengujian BCP

SKENARIO PENGUJIAN BCP	
Pelaku	• Staff Subdirektorat Pengembangan 1 • Staff Subdirektorat Pengembangan 2 • Staff Subdirektorat Pengembangan 3 • Ketua Subdirektorat Pengembangan
Pembagian Peran	• Staff Subdirektorat Pengembangan 1 sebagai *hacker* • Staff Subdirektorat Pengembangan 2 sebagai pihak yang mengatasi serangan • Staff Subdirektorat Pengembangan 3 sebagai dokumentator • Ketua Subdirektorat Pengembangan sebagai pengawas proses pengujian
Skenario	1. Staff Subdirektorat Pengembangan 1 mencoba masuk dan melakukan manipulasi data organisasi 2. Staff Subdirektorat Pengembangan 2 mengidentifikasi serangan dan melaporkan kepada ketua subdirektorat pengembangan. 3. Ketua Subdirektorat Pengembangan memerintahkan untuk melakukan prosedur penanganan 4. Staff Subdirektorat Pengembangan 2 melakukan penanganan pada sistem yang dimanipulasi 5. Ketua Subdirektorat Pengembangan melakukan pengawasan tindakan perbaikan 6. Staff Subdirektorat Pengembangan 3 melakukan dokumentasi hasil pengujian BCP.

6.1.3 Check (Pemeriksaan)

Fase ketiga dari siklus deming adalah check atau pemeriksaan yang dilakukan untuk memeriksa seluruh proses yang ada di BCP telah sesuai dengan kebutuhan perusahaan serta tujuan bisnis organisasi. Fase check pada dokumen BCP ini berisi audit internal BCP serta peninjauan manajemen yang dilakukan oleh pihak tertinggi organisasi. Fase check dilakukan pada dokumen BCP sebagai kontrol internal, selain itu fase ini juga bertujuan untuk melihat adanya ketidaksesuaian terhadap kondisi kekinian organisasi.

6.1.3.1 Audit Internal Organisasi

Proses audit internal BCP menjadi peran penting dalam melakukan pemeriksaan keberhasilan implementasi BCP di organisasi, audit internal bertujuan untuk melakukan melihat efektivitas dari implementasi BCP yang telah dibuat. Pemeriksaan ini dilakukan oleh tim auditor BCP Sub Direktorat untuk memastikan bahwa implementasi BCP telah sesuai dan mengukur sejauh apa efektifitas BCP dalam menangani gangguan.

Audit internal ini akan dilakukan dengan menggunakan formulir audit checklist yang terdapat pada dokumen produk dan pada lampiran E.

Berikut merupakan beberapa hal yang harus dilakukan auditor saat menjalankan audit internal :

- Kesesuaian dokumen BCP dengan tujuan dan kebutuhan organisasi
- Kesesuaian dokumen BCP dengan kerangka standar yang digunakan
- Memastikan keberhasilan implementasi BCP
- Kesesuaian peran dan tanggung jawab setiap SDM dalam struktur Komite BCP
- Kesesuaian proses audit dengan perencanaan dan menjaga objektifitas dari hasil audit

6.1.3.2 Peninjauan Manajemen

Selain melakukan audit internal, pada fase check juga terdapat tahapan peninjauan manajemen atau management review yang dilakukan untuk memastikan bahwa BCP telah sesuai dengan kondisi, tujuan dan kebutuhan organisasi. Fase ini dilakukan oleh pihak manajemen dengan menggunakan formulir rapat peninjaaun yang tertera pada dokumen produk dan pada Lampiran F. Berikut adalah cakupan hal yang perlu ditinjau oleh pihak manajemen:

- Kondisi kekinian dari kegiatan yang telah ditinjau
- Adanya perubahan dari internal dan eksternal yang berkaitan dengan BCP.
- Informasi performa proses keberlanjutan bisnis yang dapat berupa pemantauan, evaluasi dan hasil audit internal bagian serta perusahaan.
- Hasil dari pengujian BCP.
- Rekomendasi untuk peningkatan BCP.

6.1.4 Act (Tindakan)

Fase terakhir pada siklus deming adalah *Act* (Tindakan) yang merupakan fase dimana organisasi melakukan peningkatan secara terus menerus (*continous improvement*) untuk kinerja BCP. Hal ini dilakukan agar BCP yang diimplementasikan dapat berfungsi hingga waktu yang lama dan menjadi BCP yang bersifat dinamis mengikuti perkembangan teknologi.

6.1.4.1 Peningkatan Terus-Menerus *(Continous Improvement)*

Peningkatan terus menerus (*continous improvement*) dilakukan untuk membantu BCP dalam meningkatkan dan meperbaiki setiap fasenya sesuai dengan perkembangan teknologi. Fase ini mendukung kebutuhan organisasi, bahwa teknologi informasi akan selalu berkembang, maka dari itu BCP harus selalu dinamis dan mengikuti perkembangan TI di dunia. Proses peningkatan secara terus-menerus atau continuous

improvement adalah sebuah proses yang dilakukan dari proses-proses sebelumnya seperti:

- Fase pelatihan dan pengujian sebagai bentuk validasi BCP
- Hasil audit internal TI bagian dan perusahaan.
- Hasil peninjauan manajemen

BAB VII
PENUTUP

Bab ini akan menjelaskan kesimpulan dari penelitian, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

Kesimpulan

Kesimpulan Pertama

Penelitian ini telah menghasilkan rancangan Business Continuity Plan berbasis risiko yang diformulasikan dengan kebutuhan organisasi dan kedua acuan standar kerangka kerja yaitu ISO 22301:2012 dan Griffith University. Business Continuity Plan merupakan suatu dokumen yang unik dimana harus dilandasi oleh kebutuhan masing-masing perusahaan, setiap perusahaan pasti mempunyai kebutuhan BCP yang berbeda tergantung dengan bidang dari bisnis yang dilakukannya. Dari situ maka dibutuhkan kerangka kerja dengan industri sejenis, dalam penelitian ini adalah kerangka kerja Griffith University, yang dapat membantu dalam pembuatan kerangka kerja BCP di bidang tertentu.

Untuk keberlanjutan penelitian ini, diharapkan rancangan BCP dari penelitian ini dapat terus dikembangkan, karena kerangka BCP dengan pendekatan risiko memerlukan sebuah fase peningkatan secara terus-menerus (continuous improvement) yang harus dilakukan secara rutin, dan diharapkan dokumen BCP dapat di implementasikan pada organisasi bidang pendidikan lainnya sesuai dengan langkah – langkah yang telah ditentukan.

Kesimpulan Kedua

Penelitian ini telah menjawab ketiga rumusan masalah penelitian dan tujuan penelitian yaitu:

1. Penelitian ini telah menghasilkan analisis risiko beserta penilaiannya untuk teknologi informasi STIE Perbanas yang

sesuai dengan metode OCTAVE dan FMEA. Dari hasil analisis risiko tersebut didapatkan kesimpulan sebagai berikut :

- Terdapat total 48 risiko yang didapatkan dari hasil analisis OCTAVE.
- Terdapat 2 risiko dengan level very high yaitu manipulasi data karena terdapat hacker yang memanipulasi data dan server tidak beroperasi karena kerusakan pada bangunan
- Terdapat 6 risiko dengan level high yaitu server tidak beroperasi karena genset dan ups mati, SIM mengalami gangguan karena server down, pencurian data karena hacker, data tidak dapat diakses karena server down, manipulasi data karena username diketahui pengguna lain dan sharing password mahasiswa karena pemadaman listrik
- Selain itu terdapat pula 11 risiko dengan level medium dan juga 29 risiko dengan level low

2. Penelitian ini telah menghasilkan analisis dampak bisnis untuk teknologi informasi STIE Perbanas sesuai dengan ISO 22317. Dari hasil analisis dampak bisnis tersebut didapatkan kesimpulan sebagai berikut :

- Terdapat 2 layanan TI yang bersifat sangat kritis pada STIE Perbanas yaitu pengembangan sistem informasi baru dan SIM Akademik, 1 layanan yang bersifat kritis yaitu SIM Keuangan dan 1 layanan bersifat minor yaitu melakukan penambahan fitur dari SI yang telah ada.
- Terdapat 4 proses bisnis dengan tingkat sangat kritis yaitu melaksanakan proses coding untuk pembuatan sistem informasi, melakukan backup database sistem informasi di ITS, menganalisis proses bisnis organisasi proses KRS, dan membuat dokumentasi program dan database sistem informasi.
- Terdapat identifikasi nilai MTD (*Maximum Tolerable Downtime*) dan RTO (*Recovery Time Objective*) serta penilaian dampak ditinjau dari segi finansial, reputasi dan target teknis untuk masing masing proses bisnis.

3. Penelitian ini telah menghasilkan rancangan Business Continuity Plan berbasis risiko yang telah diformulasikan dengan kebutuhan STIE Perbanas dan kedua acuan standar kerangka kerja ISO 22301:2012 dan Griffith University.

Saran

Saran untuk keberlanjutan penelitian ini

Dokumen BCP adalah dokumen yang terus berkembang, strategi yang dibuat pada dokumen ini mungkin saja akan berubah pada tahun-tahun kedepan karena kerangka BCP disusun dengan kebutuhan dari organisasi, dimana kebutuhan tersebut dapat berubah sesuai dengan perkembangan teknologi informasi. Saat kebutuhan organisasi berubah maka strategi pada penelitian ini juga otomatis berubah, maka dari itu dibutuhkan peningkatan terus-menerus (continous improvement) untuk kelangsungan dari penelitian ini kedepannya. Saran lainnya dari keberlanjutnya penelitian ini pada pengerjaan analisis risiko, untuk melihat kepada Log yang dimiliki oleh pihak DPTSI untuk dapat mengetahui tentang data historis terkait perangkat TI yang dimiliki oleh organisasi.

Saran untuk penelitian selanjutnya

Diharapkan dokumen BCP pada penelitian ini dapat di implementasikan pada organisasi pendidikan lainnya sesuai dengan langkah – langkah yang telah dijabarkan. Diharapkan juga dengan pembuatan dokumen BCP ini dapat membuat organisasi pendidikan lain lebih aware terhadapat pentingnya BCP pada organisasi TI. Sehingga organisasi maupun di bidang pendidikan atau yang lain dapat pula mengimplementasikan BCP untuk keberlanjutan proses bisnisnya.

DAFTAR PUSTAKA

[1] "Profil DPTSI," Direktorat Pengembangan Teknologi dan Sistem Informasi, 2013. [Online]. Available: http://dptsi.its.ac.id/?page_id=150.

[2] E. Arnold, Series on Seismology / Southeast Asia Association of Seismology and Earthquake Engineering, Malaysia, 1986.

[3] S. L. Putri, Perancangan Business Continuity Plan Untuk Teknologi Informasi Pada Studi Kasus STIE Perbanas, Surabaya, 2015.

[4] S. Snedaker, Business Continuity and Disaster Recovery For IT Professional, Elsevier. INC, 2014.

[5] U. Solehudin, "Business Continuity and Disaster Recovery Plan," *Proteksi dan Teknik Keamanan Sistem Informasi*, 2005.

[6] N. B. Kurniawan, "Manajemen Risiko Teknologi Informasi Studi Kasus Pada Badan Pusat Statistik Produk Layanan: Pelayanan Statistik Terpadu (PST)," 2013.

[7] C. Duffield dan B. Trigunarsyah, Project Management Conception to Completion, Engineering Education Australia, 1999.

[8] I. Soeharto, Manajemen Proyek, Dari Konseptual sampai Operasional, Jakarta: Erlangga, 1995.

[9] ISO 31000:2009, "Risk Management - Princples and Guidelines," 2009.

[10] M. Labombang, "Manajemen Risiko dalam Proyek Konstruksi," *SMARTek (Sipil, Mesin, Arsitektur, Elektro)*, pp. 1-2, 2011.

[11] S. Snedaker, Business Continuity and Disaster Recovery For IT Professional, Elsevier, Inc, 2014.

[12] C. a. D. Alberts, OCTAVE Method Implementation Guide V2.0, Pittsburgh, PA: Software Engineering Institute, Carnegie, 2005.

[13] B. Supradono, "Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE (Operationally Critical Threat, Asset, And Vulnerability Evaluation)," *Media Elektrika, Vol 2, No 1,* pp. 4-8, 2009.

[14] D. Stamatis, Failure Mode and Effect Analysis (FMEA): From Theory to Execution, Milwaukee, 2003.

[15] ISO/IEC 22301, Societal Security-Business Continuity Management Systems-Requirements., 2012.

[16] ISO 22317:2015, "Societal Security, Business Continuity Management Systems - Business Impact Analysis.," 2015.

[17] A. Hiles, The Definitive Handbook of Business Continuity Management. Second Edition, John Wiley & Sons, Ltd, 2007.

[18] C. Brooks, M. Bedernjak, I. Juran dan J. Merryman, "Disaster Recovery Strategy with Tivoli Storage," IBM, 2002.

[19] Griffith University, "Business Continuity Framework," Griffith University, 2013.

[20] A. Affandi, "Memorandum Akhir Jabatan Ketua Lembaga Pengembangan Teknologi & Sistem Informasi," Surabaya, 2016.

[21] IBM, "IT service management: is it now too important to leave to the IT department alone?," *IBM Global Technology Services,* p. 3, 2007.

[22] J. v. Bon, A. d. Jong, A. Kolthof, M. Pieper, R. Tjassing, A. Veen dan T. Verheijen, Foundations of IT Service Management Based on ITIL V3, Van Haren Publishing, 2007.

[23] Y. Haile-Selassie dan W. Hailegiorgis, "ICTET," 01 July 2011. [Online]. Available: http://www.ictet.org/downloads/Mas_5yR6lF_xX7n.pdf . [Diakses 22 October 2014].

[24] R. Esteves dan P. Alves, "Implementation of an Information Technology Infrastructure Library Process – The Resistance to Change," *Procedia Technology,* 2013.

[25] "Pink Elephent," 2005. [Online]. Available: http://pinkelephant.co.uk/itil-process-case-study/. [Diakses 22 October 2014].

[26] P. Elephant, "The Benefits of ITIL," *The Benefits of ITIL White Paper*, 2008.

[27] A. Rachmi, T. D. Susanto dan A. Herdiyanti, "Pembuatan Standard Operating Procedure (SOP) Service Desk Berdasarkan Kerangka Kerja ITIL V3 dengan Menggunakan Metode Analisis Gap Layanan (Studi Kasus : PT. XYZ, Tangerang)," *Jurnal Teknik Pomits*, vol. 3, 2014.

[28] R. S. P, T. Wurijanto dan E. Sutomo, "Stikom Institutional Repositories," 2013. [Online]. Available: http://sir.stikom.edu/647/. [Diakses 20 October 2014].

[29] S. D. Haes dan W. V. Grembergen, "IT Governance and Its Mechanisms," *Information Systems Control Journal*, 2004.

[30] I. Central, "ITIL Central," 2005. [Online]. Available: http://itsm.fwtk.org/History.htm. [Diakses 19 October 2014].

[31] A. Cartlidge, C. Rudd, M. Smith, P. Wigzel, S. Rance, S. Shaw dan T. Wright, An Introductory Overview of ITIL 2011, Norwich: TSO (The Stationery Office), 2012.

[32] UCISA, "UCISA," [Online]. Available: https://www.ucisa.ac.uk/representation/activities/ITIL/serviceoperation.aspx. [Diakses 17 October 2014].

[33] J. O. Long, ITIL 2011 at a Glance, Raleigh, 2012.

[34] "Boundless," 2013. [Online]. Available: https://www.boundless.com/marketing/textbooks/boundless-marketing-textbook/services-marketing-6/service-quality-51/the-gap-model-254-4140/. [Diakses 21 October 2014].

[35] "FAO Corporate Document Repositori," [Online]. Available: http://www.fao.org/docrep/w7295e/w7295e04.htm. [Diakses 22 October 2014].

[36] "EPA Quality System," 2008. [Online]. Available: http://www.epa.gov/quality/faq7.html. [Diakses 22 October 2014].

[37] K. P. A. N. d. R. B. R. Indonesia, "Pedoman Penyususnan Standar Operasional Prosedur Administrasi Pemerintahan," Jakarta, 2012.

[38] T. D. Susanto, Manajemen Layanan Teknologi Informasi, 2014.

[39] J. Warren, "KEY PERFORMANCE INDICATORS (KPI) – DEFINITION AND ACTION," *At Internet,* p. 5, 2011.

[40] "KPI Library," KPI Library, [Online]. Available: http://kpilibrary.com/. [Diakses 12 May 2015].

[41] "ITIL Wiki," AXELOS Limited, 13 September 2014. [Online]. Available: http://wiki.en.it-processmaps.com/index.php/ITIL_KPIs_Service_Operation. [Diakses 5 May 2015].

[42] IT Service Management Forum, An Introductory Overview of ITIL 2011, London: TSO (The Stationery Office), 2012.

[43] I. M. F. C. FISM, ITIL Process Assessment Framework, Britannia, 2010.

[44] Hendershott Consulting Inc, "ITIL Assessments," Hendershott Consulting Inc, 28 April 2010. [Online]. Available: http://hci-itil.com/options_assessment.html. [Diakses 20 December 2014].

[45] Unit Sistem Informasi PT. KAI (Persero) Daop 8 Surabaya, "Sekilas IT 8 Surabaya," Unit Sistem Informasi PT. KAI (Persero) Daop 8 Surabaya, Surabaya, 2014.

[46] Office of Government Commerce, Continual Service Improvement ITIL V3, Office of Government Commerce, 2007.

[47] Office of Government Commerce, ITIL Version 3 Service Operation, Office of Government Commerce, 2007.

[48] SWA Online, "IDC: Belanja TIK 2013 Capai US$ 32,8 Miliar," 2013. [Online]. Available: http://swa.co.id/business-research/idc-belanja-tik-2013-capai-us-328-miliar. [Diakses 24 December 2014].

[49] V. L. LAPÃO, Á. REBUGE, M. M. SILVA dan R. GOMES, "ITIL Assessment in a Healthcare Environment: The Role of IT Governance at Hospital São Sebastião," *Medical Informatics in a United and Healthy Europe*, 2009.

[50] IBM, “Leading Through Connections,” *Insight from the Global Chief Executive Officer Study*, pp. 12-13, 2012.

[51] K. A. Sakti dan H. P. Hadi, “Analisis Tingkat Kematangan Sistem Service Desk Kepegawaian Berdasarkan Framework ITIL V3 Kantor Badan Kepegawaian Daerah Provinsi Jawa Tengah,” *Jurnal Ilmiah Manajemen Teknologi Informasi Universitas Dian Nuswantoro Semarang*, 2014.

[52] Y. dan D. I. Sensuse, “Rancang Tata Kelola Service Desk Berbasis ITIL V3 Studi Kasus pada Hasnur Group,” *Jurnal Ilmiah Manajemen Teknologi Informasi Universitas Indonesia*, 2012.

[53] I. Wilson, “Service Support Assessment,” OGC, Research & Guidance (WFD), Norwich, 2001.

[54] E. Gummeson, Qualitative methods in management research, Chartwell-Bratt: Lund: Norway: Studentlitteratur, 1998.

[55] R. Yin, Case Study Research: Design and Methods, Beverly Hills: Calif: Sage Publications, 1984.

[56] J. McKinney, Constrctive Typology and Social Theory, New York: Aplleton-Century-Crofts, 1966.

[57] R. Smith, “"The logic and design of case study research"," *The Sport Psychologist*, vol. 2, pp. 1-12, 1988.

[58] R. Yin, Case Study Research Design and Method, Newbury Park: Sage, 1989.

[59] R. Yin, Case study research: Design and methods (3rd ed.), Thousand Oaks: CA: Sage, 2003.

[60] B. Potgieter, J. B. dan C. L. , “Evidence that use of the ITIL framework is effective,” dalam *Proceeding of the 18th Annual Conference of the National Advisory Committee on Computing Qualifications*, Tauranga, New Zealand, 2005.

Biodata Penulis

Penulis bernama lengkap Caesar Fajriansah, biasa dipanggil Caesar. Penulis dilahirkan di Jakarta, 23 Juni 1995. Penulis telah menempuh pendidikan formal di SDNP Komplek IKIP Jakarta, SMP Labschool Jakarta, dan SMA Labschool Jakarta. Setelah lulus dari sekolah menengah, penulis meneruskan pendidikan di Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya dan terdaftar dengan NRP 5210100179. Di Jurusan Sistem Informasi penulis mengambil bidang studi Manajemen Sistem Informasi (MSI).

Adapun pengalaman yang didapatkan penulis selama di ITS, yakni berkecimpung di organsiasi kemahasiswaan di Fakultas Teknologi Informasi selama dua tahun kepengurusan. Penulis pernah menjalani kerja praktik di Perusahaan Telekomunikasi yaitu PT. Telkom Indonesia Graha Merah Putih Jakarta pada Divisi IS Center selama kurang lebih 1,5 bulan pada tahun 2016.

Penulis memiliki hobi bermain musik dan berolahraga. Penulis juga memiliki mimpi untuk dapat memiliki website yang bergerak dibidang musik. Penulis dapat dihubungi melalui e-mail caesar.fajriansah@gmail.com

LAMPIRAN A- HASIL WAWANCARA

Tabel A. 1 Hasil Wawancara [1]

Tujuan Interview	:	Wawancara dilakakukan untuk mengetahui kondisi kekinian, proses bisnis, serta informasi mengenai penerapan teknologi infromasi dari Sub Direktorat Pengembangan Sistem Informasi.
Tanggal	:	Jumat, 11 November 2016
Waktu	:	10.00 – 10.45
Lokasi	:	Direktorat Pengembangan Teknologi dan Sistem Informasi
Narasumber	:	Anny Yuniarti, S.Kom., M.Comp.Sc
jabatan	:	Ketua Sub Direktorat Pengembangan Sistem Informasi DPTSI

Fase 1 Membangun aset berdasarkan ancaman profil	
Obyektif 1 : Mendapatkan informasi mengenai aset kritis teknologi informasi yang telah diterapkan organisasi	
No.	Pertanyaan
1.	Bagaimana proses umum penerapan teknologi informasi di bagian infrastruktur? **Jawaban:** Pusbang ITS menangani sistem informasi di lingkungan its, Melaksanakan penugasan dari rektor dan wakil rektor untuk membuat sistem informasi,
2.	Apa sajakah fungsional organisasi yang mendukung penggunaan teknologi dan sistem informasi? **Jawaban:** Kepala, langsung ke SDM ke tenaga pendidikan, developer, analisis proses bisnis, dan dokumentasi, bagian keuangan (administratif).

3.	SIM apasajakah yang dikembangkan dan dikelola oleh pihak LPTSI ? **Jawaban:** Terdapat banyak SIM yang dikembangkan dan dikelola, namun SIM yang diutamakan adalah 3 SIM besar yang terdiri dari SIM kepegawaian, SIM keuangan, dan SIM akademik, karena ketiga SIM tersebut memiliki tingkat kepentingan yang tinggi.
Obyektif 2: Menggali Informasi mengenai identifikasi ancaman terhadap aset teknologi dan informasi	
4.	Bagaimana ruang lingkup dari layanan pengembangan SIM yang disediakan oleh LPTSI? **Jawaban:** Ruang lingkup dari pengembangan SIM adalah pembuatan SIM dari awal hingga dapat diserahkan ke pelanggan/unit dan penambahan modul SIM yang sudah berjalan.
Obyektif 3: Menggali informasi mengenai praktik keamanan terkini yang telah dilakukan oleh organisasi	
5.	Apakah setiap user sistem memiliki hak akses yang berbeda? **Jawaban:** Iya setiap user memiliki hak akses yang berbeda
6.	Apakah organisasi menerapkan standar keamanan untuk melindungi aset teknologi dan sistem informasi? **Jawaban:** Pembaharuan metode penanganan permasalahan sehingga tidak terjadi pembobolan. Standar pembuatan sim baru databasenya disatukan jadi sql server, jika dulu ada yang mysqql, postgre. Sekarang ada kebijakan baru untuk pembuatan database di sql server.
7.	Apakah pernah terjadi gangguan akibat manusia misalnya pembobolan data? **Jawaban:**

	Yang paling baru adalah pembobolan Integra, yang melakukan *reset* dari data semua akun Integra.
Obyektif 4: Menggali informasi mengenai dampak bisnis dari dari layanan yang diberikan oleh organisasi	
8.	Apa saja layanan TI yang ada pada organisasi dan bagaimana tingkat prioritas untuk masing masing layanan? Jawaban: Terdapat kurang lebih 10 SIM yang dibuat oleh Sub Direktorat Pusbang, contohnya seperti SIM Akademik dan SIM kepegawaian.
9.	Apa saja aktivitas/proses bisnis yang berlangsung pada proses bisnis kritis yang dimiliki organisasi? Bagaimana prioritisasi aktivitas tersebut? **Jawaban:** Pada SIM Akademik contohnya, terdapat proses pengambilan mata kuliah atau FRS, jadwal mata kuliah, dll. Tidak terdapat prioritasi dari aktivitas tersebut.
10.	Apakah dampak yang terjadi pada layanan bila terjadi gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis) **Jawaban:** Dampaknya bisa dari beberapa kategori, bisa ke finansial, reputasi juga tujuan bisnis. Karena DPTSI berada dibawah ITS maka dapat memberikan citra buruk di mata Institut

Tabel A. 2 Hasil Wawancara [2]

Tujuan Interview	:	Pada wawancara ini akan digali lebih dalam lagi mengenai aset serta risiko TI yang terdapat pada DPTSI. Dilakukan juga identifikasi aset TI, kebutuhan keamanan, keamanan TI yang

		telah diterapkan, identifikasi ancaman dan risiko dan juga dampak terhadap proses bisnis kritis apabila terkena gangguan. Selain itu untuk mengetahui proteksi asset informasi, kebutuhan keamanan, keamanan TI yang telah diterapkan.
Tanggal	:	Rabu, 23 November 2016
Waktu	:	10.00-11.00
Lokasi	:	Direktorat Pengembangan Teknologi dan Sistem Informasi
Narasumber	:	Royyana M Ijtihadie, S.Kom.,M.Kom.,Ph.D
Jabatan	:	Ketua Sub Direktorat Infastruktur dan Keamanan Teknologi Informasi

Fase 1 Membangun aset berdasarkan ancaman profil	
Obyektif 1: Menggali Informasi mengenai identifikasi ancaman terhadap aset teknologi dan informasi	
1.	Apa sajakah aset teknologi yang dapat memberikan ancaman pada proses bisnis organisasi? **Jawaban:** Hardware - Server - PC Software - SIM Akademik - SIM Kepegawaian - SIM Keuangan Data - Data Mahasiswa - Data Transaksi SIM - Data Keuangan Network - Core Switch

	- Distribution Switch - Access Switch People - Pegawai TI - Pegawai Non-TI
2.	Apa saja kebutuhan keamanan untuk aset tersebut? **Jawaban:** - Server membutuh firewall, jaringan internet - AC harus menyala - Fire alarm menyala - Adanya sumber listrik cadangan - Listrik harus tetap menyala
3.	Bencana alam apa saja yang mungkin dapat terjadi dan mengancam aset teknologi dan sistem informasi di fungsional kritis perusahaaan? **Jawaban:** Semua kejadian dan musibah bisa saja terjadi
4.	Apakah pernah terjadi gangguan akibat manusia misalnya pembobolan data? **Jawaban:** Pernah terjadi pada SIM Integra
Obyektif 2: Menggali informasi kebutuhan keamanan yang dibutuhkan organisasi	
5.	Bagaimana usaha yang telah dilakukan organisasi dalam menghadapi ancaman yang ada? **Jawaban:** - Praktik *ring backup* antar *distribution switch* untuk jaringan - Mneghindari ancaman keamanan data dan rule/pengaturan data (virus) menggunakan firewall - Spam filter pada email - Hak akses berbeda
6.	Berapa kali organisasi melakukan backup data pada area fungsional bisnis kritis? **Jawaban:** Back-up Data dilakukan hanya jika dibutuhkan

7.	Berapa kali organisasi melakukan maintenance terhadap aset teknologi informasi yang mendukung fungsional bisnis kritis organisasi? **Jawaban:** Maintenance dilakukan jika dibutuhkan, yang di maintenance server, core switch, dan berbagai perangkat.
8.	Apakah terdapat mekanisme proteksi keamanan aset teknologi dan informasi pada fungsional bisnis kritis organisasi? **Jawaban:** Belum terdapat mekanisme proteksi keamanan dari aset teknologi informasi.
Obyektif 3: Mengidentifikasi kelemahan organisasi	
11.	Apakah terdapat SOP terkait keamanan teknologi dan informasi organisasi? **Jawaban:** SOP terkait keamanan teknologi belum ada
12.	Apakah terdapat permasalahan organisasi apabila terjadi gangguan pada aset teknologi dan informasi? **Jawaban:** Tentu saja, jika jaringan mati maka internet satu ITS pun akan mati, jika SIM akademik contohnya Integra mati maka mahasiswa dan dosen tidak bisa melakukan transaksi akademik.
Fase 2 Identifikasi Kelemahan Infrastruktur	
Obyektif 1 : Mengidentifikasikan komponen aset teknologi dan informasi yang diterapkan	
13.	Apa sajakah komponen TI yang digunakan pada fungsional kritis organisasi? **Jawaban:** Untuk server dibagi lagi untuk beberapa layanan, untuk data yang kritis contohnya adalah data mahasiswa, dan ketransaksi SIM. Untuk SIM yang termasuk kritis adalah SIM Akademik dan SIM Kepegawaian

14.	Apakah sistem memiliki kebutuhan infrastruktur yang sama? Jawaban: Tidak, setiap sistem memiliki kebutuhan insfrastruktur yang berbeda, karena sistemnya jelas berbeda dan fungsinya pun berbeda – beda.
	Apa saja kerentanan dari masing-masing komponen TI dari organisasi? **Jawaban:** Kinerja Procesor menurun akibat terlalu banyak akses transaksi • RAM mengalami kelebihan data • Terjadi pemadaman listrik dari PLN • Genset tidak dapat berfungsi karena mengalami kerusakan • CPU tidak dapat berfungsi karena mengalami kerusakan • Monitor, Keyboard, dan Mouse tidak berfungsi • Kerusakan pada kabel dan konektor jaringan • Antivirus tidak dapat mendeteksi virus • Gangguan atau kerusakan dikarenakan putusnya kabel • Konektor jaringan yang tidak terpasang dengan baik (longgar) • Susunan pengkabelan yang salah • Switch tidak bisa meneruskan traffic • Server tidak beroperasi • Hacking/Cracking • Pemadaman listrik
Obyektif 2 : Mengidentifikasikan kelemahan aset teknologi informasi yang diterapkan pada fungsional kritis organisasi	
15.	Kelemahan teknis apa saja yang terdapat pada organisasi terkait dengan teknologi informasi? **Jawaban:**

	Belum adanya SOP dan standar keamanan belum ada, back up data dilakukan bidang aplikasi bukan pada bagian infrastruktur sendiri. Lalu untuk *smoke detector* pada ruang server juga belum ada.
16.	Berapa lama waktu yang dibutuhkan oleh server untuk melakukan booting setelah kondisi server mati? Bagaimana cara backup yang dilakukan? **Jawaban:** Belum terdapat ketentuan seperti itu untuk server, untuk back-up dilakukan oleh bidang aplikasi bukan dari DPTSI.
Obyektif 3: Menggali informasi mengenai dampak bisnis dari dari layanan yang diberikan oleh organisasi	
17.	Apa saja layanan TI yang ada pada organisasi dan bagaimana tingkat prioritas untuk masing masing layanan? Jawaban: Terdapat banyak SIM yang dibuat oleh DPTSI, untuk tingkat prioritasi dilihat dari banyaknya *user* yang menggunakan saja.
18.	Apa saja aktivitas/proses bisnis yang berlangsung pada proses bisnis kritis yang dimiliki organisasi? Bagaimana prioritisasi aktivitas tersebut? **Jawaban:** Terdapat beberapa proses yang ada pada setiap SIM dan itu berbeda, jika SIM keuangan ya berarti terdapat proses terkait finansial seperti penggajian, dll. Jika SIM akademik berisi proses tentang perkuliahan.
19.	Apakah dampak yang terjadi pada layanan bila terjadi gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis) **Jawaban:** Jika terjadi kegagalan maka reputasinya berkurang di ITS.

20.	Apakah organisasi memiliki toleransi waktu dalam tahap pemulihan sistem apabila terjadi gangguan? **Jawaban:** Belum terdapat hal seperti toleransi dalam pemulihan sistem pada DPTSI

Tujuan Interview	:	Pada wawancara ini akan digali lebih dalam lagi mengenai aset serta risiko TI yang terdapat pada DPTSI. Dilakukan juga identifikasi aset TI, kebutuhan keamanan, keamanan TI yang telah diterapkan, identifikasi ancaman dan risiko dan juga dampak terhadap proses bisnis kritis apabila terkena gangguan. Selain itu untuk mengetahui proteksi asset informasi, kebutuhan keamanan, keamanan TI yang telah diterapkan.
Tanggal	:	Selasa, 17 Januari 2017
Waktu	:	10.00-11.00
Lokasi	:	Perpustakaan ITS Lantai 6
Narasumber	:	Cahya Purnama Dani, A.Md.
Jabatan	:	Staff Sub Direktorat Infastruktur dan Keamanan Teknologi Informasi

Fase 1 Membangun aset berdasarkan ancaman profil	
Obyektif 1: Menggali Informasi mengenai identifikasi ancaman terhadap aset teknologi dan informasi	
1.	Apa sajakah aset teknologi yang dapat memberikan ancaman pada proses bisnis organisasi? **Jawaban:**

	Aset kritis yang mampu memberi ancaman antara lain ada server serta data penting organisasi. Kerusakan pada server dapat menjadi ancaman terhadap hilangnya data. Lalu untuk perangkat lain juga terdapat beberapa kabel jaringan seperti switch. Selain itu untuk hardware terdapat sumber listrik cadangan untuk yaitu genset.
2.	Apa saja kebutuhan keamanan untuk aset tersebut? **Jawaban:** - Ruangan server harus memiliki perangkat keamanan - Spesifikasi kebutuhan keamanan tiap aset yang terverifikasi - Penyimpanan data backup di tempat yang aman - Log yang merekam setiap perubahan pada SIM - Pemasangan firewall pada server
3.	Bencana alam apa saja yang mungkin dapat terjadi dan mengancam aset teknologi dan sistem informasi di fungsional kritis perusahaaan? **Jawaban:** Bencana alam dapat terjadi kapan saja maka dari itu dibutuhkan lokasi yang aman untuk menempatkan aset.
4.	Apakah pernah terjadi gangguan akibat manusia misalnya pembobolan data? **Jawaban:** Untuk pembobolan di ruang server belum pernah terjadi. Karena akses keamanan menuju ruang fasilitas aset menggunakan *finger print* untuk menjaga keamanan, serta terdapat konfigurasi untuk standar keamanan.
Obyektif 2: Menggali informasi kebutuhan keamanan yang dibutuhkan organisasi	
5.	Bagaimana usaha yang telah dilakukan organisasi dalam menghadapi ancaman yang ada?

	Jawaban: Usaha kebanyakan masih dalm hal-hal teknis seperti memasang firewall dengan tingkat yang berbedauntuk keamanan sistem, memasang spam filter untuk setiap email yang masuk, memasang antivirus, hak akses yang berbeda dari setiap karyawan. Terdapat notifikasi ke bagian admin saat terjadi akses tidak berwenang, menerapkan enkripsi untuk melindungi aset informasi, juga diterapkan enkripsi dari password dan penggunaan https.
6.	Berapa kali organisasi melakukan backup data pada area fungsional bisnis kritis? **Jawaban:** Dilakukan backup secara berkala dan ada prosedur yang mengaturnya
7.	Berapa kali organisasi melakukan maintenance terhadap aset teknologi informasi yang mendukung fungsional bisnis kritis organisasi? **Jawaban:** Maintenance juga dilakukan jika dibutuhkan, proses maintenance dilakukan pada perangkat keras serta perangkat-perangkat jaringan.
8.	Apakah terdapat mekanisme proteksi keamanan aset teknologi dan informasi pada fungsional bisnis kritis organisasi? **Jawaban:** Mekanisme proteksi keamanan masih belum ada, penyelesaian gangguan keamanan masih berdasarkan pengalaman dan mengandalkan ilmu dari masing-masing staff.
Obyektif 3: Mengidentifikasi kelemahan organisasi	
9.	Apakah tersedia peraturan untuk mengamankan lokasi penting seperti ruang server dari risiko perangkat atau bahan yang dapat membahayakan aset informasi **Jawaban:**

	Tidak ada peraturan resmi dan tanda larangan. Untuk orang yang masuk juga tidak diperingatkan ataupun diingatkan dan tidak diperiksa
10.	Apakah terdapat permasalahan organisasi apabila terjadi gangguan pada aset teknologi dan informasi? **Jawaban:** Iya, staff di lantai 6 ini jadi tidak bisa bekerja. Jika terjadi gangguan juga staff jadi dapat bekerja lembur untuk memperbaiki.
Fase 2 Identifikasi Kelemahan Infrastruktur	
Obyektif 1 : Mengidentifikasikan komponen aset teknologi dan informasi yang diterapkan	
11.	Apa sajakah komponen utama TI yang terdapat pada pada fungsional kritis organisasi? **Jawaban:** Masing-masing dari aset memiliki komponen utama yang berbeda untuk server diantaranya processor, dan memory. Untuk jaringan ada switch, kabel, dll.
12.	Apakah kerentanan dari komponen utama TI yang ada di organisasi? **Jawaban**: Untuk server kerentanannya jaringan atau koneksi server dapat terputus, processor memiliki terlalu banyak data, genset juga bisa kehabisan bahan bakar. Untuk jaringan, kabel bisa saja rusak karena digigit tikus, switch sering *hang* dikarenakan terlalu banyaknya arus data, terjadinya looping pada switch, dll.
Obyektif 2 : Mengidentifikasikan kelemahan aset teknologi informasi yang diterapkan pada fungsional kritis organisasi	
13.	Kelemahan teknis apa saja yang terdapat pada organisasi terkait teknologi informasi? **Jawaban:** Belum terdapat prosedur pengamanan dan penggunaan dari aset TI organisasi, tidak tersedianya daftar data/informasi yang harus di-

	backup, pada organisasi belum terdapat proses pemeriksaan dan perawatan perangkat PC serta peraturan keamanan untuk ruang penempatan aset TI
14.	Apakah ruang penempatan aset TI telah dibuat sesuai dengan rancangan yang dapat menghindari dari ancaman seperti bencana alam (kebakaran, gempa, dl) serta dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai? **Jawaban:** Untuk ruang server yang di DPTSI telah sesuai dengan standar keamanan, namun untuk ruang server di lantai 6 masih belum mengikuti standar.
15.	Apakah terdapat proses pemeriksaan pada tiap aset yang digunakan untuk mengidentifikasi kemungkinan adanya celah kelemahan? **Jawaban:** Dilakukan pemeriksaan khususnya jaringan tetapi tidak secara rutin, hanya dilakukan jika terdapat insiden
Obyektif 3: Menggali informasi mengenai dampak bisnis dari dari layanan yang diberikan oleh organisasi	
16.	Apakah dampak yang terjadi pada layanan bila terjadi gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis) **Jawaban:** Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)
17.	Apakah dampak kerugian yang terkait dengan gangguan pada aset utama sudah ditetapkan sesuai dengan definisi yang ada? **Jawaban:** Sudah melakukan perencanaan dampak serta langkah-langkah mitigasinya

LAMPIRAN B – ANALISIS RISIKO

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
Hardware	Server	1	Server tidak beroperasi	8	Gempa Bumi	2	• Penurunan citra organisasi • Proses bisnis terhambat	3	Lokasi server terdapat di lantai 6	48
					Banjir	3		2	Lokasi server terdapat di lantai 6	48
					Kebakaran	3		3	Terdapat *fire extinguisher*	72
					Kerusakan pada bangunan	5		5	Pemantauan lingkungan lokasi penempatan server	200
					Kelalaian manusia	3		3	Pemberian informasi terkait penanganan server	72

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
		2	Server tidak beroperasi	7	Pemadaman listrik	7	• Penurunan citra organisasi • Proses bisnis terhambat	2	Terdapat Genset dan UPS saat listrik mati	98
					Genset dan UPS mati	5		5	Genset dan UPS diletakkan di lokasi yang aman	175
		3	Kinerja server menurun	6	Processor memiliki terlalu banyak data	5		3	Proses maintenance perangkat server	90

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
					RAM mengalami kelebihan memori	3	• Menurunnya produktivitas kinerja • Penurunan citra organisasi	4	Proses maintenance perangkat server	72
					Harddisk penuh	4		4	Proses maintenance perangkat server	96
		4	Kerusakan data pada server	7	Serangan DDOS pada server	3	Proses bisnis terhambat	4	Proses maintenance perangkat server	84

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
					Kelalaian Database Administrator	4		4	Peningkatan kompetensi Database Administrator	112
		5	Data hilang	7	Virus	2	• Berkurangnya reputasi di ITS • Proses bisnis terhambat • Penyalahgunaan data	3	Memasang anti virus	42
					Kelalaian Database Administrator	3		4	Peningkatan kompetensi Database Administrator	84

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
	PC	6	Kerusakan pada PC	5	Gempa Bumi	2	• Menurunnya produktivitas kinerja • Proses bisnis terhambat • Organisasi mengalami kerugian finansial	3	Lokasi ruang kerja dekat dengan pintu keluar	30
					Banjir	2		3	Lokasi ruang kerja cukup tinggi	30
					Kebakaran	2		5	Terdapat *fire extinguisher*	50
					Kerusakan pada bangunan	3		3	Gedung dari DPTSI merupakan gedung baru	45
					Kelalaian manusia	3		4	Karyawawn memiliki kemampuan terkait penanganan PC	60

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
					Kerusakan pada monitor, keyboard, atau mouse	4		3	Terdapat maintenance perangkat TI	60
		7	PC tidak dapat beroperasi	3	Pemadaman listrik	7	• Menurunnya produktivitas kinerja • Proses bisnis terhambat	3	Terdapat Genset dan UPS saat listrik mati	63
					Genset dan UPS mati	4		3	Genset dan UPS diletakkan di lokasi yang aman	36

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
		8	Data hilang	5	Data terkena virus	4	• Menurunnya produktivitas kinerja • Proses bisnis terhambat	2	• Melakukan *update* rutin untuk antivirus • Menggunakan spam filter	40
Software	• SIM Akademik • SIM Kepegawaian • SIM Keuangan	9	SIM tidak dapat diakses	8	Server down	6	• Menurunkan reputasi di ITS • Proses bisnis terhambat	3	Proses maintenance server	144
					Pemadaman listrik	6		2	Terdapat Genset dan UPS saat listrik mati	96
		10	SIM mengalami gangguan	7	SIM terkena serangan (*hacking)*	5		3	Terdapat *firewall* dan pengamanan jaringan	105

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
					SIM terkena virus	4		2	Menggunakan antivirus dan virus scanner	56
Data	• Data Mahasiswa • Data Transaksi SIM • Data Keuangan	11	Data tidak dapat diakses	7	Pemadaman listrik	6	• Menurunnya produktivitas kinerja • Proses bisnis terhambat	2	Terdapat Genset dan UPS saat listrik mati	84
					Server down	6		3	Proses maintenance server	126
		12	Manipulasi data	8	Terdapat *hacker* yang memanipulasi data	5	• Komplain dari civitas akademika • Proses bisnis terhambat	5	Penggunaan *firewall* dan pengamanan jaringan	200
					Username dan password	4		5	Diadakan sosialisasi dan pemberitahuan	160

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
					diketahui oleh pengguna lain				terkait akun untuk civitas akademika	
		13	Pencurian data	8	Terdapat *hacker* yang mencuri data	4	• Penyalahgunaan data • Menurunkan reputasi di ITS	5	Penggunaan *firewall* dan pengamanan jaringan	160
		14	Data hilang	8	Kelalaian manusia	3	• Komplain dari civitas akademika • Berkurangnya kepercayaan dari ITS	2	Telah memiliki karyawan TI yang kompeten dibidangnya	48
					Server rusak	3		4	Melakukan maintenance dan back up server	96

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
Jaringan	• Core Switch • Distribution Switch • Access Switch	15	Switch tidak dapat beroperasi	7	Beban koneksi melampaui kemampuan switch	4	• Komplain dari civitas akademika • Proses bisnis terhambat	4	Melakukan maintenance pada switch	112
				8	Kerusakan pada koneksi dan konektor kabel	4	• Komplain dari civitas akademika • Menurunkan reputasi di ITS	3	Melakukan maintenance pada switch	96
				7	Pemadaman listrik	5	• Komplain dari civitas akademika • Menurunkan reputasi di ITS	2	Melakukan maintenance pada switch	70

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
				7	Overload	4	• Komplain dari civitas akademika • Menurunkan reputasi di ITS	3	Melakukan maintenance pada switch	84
	Wifi dan Router	16	Internet mati	7	Wifi rusak	3	• Komplain dari civitas akademika • Proses bisnis terhambat • Produktivitas menurun	4	Melakukan maintenance pada perangkat TI	84
					Pemadaman listrik	6		2	Terdapat Genset dan UPS saat listrik mati	84
					Genset mati	3		2	Genset dan UPS diletakkan di lokasi yang aman	42

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
		17	Akses internet lambat	6	Kesalahan konfigurasi	4		3	Melakukan maintenance perangkat TI	72
People	Pegawai Non-TI	18	Penyalahgunaan data organisasi	5	Penurunan kompetensi pegawai non TI	3	Tersebarnya data organisasi	4	Telah memiliki karyawan non TI yang kompeten di bidangnya	60
		19	Data yang ada tidak valid	5	Kesalahan dalam input data	5	• Menurunkan reputasi di ITS • Komplain dari civitas akademika	2	Adanya pelatihan untuk karyawan	50

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
		20	Pelanggaran regulasi	4	Penyalahgunaan akses regulasi	2	Berkurangnya kepercayaan civitas akademika	3	Adanya kebijakan dari regulasi DPTSI	24
	Pegawai TI	21	Penyalahgunaan data organisasi	6	Penurunan kompetensi pegawai non TI	3	Tersebarnya data organisasi	*3*	Telah memiliki karyawan TI yang kompeten di bidangnya Melakukan evaluasi kinerja TI	54
		22	Data yang ada tidak valid	5	Kesalahan dalam input data	*4*	• Menurunkan reputasi di ITS • Komplain dari civitas akademika	*2*	Adanya pelatihan untuk karyawan	40

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
		23	Pelanggaran regulasi	4	Penyalahgunaan akses regulasi	2	Berkurangnya kepercayaan civitas akademika	3	Adanya kebijakan dari regulasi DPTSI	24
	Dosen	24	Penyalahgunaan data organisasi	6	Penurunan kompetensi dosen	2	Tersebarnya data organisasi	3	Adanya pelatihan dan sosialisasi untuk dosen	36
		25	Data yang ada tidak valid	5	Kesalahan dalam input data	3	Komplain dari civitas akademika	3	Adanya pelatihan dan sosialisasi untuk dosen	45

Kategori	Aset Terkait	ID Risiko	Risiko	SEV	Penyebab Kegagalan	OCC	Dampak	DET	Praktik Kontrol Organisasi	RPN
	Mahasiswa	26	Sharing password mahasiswa	7	Manipulasi data	6	• Komplain dari civitas akademika • Menurunkan reputasi di ITS	4	Sosialiasi kepada mahasiswa	168

“Halaman ini sengaja dikosongkan”

LAMPIRAN C - ANALISIS DAMPAK BISNIS

Prioritasi Proses Bisnis

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Tingkat Kritis	Keterangan
Developer	Menyediakan aplikasi sistem informasi berbasis web	Sangat Kritis	Penyediaan sistem informasi berbasis web merupakan tujuan utama dari Sub Direktorat
	Mengelola aplikasi sistem informasi berbasis web	Sangat Kritis	Mengelola komponen-komponen yang mendukung keberlangsungan dari sistem informasi, jika terjadi gangguan maka proses utama tidap dapat dijalankan
	Melakukan pengujian program atau modul sistem informasi	Kritis	Apabila terjadi gangguan maka sistem informasi yang telah dibuat tidak dapat diuji keberhasilannya.
	Memaksimalkan kinerja aplikasi sistem informasi	Kritis	Melakukan penambahan fungsi yang dibutuhkan oleh sistem, jika terjadi masalah tidak akan menggangu proses lain
	Menyelesaikan keluhan terkait sistem informasi di ITS	Kritis	Penyelesaian keluhan dari pengguna, jika terjadi gangguan akan berpengaruh pada kepuasan pengguna
Analyst	Menganalisis proses bisnis organisasi	Kritis	Dilakukan untuk mengevaluasi kegiatan-kegiatan proses bisnis

			organisasi agar berjalan sesuai keinginan
	Memaksimalkan kinerja aplikasi sistem informasi	Kritis	Mengidentifikasi kebutuhan-kebutuhan yang diperlukan untuk memaksimalkan kinerja, jika terjadi masalah tidak menggangu proses lain
Dokumentasi	Menyediakan aplikasi sistem informasi berbasis web	Kritis	Melakukan dokumentasi hasil pembuatan program dan sistem informasi untuk laporan di masa depan, jika terjadi gangguan akan mempersulit pembuatan aplikasi di masa depan.
	Memaksimalkan kinerja aplikasi sistem informasi	Minor	Melakukan inventarisasi jumlah sistem informasi yang ada di ITS, jika terjadi masalah tidak akan mengganggu proses lain
	Menyelesaikan keluhan terkait sistem informasi di ITS	Minor	Melakukan pencatatan untuk setiap keluhan untuk selanjutnya diperbaiki.

Analisis Dampak Gangguan

Risiko	Penyebab	Fungsional Bisnis	Proses Bisnis Terkait	Dampak		
				Finansial	Reputasi	Target Proses Bisnis
Server tidak beroperasi	• Gempa Bumi • Banjir • Kebakaran • Kerusakan pada bangunan • Kelalaian manusia	Developer	Menyediakan aplikasi sistem informasi berbasis web	Tidak menimbulkan kerugian finansial	Berdampak besar pada reputasi organisasi	Mengganggu 25% dari target proses bisnis
			Mengelola aplikasi sistem informasi berbasis web	Menimbulkan kerugian finansial biaya sebanyak <5%	Berdampak besar pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
			Melakukan pengujian program atau	Tidak menimbulkan kerugian finansial	Berdampak sedang pada	Mengganggu 10% dari target proses bisnis

			modul sistem informasi		reputasi organisasi	
			Memaksimalkan kinerja aplikasi sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak kecil pada reputasi organisasi	Mengganggu 10% dari target proses bisnis
			Menyelesaikan keluhan terkait sistem informasi di ITS	Tidak menimbulkan kerugian finansial	Berdampak besar pada reputasi organisasi	Mengganggu 10% dari target proses bisnis
		Analyst	Menganalisis proses bisnis organisasi	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
			Memaksimalkan kinerja aplikasi sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak sedang pada	Mengganggu 15% dari target proses bisnis

					reputasi organisasi	
		Dokumentasi	Menyediakan aplikasi sistem informasi berbasis web	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
			Memaksimalkan kinerja aplikasi sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
			Menyelesaikan keluhan terkait sistem informasi di ITS	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
Manipulasi Data	Terdapat *hacker* yang memanipulasi data	Developer	Menyediakan aplikasi sistem informasi berbasis web	Menimbulkan kerugian finansial biaya	Berdampak sedang pada	Mengganggu 25% dari target proses bisnis

	Username dan password diketahui oleh pengguna lain			sebanyak <5%	reputasi organisasi	
			Mengelola aplikasi sistem informasi berbasis web	Menimbulkan kerugian finansial biaya sebanyak <5%	Berdampak besar pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
			Melakukan pengujian program atau modul sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 10% dari target proses bisnis
			Memaksimalkan kinerja aplikasi sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 10% dari target proses bisnis
			Menyelesaikan keluhan terkait	Tidak menimbulkan	Berdampak besar pada	Mengganggu 15% dari

			sistem informasi di ITS	kerugian finansial	reputasi organisasi	target proses bisnis
		Analyst	Menganalisis proses bisnis organisasi	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
			Memaksimalkan kinerja aplikasi sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak kecil pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
		Dokumentasi	Menyediakan aplikasi sistem informasi berbasis web	Tidak menimbulkan kerugian finansial	Berdampak sedang pada reputasi organisasi	Mengganggu 15% dari target proses bisnis
			Memaksimalkan kinerja aplikasi sistem informasi	Tidak menimbulkan kerugian finansial	Berdampak kecil pada	Mengganggu 15% dari target proses bisnis

					reputasi organisasi	
			Menyelesaikan keluhan terkait sistem informasi di ITS	Tidak menimbulkan kerugian finansial	Berdampak besar pada reputasi organisasi	Menggangu 15% dari target proses bisnis

LAMPIRAN D – GAMBARAN UMUM MODUL PELATIHAN DAN PENGUJIAN BCP

	Gambaran Umum Modul Pelatihan Keberlanjutan Bisnis
Nama Pelatihan	Pelatihan *backup* dan *restore data*
Jenis Pelatihan	Pemberian materi dan praktik percobaan
Deskripsi Pelatihan	
Pelatihan backup dan restore data dilakukan untuk memberi pengetahuan umum mengenai back up dan restore data serta cara melakukannya. Materi yang terdapat pada pelatihan ini berisi tentang pengertian, manfaat, tujuan, tipe serta cara melakukan back up dan restore. Output dari pelatihan ini diharapkan SDM TI dapat memiliki wawasan mengenai tata cara melakukan back up dan restore dengan benar.	
Sasaran Pelatihan	Seluruh SDM TI
Materi Umum	
Materi yang diberikan kepada seluruh SDM TI adalah sebagai berikut: ▪ Penjelasan mengenai pentingnya *backup* dan *restore data* ▪ Prioritas data dalam melakukan *backup* ▪ Tata cara melakukan *backup* dan *restore data* ▪ Penjadwalan dari proses *backup* dan *restore data*	

	Gambaran Umum Modul Pelatihan Keberlanjutan Bisnis
Nama Pelatihan	Pelatihan antisipasi penyerangan sistem oleh *hacker*
Jenis Pelatihan	Pemberian materi dan praktik percobaan
Deskripsi Pelatihan	
Pelatihan dari antisipasi penyerangan sistem dari hacker memiliki tujuan untuk memberi pengetahuan terkait bagaimana tata cara penanganan sistem apabila terjadi penyerangan. Output dari pelatihan ini diharapkan dapat meningkatkan kemampuan bagian SDM TI dalam menangani insiden penyerangan.	
Sasaran Pelatihan	Seluruh SDM TI
Materi Umum	
Materi yang diberikan kepada seluruh SDM TI adalah sebagai berikut: • Pengetahuan umum mengenai penyeranganan hacker • Prosedur manajemen insiden • Prosedur keamanan data • Pembagian tanggung jawab saat terjadi insiden • Tata cara penanganan sistem dari penyerangan hacker	

	Gambaran Umum Modul Pelatihan Keberlanjutan Bisnis

Nama Pelatihan	Pelatihan pengamanan aset TI
Jenis Pelatihan	Pemberian materi dan praktik percobaan
Deskripsi Pelatihan	
Pada saat terjadi kerusakan perlu dilakukan harus melakukan pengamanan terhadap aset TI kritis, hal ini dapat mengurangi dampak bencana terhadap proses bisnis TI terutama aset TI kritis. Pengamanan aset TI juga diharapkan dapat memberikan keamanan kepada aset kritis saat terjadi gangguan.	
Sasaran Pelatihan	Seluruh SDM TI
Materi Umum	
Materi yang diberikan kepada seluruh SDM TI adalah sebagai berikut: • Pengetahuan mengenai pentingnya pengamanan aset TI • Prioritasi aset TI saat terjadi insiden • Pembagian tanggung jawab pengamanan saat terjadi insiden • Langkah–langkah pengamanan aset TI	

	Gambaran Umum Modul Pelatihan Keberlanjutan Bisnis
Nama Pelatihan	Pelatihan dan sosialisasi pengamanan data
Jenis Pelatihan	Pemberian materi dan sosialisasi
Deskripsi Pelatihan	
Pelatihan dan sosialisasi tentang keamanan data bertujuan untuk memberi pengetahuan tentang pentingnya keamanan data kepada seluruh karyawan DPTSI agar tiap karyawan dapat memiliki awareness yang tinggi terhadap data dan keamanannya. Output dari pelatihan ini adalah diharapkan dapat meningkatkan kesadaran seluruh karyawan dalam hal keamanan data.	

Sasaran Pelatihan	Seluruh SDM TI
Materi Umum	
Materi yang diberikan kepada seluruh SDM TI adalah sebagai berikut: • Pengetahuan umum serta penjelasan mengenai pentingnya memperhatikan keamanan data • Dampak yang diberikan dari tidak diperhatikannya keamanan data • Pengelolaan keamanan password dan prosedur manajemen password • Keamanan pada jaringan dan internet • Tata cara melakukan keamanan data	

SKENARIO PENGUJIAN BCP	
Pelaku	• Staff Subdirektorat Pengembangan 1 • Staff Subdirektorat Pengembangan 2 • Staff Subdirektorat Pengembangan 3 • Ketua Subdirektorat Pengembangan
Pembagian Peran	• Staff Subdirektorat Pengembangan 1 sebagai *hacker* • Staff Subdirektorat Pengembangan 2 sebagai pihak yang mengatasi serangan • Staff Subdirektorat Pengembangan 3 sebagai dokumentator • Ketua Subdirektorat Pengembangan sebagai pengawas proses pengujian
Skenario	7. Staff Subdirektorat Pengembangan 1 mencoba masuk dan melakukan manipulasi data organisasi 8. Staff Subdirektorat Pengembangan 2 mengidentifikasi serangan dan melaporkan kepada ketua subdirektorat pengembangan. 9. Ketua Subdirektorat Pengembangan memerintahkan untuk melakukan prosedur penanganan

	10. Staff Subdirektorat Pengembangan 2 melakukan penanganan pada sistem yang dimanipulasi 11. Ketua Subdirektorat Pengembangan melakukan pengawasan tindakan perbaikan 12. Staff Subdirektorat Pengembangan 3 melakukan dokumentasi hasil pengujian BCP.

SKENARIO PENGUJIAN BCP	
Pelaku	• Staff Subdirektorat Pengembangan 1 • Staff Subdirektorat Pengembangan 2 • Ketua Subdirektorat Pengembangan
Pembagian Peran	• Staff Subdirektorat Pengembangan 1 sebagai pelaku *backup* dan *restore data* • Staff Subdirektorat Pengembangan 2 sebagai dokumentator • Ketua Subdirektorat Pengembangan sebagai pengawas proses pengujian
Skenario	1. Staf Subdirektorat Pengembangan 1 melakukan backup data penting organisasi dari sistem 2. Ketua Subdirektorat Pengembangan menghapus data pada sistem yang sebelumnya telah dibackup. 3. Staff Subdirektorat Pengembangan 1 sebagai melakukan restore data dari data yang sebelumnya dihapus 4. Staff Subdirektorat Pengembangan 1 melihat kesesuaian data hasil restore dengan data backup yang sebelumnya dilakukan 5. Ketua Subdirektorat Pengembangan melakukan pengawasan pengujian

	6. Staff Subdirektorat Pengembangan 2 mendokumentasikan hasil pengujian backup dan restore data.

LAMPIRAN E - FORMULIR AUDIT INTERNAL

No.	Audit Checklist	Status			Evidence
		Yes	No	Partial	
1. Kebutuhan Keberlanjutan Bisnis Organisasi					
1.1	Apakah BCP telah diimplementasikan secara keseluruhan?				
1.2	Apakah dokumen BCP telah dipahami oleh keseluruhan organisasi?				
1.3	Apkah terdapat pihak senior management yang bertanggung jawab terhadap keseluruhan BCP?				
1.4	Apakah BCP yang dibuat mencakup risiko di bidang teknologi informasi di organisasi?				
1.5	Apakah BCP yang dibuat dapat mengurangi risiko yang timbul dari implementasi teknologi informasi?				
1.6	Apakah BCP yang dibuat telah memperhatikan aspek keberlanjutan operasional bisnis organisasi?				
1.7	Apakah BCP dapat mengikuti perkembangan dunia teknologi informasi?				

2. Tujuan BCP pada Organisasi					
2.1	Apakah dokumen BCP selaras dengan tujuan dan kebutuhan perusahaan?				
2.2	Apakah BCP telah berhasil meningkatkan keberlanjutan operasional bisnis organisasi?				
2.3	Apakah BCP dapat digunakan dalam jangka waktu yang panjang?				
2.4	Apakah BCP telah selaras dengan peraturan atau regulasi yang berlaku?				
2.5	Apakah BCP yang dibuat dapat diimplementasikan secara menyeluruh oleh organisasi?				
2.6	Apakah risiko teknologi informasi pada organisasi dapat diminimalisasi?				
2. Pengelolaan Strategi BCP					
3.1	Apakah strategi BCP telah disetujui oleh manajemen senior?				
3.2	Apakah strategi BCP telah dipahami oleh keseluruhan organisasi?				
3.3	Apakah organisasi telah mendokumentasikan strategi BCP jika terdapat gangguan				

3.4	Apakah strategi BCP telah didukung dengan prosedur yang jelas?				
3.5	Apakah strategi BCP telah dikomunikasikan kepada keseluruhan pegawai?				
3.6	Apakah strategi yang terdapat pada BCP telah berhasil diimplementasikan secara keseluruhan?				
3. Pelatihan dan Pengujian BCP di organisasi					
4.1	Apakah telah dilakukan pelatihan secara rutin untuk tim BCP?				
4.2	Apakah pelatihan telah dilakukan secara keseluruhan?				
4.3	Apakah hasil pelatihan telah terdokumentasikan?				
4.4	Apakah telah dilakukan pengujian secara rutin untuk tiap apek pada BCP?				
4.5	Apakah aspek yang diuji telah sesuai dengan SDM yang terkait?				
4.6	Apakah hasil pengujian telah terdokumentasikan?				
4. Pemeliharaan dan Peningkatan Terus-Menerus dari BCP					
5.1	Apakah terdapat prosedur pemeliharaan dari BCP?				

5.2	Apakah terdapat peninjauan untuk setiap proses BCP?				
5.3	Apakah terdapat proses untuk mengukur efektivitas BCP?				
5.4	Apakah terdapat proses untuk melakukan tindakan perbaikan dengan tujuan meningkatkan BCP?				
5.5	Apakah terdapat prosedur untuk meningkatkan kinerja BCP?				

‘‘Halaman ini sengaja dikosongka

LAMPIRAN F - FORMULIR PENINJAUAN MANAJEMEN

	**Formulir Peninjauan Manajemen**
	BCP Sub Direktorat Pengembangan Sistem Informasi
Tanggal dan Waktu Peninjauan	
Daftar Kehadiran Rapat	
Nama	Jabatan
Daftar Ketidakhadiran Rapat	
Nama	Jabatan
Disahkan Oleh	Dibuat Oleh

	Formulir Peninjauan Manajemen		
	BCP Sub Direktorat Pengembangan Sistem Informasi		
No.	Kontrol	Tindak Lanjut	Keterangan
1.	Hasil dari audit internal bagian		
2.	Perubahan internal perusahaan yang mempengaruhi BCP		
3.	Perubahan eksternal perusahaan yang mempengaruhi BCP		
4.	Sumber Daya Manusia dari BCP		
5.	Sumber Daya Teknologi Informasi dari BCP		
6.	Tinjauan keselarasan kebutuhan BCP dengan dokumen BCP		

7.	Evaluasi BCP		
8.	Rekomendasi untuk peningkatan BCP		

LAMPIRAN G - LAMPIRAN DOKUMEN KONFIRMASI KESESUAIAN HASIL ANALISIS RISIKO SUB DIREKTORAT PENGEMBANGAN SISTEM INFORMASI

SURAT KONFIRMASI

Kesesuaian Hasil Analisis Risiko untuk Sub Direktorat Pengembangan Sistem Informasi.

Dengan hormat,

Saya yang bertanda tangan dibawah ini:

Nama : Caesar Fajriansah

NRP : 5213100179

Pekerjaan : Mahasiswa Jurusan Sistem Informasi
Institut Teknologi Sepuluh Nopember

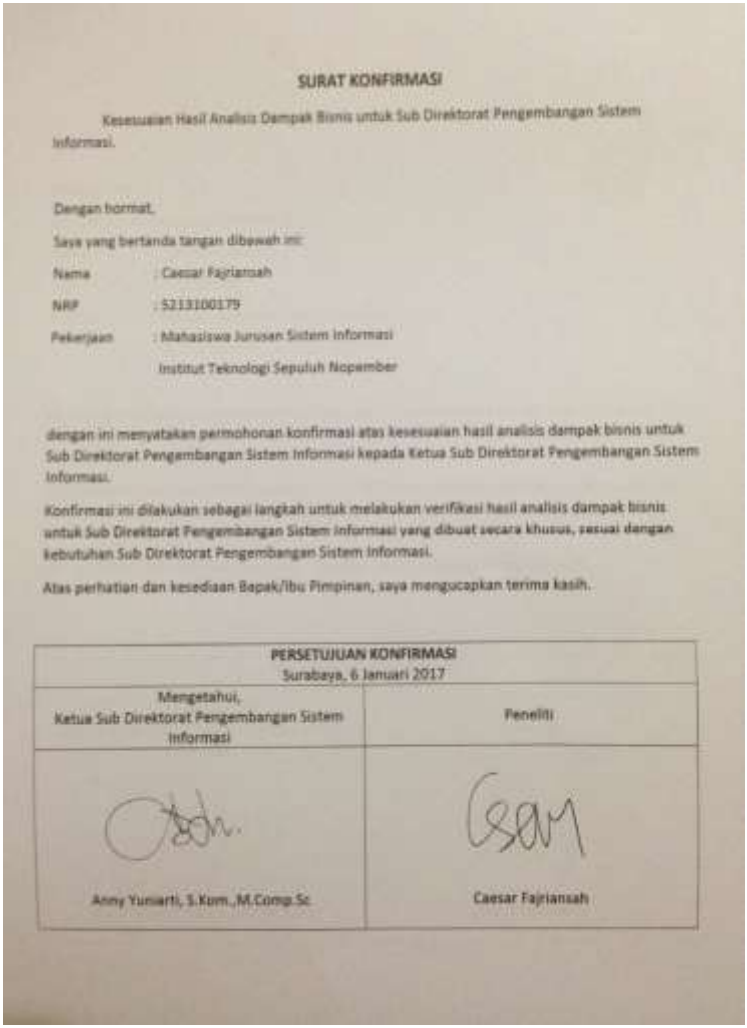
dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis risiko untuk Sub Direktorat Pengembangan Sistem Informasi kepada Ketua Sub Direktorat Pengembangan Sistem Informasi.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis risiko untuk Sub Direktorat Pengembangan Sistem Informasi yang dibuat secara khusus, sesuai dengan kebutuhan Sub Direktorat Pengembangan Sistem Informasi.

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

PERSETUJUAN KONFIRMASI Surabaya, 6 Januari 2017	
Mengetahui, Ketua Sub Direktorat Pengembangan Sistem Informasi	Peneliti
Anny Yuniarti, S.Kom.,M.Comp.Sc	Caesar Fajriansah

LAMPIRAN H - LAMPIRAN DOKUMEN KONFIRMASI KESESUAIAN HASIL ANALISIS DAMPAK BISNIS SUB DIREKTORAT PENGEMBANGAN SISTEM INFORMASI



SURAT KONFIRMASI

Kesesuaian Hasil Analisis Dampak Bisnis untuk Sub Direktorat Pengembangan Sistem Informasi.

Dengan hormat,

Saya yang bertanda tangan dibawah ini:

Nama : Caesar Fajriansah

NRP : 5213100179

Pekerjaan : Mahasiswa Jurusan Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis dampak bisnis untuk Sub Direktorat Pengembangan Sistem Informasi kepada Ketua Sub Direktorat Pengembangan Sistem Informasi.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis dampak bisnis untuk Sub Direktorat Pengembangan Sistem Informasi yang dibuat secara khusus, sesuai dengan kebutuhan Sub Direktorat Pengembangan Sistem Informasi.

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

PERSETUJUAN KONFIRMASI Surabaya, 6 Januari 2017	
Mengetahui, Ketua Sub Direktorat Pengembangan Sistem Informasi	Peneliti
Anny Yuniarti, S.Kom.,M.Comp.Sc	Caesar Fajriansah