TUGAS AKHIR – KS141501

PERANCANGAN *BUSINESS CONTINUITY PLAN* UNTUK TEKNOLOGI INFORMASI PADA STUDI KASUS STIE PERBANAS

Sabrina Leviana Putri
NRP 5212100050

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

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

FINAL PROJECT – KS141501

DESIGN OF *BUSINESS CONTINUITY PLAN* FOR INFORMATION TECHNOLOGY IN CASE STUDY STIE PERBANAS

Sabrina Leviana Putri
NRP 5212100050

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

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

Buku ini saya persembahkan untuk kedua orang tua tercinta, Ibunda Lusi Dyah Kumalawati dan Ayahanda Novyan Balia, yang selalu memberikan dukungan, semangat serta doa.

Buku ini juga dipersembahkan untuk adik kecil saya, M. Rizky Balia yang selalu menemani dan menghibur. Dik, teruslah berusaha untuk gapai mimpi - mimpimu.

KATA PENGANTAR

Segala puji hanya bagi Allah SWT, Tuhan semesta alam, atas kehendak, karunia dan rahmat dari-Nya telah mengantarkan penulis menyelesaikan tugas akhir yang berjudul "**Perancangan *Business Continuity Plan* untuk Teknologi Informasi pada Studi Kasus STIE PERBANAS".** Tugas akhir ini dibuat dalam rangka menyelesaikan gelar sarjana di Jurusan Sistem Informasi Fakultas Teknologi Informasi Institut Teknologi Sepuluh Nopember Surabaya.

Terima kasih tiada henti terucap untuk seluruh pihak yang sangat luar biasa dalam membantu penelitian ini, yaitu:

- Untuk Dosen Pembimbing, Dr. Apol Pribadi, S.T., M.T., terima kasih atas segala bimbingan, ilmu, semangat serta motivasi selama penelitian berlangsung.
- Untuk Bapak Dr. Aris Tjahyanto, M.Kom, selaku Ketua Jurusan Sistem Informasi ITS, yang telah menyediakan fasilitas terbaik untuk kebutuhan penelitian mahasiswa.
- Untuk Bapak Dr. Drs. Emanuel Kritijadi, MM, selaku Pembantu ketua I Bidang Akademik dan Bapak Hariadi Yutanto, S.Kom, M.Kom selaku Kasie TIK terima kasih telah memberikan informasi, pengetahuan selama penelitian.
- Untuk Ibu Feby Artwodini, S.Kom., M.T dan Ibu Anisah Herdiyanti, S.Kom., M.Sc sebagai dosen penguji peneliti, terima kasih atas kritikan dan masukan yang bersifat membangun untuk peningkatan kualitas penelitian ini.
- Untuk seluruh karyawan di STIE Perbanas, terima kasih atas segala informasi, bantuan serta dukungan untuk penelitian ini.
- Untuk sosok sahabat terbaik dalam setiap tahapan proses penelitian ini, Derry Azwar Rizaldy. Terima kasih untuk segala dukungan dan telah menjadi penyemangat saat masa penelitian.
- Untuk teman-teman yang bersama dengan peneliti mengambil proyek tugas akhir di STIE Perbanas yaitu Ardhana, Danar dan Andrianto, terima kasih untuk dukungannya.

- Untuk sahabat sekaligus *support system* terbaik yang saya miliki, Aulia, Laras, Ika, Asti, Anggun, Annisa dan Ameilia terima kasih telah selalu mendukung dan membantu segala proses penelitian.
- Untuk seluruh teman-teman Laboratorium PPSI dan teman – teman SOLA12IS, terima kasih untuk kebersamaannya dan dukungannya dalam penelitian.
- Untuk sahabat, orang orang terkasih serta seluruh pihak yang tidak bisa disebutkan satu-persatu di buku ini.

Diharapkan penelitian ini bisa bermanfaat untuk perkembangan penelitian mengenai perencanaan keberlangsungan bisnis pada organisasi pendidikan. Karena setiap insan tidak luput dari kesalahan, peneliti akan sangat sangat terbuka akan adanya kritik dan saran untuk penelitian selanjutannya.

LEMBAR PENGESAHAN

PERANCANGAN *BUSINESS CONTINUITY PLAN* UNTUK TEKNOLOGI INFORMASI PADA STUDI KASUS STIE PERBANAS

TUGAS AKHIR

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

Oleh:

SABRINA LEVIANA PUTRI
5212 100 050

Surabaya, Januari 2016

KETUA
JURUSAN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

PERANCANGAN *BUSINESS CONTINUITY PLAN* UNTUK TEKNOLOGI INFORMASI PADA STUDI KASUS STIE PERBANAS

TUGAS AKHIR

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

Oleh :

Sabrina Leviana Putri
5212 100 050

Disetujui Tim Penguji : Tanggal Ujian : Januari 2016
Periode Wisuda : Maret 2016

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

Feby Artwodini, S.Kom., M.T **(Penguji 1)**

a.n
Kaprodi SI

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

PERANCANGAN *BUSINESS CONTINUITY PLAN* UNTUK TEKNOLOGI INFORMASI PADA STUDI KASUS STIE PERBANAS

Nama Mahasiswa : SABRINA LEVIANA PUTRI
NRP : 5212 100 050
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing : Dr. Apol Pribadi S., S.T, M.T

ABSTRAK

Studi kasus pada penelitian ini adalah STIE (Sekolah Tinggi Ilmu Ekonomi) Perbanas yang merupakan suatu perguruan tinggi dan bergerak di bidang pendidikan. STIE Perbanas menggunakan teknologi informasi untuk mendukung jalannya operasional proses bisnis dan untuk dapat mendukung 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). Dokumen BCP diharapkan dapat membantu STIE Perbanas untuk mengambil tindakan saat terjadi ancaman dan bencana.

Metode yang dilakukan dalam penelitian ini adalah melakukan formulasi kerangka kerja BCP dan 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 dan Kerangka Kerja BCM Griffith University.

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. Hasil dokumen BCP yang telah sesuai tersebut kemudian akan diverifikasi dan divalidasi oleh organisasi.

Kata Kunci: Business Continuity Plan, Griffith University, ISO 22301:2012, Manajemen Risiko, Risiko, Teknologi Informasi.

DESIGN OF BUSINESS CONTINUITY PLAN FOR INFORMATION TECHNOLOGY IN CASE STUDY STIE PERBANAS

Name	**: SABRINA LEVIANA PUTRI**
NRP	**: 5212 100 050**
Department	**: Information Systems FTIF -ITS**
Supervisor	**: Dr. Apol Pribadi S., S.T, M.T**

ABSTRACT

The case studies in this research is STIE (Sekolah Tinggi Ilmu Ekonomi) Perbanas which is a college that engaged in education field. STIE Perbanas use information technology (IT) to support their business processes and operational activities also to support their information technology services. To be able to maintain business continuity, organization need a plan that would identify risks to the disaster then provide procedures and strategies to reduce or minimize risk. This plan is called the Business Continuity Plan (BCP). BCP document is expected to help STIE Perbanas to take action in the event of threats and disasters.

The method used in this research is to conduct BCP framework formulation and perform risk analysis and business impact analysis. BCP framework formulation is done by identify the needs and desires of the organization's business continuity and adjust it with BCP standard framework that is used as a reference, ISO 22301: 2012 and BCM Framework Griffith University. From the results of the formulations organization will have BCP framework that suitable to the needs of the organization.

BCP document produced by reviewing the results of the risk assessment and business impact assessments that were adjusted to the results of BCP formulation framework. So later, organization

will be able to have a BCP document that suitable with the needs and desires of the organization. Result of BCP document that are compliant will then be verified and validated by the organization.

Keywords: Business Continuity Plan (BCP), Griffith Universtiy, ISO 22301:2012, risk, risk management, information technology.

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

Pendidikan adalah salah satu faktor utama yang berperan penting dalam pembangunan nasional. Becker mengatakan bahwa seseorang dapat menginvestasikan diri mereka sendiri melalui pendidikan, pelatihan dan pengembangan keterampilan baru. Investasi manusia ini kedepannya akan menghasilkan aliran pendapatan di masa mendatang (Becker, 1976). Sebagai investasi, pendidikan akan menghasilkan dua tingkat balikan (return), yaitu tingkat balikan individu (individual return) dan tingkat balikan sosial (social return). Sehingga tidak hanya pendidikan dapat membantu individu, namun pendidikan juga secara tidak langsung berdampak pada taraf hidup masyarakat (Ali, 2009). Menurut Schultz, pendidikan sebagai komponen konsumsi yang bersifat tetap merupakan sumber penggunaan masa depan yang sama sekali tidak masuk dalam pendapatan nasional terukur (Schultz, 1965).

Dengan tingginya tingkat kompetitif global, organisasi pendidikan juga bersaing untuk dapat memberikan layanan edukasi yang sebaik-baiknya. Salah satu usaha yang dilakukan adalah dengan melakukan implementasi sistem informasi atau teknologi informasi. Sistem Informasi pada suatu perguruan tinggi biasanya lebih kompleks daripada sistem informasi yang ada pada organisasi komersil dan harus memberikan perhatian terhadap kustomernya (pelajar dan pekerja) (Luo and Warkentin, 2004). Tingginya penggunaan penerapan teknologi informasi pada organisasi pendidikan menghadirkan berbagai peluang dan juga tantangan baru (Awad & Battah, 2011).

Salah satu tantangan organisasi pendidikan adalah bagaimana dapat menghadapi ancaman, salah satunya bencana alam. Kondisi letak geografi Infonesia 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 (Arnold, 1986).

Walaupun terdapat berbagai macam ancaman yang dihadapi organisasi pendidikan, pada kenyataannya belum banyak organisasi yang melakukan perisapan apabila hal itu terjadi. Pada survey yang dilakukan COMDISCO, 82% perusahaan tidak memiliki persiapan apa – apa terkait bencana yang dapat terjadi pada sistem komputer yang mereka miliki (COMDISCO, 1997). Pada survey lain yang dilakukan oleh IBM, 92 % dari bisnis yang dilakukan melalui internet tidak memiliki persiapan apapun apabila terjadi bencana terkait teknologi informasi (IBM, 2009). Survey ini dilakukan kepada 224 pimpinan perusahaan di seluruh dunia.

Menurut studi yang dilakukan pada organisasi –organisasi di Amerika Serikat yang telah mengalami bencana, 40% dari organisasi tersebut lumpuh terkena dampak dari bencana sehingga tidak dapat melanjutkan operasi bisnisnya lagi dan 25% dari organisasi tersebut berhasil menjalankan kembali setelah menutup bisnisnya dalam kurang lebih tiga tahun (Doughty, 2000). Hal ini menunjukkan bahwa dalam perkembangannya, organisasi pendidikan tidak hanya perlu untuk menggunakan teknologi informasi, namun juga perlu untuk mempersiapkan pengelolaan risiko dengan benar sehingga organisasi dapat merespon ancaman yang terjadi.

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. Manajemen risiko adalah suatu kegiatan untuk mengidentifikasi risiko, menganalisa risiko dan merespon terhadap

risiko (Merna & Al-Thani, 2008). Dengan melakukan manajemen risiko maka, perusahaan dapat memimalisir 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.

Selain itu untuk dapat tetap menjalankan proses bisnisnya dalam situasi normal maupun kritikal dan memiliki ketahananan terhadap risiko yang mungkin terjadi, maka suatu organisasi perlu memiliki perencanaan keberlangsungan bisnis atau yang biasa disebut dengan business continuity planning (BCP). BCP memiliki fokus utama terhadap: bagaimana menjamin kontinyuitas dari bisnis ketika kehilangan akses terhadap manusia, fasilitas, sistem informasi, layanan dan sumber daya (Snedaker, 2014).

Berdasarkan uraian tersebut, maka perguruan tinggi dipilih sebagai obyek yang akan diteliti berkaitan dengan peran perguruan tinggi sebagai salah satu bentuk dukungan terhadap pendikan dan perekonomian nasional. Menurut UUD No. 20 tahun 2003 pasal 20 ayat 1 dan 2, perguruan tinggi dapat berupa akademi, politeknik, sekolah tinggi, institut atau universitas dan perguruan tinggi berkewajiban menyelenggarakan pendidikan, penelitian dan pengabdian terhadap masyarakat.

Pada penelitian ini akan dilakukan perancangan BCP yang sesuai untuk STIE PERBANAS yang merupakan sekolah tinggi ilmu ekonomi yang berlokasi di Surabaya, Indonesia. Melalui surat Keputusan Menteri Pendidikan dan Kebudayaan RI No. 0510/0/1985 tanggal 12 Agustus 1985, dilaksanakan perubahan bentuk dan nama dari Akademi Ilmu Perbankan PERBANAS Surabaya (AIP PERBANAS Surabaya) menjadi Sekolah Tinggi Ilmu Ekonomi PERBANAS Surabaya (STIE PERBANAS Surabaya). STIE PERBANAS menyelenggarakan pendidikan untuk beberapa program studi yaitu pasca sarjana, strata 1 akuntansi, strata s1 manajemen, diploma akuntansi dan diploma akuntansi & perbankan.

STIE Perbanas menggunakan Teknologi Informasi dalam proses bisnisnya dan untuk mengelola layanan yang dimiliki. Walaupun telah memiliki aset teknologi informasi yang berjalan, STIE Perbanas 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. Salah satu bencana yang telah terjadi pada STIE Perbanas adalah kebakaran pada ruang server data pada pertengahan tahun 2015. Kejadian ini meningkatkan kewaspadaan organisasi akan pentingnya pengelolaan risiko dan perancangan BCP.

STIE Perbanas 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. STIE Perbanas memerlukan kerangka BCP yang disesuaikan dengan kebutuhan dan juga kondisi kekinian organisasi untuk memudahkan organisasi dalam menjaga keberlanjutan proses bisnisnya.

1.2 Rumusan Permasalahan

Berdasarkan latar belakang diatas, maka rumusan masalah yang akan diteliti pada Tugas Akhir ini adalah sebagai berikut :

1. Apa hasil analisis risiko pada STIE Perbanas?
2. Apa hasil analisis dampak bisnis pada STIE Perbanas?
3. Bagaimana rancangan Business Continuity Plan berbasis risiko yang sesuai dengan kebutuhan STIE Perbanas?

1.3 Batasan Masalah

Berdasarkan perumusan masalah diatas, maka batasan

masalah dari Tugas Akhir ini adalah sebagai berikut:

1. Penelitian ini dilakukan pada bagian Teknologi Informasi STIE Perbanas
2. Analisis risiko terbatas terhadap analisis risiko yang ada pada bagian Teknologi Informasi STIE Perbanas
3. Proses pengerjaan BCP fokus pada proses bisnis kritis dan risiko TI yang bernilai tinggi pada STIE Perbanas
4. Metode yang digunakan untuk penelitian adalah wawancara dan observasi dengan menggunakan referensi OCTAVE dan FMEA untuk manajemen risiko, ISO 22317:2015 untuk analisa dampak bisnis serta Kerangka Kerja BCMS ISO 22301:2012 dan Kerangka Kerja Griffith University untuk manajemen keberlangsungan bisnis.

1.4 Tujuan Penelitian

Tujuan yang diharapkan dari penelitian tugas akhir ini adalah sebagai berikut:

1. Menghasilkan identifikasi dan penilaian risiko pada teknologi informasi STIE Perbanas
2. Menghasilkan identifikasi faktor kritis pada teknologi informasi STIE Perbanas
3. Menghasilkan rancangan kerangka kerja *Business Continuity Plan* (BCP) yang sesuai dengan kebutuhan STIE Perbanas
4. Menghasilkan *Business Continuity Plan* (BCP) yang berbasis risiko untuk STIE Perbanas

1.5 Manfaat Penelitian

Manfaat yang didapat dari penelitian tugas akhir ini adalah sebagai berikut:

1. Perusahaan mengetahui risiko-risiko yang dapat muncul pada bagian Teknologi Informasi STIE Perbanas
2. Perusahaan mengetahui faktor kritis dari analisa dampak bisnis yang ada pada bagian Teknologi Informasi STIE Perbanas
3. Perusahaan mendapatkan acuan kerangka kerja Business Continuity Plan (BCP) yang sesuai dengan kebutuhan STIE Perbanas
4. Perusahaan memiliki sebuah rancangan Business Continuity Plan (BCP) berbasis risiko

1.6 Sistematika Penulisan

Sistematika penulisan dari buku tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini dijelaskan mengenai latar belakang, perumusan masalah, batasan masalah, manfaat, tujuan, sistematika penulisan dan relevansi yang diterapkan dalam memaparkan tugas akhir.

BAB II TINJAUAN PUSTAKA

Pada bab ini dijelaskan mengenai referensi atau acuan yang digunakan untuk membantu pengerjaan Tugas Akhir yang meliputi risiko, manajemen risiko, OCTAVE, metode FMEA, Business Impact Analysis (BIA), ISO 22317:2015, Business Continuity Management Systems, Business Continuity Planning (BCP), Disaster Recovery Plan (DRP), Kerangka Kerja BCMS ISO 22301:2012, Kerangka Kerja BCM ISO Griffith University dan Profil STIE Perbanas.

BAB III METODOLOGI PENELITIAN

Pada bab ini dijelaskan mengenai langkah–langkah penelitian tugas akhir yang dilakukan. Langkah–langkah yang

digunakan terangkum dalam sebuah diagram sistematis dan akan dijelaskan tahap demi tahap.

BAB IV PERANCANGAN

Pada bab ini dijelaskan mengenai bagian perancangan yang mencakup profil organisasi yang berkaitan dengan penelitian, pengumpulan data dan informasi, pengolahan data informasi dan validasi BCP

BAB V IMPLEMENTASI

Bab ini akan membahas terkait hasil pengumpulan data dan informasi, langkah-langkah yang dilakukan dalam proses formulasi kerangka Business Continuity Planning (BCP) yang disesuaikan dengan kebutuhan perusahaan, hasil kerangka kerja BCP dan hambatan yang dihadapi saat penelitian.

BAB VI HASIIL DAN PEMBAHASAN

Bab ini akan menjelaskan setiap fase yang ada pada kerangka BCP perusahaan yang telah disesuaikan dengan kebutuhan di perusahaan.

BAB VI PENUTUP

Bab ini akan menjelaskan kesimpulan dari penelitian ini, serta saran perbaikan untuk penelitian berikutnya, agar kualitas dari penelitian dapat terus meningkat.

1.7 Relevansi Tugas Akhir

Topik yang diangkat pada tugas akhir ini adalah mengenai proses perancangan *Business Continuity Planning* (BCP). Topik tersebut berkaitan dengan mata kuliah manajemen risiko serta perencanaan keberlangsungan bisnis. Mata kuliah perencanaan keberlangsungan bisnis merupakan salah satu mata kuliah pilihan pada laboratorium Pengembangan dan Perancangan Sistem Informasi (PPSI)

Halaman ini sengaja dikosongkan

BAB II
TINJAUAN PUSTAKA

Tinjauan pustaka berisi tentang literatur dan teori yang berhubungan dengan permasalahan tugas akhir

2.1 Penelitian Sebelumnya

Dalam pengerjaan buku tugas akhir ini, akan digunakan beberapa penelitian sebelumnya untuk menjadi pedoman dalam proses pengerjaan. Pada Tabel 2.1 akan dijelaskan deskripsi, hasil dan hubungan dari penelitian-penelitian terkait terhadap tugas akhir.

Tabel 2.1 Penelitian Sebelumnya

Judul : A Cyclic Approach to Business Continuity Planning (Botha & Solms, 2004)	
Nama Peneliti	Jacques Botha dan Rossouw Von Solms
Tahun Penelitian	2004
Hasil Penelitian	Penelitian ini menghasilkan suatu model teoritis untuk dijadikan metode implementasi *business continuity planning* (BCP) yang dapat diterapkan secara general dan juga diimplementasikan pada organisasi kecil hingga menengah.
Hubungan penelitian dengan Tugas Akhir	Penelitian ini memberikan gambaran besar terhadap proses dan langkah-langkah pengimplementasian *business continuity planning* (BCP) yang merupakan suatu siklus dan berlangsung terus menerus.

	Selain itu penelitian ini juga menjadi literatur bagi peneliti untuk memperdalam proses yang ada pada BCP itu sendiri.
Judul : Evaluation of Business Continuity and Information Disaster Recovery Mechanism in Top Universities in North Cyprus (Yisa & Baba, 2014)	
Nama Peneliti	Victor Legbo Tisa dan Meshach Baba
Tahun Penelitian	2014
Hasil Penelitian	Dalam penelitian ini dilakukan evaluasi terhadap kebutuhan suatu organisasi pada perguruan tinggi atau institusi untuk menerapkan *business continuity planning* (BCP) dan *disaster recovery planning* (DRP) yang efektif dan efisien. Selain itu hasil dari penelitian ini juga meliputi kelemahan dan kerentanan BCP yang telah digunakan pada perguruan tinggi.
Hubungan dengan Tugas Akhir	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 : *Business Continuity Plan* pada Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara (Amanda, 2014)	
Nama Peneliti	Anindita Alisia Amanda

Tahun Penelitian	2014
Hasil Penelitian	Penelitian in menghasilkan suatu kerangka kerja *business continuity planning* (BCP) berbasis risiko yang sesuai dengan kebutuhan perusahaan dan juga di formulasikan mengacu pada beberapa standar yaitu : ISO 22301:2012, Bank of Japan dan Dutch Financial Sector.
Hubungan dengan Tugas Akhir	Penelitian ini merupakan suatu bahan referensi dalam langkah-langkah pembuatan kerangka kerja *business continuity planning* (BCP) dan bagaimana menbuat suatu BCP yang benar – benar sesuai dengan kebutuhan dan tujuan suatu organisasi.

2.2 Risiko

Menurut Australian/NZ Standard 4360 : 1999, risiko adalah suatu kesempatan atas sesuatu untuk terjadi yang akan memiliki dampak terhadap tujuan. Sedangkan berdasarkan 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.

PMBoK (Project Management Body of Knowledge) adalah buku yang berisi mengenai pedoman untuk manajemen proyek yang diterbitkan oleh Project Management Institute (PMI) yang juga mendeskripsikan mengenai definisi dari risiko. Risiko menurut PMBoK adalah sebuah kejadian yang tidak pasti atau

sebuah kondisi yang apabila terjadi, akan menimbulkan efek setidaknya pada satu tujuan proyek.

Sedangkan menurut IRM (Institute of Risk Management), risiko adalah sebuah kombinasi dari kemungkinan terjadinya suatu kejadian yang sifatnya tidak pasti dan segala bentuk konsekuensi yang timbul karenanya. Konsekuensi dari kejadian tersebut dapat berupa hal yang positif dan negatif. Apabila kosekuensi kejadian bersifat positif, hail ini akan menghasilkan kesempatan (opportunity) bagi perusahaan atau organisasi. Namun apabila konsekuensi kejadian bersifat negatif , maka akan menghasilkan ancaman (threat) bagi perusahaan atau organisasi.

Selain itu definisi risiko lainnya menurut (Alijoyo, 2006), definisi risiko berdasarkan dua sudut pandang, yaitu output dan proses. 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".

Risiko (risk) memiliki perbedaan dengan ketidakpastian (uncertainty). Semua risiko adalah suatu ketidakpastian, namun tidak semua ketidakpastian merupakan risiko. Pemahaman ini perlu agar tidak terjadi kerancuan.

Risiko Teknologi Informasi

Penggunaan TI yang berkembang pesat meningkatkan depedensi dan interdepedensi perusahaan terhadap teknologi informasi, hal ini membuat risiko TI juga semakin meningkat. Risiko TI adalah suatu event atau kejadian yang tidak direncanakan dan berdampak pada kegagalan atau penyalahgunaan TI yang mengancam tujuan bisnis (George & Hunter, 2007).

ISACA (Information Systems Audit and Control Association) mendefinisikan risiko teknologi informasi sebagai suatu risiko bisnis yang berkaitan dengan penggunaan,

kepemilikan, operasional, keterlibatan, pengaruh dan adopsi TI dalam suatu perusahaan atau organisasi.

Risiko TI muncul saat perusahaan atau organisasi telah implementasi TI. Risiko TI sendiri merupakan suatu kejadian terkait seluruh aspek dalam teknologi informasi tidak direncanakan dan dapat menimbulkan dampak pada perusahaan. dampak dari risiko tersebut.

2.3 Manajemen Risiko

Manajemen risiko adalah suatu kegiatan yang didalamnya terdapat aktifitas mengidentifikasi, melakukan penilaian dan mitigasi risiko untuk dapat meminimalisir terjadinya risiko atau dampak dari risiko tersebut. Menurut ISO 31000:2009 manajemen risiko adalaah suatu aktivitas terkoordinir yang dilakukan untuk menjalankan dan mengawai perusahaa atau organisasi dengan menggunakan pengekatan risiko.

Institute of Risk Management (IRM) mendefinisikan manajemen risiko sebagai suatu proses yang bertujuan untuk membantu organisasi atau perusahaan dalam memahami, mengevaluasi dan mengambil tindakan untuk risiko-risiko yang muncul, dengan meningkatkan kemungkinan untuk berhasil dan mengurangi kemungkinan kegagalan.

Menurut Australian/NZ Standard 4360 : 1999, manajemen risiko merupakan suatu proses yang bersifat logis dan sistematis dalam mengidentifikasi, menganalisa, mengevaluasi, mengendalikan, mengawasi, dan mengkomunikasikan risiko yang berhubungan dengan segala aktivitas, fungsi atau proses dengan tujuan perusahaan mampu meminimasi kerugian dan memaksimumkan kesempatan.

Definisi manejemen risiko menurut (Djohanputro, 2008), adalah suatu proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternatif penanganan resiko, dan memonitor dan mengendalikan penanganan resiko.

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

2.3.1 Manajemen Risiko Teknologi Informasi

Manajemen risiko teknologi informasi merupakan suatu subset dari keseluruhan manajemen risiko bisnis (Snedaker, 2014). Menurut National Institute Risk Technology (NIST) dalam publikasinya menyatakan, manajemen risiko teknologi informasi adalah suatu rangkaian proses yang meliputi penilaian risiko, mitigasi risiko dan evaluasi dari komponen TI sebuah organisasi atau perusahaan.

Manajemen risiko TI merupakan bagian dari proses pengelolaan risiko TI di sebuah organisasi atau perusahaan yang melakukan proses pengelolaan risiko TI. Proses ini berupa : identifikasi, penilaian dan mitigasi risiko yang terjadi di organisasi tersebut. Manajemen risiko juga dilakukan dengan tujuan sebagai tindakan perlindungan bagi seluruh aset TI dan untuk meminimalisir risiko maupun dampak dari risiko yang berkaitan dengan teknologi informasi/sistem informasi.

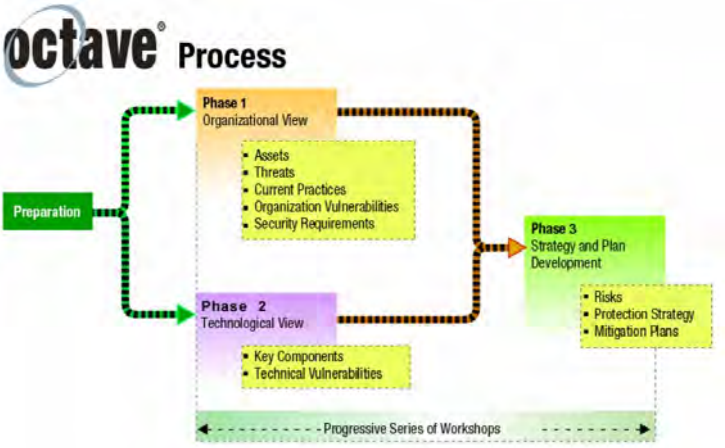
2.4 OCTAVE

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 (Alberts, et al., 2003).

Menurut Parthajit Panda, pendekatan OCTAVE merupakan suatu kerangka karja yang dapat membuat organisasi memahami, menilai dan menyampaikan risiko keamanan informasi dari perspektif organisasi.OCTAVE bukan suatu produk, melainkan

metodologi berbasis proses untuk mengidentifikasi, memprioritisasi dan mengelola risiko keamanan informasi (Panda, 2005).

Metode OCTAVE menggunakan pendekatan tiga fase untuk melakukan pemeriksamaan terhadap permasalahan dalam bidang organsiasi maupun teknologi, yang mana nantinya akan membentuk gambaran komprehensif mengenai kebutuhan perusahaan terhadap keamanan sistem informasi. Metode OCTAVE dibagi menjadi 8 proses : 4 proses terdapat di fase 1, 2 proses terdapat di fase 2 dan 2 proses lainnya terdapat di fase 3.



Gambar 2.1 Kerangka Kerja OCTAVE (Sumber : OCTAVE)

2.4.1 Tahapan OCTAVE

Berikut merupakan tahapan dari metode OCTAVE

1.Tahap Persiapan

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

2. Fase 1 : Membangun Profil Risiko Berbasis Aset

Fase ini merupakan fase dari evaluasi dari pandangan organisasi (organizational view). Tim analisis akan menentukan apa saja aset

yang penting untuk suatu organisasi dan apa saja yang dilakukan untuk menjaga aset tersebut. Setelah itu akan diidentifikasi masing masing ancaman untuk tiap aset kritis sehingga menghasilkan profil ancaman untuk aset. Proses - proses yang ada pada fase 1 adalah sebagai berikut.

Proses 1 : Mengidentikasi pengetahuan dari senior manajemen
Proses 2 : Mengidentikasi pengetahuan mengenai area operasional
Proses 3 : Mengidentifikasi pengetahuan dari staf
Proses 4 : Membuat profil ancaman

3. Fase 2 : Mengidentifikasi Kerentanan Infrastruktur

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

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

4. Fase 3 : Mengembangkan Strategi Keamanan dan Perencanaan

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

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

2.5 Metode FMEA (Failure Mode and Effect Analysis)

FMEA (Failure Modes and Effects Analysis) adalah suatu 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.

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 diperllukan
8. Menentukan nilai keefektifan kontrol yang sedang berjalan (detection)
9. Melakukan kalkulasi nilai RPN (risk priority number)
10. Menentukan tindakan untuk mengurangi kegagalan

Untuk dapat menggunakan FMEA sebagai alat untuk melakukan penilaian risiko dan menghasilkan keluaran yang akurat, maka terlebih dahulu ada beberapa hal yang perlu dilakukan penentuan nilai, yaitu severity, occurence dan detection. Berikut adalah pembahasan dari ketiganya.

2.5.1 Penentuan Nilai Dampak (*Severity* = S)

Pengukuran nilai dampak akan dilihat seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek aspek penting dalam organisasi. Terdapat tiga aspek yang akan dijabarkan yaitu aspek jadwal, aspek biaya dan aspek teknis. Pada tabel 2.2 dibawah, terdapat penjelasan nilai deteksi dan kemampuan metode deteksi terhadap risiko.

Tabel 2.2 Nilai Dampak (Sumber : FMEA)

Dampak	Dampak dari Efek	Ranking
Akibat Berbahaya	Melukai Pelanggan atau Karyawan	10

Dampak	Dampak dari Efek	Ranking
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

2.5.2 Penentuan Nilai Kemungkinan (*Occurence* = O)

Nilai kemungkinan atau *occurence* merupakaan pengukuran terhadap tingkat frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat menghasilkan kegagalan. Pada tabel 2.3 dibawah, terdapat penjelasan nilai kemungkinan dan kemungkinan terjadinya risiko.

Tabel 2.3 Nilai Kemungkinan (Sumber : FMEA)

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

2.5.3 Petunjuk Pemberian Skor i (Detection = D)

Nilai deteksi atau *detection* merupakan suatu nilai pengukuran terhadap kemampuan organisasi dalam melakukan kontrol dan kendali terhadap suatu gangguan atau kegagalan yang

akan terjadi. Pada tabel 2.4 dibawah, terdapat penjelasan nilai deteksi dan kemampuan metode deteksi terhadap risiko.

Tabel 2.4 Nilai Deteksi (Sumber : FMEA)

Deteksi	Kriteria Deteksi	Ranking
Hampir tidak mungkin	Tidak ada metode detensi	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

2.5.4 Penentuan Level Risiko (RPN)

Dalam metode FMEA, angka prioritas akhir risiko disebut RPN atau *risk priority number*. RPN merupakan suatu haisl matematis dari dampak (*Severity)*, kemungkinan terjadinya penyebab dari risiko yang akan menimbulkan kegagalan (*Occurence)* dan kemampuan dalam mendeteksi kegagalan (*detection)*. Nilai RPN ditunjukan dengan persamaan berikut :

$$RPN = S * O * D$$

Berikut merupakan tabel yang menunjukkan penentuan dari nilai RPN yang didapat :

Tabel 2.5 Penentuan Level Risiko

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

Skala Nilai RPN yang didapat dari perhitungan diatas akan menghasilkan level resiko tertentu. Level risiko digunakan untuk menilai risiko mana yang memiliki nilai paling tinggi dan untuk prioritisasi risiko. Untuk risiko yang memiliki nilai tinggi, maka akan dilakukan strategi mitigasi untuk menjaga keberlangsungan operasional bisnis saat gangguan tersebut terjadi.

2.6 *Business Impact Analysis* (BIA)

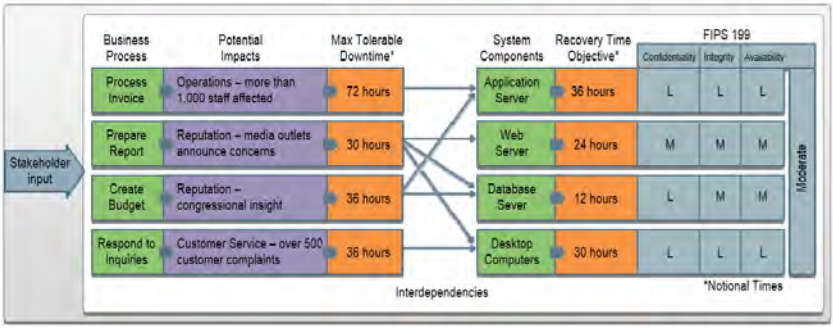
Menurut Federal Financial Institutions Examination Council (FFIEC), *business impact analysis* (BIA) merupakan langkah awal dalam proses perencanaan BCP yang didalamnya terdapat hal – hal sebagai berikut :

- Penilaian dan prioritisasi semua proses dan fungsi bisnis

- Pengidentifikasian potensi dampak dari gangguan pada bisnis yang dapat menyebabkan suatu kejadian yang tidak dapat terkontrol terjadi pada fungsi dan proses bisnis
- Pengidentifikasian peraturan – peraturan yang dibutuhkan untuk proses dan fungsi bisnis
- Mengestimasi maksimal waktu *downtime* yang dapat ditoleransi dan batas level kerugian yang dapat diterima terkait dengan fungsi dan proses bisnis
- Melakukan estimasi *recovery time objectives* (RTO), *recovery point objectives* (RPO) dan *recovery critical path*

Selain itu dipaparkan juga oleh 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. 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.

National Institute of Standards and Technology (NIST) menjabarkan BIA sebagai salah satu aktifitas yang bertujuan untuk menkorelasikan sistem dengan proses bisnis maupun layanan yang tersedia dan dari informasi tersebut di dapat karakterisasi dari konsekuensi yang ada pada setiap gangguan.



Gambar 2.2 Contoh BIA (Sumber : NIST, 2010)

Dari contoh BIA pada gambar 2.2 dapat dilihat bahwa BIA adalah proses analisis dan prioritisasi untuk mengidentifikasi potensi dampak yang dapat terjadi pada proses bisnis beserta komponen sistem yang terkait apa bila terjadi gangguan.

2.7 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 (ISO 22317:2015).

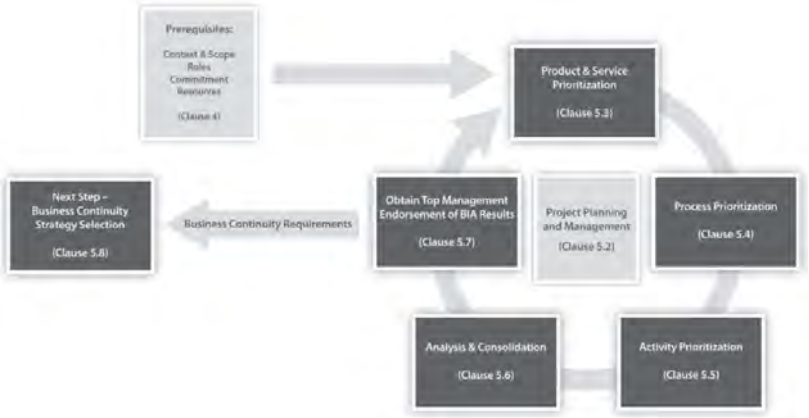
Tujuan dari dibentuknya ISO 22317:2015 ini adalah sebagai berikut.

1. Menyediakan dasar untuk memahami, mengembangkan, mengiplementasi, meninjau, menjaga dan secara terus

menerus meningkatkan keefektifan dari proses analisis dampak bisnis pada organisasi
2. Menyediakan panduan untuk perencanaan, mengerjaan dan pelaporan analisis dampak bisnis.
3. Membantu organisasi untuk menjalankan analisis dampak bisnis dengan cara yang sesuai dengan praktik yang baik
4. Membantu membuat koordinasi antara analisis dampak bisnis dengan program BCM.

BIA bertujuan 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. Menurut ISO 22317:2015 BIA merupakan suatu siklus yang membutuhkan masukan (*input)* dan menghasilkan keluaran (*output)*. Selain itu siklus tersebut berjalan dalam suatu manajemen proyek yang 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).



Gambar 2.3 Kerangka Kerja BIA (Sumber : ISO 22317:2015)

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

Proses analisis dampak bisnis atau *business impact analysis* yang terdapat pada ISO 22317:2015 terdapat 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 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.

2.8 Business Continuity Management Systems

Business Continutiy Management Systems (BCMS) adalah suatu bagian dari keseluruhan sistem manajemen. BCMS adalah sekumpulan elemen elemen yang saling berelasi dan digunakan organisasi untuk melakukan implementasi, operasi, monitor, *review*, manjaga dan meningkatkan keberlangsungan bisnis atau *business continuity* (BC). Elemen elemen ini melingkupi pekerja, kebijakan, perencanaan, prosedur, proses, struktur dan sumber daya (ISO 22301:2012).

Menurut Australian National Audit Offfie, *Business Continuity Management* (BCM) merupakan suatu pengembangan, pengimplementasian dan pemeliharaan dari kebijakan, kerangka kerja dan program yang digunakan untuk membantu mengelola gangguan bisnis sekaligus membangun ketahanan organisasi. BCM merupakan suatu kemampuan untuk membantu dalam mencegah, mempersiapkan, merespon, mengelola dan melindungi dampak dari gangguan (Australian National Audit Office (ANAO), 2009).

Business Continuity Management adalah pengembangan strategi, perencanaan dan langkah-langkah untuk menjaga apabila ada proses bisnis yang terkena gangguan. BCM membutuhkan suatu perencanaan untuk dapat melingkupi hal tersebut, perencanaan ini disebut BCP atau *business continuity plan.* Sehingga dapat dikatakan bahwa *business continuity plan* merupakan output dari business continuity management.

2.9 Business Continuity Planning (BCP)

Griffith University Australia memaparkan bahwa definisi *business continuity plan* (BCP) adalah suatu perencanaan untuk dapat menghasilkan suatu keadaan dimana operasional bisnis berjalan terus menerus dan tidak terganggu dalam semua konteks. Hal ini berfokus pada ketahanan sumber daya manusia, proses, hak milik, platforms, provider dan juga tingkat ketersediaan dan integritas informasi (Griffith University, 2013).

Menurut ISO 22301:2012, *business continuity plan* (BCP) didefinisikan sebagai dokumen berisi prosedur yang bertujuan untuk menjadi panduan perusahaan dalam merespon, melindungi, melanjutkan dan mengembalikan (*respond, recover, resume, restore)* proses bisnis perusahaan ke level yang telah didefinisikan sebelumnya setelah terjadi gangguan (ISO 22301:2012).

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 (Hiles, 2007).

Selain itu, definisi lain dari *Business Continuity Plan* (BCP) menurut SANS Institute adalah suatu aktivitas yang diperlukan untuk menjaga suatu organisasi agar tetap berjalan selama periode dimana terjadi pemindahan atau gangguan terhadap proses operasi normal (SANS Institute, 2002).

2.10 Disaster Recovery Plan (DRP)

Disaster Recovery Plan (DRP) adalah suatu perencanaan yang didesain itu mengembalikan 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 (Brooks, et al., 2002).

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. (Snedaker, 2014). Terdapat 10 langkah dalam mengimplementasikan *Disaster Recovery Plan* (DRP) (Rosenbeerg, 2006) :

1. *Define key assets, threats and scenarios*
2. *Determine the recovery window*
3. *Defining recovery solutions*
4. *Draft a disaster recovery plan*
5. *Establish a communications plan and assign roles*
6. *Disaster recovery site planning*
7. *Accessing data and applications*
8. *Document the disaster recovery plan, in detail*
9. *Test the disaster recovery plan*
10. *Refine and retest the disaster recovery plan*

Sehingga dapat disimpulkan bahwa DRP adalah suatu bagian dari BCP yang mengatur proses perencanaan untuk memulikan operasional sistem TI saat terjadi gangguan atau bencana.

2.11 Hubungan BCP dengan DRP

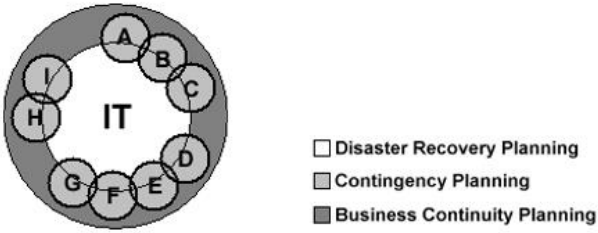
Walaupun memiliki tujuan yang sama untuk menjaga operasional bisnis dan menjaga bsinis dari dampak bencana maupun gangguan, *Disaster Recovery Plan* (DRP) dan *Business Continuity Plan* (BCP) merupakan dua hal yang berbeda. Menurut Rosenbeerg (Rosenbeerg, 2006), perbedaan dari BCP dan DRP adalah sebagai berikut :

- *Business Continuity Plan* (BCP) adalah mengenai bagaimana mendefinisikan aset, ancaman dan skenario yang dapat berdampak bagi organisasi dan mengambil keputusan-keputusan mengenai bagaimana dan sampai tahapan mana

mitigasi risiko dilakukan. Dalam kata lain, BCP adalah bagaimana mencegah terjadinya skenario bencana (*disaster scenario)*.

- *Disaster Recovery Plan* (DRP) adalah bagaimana mendefinisikan aksis perencanaan yang konsisten untuk dapat menghadapi berbagai skenario bencana. Dalam kata lain, DRP adalah bagaimana respon organisasi apabila skenario bencana (*disaster scenario)* terjadi.

Menurut Botha dan Solms, BCP dan DRP memiliki keterkaitan yang erat antara yang satu dengan yang lain. Seperti yang terlihat pada gambar 2.4, DRP merupakan suatu komponen aktif dari BCP yang difokuskan untuk pemulihan semua fungsi terkait TI (Botha & Solms, 2004).



Gambar 2.4 Hubungan antara DRP, CP dan BCP (Sumber : Botha & Solms, 2004)

Pada buku pedoman *Contingency Planning Guide for Federal Information Systems* yang dikeluarkan oleh *National Institute of Standards and Technology (NIST*), terdapat penjelasan mengenai berbagai perencanaan yang dapat dilakukan apabila terjadi suatu kejadian yang menggangu keberlangsungan organisasi. Berikut adalah penjabaran dari perbedaan dari BCP dan DRP dari pedoman tersebut :

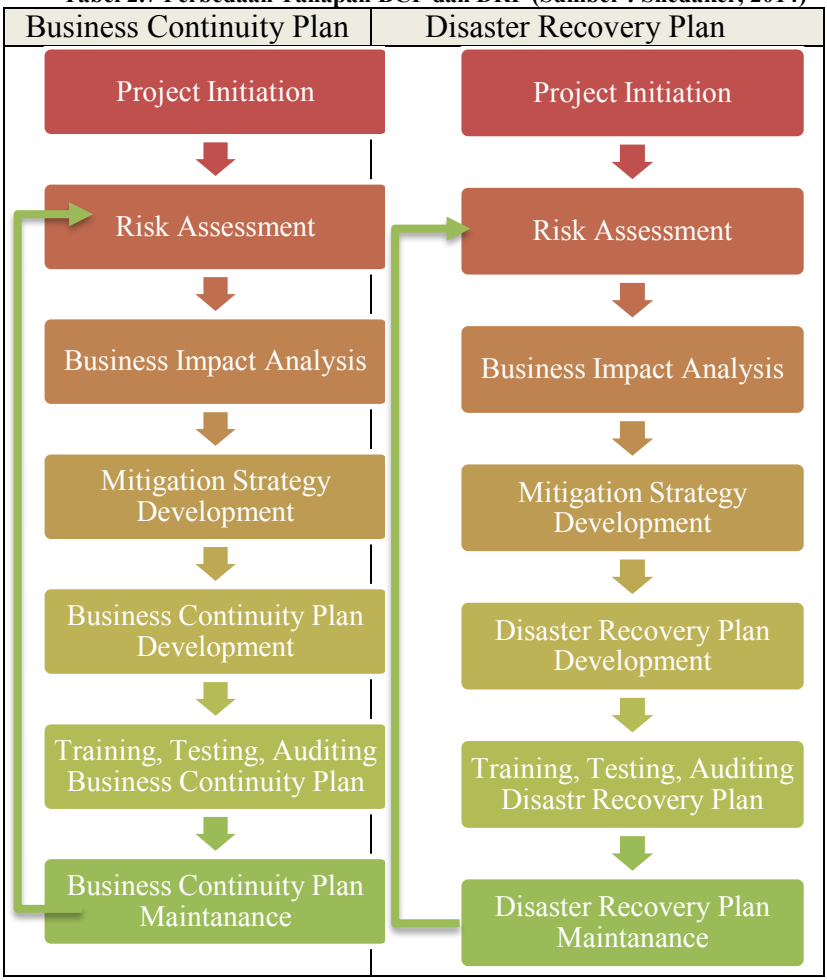
Tabel 2.6 Perbedaan BCP dan DRP (Sumber : NIST, 2010)

Jenis Perencanaan	Tujuan	Ruang Lingkup	Waktu pelaksanaan	Fokus
Business Continuity Plan (BCP)	Menyediakan prosedur untuk menjaga proses operasional bisnis dari gangguan yang bersifat signifikan.	Perencanaan dapat dibuat untuk satu unit proses bisnis saja atau untuk keseluruhan proses pada perusahaan atau organisasi	Perencanaan ini dilaksanakan setelah dan selama terjadinya gangguan	Perencanaan fokus pada proses bisnis yang berjalan di suatu organisasi atau perusahaan
Disaster Recovery Plan (DRP)	Menyediakan prosedur untuk melakukan relokasi operasional sistem informasi ke tempat alternatif lain	Perencanaan dibuat untuk sistem informasi yang mengalami gangguan dan membutuhkan relokasi tempat	Perencanaan ini dilaksanakan setelah terjadinya gangguan	Perencanaan fokus pada sistem informasi yang di implementasikan suatu organisasi atau perusahaan

Susan Snedaker dalam bukunya yang berjudul *Business Continuity and Disaster Recovery for IT Professional* menjabarkan mengenai bagaimana perusahaan atau organisasi dapat menjaga

proses bisnis dari gangguan maupun bencana yang terjadi. Berikut adalah perbedaan tahapan pada BCP dan DRP (Snedaker, 2014).

Tabel 2.7 Perbedaan Tahapan BCP dan DRP (Sumber : Snedaker, 2014)



Dari tabel perbedaan diatas dapat dilihat bahwa secara konseptual BCP maupun DRP memiliki tahapan yang sama.

Namun yang membedakan adalah nantinya cakupan dari BCP sendiri adalah proses bisnis yang memiliki faktor kritis pada suatu organisasi, sedangkan cakupan dari DRP hanyalah pada teknologi informasi atau sistem informasinya saja. Berikut merupakan penjelasan dari setiap fase :

1. *Project Intiation*

   Fase awal dari pembuatan perencanaan yaitu menentukan titik awal dan akhir dari pembuatan perencanaan BCP/DRP, tujuan, kebutuhan, target-target serta perencanaan awal dari proyek.

2. *Risk Assessment*

   Penggalian data mengenai risiko-risiko yang berpotensi terjadi pada suatu organisasi. 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.

4. *Mitigation Strategy Development*

   Membangun strategi-strategi yang dapat meminimalisir, menghindari atau mentransfer risiko tersebut.

5. *BC/DR Plan Development*

   Mulai membangun perencanaan business continuity/disaster recovery dimulai dengan membuat outline metodologi perencanaan yang akan digunakan.

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 Maintanance*

Menjaga kevalidan BCP/DRP dengan melakukan peninjauan kembali dan memperbarui perencanaan apabila ada proses bisnis yang berubah.

Sehingga dari hal ini dapat disimpulkan bahwa BCP dan DRP memiliki tujuan yang sama yaitu untuk menjaga keberlangsungan bisnis utama pada suatu organisasi. Cakupan BCP 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.

2.12 Kerangka Kerja BCMS ISO 22301:2012

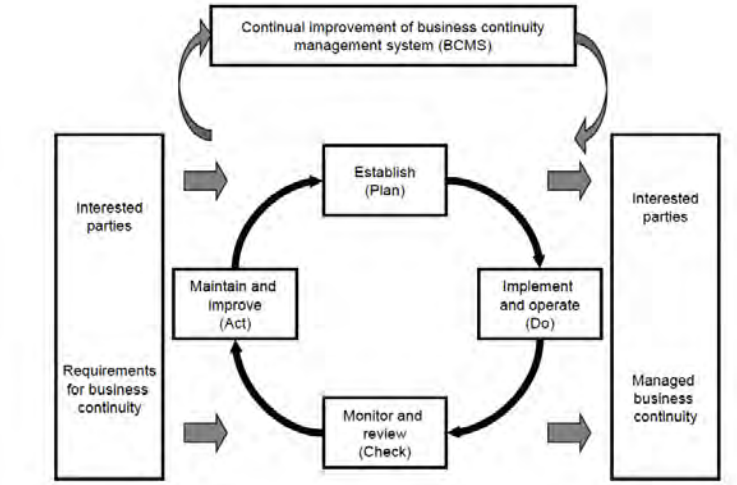
ISO 22301:2012 merupakan suatu produk yang dikeluarkan oleh Internal Organization for Standardization (ISO) yang mana difokuskan pada bidang pengelolaan sistem keberlangsungan bisnis atau *business continuity management systems* (BCMS). ISO 22301:2012 menspesifikasikan kebutuhan untuk merencanakan, membangun, 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 (ISO 22301:2012).

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.

Standar ini menjelaskan mengenai bagaimana merangkai perencanaan keberlangsungan bisnis, dan juga elemen elemen lain yang terkait didalamnya seperti kebijakan mengenai keberlangsungan bisnis, penilaian risika, analisis dampak bisnis, strategi mengenai keberlangsungan bisnis, pelatihan dan juga testing. Standar ini dapat digunakan untuk melakukan review terhadap keseluruhan sistem dan bagaimana meningkatkan kinerjanya.

Alasan mengapa peneliti penggunaan ISO 22301:2012 sebagai kerangka BCP pada standar ini, karena standar ini dikenal relevan dan komprehensif dengan topik penelitian. Standar ini merupakan standar yang telah diakui secara internasional dan juga digunakan di organisasi seluruh dunia. Selain itu standar ini juga dapat disertifikasikan apabila suatu organisasi ingin membuktikan kesesuaian *business continuity management* yang telah berjalan kepada masyarakat luar.

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 (ISO 22301:2012).



Gambar 2.5 Model PDCA untuk Kerangka Kerja BCMS (Sumber : ISO 22301, 2012)

Penjelasan mengenai siklus PDCA tersebut akan dijelaskan pada tabel 2.8 berikut.

Tabel 2.8 Penjelasan Model PDCA (Sumber ISO 22301:2012)

Plan (Establish)	Membuat kebijakan mengenai keberlangsungan bisnis, objektif, target, kontrol, proses dan prosedur yang relevan untuk meningkatkan keberlangsungan bisnis agar mendapatkan hasil yang selaras dengan kebijakan dan objektif keseluruhan organisasi.
Do (Implement and operate)	Mengimplementasikan dan mengoperasikan kebijakan mengenai keberlangsungan bisnis, kontrol, proses dan prosedur.

Check (Monitor and review)	Melakukan pemantauan dan *review* kinerja dari kebijakan mengenai keberlangsungan bisnis dan objektif, melaporkan hasil kepada manajemen untuk dilakukan *review* lalu menentukan dan melakukan pengesahan terhadaptindakan yang digunakan untuk memperbaiki dan peningkatkan performa.
Act (Maintain and Improve)	Melakukan pemeliharaan dan peningkatan BCMS dengan melakukan tindakan korektif berdasarkan hasil *review* dari manajemen dan meninjau ulang cakupan dari BCMS termasuk kebijakan dan objektif yang terkait,

Seperti yang dapat kita lihat pada gambar 2.5 pada siklus Plan-Do-Check-Act (PDCA) terdapat beberapa masukan dan keluaran pada siklus. Masukan (*input model* pada siklus tersebut adalah *interested parties* atau pihak-pihak yang bersangkutan dan *requirements for business continuity* atau kebutuhan untuk keberlangsungan bisnis. Kedua hal tersebut merupakan hal yang menjadi masukan untuk nantinya diolah pada siklus PDCA. Sedangkan keluaran (*output)* pada siklus tersebut adalah adalah *interested parties* atau pihak-pihak yang bersangkutan dan *managed business continuity* atau keberlangsungan bisnis yang telah terkelola.

Selain keluaran dan masukan, pada model Plan-Do-Check-Act (PDCA) terdapat suatu siklus *continual improvement of business continuity management systems* atau peningkatan sistem BCMS secara berkelanjutan. Siklus ini merupakan suatu siklus yang bertujuan untuk tetap menjaga keintegritasan keberlangsungan bisnis yang telah sebelumnya dibuat. Pada siklus ini organisasi secara berkelanjutan dapat terus menerus

menyempurnakan pengelolaan keberlangsungan bisnisnya sesuai dengan kondisi yang ada.

Pada ISO 22301:2012 terdapat 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 2.9 Klausa pada OSP 22301:2012 terkait dengan siklus PDCA (Sumber : ISO 22301:2012)

Fase	Klausa	Keterangan Klausa
Plan	4	Klausa 4 ini menjelaskan mengenai kebutuhan diperlukan suatu organisasi untuk membangun BCMS termasuk kebutuhan pihak ketiga dan cakupan dari BCMS
	5	Klausa 5 ini menjelaskan mengenai kebutuhan spesifik dati peran manajemen atas dalam BCMS. Hal ini 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. Didalam fase ini terdapat proses pengelolaan risiko dan juga analisis dampak bisnis (BIA).

Fase	Klausa	Keterangan Klausa
	7	Klausa 7 menjelaskan praoses yang mendukung operasi BCMS yang terkait dengan membangun kompetensi dan komunikasi atas kebutuhan pihak – pihak terkait serta melakukan dokumentasi, kontrol dan menjaga informasi pada BCMS
Do	8	Klausa 8 menjelaskan kebutuhan keberlanjutan bisnis untuk dapat 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.

Fase	Klausa	Keterangan Klausa
		• Pelatihan dan pengujian BCMS.
Check	9	Klausa 9 menjelaskan mengenai kebutuhan yang diperlukan untuk melakukan pengukuran terhadap kinerja pengelolaan keberlangsungan bisnis, kesesuaian BCMS yang telah ada dengan standar internasional dan ekspektasi manajemen, juga umpan balik dari pihak manajemen terkait dengan ekspektasi yang dimiliki
Act	10	Klausa 10 menjelaskan mengenai bagaiman mengidentifikasi dan melakukan tindakat terhadap ketidak sesuaian BCMS terhadap hal – hal yang teah ditetapkan dengan melakukan tindakan korektif atau perbaikan

2.13 Kerangka Kerja BCM Griffith University

Griffith University atau universitas Griffith merupakan salah universitas penelitian yang berada pada Queensland, Australia. Universitas yang beriri sejak 1971 ini kini telah memiliki 5 kampus pada 3 kota berbeda. Universitas ini berfokus pada berbagai bidang sebagai berikut :

- Seni, pendidikan dan hukum
- Bisnis
- Kesehatan
- Ilmu Pengetahuan

Pada tanggal 5 Agustus 2013, Griffith University mempublikasikan standar yang telah dirancang mengenai kerangka kerja keberlangsungan bisnis yang mana difokuskan untuk universitas atau organisasi pendidikan. Kerangka kerja BCM ini juga diimplementasikan pada Griffith University dan telah disetujui oleh dewan universitas (*university council)* dan akan dilakukan *review* setiap 5 tahun sekali. 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 penggunaan kerangka kerja BCP *Griffith University* sebagai kerangka acuan untuk penelitian ini adalah karena standar ini relevan dengan bentuk organisasi pada studi kasus yaitu organisasi pendidikan. 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.

2.13.1 Sudut pandang Griffith University terhadap BCP

Berikut ini merupakan beberapa hal yang dijabarkan oleh Griffith University mengenai pandangan dari BCMS maupun BCP, dan pentingnya BCP untuk melindungi proses bisnis kritis di organisasi pendidikan

2.13.1.1 Definisi BCP oleh Griffith University

BCP merupakan suatu fungsi dalam program keberlangsungan bisnis atau *business continuity* (BC). BCP sendiri adalah suatu proses kontinyu dalam melakukan identifikasi

terhadap bencana dan kerentanan dari universitas, kemungkinan terjadinya bencana, potesi konsekuensi teradap 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.

2.13.1.2 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 :

1. **Memahami proses bisnis**

   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,

2. **Menilai Risiko**

   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.

3. **Mempersiapkan BCP**

   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

4. **Melakukan Pengujian Perencanaan**

   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.

2.13.1.3 Hal – hal yang perlu diperhatikan manajemen dalam BCP

BCP dimiliki dan dikembangkan oleh senior manajemen yang berkepentingan. Tiap proses kritis harus memiliki strategi keberlangsungannya masing masing, yang mana dapat membutuhkan satu individu ataupun pihak masal. Semua asumsi yang dibuat melalui tahapan perencanaan akan dirangkai dan

divalidasi untuk memastikan bahwa organisasi memiliki kemampuan atau kapabilitas yang sesuai saat dibutuhkan.

Berikut adalah hal – hal yang harus dipastikan mengenai BCP oleh senior manajemen.

1. BCP ditulis dan disebarluaskan sehingga personel atau kelompok tertentu dapat melakukan implementasi dalam waktu yang diperlukan
2. Dalam BCP terdapat penjelasan spesifik terhadap deskripsi kondisi yang mendukung aktivasi perencanaan
3. Dalam BCP terdapat penjelasan spesifik mengenai langkah yang harus diambil segera saat terjadi gangguan
4. Dalam BCP terdapat penjelasan spesifik mengenai aset dan sumber daya kunci yang dibutuhkan untuk mendukung proses kritis
5. BCP bersifat fleksibel dalam merespon skenario bencana atau ancaman dan perubahan kondisi internal
6. BCP lebih menfokuskan mengenai bagaimana bisnis dapat tetap berjalan apabila suatu fasilitas, area kerja atau fungsi yang spesifik mengalami gangguan daripada fokus pada masing – masing gangguan.
7. BCP efektif dalam meminimalisir ketidakberlangsungan dan kerugian
8. BCP tersedia dalam beberapa format termasuk *hardcopy* dengan salinan yang disimpan di tempat berbeda
9. BCP terintegrasi dengan perencanaan bisnis yang telah berjalan dan siklus hidup dari pengembangan system

2.13.1.4 Tujuan Utama BCP

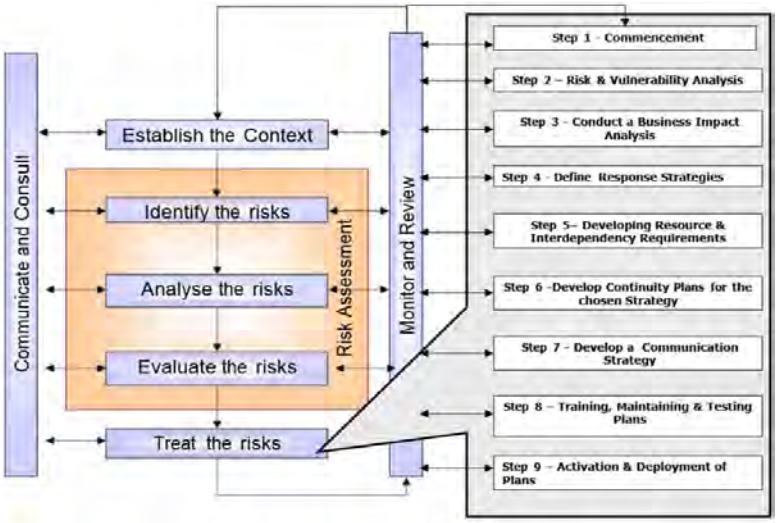
Berikut adalah tujuan utama dari BCP yang dijabarkan oleh Griffith University :

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

2.13.2 Metodologi 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 2.6 Kerangka Kerja BCP Griffith University (Sumber : Griffith University)

Ada 9 tahapan yang akan digunakan pada proses yaitu yang dipaparkan dalam proses tersebut, yaitu permulaan, analisis risiko dan kerentanan, melakukan analisis dampak bisnis, mendefinisikan respon strategi, mengembangkan sumber daya dan ketergantungan interdependensi antar kebutuhan, mengembangkan perencanaan keberlangsungan sesuai dengan strategi yang dipiilh, mengembangkan strategi komunikasi, melakukan pelatihan, pemeliharaan dan pengujian perencanaan serta yang terakhir, aktivasi dan pelaksanaan perencanaan. Tahap 1 meliputi mengenai aktivitas konfirmasi komitmen manajemen terhadap proses ini sehingga tidak dijelaskan pada bagian selanjutnya. Berikut ini akan dijelaskan lebih terperinci mengenai langkah 2 hingga 9.

Tahap 2 : Analisis Risiko dan Kerentanan

Pada bagian ini dibutuhkan beberapa pemahaman mengenai fungsi utama universitas, proses – proses yang kritis, aset (semua yang memiliki nilai atau kegunaan), penjelasan mengenai kontribusi dari masing – masing aset dan kerentanan dari suatu aset atau proses pada gangguan yang terjadi.Untuk melakukan analisis

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

1. Mengidentifikasi ancaman atau bencana pada keberlangsungan dan proses dari fungsi bisnis utama, sistem, informasi, sumber daya manusia, aset, partner*outsource* dan sumber daya lain yangmendukung ataau didukung olehnya
2. Secara sistematis menganalisa kemungkinan (*likelihood)* dan konsukuensi atau dampak dari gagngguan dan melakukan pengukuran berdasarkan yang telah ada pada kerangka kerja manajemen risiko
3. Melakukan evaluasi terhadap gangguan berdasarkan risiko manakah yang perlu untuk ditindak lanjuti
4. Mengidentifikasi perlakuan yang akan dilakukan diselaraskan 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 BIAm dan dibuat berdasarkan maksimal penghentian perkejaan yang dapat diterima atau *maximum accetable outage* (MAO) yang diidentifikasi untuk masing masing proses kritis. Untuk menentukan strategi keberlangsungan bisnis yang sesuai, berikut adalah hal – hal utama perlu dilakukan oleh senior manajemen :

1. Menjaga fungsi utama dari universitas dan proses bisnis kritis yang dimiliki
2. Menstabilisasi, menopang, memulihkan dan mengembalikan fungsi, layanan, proses kritis dan sumber daya yang memiliki ketergantungan atau mendukung mereka.

Respon strategi akan diinformasikan oleh jangka waktu yang disetujuui untuk pemulihan dari proses kritis (*Recovery Time Objectives – RTO)*. RTO merupakan target waktu untuk suatu proses kritis dalam melanjutnya operasinya sebelum melebihi MAO atau mempengaruhi objektif. Saat diperlukan, strategi juga akan membahas mengenai pengembalian target atau *Recovery Point Objective*(RPO) untuk integritas dan ketersediaan data. Dalam memilih respon strategi berikut adalah hal – hal yang perlu diperhatikan :

1. Tipe bencana yang dapat terjadi
2. Prosedur alternatif untuk dapat melanjutkan keselutuhan proses atau ke level minimal yang dapat diterima hingga pemulihan dapat dilakukan

3. Kemampuan untuk dapat 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 bisni

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 Sesuai dengan Strategi yang Dipilih

Dalam perencanaan keberlangsungan bisnis (BCP) yang akan dibuat, di dalamnya akan memaparkan hal – hal sebagai berikut.

1. Proses kritis yang akan dilanjutkan atau dilakukan pemulihan
2. Peran dan tanggung jawab yang telah ditentukan dan detail kontak mengenai orang atau tim yang memiliki kewenangan 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 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. Mendeteksi adanya gangguan
2. Secara teratur mengawasi adanya kejadian tertentu
3. Mengelola komunikasi internal antar unviersitas dan menerima, mendokumentasi serta merespon kepada komunikasi dari pihak terkait lain
4. Memasukan ketersediaan sarana komunikasi saat terjadi peristiwa

5. Menfasilitasi komunikasi terstruktur dengan responden darurat
6. Mencatat informasi pentong mengenai peristiwa, langkah yang dilakukan dan keputusan yang dibuat

Tahap 8 : Pelatihan, Pemeliharaan dan Pengujian Perencanaan

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 orientasi pegawai dan 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* dokumen
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.

2.14 Profil STIE Perbanas

Studi kasus pada penelitian ini adalah STIE (Sekolah Tinggi Ilmu Ekonomi) Perbanas. Sekolah tinggi ini terletak di kota Surabaya, Jawa Timur.

2.14.1 Profil dan Sejarah STIE Perbanas

STIE Perbanas awalnya dibentuk oleh Perhimpunan bank-bank nasional swasta (PERBANAS) yang merupakan organisasi perbankan yang mendirikan Kursus Kader Bank Tingkat "A" dan Kursus Kader Bank Tingkat "B" untuk SLTA. Setelah itu, Pengembangan lembaga dari Pendidikan Kader Bank "B" Lisan menjadi Akademi Ilmu Perbankan PERBANAS Surabaya (AIP PERBANAS Surabaya) dilaksanakan pada tanggal 29 Januari 1970 sesuai dengan Surat Keputusan PERBANAS Pusat No. 25/PERBANAS/1970.

Pada tahun 1982 dibuka Jurusan Manajemen, dan dengan SK. Menteri Pendidikan dan Kebudayaan RI No. 0356/1982 tanggal 2 Nopember 1982 nama Akademi Ilmu Perbankan PERBANAS Surabaya diubah menjadi Akademi Ilmu Perbankan dan Manajemen PERBANAS Surabaya (AIPM PERBANAS Surabaya). Setelah itu pada tanggal 12 agustus 1985 melalui surat Keputusan Menteri Pendidikan dan Kebudayaan RI No. 0510/0/1985 tangal 12 Agustus 1985 dilaksanakan perubahan bentuk dan nama menjadi Sekolah Tinggi Ilmu Ekonomi PERBANAS Surabaya (STIE PERBANAS Surabaya) yang menyelenggarakan pendidikan untuk 2 (dua) jurusan, yaitu Jurusan Manajemen dan Jurusan Akuntansi. Sedangkan Program Studi Manajemen (S2) mulai diselenggarakan sejak tahun 2006 dengan SK no 4892/D/T/2006.

Sejak Januari 2006, STIE Perbanas Surabaya telah memperoleh sertifikasi ISO 9001:2000. Dengan sertifkasi ISO tersebut STIE Perbanas akhirnya mampu menempati peringkat ke 26 untuk Penjaminan Mutu Perguruan Tinggi secara nasional melalui peringkatan DIKTI.

Pada tahun 2009 STIE Perbanas Surabaya mendapat pengakuan dari Kopertis Wilayah VII sebagai 5 besar perguruan tinggi unggulan di Jawa Timur untuk kelompok institut, sekolah tinggi, akademi dan politeknik. Selain itu STIE Perbanas Surabaya juga menjadi perguruan tinggi berprestasi di Jawa Timur dalam bidang penelitian dan pengabdian masyarakat serta dalam bidang tata kelola. Bentuk lain dari pengakuan atas kualitas pengelolaan Perguruan Tinggi adalah diperolehnya bantuan dana dari Direktorat Jenderal Pendidikan Tinggi, Departemen Pendidikan Nasional Republik Indonesia, untuk pengembangan pendidikan STIE Perbanas Surabaya tahun 2007 – 2011.

Profesionalisme dosen didukung dengan pengembangan keahlian di bidang masing-masing. Beberapa sertifikasi yang dimiliki dosen adalah *Certified Profesional Marketing, Financial Planner, Certified Financial Analyst* (CFA), *Financial Planner*, *Certified Wealth Management* (CWM), *Certified Professional Management Accountant* (CPMA), Manajemen Risiko Bank, Manajemen Koperasi Jasa Keuangan, serta *Lead Auditor* yang secara khusus mendukung implementasi ISO namun sekaligus mendukung implementasi penjaminan mutu akademik.

Tabel 2.10 Profil Organisasi

PROFIL ORGANISASI	
Nama Organisasi	STIE Perbanas
Lokasi Organisasi	Surabaya, Jawa Timur Kampus 1 : Jalan Nginden Semolo, Surabaya Kampus 2 : Jalan Wonorejo Indah Timur, Surabaya
Tahun Berdiri	1970
Jenis Usaha	Organisasi Pendidikan - Sekolah Tinggi Ilmu Ekonomi
Jumlah Kampus	2 Kampus Utama Kampus 1 : Jalan Nginden Semolo, Surabaya Kampus 2 : Jalan Wonorejo Indah Timur, Surabaya
Logo Perusahaan	

2.14.2 Visi dan Misi STIE Perbanas

Visi misi dari organisasi STIE Perbanas adalah sebagai berikut

Visi

Menjadi Perguruan Tinggi terkemuka yang memiliki keunggulan kompetitif di bidang bisnis dan perbankan yang berwawasan global

Misi

1. Menyelenggarakan pendidikan dan pengajaran yang memiliki keunggulan kompetitif di bidang bisnis dan perbankan yang berwawasan global.
2. Menyelenggarakan penelitian dan pengabdian kepada masyarakat yang berkualitas, yang dapat memberikan kontribusi bagi pengembangan ilmu dan praktek di bidang bisnis dan perbankan serta peningkatan kesejahteraan masyarakat.
3. Menjalin kerjasama yang berkesinambungan dengan berbagai instansi yang terkait, baik di dalam maupun luar negeri dalam rangka pelaksanaan Tri Dharma Perguruan Tinggi.
4. Melakukan penataan manajemen yang menciptakan suasana akademik yang berorientasi pada tata kelola Perguruan Tinggi yang sehat, dinamis, ramah dan bersahabat.

Tujuan

1. Menghasilkan lulusan yang :
    a. Menguasai konsep dan teori di bidang bisnis dan perbankan.
    b. Mampu menerapkan konsep dan teori tersebut di dunia praktek yang berwawasan global.
    c. Mampu menganalisa dan memberikan saran pemecahan masalah di bidang bisnis dan perbankan.
    d. Memiliki pengetahuan, ketrampilan, dan keahlian tambahan di bidang teknologi informasi, bahasa asing dan jasa keuangan lainnya sebagai pendukung profesi yang ditekuni.
    e. Memiliki sikap bersahabat, komunikatif, jiwa kepemimpinan dan kepribadian yang kuat untuk mendukung keberhasilan dalam kehidupan bermasyarakat dengan tetap memegang teguh kode etik profesi.

2. Menghasilkan penelitian dan pengabdian masyarakat yang berkualitas dan bermanfaat bagi kemanusiaan pada umumnya.
3. Menjalin kerjasama dengan instansi dalam negeri dan luar negeri.
4. Menciptakan penataan manajemen yang baik sehingga terwujud suasana akademik yang berorientasi pada tata kelola Perguruan Tinggi yang sehat, dinamis, ramah dan bersahabat.

Budaya

1. Perbaikan terus menerus, mengandung arti bahwa dalam mewujudkan Visi Sekolah Tinggi, Sivitas Akademika senantiasa melakukan perbaikan dalam segala aspek, baik yang menyangkut pengembangan input, proses dan output, maupun sistem dan pemberian pelayanan, yang didalamnya terutama mengandung nilai inovatif, kreatif dan konsisten.
2. Orientasi kedepan, mengandung arti bahwa perbaikan terus menerus tersebut tidak hanya berorientasi pada kepentingan jangka pendek dan menengah, tetapi juga pada kepentingan jangka panjang, yang didalamnya terutama mengandung nilai idealistik, sistematis, terukur dan keberlangsungan (sustainability).
3. Memberikan hasil terbaik, mengandung arti bahwa perbaikan terus menerus yang berorientasi kedepan tersebut perlu didukung oleh karya terbaik yang merupakan tujuan setiap pekerjaan yang dilakukan oleh Sivitas Akademika yang didalamnya terutama mengandung nilai integritas, kerja keras, efektif dan efisien, kedisiplinan, ketulusan dan komitmen.
4. Saling menghargai, mengandung arti bahwa perbaikan terus menerus yang berorientasi kedepan dengan senantiasa memberikan hasil terbaik tersebut perlu disertai

dengan sikap dan perilaku yang senantiasa menjadikan pihak lain sebagai mitra kerja yang perlu mendapat perlakuan yang proporsional sesuai dengan harkat dan martabatnya sebagai manusia, yang didalamnya terutama mengandung nilai empati, kebersamaan dan kerendahan hati.

5. Peduli dan ramah lingkungan, mengandung arti bahwa kualitas lingkungan merupakan tanggung jawab bersama, sehingga Sivitas Akademika senantiasa ikut menjaga dan memelihara lingkungan internal maupun eksternal, dari segi fisik maupun sosial, yang didalamnya terutama mengandung nilai peduli, bersih, tertib, harmoni, ramah dan bersahabat.

2.14.3 Sistem Pengajaran pada STIE Perbanas

Berikut merupakan sistem pengajaran yang diterapkan pada STIE Perbanas untuk dapat menjamin ketercapaian kualitas lulusan yang baik

1. *Comprehensive Evaluation*
   Comprehensive Evaluation merupakan sistem pengajaran dimana dilakukan evaluasi atas hasil pembelajaran mahasiswa yang secara terus menerus selama satu semester. Sistem ini menjadikan proses belajar berlangsung lebih terarah dan berkesinambungan.
2. *Laboratory-Based Learning*
   Selain pembelajaran di kelas, sistem pembelajaran juga dilakukan di laboratorium yang dilengkapi dengan peralatan IT dan aplikasi software. Pendekatan diharapkan dapatmeningkatkan kompetensi teknis (hard skills) lulusan dan lebih mempersiapkan mereka memasuki dunia kerja.
3. *Student-Centered Learning*
   Student-Centered Learning merupakan suatu pendekatan belajar yang menempatkan mahasiswa sebagai subyek dalam proses belajar sehingga mengembangkan inisiatif dan kreativitas serta potensi keterampilan sosial yang lain

(soft skills). Mahasiswa tidak sekedar memiliki pengetahuan, tetapi juga sikap dan keterampilan profesional yang diperlukan saat bekerja. Pendekatan ini menggunakan metode belajar interaktif dan variatif seperti diskusi, studi kasus, studi lapangan, laboratorium, dan role play agar suasana belajar menyenangkan

4. *Hands-on Experiencce*
   Hands-on Experience merupakan sistem pembelajaran tidak hanya bersifat teori, tetapi juga memberikan pengalaman praktek dalam dunia kerja yang kompleks. Bekerja sama dengan beberapa perusahaan dari berbagai industri, STIE Perbanas menjalankan program magang yang membekali mahasiswa dengan pengalaman praktek dan tantangan dunia kerja.

2.14.4 Penghargaan dan Prestasi STIE Perbanas

Berikut merupakan penghargaan dan prestasi yang didapatkan oleh STIE perbanas dalam cakupan nasional dan internasional selama kurun waktu 4 tahun terakhir.

1. Penghargaan Indonesia Green Awards 2014 kategori Green Awards 2014 oleh The La Tofi School of SCR tahun 2014
2. Memperoleh ranking Webomatrik Peringkat Website Dunia ke 117 Perguruan Tinggi nasional di tahun 2013
3. Penghargaan Perguruan Tinggi Unggul Kelompok Sekolah Tinggi oleh Kopertis Wilayah VII tahun 2014
4. Penghargaan Best Communication And Management School 2013 kategori indonesia best university 2013 oleh Mix Maxcomm Magazine di tahun 2013
5. Mendapatkan seritifikat keanggotaan IAMURE Multiciplinary Research di tahun 2013
6. Memperoleh penghargaan sebagai "Perguruan Tinggi Pelopor Pelatihan dan Sertifikasi Kompetensi" pada ajang Jatim Kompeten Awards leh Pemprov Jatim di tahun 2013

2.14.5 Fungsional Bisnis dan Proses Bisnis STIE Perbanas

Seperti kebanyakan organisasi lain, STIE Perbanas memiliki fungsional bisnis dengan tugas pokoknya masing – masing. Fungsional bisnis ini dibangun untuk membantu organisasi dalam menjalankan proses bisnissnya dan mencapai tujuan dari organisasi. Puncak tertinggi dari struktur STIE Perbanas adalah Ketua STIE Perbanas. Perbanas sendiri secara struktural masih berada di bawah naungan Yayasan Pendidikan Perbanas Jawa Timur yang mana merupakan Badan Hukum Penyelenggara Sekolah Tinggi Ilmu Ekonomi Perbanas Surabaya.

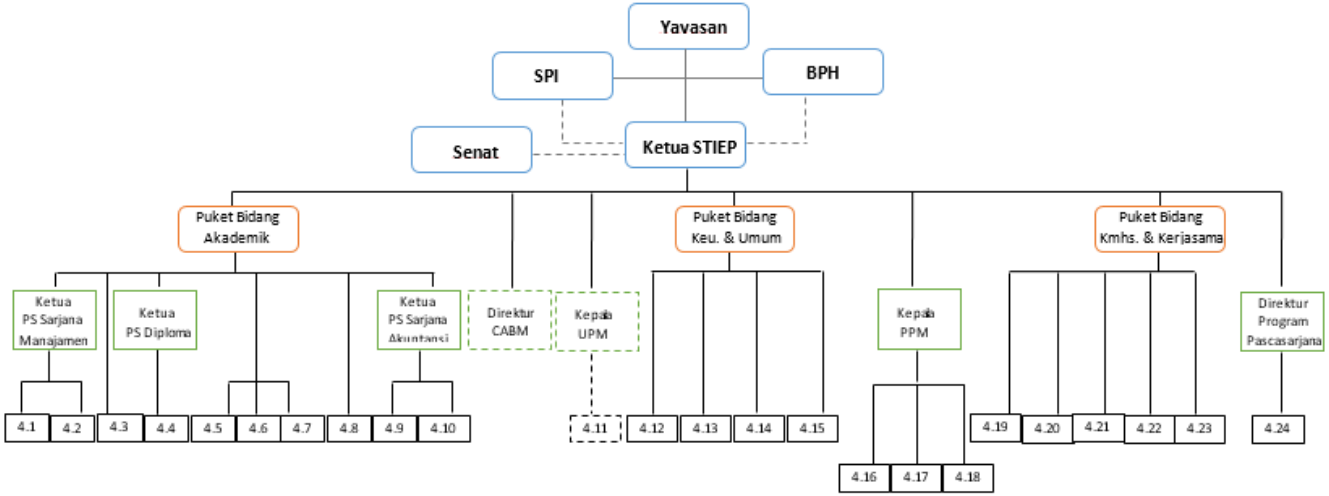
Ketua STIE Perbanas memiliki 3 pembantu ketua (Puket), yaitu Pembantu Ketua I – bidang akademik, Pembantu Ketua 2 – bidang keuangan & umum dan Pembantu Ketua 3 – bidang kemahasiswaan dan kerjasama. Masing masing dari pembantu ketua bertanggung jawab terhadap beberapa bidang lainnya. Berikut adalah pembagian tugas dari masing masing pembantu ketua STIE Perbanas

- Pembantu Ketua 1 (Bidang Akademik) : Pembantu Ketua 1 membawahi Sekretaris Program Studi (PS) Sarjana Manajemen, Kepala Laboratorium Manajemen, Kepala Bagian Akademik, Sekretaris PS Diploma, Kepala Laboratorium Komputer & PTP, Kepala Laboratorium Bahasa, Kepala Laboratorium Bank STIE, Kepala Bagian Perpustakaan, Sekretaris PS Sarjana Akuntansi dan Kepala Laboratorium Akuntansi
- Pembantu Ketua 2 (Bidang Keuangan dan Umum) : Pembantu Ketua 2 membawahi Kepala Bagian SDM, Kepala Bagian Keuangan, Kepala Bagian Umum dan Kepala Bagian Teknologi Informasi dan Komunikasi (TIK)
- Pembantu Ketua 3 (Bidang Kemahasiswaan dan Kerjasama) : Pembantu Ketua 3 membawahi Kepala Bagian Humas, Kepala Bagian Kerjasama, Kepala

Perbanas Career Center dan Kepala Bagian Kemahasiswaan Kepala Student Advisory Center

2.14.5.1 Struktur Organisasi

Struktur organisasi menjabarkan mengenai perbedaan wewenang dan pembagian tanggung jawab antar setiap bagian untuk dapat mencapai tujuan dari suatu organisasi. Berikut merupakan struktur organisasi dari STIE Perbanas.



Gambar 2.7 Struktur Organisasi STIE Perbanas

Berikut adalah keterangan Struktur Organisasi Yayasan Pendidikan STIE Perbanas:

4.1 Sekretaris Program Studi (PS) Sarjana Manajemen
4.2 Kepala Laboratorium Manajemen
4.3 Kepala Bagian Akademik
4.4 Sekretaris PS Diploma
4.5 Kepala Laboratorium Komputer & PTP
4.6 Kepala Laboratorium Bahasa
4.7 Kepala Laboratorium Bank STIE
4.8 Kepala Bagian Perpustakaan
4.9 Sekretaris PS Sarjana Akuntansi
4.10 Kepala Laboratorium Akuntansi
4.11 Wakil Ketuan Unit Penjaminan Mutu (UPM)
4.12 Kepala Bagian SDM
4.13 Kepala Bagian Keuangan
4.14 Kepala Bagian Umum
4.15 Kepala Bagian Teknologi Informasi dan Komunikasi (TIK)
4.16 Kepala Bidang Abdimas
4.17 Kepala Bidang Penelitian
4.18 Kepala Pengelolaan Jurnal dan Penerbitan Buku
4.19 Kepala Bagian Humas
4.20 Kepala Bagian Kerjasama
4.21 Kepala Perbanas Career Center
4.22 Kepala Bagian Kemahasiswaan
4.23 Kepala Student Advisory Center
4.24 Sekretaris Program Pascasarjana

2.14.5.2 Proses Bisnis STIE Perbanas

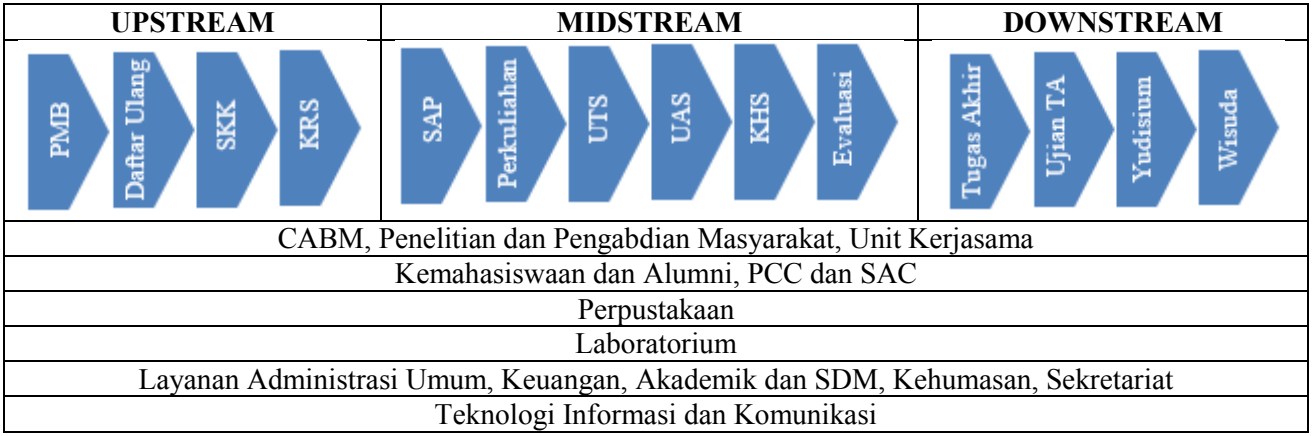
Proses Bisnis STIE Perbanas dibagi menjadi 3 bagian umum yaitu bagian *upstream*, bagian *midstream* dan juga bagian *downstream* seperti yang dapat dilihat dari gambar 2.8. Bagian Upstream adalah proses bisnis organisasi yang dilakukan sebelum proses utama dilakukan. Proses bisnis organisasi diawali dengan Penerimaan Mahasiswa Baru (PMB), setelah itu dilakukan daftar ulang untuk mahasiswa baru. Sebelum memasuki masa perkuliahan, mahasiswa baru harus menjalani sosialisasi kehidupan kampus (SKK). Selain itu mahasiswa juga wajib untuk mengisi KRS (Kartu Rencana Studi) untuk dapat menentukan mata kuliah dan jadwal perkuliahan.

Bagian *midstream* merupakan bagian utama dalam proses bisnis organisasi. Proses pada bagian ini diawali dengan satuan acara perkuliahan (SAP). Setelah itu berjalanlah proses perkuliahan, proses ini diikuti dengan proses UTS (Ujian Tengah Semester) dan UAS (Ujian Akhir Semester) untuk dapat mengukur kinerja dan memberikan penilaian terhadap kinerja mahasiswa saat menjalani proses perkuliahan. Setelah itu nilai dari mahasiswa akan dibagi melalui KHS (Kartu Hasil Studi) dan kemudian proses ini akan dievaluasi dan ditingkatkan sesuai dengan keputusan manajemen.

Bagian yang terakhir adalah bagian *downstream*. Proses pada bagian ini dilakukan apabila mahasiswa telah selesai menjalani proses pada bagian *midstream*. Proses pada bagian ini antara lain adlaah mengambilan tugas akhir dan ujian tugas akhir. Apabila mahasiswa telah dinyatakan lulus sidang ujian tugas akhir dan melengkapi persyaratan yang ditentukan, maka mahasiswa akan menjalani proses yudisium dan yang paling akhir adalah proses wisuda.

Selain itu, proses bisnis yang ada pada bagian *upstream*, *midstream* maupun *downstream* dilakukan oleh berbagai fungsional bisnis yang ada pada STIE Perbanas. Berbagai fungsional bisnis nantinya akan menjalankan tugas pokoknya masing – masing dengan tujuan untuk dapat menjalankan proses utama bisnis yang ada.

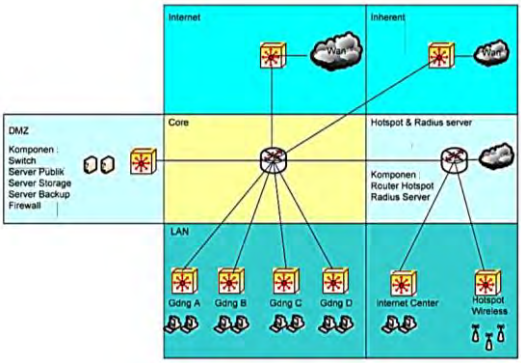
Berikut merupakan bagan proses bisnis organisasi berdasarkan Pedoman Mutu STIE Perbanas.



Gambar 2.8 Proses Bisnis STIE Perbanas

2.14.5.3 Teknologi Informasi STIE Perbanas

Pengelolaan Teknologi Informasi STIE Perbanas meupakan tanggung jawab dari bagian Teknologi Informasi dan Komunikasi (TIK). Seperti yang terlihat pada gambar 2.7, bagian Teknologi Informasi dan Komunikasi STIE Perbanas berada di bawah tanggung jawab pembantu ketua bidang keuangan dan umum. STIE Perbanas telah memiliki cetak biru (*blue print)* untuk pengembangan TIK. Didalam *blueprint* ini terdapat semua panduan umum mengenai pengembangan dan pengelolaan bidang TIK untuk 5 tahun kedepan. STIE Perbanas telah menyediakan sistem informasi melalui sistem jaringan komputer untuk dapat membantuk pembelajaran dan pengelolaan informasi secara *online* dan terintegrasi. Selain itu STIE Perbanas juga telah memiliki sarana dan prasarana seperti komputer, koneksi internet dan juga intranet seperti pada gambar 2.9.



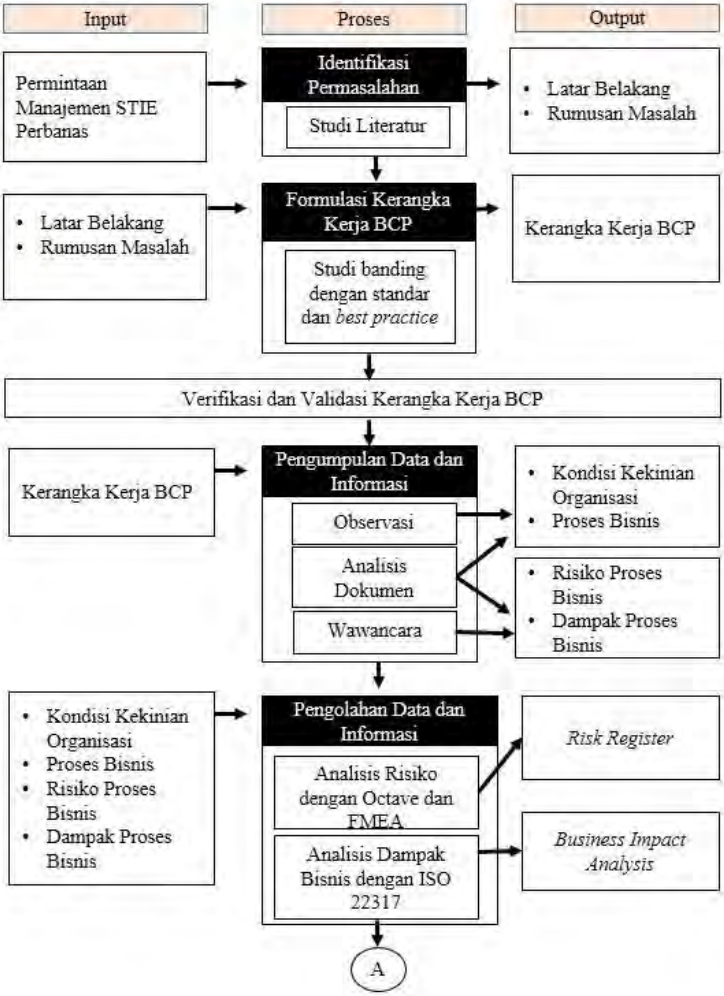
Gambar 2.9 Infrastruktur jaringan internet dan intranet

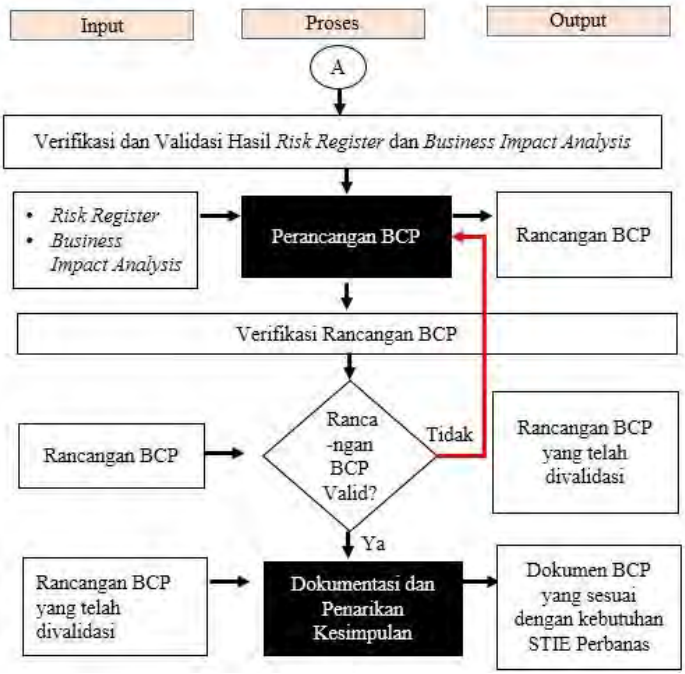
Pengembangan sistem informasi (SISFO) pada STIE Perbanas bertujuan untuk mengumpulkan, mengelola dan menyajikan data dan informasi. SISFO telah menjangkau seluruh unit kerja dan mencakup 19 jenis aplikasi dengan 1.041 sub menu. Sistem informasi ini juga bertujuan sebagai alat komunikasi sosial untuk dosen dan mahasiswa.

Selain itu layanan lain yang diberikan oleh Bagian Teknologi Informasi dan Komunikasi (TIK) adalah layanan *e-Learning* yang berbasis *Moodle*, *e-library* dan *Repository Banking and Finance* (Rebaf), *email,* info PMB, *career center* dan informasi program studi. Akses internet pada STIE Perbanas merupakan 2 MB dari vendor Telkom-Astinet dan 1,384 dari Telkom-speedy.

BAB III
METODOLOGI PENELITIAN

Pada bagian metodologi akan dijelaskan urutan aktivitas proses dari pengerjaan tugas akhir beserta deskripsi untuk masing masing proses yang ada.





3.1 Identifikasi Permasalahan

Tahapan identifikasi permasalahan merupakan tahapan awal yang akan dilakukan untuk menyusun tugas akhir ini. Peneliti mendapatkan masukan berupa permintaan dari senior manajemen STIE Perbanas untuk dapat melakukan identifikasi risiko dan implementasi BCP pada organisasi.

Dalam tahap ini dilakukan studi literatur terhadap referensi berupa jurnal internasional, paper, buku dan informasi pada internet. Hal ini dilakukan untuk memperkuat pengidentifikasian masalah dan melakukan pendalaman terhadap topik. Tahapan ini akan menghasilkan latar belakang dan rumusan masalah yang dijadikan dasar untuk memulai penelitian.

3.2 Formulasi Kerangka Kerja BCP

Setelah tahapan pengolahan data dan informasi dilakukan formulasi model BCP. Dalam melakukan formulasi kernagka kerja BCP, peneliti melakukan studi literatur untuk menentukan standar dan *best practice* yang tepat untuk diformulasikan sebagai model BCP. Selain itu peneliti juga melakukan studi banding terhadap standar dan *best practice,* sehingga kerangka kerja BCP sesuai dengan kondisi dan kebutuhan perusahaan.

Perancangan kerangka BCP ini melihat standar dan *best practice* yang ada. Dengan itu diharapkan akan didapatkan kerangka kerja BCP yang sesuai untuk kebutuhan STIE Perbanas. Standar yang digunakan adalah ISO 22301:2012 dan *best practice* lainnya adalah kerangka kerja BCP Griffith University yang penerapannya dikhususkan untuk organisasi pendidikan.

3.2.1 Verifikasi

Tahapan verifikasi dilakukan dengan meninjau kesesuaian kerangka kerja BCP dengan standar dan *best practice* yang akan digunakan. Kerangka Kerja BCP nantinya diharapkan merupakan formulasi yang sesuai dengan proses yang ada pada standar maupun *best practice*.

3.2.2 Validasi

Tahapan validasi dilakukan kepada pihak organisasi untuk memastikan bahwa model BCP yang telah dibuat sesuai dan tepat. Proses validasi merupakan proses yang penting dalam penelitian untuk memastikan bahwa model BCP sesuai dengan standar internasional dan *best practice* serta sebagai bentuk konfirmasi dari organisasi untuk dapat melanjutkan proses perancangan BCP. Validasi dilakukan dengan melakukan konfirmasi kesesuaian model BCP dengan kebutuhan organisasi kepada ketua organisasi STIE Perbanas.

3.3 Pengumpulan Data dan Informasi

Pada tahapan pengumpulan data dan informasi ada beberapa metode yang dilakukan, antara lain adalah wawancara, observasi penelitian dan mempelajari dokumen organisasi yang telah

dimiliki organisasi. Pada tahapan ini akan dilakukan proses verifikasi kepada pihak perusahan untuk dapat memastikan pada data dan informasi yang didapat benar dan dapat dipertanggungjawabkan. Dari proses ini akan didapat hasil berupa kondisi kekinian organisasi, proses bisnis, dampak proses bisnis dan risiko dari proses bisnis. Berikut adalah penjelasan dari beberapa metode tahapan pengumpulan data dan informasi.

3.3.1 Observasi

Metode observasi akan dilakukan pada bagian teknologi informasi di STIE Perbanas. Tujuan dari metode ini adalah untuk mendapatkan gambaran langsung dari proses bisnis organisasi. Metode ini dilakukan dengan cara melakukan pengamatan terhadap kinerja dan aktivitas yang ada pada bagian teknologi informasi STIE Perbanas. Hal ini dilakukan untuk menggali informasi mengenai risiko proses bisnis dan dapat menentukan BCP yang sesuai untuk kebutuhan STIE Perbanas.

3.3.2 Analisis Dokumen

STIE Perbanas memiliki beberapa dokumen yang dapat dipelajari untuk dapat melakukan analisis yang lebih akurat. Dokumen seperti rencana strategis, kebijakan dan prosedur ini dapat menjadi bahan peneliti untuk dapat memperdalam proses bisnis dan lingkungan organisasi. Diharapkan penelitian akan lebih relevan dan sesuai dengan kondisi kekinian organisasi.

Hasil analisis dari dokumen-dokumen tersebut nantinya akan dihasilkan data proses bisnis organisasi, dampak dari masing masing aktivtas proses bisnis serta ancaman yang terjadi pada proses binis.

3.3.3 Wawancara

Metode wawancara akan dilakukan kepada ketua organisasi, kepala bagian teknologi informasi dan bidang Akademik STIE Perbanas. Wawancara akan dilakukan untuk dapat melakukan mengumpulkan data dan informasi yang dibutuhkan pada penelitian. Dalam metode ini akan digali informasi mengenai

proses bisnis, kondisi organisasi, risiko proses bisnis dan dampak proses bisnis.

3.4 Pengolahan Data dan Informasi

Setelah data dan informasi mengenai kondisi kekinian organisasi, proses bisnis, dampak proses bisnis dan risiko proses bisnis telah didapatkan dari tahapan sebelumnya, maka data akan diolah dengan analisis dampak bisnis dan analisis risiko. Hasil dari tahap pengolahan ini nantinya adalah *business impact analysis* (BIA) dan *risk register*. Dalam tahapan pengolahan data dan informasi berikut penjelasan dari masing masing proses didalamnya.

3.4.1 Analisis Risiko dengan Octave dan FMEA

Pada proses analisis risiko acuan yang digunakan adalah kerangka kerja Octave, yang mana nantinya risiko tersebut akan dipastikan menjadi sebuah ancaman yang apabila terjadi. Proses identifikasi risiko dilakukan berdasarkan lima komponen sistem informasi, yaitu perangkat keras, perangkat lunak, data, prosedur, dan sumber daya manusia.

Setelah 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.

3.4.2 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.

Keluaran dari proses ini akan menghasilkan tabel *Business Impact Analysis* (BIA) 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 pengeolahan data dan informasi yaitu *risk register* dan *business impact analysis* telah sesuai dan dapat diterima oleh organisasi. Validasi dilakukan dengan melakukan konfirmasi *risk register* dan *business impact analysis* Kasie bagian teknologi informasi dan komunikasi (TIK). Sehingga diharapkan nantinya *risk register* dan *business impact analysis* telah sesuai dengan kebutuhan organisasi.

3.5 Perancangan BCP

Perancangan BCP untuk STIE Perbanas dilakukan dengan menerapkan model BCP yang telah diformulasikan dari standar 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. Proses dimulai dari melakukan penentuan tujuan, ruang lingkup serta sumber daya manusia dalam perusahaan, baik dari level strategis (*top management*) hingga level teknis.

Keluaran dari proses ini merupakan rancangan BCP yang sesuai dengan standar dan *best practice* serta kebutuhan organisasi.

3.5.1 Verifikasi BCP

Tahapan verifikasi dilakukan dengan meninjau 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

Tahapan validasi dilakukan pada rancangan BCP sebagai bentuk persetujuan perusahaan 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.

Apabila rancangan BCP telah divalidasi maka proses akan berlanjut ke dokumentasi BCP dan penarikan kesimpulan. Namun, apabila menurut organisasi hasil rancangan BCP belum valid maka akan kembali dilakukan ropses perancangan BCP sesuai dengan hasil konsultasi dengan pihak organisasi.

3.7 Dokumentasi BCP dan Penarikan Kesimpulan

Tahapan akhir dalam penelitian ini adalah melakukan dokumentasi tugas akhir. Dokumentasi yang lengkap, jelas dan runtut akan berguna untuk menjadi acuan untuk organisasi dan juga berguna bagi peniliti untuk dapat melakukan pemeriksaan dan perbaikan. Selain dokumentasi BCP, juga terdapat penarikan kesimpulan akhir dari hasil penelitian.

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Bab ini menjelaskan mengenai fungsional bisnis dan proses bisnis yang terlibat dalam penelitian, persiapan pengumpulan data dan informasi, pengolahan data dan informasi serta validasi BCP untuk perancangan pada penelitian ini.

4.1 Fungsional Bisnis yang Terlibat dalam Penelitian

Pada penelitian ini terdapat 4 fungsional bisnis yang dilibatkan dalam penyusunan BCP organisasi, yaitu bagian TIK, bagian akademik, bagian kemahasiswaan dan bagian keuangan. Alasan peneliti memilih 4 fungsional tersebut adalah karena berdasarkan hasil konsultasi dengan manajemen, proses bisnis utama dari organisasi memiliki ketergantungan tinggi di 4 fungsi tersebut. Selain itu 4 fungsional bisnis ini juga telah memiliki ketergantungan pada sistem informasi dan teknologi informasi untuk menjalankan proses bisnisnya. Penjelasan fungsional bisnis yang terkait dalam pembuatan BCP di penelitian ini adalah:

1. Bagian Akademik
   Bagian akademik merupakan bagian yang melakukan pengelolaan seluruh program dan aktivitas akademik yang dilakukan oleh organisasi. Aktivitas akademik merupakan aktivitas seputar akademik dari mahasiswa masuk hingga mahasiswa lulus dari STIE Perbanas yang mana hal ini meliputi KRS, kegiatan perkuliahan, UTS/UAS hingga wisuda.
2. Bagian Kemahasiswaan
   Bagian kemahasiswaan merupakan bagian yang bertugas untuk melakukan kegiataan terkait kemahasiswaan seperti melakukan penerimaan mahasiswa baru dan juga memantau kegiatan- kegiatan yang meningkatkan *softskill* dari mahasiswa.
3. Bagian TIK

Bagian Teknologi Informaasi dan Komunikasi merupakan bagian yang berfungsi dalam menyediakan serta memelihara layanan Teknologi Informasi untuk mendukung keseluruhan proses bisnis yang ada di STIE Perbanas. Bagian TIK juga bertanggung jawab dalam pengembangan layanan teknologi dan sistem informasi dan memastikan bahwa layanan TIK yang dimiliki oleh organisasi berjalan dengan lancar.

4. Bagian Keuangan
   Bagian Keuangan merupakan bagian yang mengelola akuntansi dan administrasi dari keuangan organisasi. Proses pengelolaan ini meliputi proses pembayaran biaya sekolah, proses penggajian dan juga proses pengelolaan anggaran biaya.

4.2 Proses Bisnis yang Terlibat dalam Penelitian

Dari empat fungsional bisnis yang berada di STIE Perbanas tersebut, pada bagian ini akan dijelaskan lebih lanjut mengenai proses bisnis dari masing masing fungsional yang terkait dengan sistem informasi yang berjalan. Proses yang akan dijabarkan berikut merupakan proses yang berjalan dan bergantung kepada teknologi informasi dan sistem informasi secara langsung. Selain itu proses-proses berikut juga merupakan proses penting bagi keberlangsungan proses bisnis organisasi. Berikut merupakan proses bisnis terkait sistem dari keempat fungsional bisnis yang ada.

Tabel 4.1 Proses Bisnis Terkait Sistem

FUNGSIONAL BISNIS	PROSES BISNIS TERKAIT SISTEM
Akademik	Proses KRS
	Pengelolaan Data Perpustakaan
	Pengelolaan Nilai Mahasiswa
	Proses wisuda
	Proses Pengajaran melalui E-Learning

FUNGSIONAL BISNIS	PROSES BISNIS TERKAIT SISTEM
Kemahasiswaan	Pendaftaran Mahasiswa Baru
	Proses Pengelolaan *Softskill*
TIK	Melakukan Pemantauan Teknologi
	Melakukan Pengelahan Data Elektronik
	Melakukan Pengelolaan Konfigurasi Perangkat
	Menyediakan Layanan SI/TI untuk Mendukung Proses Pengajaran
	Disaster Recovery Planning
Keuangan	Pengelolaan Pembayaran Biaya Kuliah
	Penggajian Honor Mengajar
	Pengajuan Anggaran

4.3 Persiapan Pengumpulan Data dan Informasi

Pengumpulan data dan informasi akan dilakukan dengan menggunakan teknik *interview* atau wawancara, analisis dokumen dan observasi.

4.3.1 Wawancara

Proses wawancara akan dilakukan kepada Bidang Akademik dan Bagian TIK STIE Perbanas. Diharapkan bahwa setelah wawancara didapatkan data dan informasi mengenai proses bisnis organisasi, kondisi organisasi, risiko proses bisnis dan dampak terhadap proses bisnis kritis organisasi.

Tabel 4.2 Perancangan Pengumpulan Data dan Informasi dengan Wawancara

Nama Proses	Pengumpulan Data dan Informasi
Teknik	***Interview*/Wawancara**

Nama Proses	Pengumpulan Data dan Informasi
	Teknik wawancara nantinya akan dilakukan dengan tanya jawab secara langsung kepada pihak yang akan diwawancara. Wawancara akan dilakukan secara terstruktur yang mana peneliti telah menyiapkan pertanyaan pertanyaan yang dibutuhkan terlebih dahulu.
Objek	Proses bisnis organisasi, kondisi kekinian organisasi, risiko proses bisnis dan dampak terhadap proses bisnis kritis organisasi.
Kebutuhan proses	• *Interview protocol* • *Sound recorder* • Notes dan Peralatan tulis
Tahapan pelaksanaan	Tahapan dalam melakukan wawancara adalah sebagai berikut : • Menetapkan tujuan dan jumlah wawancara yang akan dilakukan • Menentukan Narasumber • Membuat Interview Protocol • Mengkonsultasikan Interview Protocol • Memulai Proses wawancara

Nama Proses	Pengumpulan Data dan Informasi
	• 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 Tujuan Wawancara

Wawancara Ke-	Narasumber	Tujuan Wawancara
1	Bidang Akademik	Wawancara ini bertujuan untuk mengetahui proses bisnis dan kondisi kekinian dari STIE Perbanas. Pada wawancara ini akan digali lebih dalam lagi mengenai proses bisnis terkait TI yang ada di bagian akademik. Selain itu juga dilakukan wawancara untuk identifikasi aset TI, kebutuhan keamanan, keamanan TI yang telah diterapkan, identifikasi ancaman dan risiko dan juga dampak terhadap proses bisnis kritis apabila terkena gangguan.
2	Bagian TIK	Pada wawancara ini akan digali lebih dalam lagi mengenai proses bisnis yang dilakukan

Wawancara Ke-	Narasumber	Tujuan Wawancara
		oleh bagian TIK. Selain itu juga dilakukan wawancara untuk identifikasi aset TI, kebutuhan keamanan, keamanan TI yang telah diterapkan, identifikasi ancaman dan risiko dan juga dampak terhadap proses bisnis kritis apabila terkena gangguan dari sudut pandang bagian TIK .

1. Profil Narasumber Wawancara

Dalam melakukan wawancara, peneliti terlebih dahulu harus menentukan narasumber. Narasumber yang akan dipilih nantinya harus sesuai dengan tujuan wawancara, berada dalam kapasitas objek wawancara, dapat memberikan informasi yang valid dan sesuai serta relevan dengan cakupan dari wawancara itu sendiri. Berikut merupakan profil dari narasumber yang akan diwawancara dalam penelitian.

Tabel 4.4 Narasumber Penelitian

Nama	Jabatan
Dr. Drs. Emanuel Kritijadi, MM	Pembantu ketua I Bidang Akademik
Hariadi Yutanto, S.Kom, M.Kom	Kasie TIK (Manajemen Jaringan dan Technical Support)

2. Daftar Pertanyaan Wawancara (*Interview Protocol)*

Berikut merupakan daftar pertanyaan yang tercantum pada *interview protocol*

Tabel 4.5 Daftar Pertanyaan pada *Interview Protocol*

No	Tujuan pertanyaan	Standar Acuan terkait	Detail ringkas pertanyaan
1	Wawancara ini bertujuan untuk mengetahui proses bisnis dan kondisi kekinian dari STIE Perbanas. Pada wawancara ini akan digali lebih dalam lagi mengenai proses bisnis terkait TI.	*Tidak da*	• Proses bisnis di STIE Perbanas • Data struktur organisasi dan peran fungsi yang terlibat dalam proses bisnis
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 – Membangun profil ancaman berbasis risiko**	• Aset kritikal yang dapat memberi ancaman pada organisasi • Kebutuhan keamanan dari SI/TI organisasi • Ancaman yang mungkin terjadi kepada aset SI/TI • Praktik keamanan SI/TI yang telah dilakukan

No	Tujuan pertanyaan	Standar Acuan terkait	Detail ringkas pertanyaan
			oleh organisasi • Kelemahan Organisasi
		OCTAVE Fase 2 – Mengidentifikasi Kelemahan Infrastruktur	• Komponen aset SI/TI yang ada di orgainsasi • Kelemahan teknis aset SI/TI
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 yang ada pada organisasi • tingkat prioritas untuk masing masing layanan
		ISO 22317 Klausa 5.4 – Prioritisasi Proses	• Proses bisnis yang berlangsung terkait TI • Prioritisasi untuk masing – masing

No	Tujuan pertanyaan	Standar Acuan terkait	Detail ringkas pertanyaan
			proses tersebut
		ISO 22317 Klausa 5.5 - Prioritisasi Aktivitas	• Aktivitas yang berlangsung pada proses bisnis terkait TI • Prioritisasi terhadap aktivitas teresbut
		ISO 22317 Klausa 5.6 Analisis dan Konsolidasi	• Dampak yang terjadi pada layanan bila terjadi gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis) • Waktu yang ditoleransi organisasi terkait gangguan

No	Tujuan pertanyaan	Standar Acuan terkait	Detail ringkas pertanyaan
			• Toleransi waktu dalam tahap pemulihan sistem apabila terjadi gangguan • Respon organisasi terhadap proses bisnis kritis bila terjadi gangguan?

4.3.2 Analisis Dokumen

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

Tabel 4.6 Perancangan Pengumpulan Data dan Informasi dengan Analisis Dokumen

Nama Proses	Pengumpulan Data dan Informasi
Teknik	**Analisis Dokumen** Analisis dokumen nantinya akan dilakukan dengan melihat dokumen-dokumen yang dimiliki oleh STIE Perbanas yang terkait dengan penelitian dan diperbolehkan untuk dianalisis.
Tujuan	Tujuan dari analisis dokumen ini nantinya adalah agar dapat mengetahui lebih lanjut mengenai profil organisasi, proses bisnis organisasi serta kondisi kekinian dari organisasi.
Objek	• Dokumen pedoman mutu • Kebijakan TIK • Prosedur terkait TIK • Dokumen Rencana Strategis TIK
Tahapan pelaksanaan	Tahapan dalam melakukan analisis dokumen adalah sebagai berikut : • Menetapkan tujuan dan dokumen yang dibutuhkan • Mengkonsultasikan daftar dokumen yang

Nama Proses	Pengumpulan Data dan Informasi
	dibutuhkan kepada STIE Perbanas • Menganalisis dokumen-dokumen yang didapatkan • Mendokumentasikan hasil analisis dokumen

4.4 Pengolahan Data dan Informasi

Pengolahan data dan informasi merupakan proses yang dilakukan setelah proses pengambilan data. Di dalam proses ini terdapat dua analisis utama yang dilakukan, yaitu analisis risiko dan analisis dampak bisnis.

4.4.1 Analisis Risiko

Untuk melakukan analisis risiko pada penelitian kali ini, peneliti menggunakan pendekatan dengan metode OCTAVE dan metode FMEA (*Failure Modes and Effects Analysis).* 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.

2. Penilaian Risiko

Dalam melakukan penilaian risiko, metode yang akan digunakan dalam penelitian adalah metode FMEA. Proses dalam analisis ini melibatkan perhitungan nilai dari *severity* (dampak), *Occurence* (kemungkinan) dan *detection* (deteksi).

Severity atau dampak merupakan suatu pengukuran dari seberapa besar intensitas dampak dari suatu gangguan dapat mempengaruhi aspek aspek dalam organisasi. Berikut merupakan penjelasan dari kriteria nilai dampak.

Tabel 4.7 Kriteria Nilai Dampak (Sumber : FMEA)

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

Occurence atau kemungkinan merupakan suatu pengukuran dari nilai terjadinya penyebab kegagalan. Nilai kemungkinan ini merupakan tingkat frekuensi dan keseringan terjadinya gangguan yang dapat meyebabkan risiko. Berikut merupakan pejelasan dari kriteria kemungkinan.

Tabel 4.8 Kriteria Nilai Kemungkinan (Sumber : FMEA)

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

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

Tabel 4.9 Kriteria Nilai Deteksi (Sumber : FMEA)

Deteksi	Kriteria Deteksi	Ranking
Hampir tidak mungkin	Tidak ada metode detensi	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. Hasil identifikasi ini diapatkan dari perhitungan nilai prioritas risiko (*Risk Priority Number)* dengan perhitungan sebagai berikut.

RPN = Severity * Occurence * Detection

Setelah ditentukan nilai RPN untuk masing masing risiko, maka selanjutnya nilai RPN tersebut akan dikategorikan berdasarkan level risiko di Skala RPN(*Risk Priority Number)*. Berikut merupakan skala penentuan level risiko berdasarkan nilai RPN.

Tabel 4.10 Skala Nilai RPN

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

4.4.2 Analisis Dampak Bisnis

Untuk melakukan analisis dampak bisnis pada penelitian kali ini, peneliti menggunakan acuan ISO 22317 – *Business Impact Analysis*. Berikut merupakan langkah langkah dalam melakukan analisis dampak bisnis dalam penelitian ini yang mengacu pada ISO 22317 :

1. Prioritisasi Layanan SI/TI

Tahapan awal dari analisis dampak bisnis adalah terlebih dahuulu memprioritaskan layanan dan proses bisnis SI/TI yang dimiliki oleh organisasi. Tingkat dari prioritisasi layanan SI/TI ini nantinya akan dikategorikan sebagai berikut.

Tabel 4.11 Skala Tingkat Kritis Layanan TI

Tingkat Kritis	Keterangan
Sangat Kritis	Layanan TI dikategorikan kritis apabila memiliki dampak yang sangat besar apabila terjadi ancaman.
Penting	Layanan TI dikategorikan penting apabila memiliki dampak yang tidak terlalu besar apabila terjadi ancaman
Minor	Layanan TI dikategorikan minor apabila tidak memiliki dampak atau dampaknya hampir tidak terasa saat terjadi ancaman

2. Prioritisasi Proses Bisnis dan Aktivitas terkait SI/TI

Selain melakukan prioritisasi layanan SI/TI, akan dilakukan juga prioritisasi terkait proses bisnis dan aktivitas SI/TI. Aktivitas – aktivitas ini berupakan penjabaran lebih detail dari proses bisnis SI/TI yang sebelumnya telah dijabarkan. Tingkat dari prioritisasi proses bisnis ini nantinya akan dikategorikan sebagai berikut.

Tabel 4.12 Skala Tingkat Kritis Proses Bisnis TI

Tingkat Kritis	Keterangan
Sangat Kritis	Proses bisnis dikategorikan kritis apabila proses bisnis ini memiliki dampak yang sangat besar apabila terjadi ancaman.
Penting	Proses bisnis dikategorikan penting apabila proses bisnis ini memiliki dampak yang

Tingkat Kritis	Keterangan
	tidak terlalu besar apabila terjadi ancaman
Minor	Proses bisnis diaktegorikan minor apabila proses bisnis ini 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), *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO). 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.
- ***Recovery Point Objective*** **(RPO)** adalah waktu yang diperlukan setelah terjadinya gangguan, untuk memulihkan data setelah terjadinya gangguan.

4. Analisis Dampak Gangguan

Analisa dampak gangguan dilakukan untuk mengetahui dampak yang terjadi pada suatu proses bisnis. Dampak ini nantinya dibagi menjadi tiga aspek, yaitu aspek finansial, aspek reputasi dan juga aspek target teknis. Berikut

merupakan kategori dampak yang digunakan dalam penelitian.

Tabel 4.13 Kategori Dampak

Kategori Dampak	Deskripsi Dampak
Finansial	Dampak finansial dijelaskan dengan jumlah persentase biaya ekstra yang harus dikeluarkan perusahaan, bisa dalam bentuk biaya pinalti, biaya tambahan atau profit yang hilang.
Reputasi	Dampak reputasi dapat berupa opini negatif dari media atau masyarakat yang mana dapat membuat perusahaan kehilangan pelanggan yang potensial
Target Teknis	Target teknis merupakan dampak berupa persentase (%) ketidaktercapaian target atau tujuan dari perusahaan akibat ancaman tersebut.

4.5 Penentuan Strategi BCP

Dalam menentukan stragei BCP nantinya strategi BCP akan dikategorikan menjadi 4 jenis strategi, yaitu strategi preventif, strategi DRP, strategi saat terjadi gangguan dan strategi korektif. Berikut merupakan penjelasan untuk masing masing strategi :

- **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 DRP**
  Strategi DRP merupakan suatu tindakan atau aksi yang saat itu juga harus segera dilakukan oleh tim DRP, untuk dapat mengatasi penyebab dari gangguan maupun bencana yang saat itu terjadi. Strategi DRP ini hanya dijalankan saat bencana atau gangguan telah terjadi dan bersifat teknis dan mendetail. Diharapkan strategi DRP ini nantinya dapat memberikan organisasi panduan yang efektif dan efisien dalam melakukan pemulihan.
- **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 merupakan tahapan yang dilakukan untuk memastikan bahwa BCP telah sesuai dengan kebutuhan organisasi. Tahapan validasi ini nantinya akan dilakukan agar terdapat kesesuaian antara hasil penelitian dengan kebutuhan di STIE Perbanas. Untuk memastikan keabsahan dari penyusunan BCP maka peneliti akan mengajukan surat konfirmasi kesesuaikan kebutuhan dan keinginan perusahaan kepada Wakil Ketua Perbanas. Berikut merupakan tabel rencana validasi yang akan diajukan oleh peneliti kepada pihak STIE Perbanas.

Tabel 4.14 Tabel Keterangan Validasi

No	Nama Validasi	Deskripsi Verifikasi
1.	Validasi kesesuaian formulasi kerangka BCP pada STIE Perbanas	Validasi ini bertujuan untuk memastikan bahwa formulasi kerangka BCP telah sesuai dengan kebutuhan dan keinginan STIE Perbanas.
2.	Validasi kesesuaian analisis risiko STIE Perbanas	Validasi ini bertujuan untuk memastikan analisis risiko telah sesuai dengan kebutuhan organisasi berdasarkan penggalian data yang dilakukan di STIE Perbanas.
3.	Validasi kesesuaian analisis dampak bisnis STIE Perbanas	Validasi ini bertujuan untuk memastikan analisis dampak bisnis telah sesuai dengan kebutuhan organisasi berdasarkan penggalian data yang dilakukan di STIE Perbanas.
4.	Validasi Dokumen akhir BCP pada STIE Perbanas	Validasi ini bertujuan untuk memastikan bahwa dokumen akhir BCP yang

No	Nama Validasi	Deskripsi Verifikasi
		telah dibuat oleh peneliti telah sesuai dengan kebutuhan STIE Perbanas.

Halaman ini sengaja dikosongkan

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 STIE Perbanas. Berikut merupakan keterangan dari pelaksanaan tahap pengumpulan data dan Informasi dengan wawancara

Tabel 5.1 Hasil Wawancara

1.	Narasumber :	Dr. Drs. Emanuel Kritijadi, MM
	Jabatan :	Pembantu ketua I Bidang Akademik
	Tanggal :	Jumat, 30 Oktober 2015
	Lokasi :	STIE Perbanas Kampus 1
	Topik :	Kondisi kekinian organisasi, proses bisnis organisasi, identifikasi aset kritis, ancaman dan risiko serta dampak terhadap proses bisnis kritis apabila terkena gangguan.
	Hasil :	**LAMPIRAN E**
2.	Narasumber :	Dr. Drs. Emanuel Kritijadi, MM
	Jabatan :	Pembantu ketua I Bidang Akademik
	Tanggal :	Jumat, 30 Oktober 2015
	Lokasi :	STIE Perbanas Kampus 1

	Topik :	Kondisi kekinian organisasi, proses bisnis organisasi, identifikasi aset kritis, ancaman dan risiko serta dampak terhadap proses bisnis kritis apabila terkena gangguan.
	Hasil :	**LAMPIRAN F**
2.	Narasumber :	Hariadi Yutanto, S.Kom, M.Kom
	Jabatan :	Kasie TIK (Manajemen Jaringan dan Technical Support)
	Tanggal :	Kamis, 21 Oktober 2015
	Lokasi :	STIE Perbanas Kampus 2
	Topik :	Kondisi kekinian organisasi, proses bisnis organisasi, identifikasi aset kritis, ancaman dan risiko serta dampak terhadap proses bisnis kritis apabila terkena gangguan.
	Hasil :	**LAMPIRAN E dan F**

Keterangan : Hasil Wawancara terdokumentasi pada bagian lampiran.

5.1.2 Hasil Analisis Dokumen

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

1. **Dokumen pedoman mutu**

   Dokumen pedoman mutu STIE Perbanas memuat penjelasan mengenai berbagai informasi mendasar mengenai organisasi seperti profil, struktur organisasi dan proses bisnis pada STIE Perbanas.

2. **Rencana Induk Pengembangan STIE Perbanas 2013 – 2017**

   Dokumen Rencana Induk Pengembangan STIE Perbanas merupakan suatu dokumen yang memuat mengenai strategi

strategi yang akan telah direncanakan STIE Perbanas dalam periode 2013 hingga 2017. Analisis pada bagian ini akan lebih difokuskan kepada rencana strategi STIE Perbanas pada bagian pengembangan TIK.

3. Kebijakan TIK

Kebijakan TIK STIE Perbanas memuat penjelasan mengenai tugas dan fungsi pokok dari bagian TIK STIE Perbanas dan juga peraturan mengenai pengelolaan fasilitas dan layanan TIK.

4. Prosedur terkait TIK

Prosedur terkait TIK merupakan serangkaian peraturan peraturan spesifik mengenai pengelolaan layanan dan fasilitas TIK yang telah dimiliki oleh STIE Perbanas.

5.2 Formulasi Kerangka Kerja BCP STIE Perbanas

Dalam melakukan perancangan dokumen BCP, terlebih dahulu dilakukan formulasi kerangka kerja BCP STIE Perbanas. Dalam perancangan ini peneliti menggunakan pendekatan mundur dimana dilakukan penggalian kebutuhan dan keinginan pihak organisasi terlebih dahulu akan bentuk BCP. BCP ini nantinya akan digali dari keinginan pihak manajemen organisasi, terutama bagian Teknologi Informasi dan Komunikasi (TIK).

Setelah diketahui kebutuhan dari pihak organisasi untuk kerangka kerja BCP, selanjutnya dilakukan analisis terhadap kerangka kerja BCP yang akan dijadikan acuan dalam penelitian ini. Kerangka kerja BCP yang digunakan pada penelitian ini adalah Kerangka Kerja BCMS ISO 22301:2012 dan Kerangka Kerja BCM Griffith University.

Kerangka Kerja BCP STIE Perbanas nantinya adalah gabungan antara hasil analisis dari kerangka kerja BCP acuan dan kebutuhan serta keinginan dari organisasi. Sehingga diharapkan nantinya dapat dihasilkan kerangka kerja yang tepat dan sesuai.

Gambar 5.1 Formulasi Kerangka Kerja BCP

5.2.1 Penggalian Kebutuhan dan Keinginan STIE Perbanas

Tahapan pertama dalam melakukan formulasi kerangka kerja BCP STIE Perbanas adalah dengan terlebih dahulu melakukan penggalian kebutuhan organisasi akan dokumen BCP yang nantinya akan dibuat. Penggalian kebutuhan dilakukan agar rancangan kerangka kerja BCP yang nantinya dibuat dapat sesuai kondisi dan keinginan manajemen STIE Perbanas.

Penggalian kebutuhan ini dilakukan dengan melakukan wawancara dengan bagian TIK dan menyesuaikannya dengan Rencana Strategis STIE Perbanas bagian Pengembangan TIK. Berikut adalah hasil dari penggalian kebutuhan terhadap BCP yang diinginkan oleh STIE Perbanas Surabaya.

Tabel 5.2 Kebutuhan dan Keinginan STIE Perbanas

KEBUTUHAN DAN KEINGINAN STIE PERBANAS	STATUS
BCP yang dibuat dapat membantu organisasi dalam menghadapi risiko dan bencana di bidang TIK	Terverifikasi

BCP yang dibuat harus disesuaikan dengan *blueprint* teknologi informasi	Terverifikasi
BCP yang dibuat sesuai dengan operasional proses bisnis porganisasi	Terverifikasi
BCP yang dibuat dapat membantu organisasi dalam keamanan teknologi informasi	Terverifikasi
BCP dibuat dengan melihat kondisi Sumber Daya Manusia di organisasi	Terverifikasi
BCP yang dibuat dapat dilakukan pembaharuan dari waktu ke waktu	Terverifikasi
BCP yang dibuat dapat digunakan dalam jangka waktu panjang	Terverifikasi

5.2.2 Penyesuaian Kebutuhan dan Keinginan STIE Perbanas dengan Rencana Strategis STIE Perbanas

Setelah dilakukan penggalian kebutuhan dan keinginan STIE Perbanas maka selanjutnya akan dilakukan penyesuaian kebutuhan dan keinginan STIE Perbanas untuk BCP dengan isi rencana induk pengembangan (RIP) STIE Perbanas 2013 – 2017 untuk pengembangan TIK.

Tabel 5.3 Kebutuhan dan Keinginan STIE Perbanas

KEBUTUHAN DAN KEINGINAN STIE PERBANAS	ISI RIP STIE PERBANAS 2013 - 2017
1. BCP yang dibuat dapat membantu organisasi dalam menghadapi risiko dan bencana di bidang TIK	Pengembangan *Disaster Management System* bidang TIK
2. BCP yang dibuat harus disesuaikan dengan *blueprint* teknologi informasi	Peningkatan kualitas sistem Teknologi Informasi dan Komunikasi sesuai

	dengan blueprint teknologi informasi
3. BCP yang dibuat sesuai dengan operasional proses bisnis porganisasi	Pendayagunaan TIK digunakan untuk peningkatan efisiensi proses bisnis
4. BCP yang dibuat dapat membantu organisasi dalam keamanan teknologi informasi	Pengembangan sistem keamanan berbantuan teknologi informasi.
5. BCP dibuat dengan melihat kondisi Sumber Daya Manusia di organisasi	Perencanaan memperhatikan kondisi dan sumber daya internal institusi, khususnya kinerja dari masing-masing Fakultas, Program Studi dan seluruh unit kerja yang ada
6. BCP yang dibuat dapat dilakukan pembaharuan dari waktu ke waktu	Perencanaan dilakukan sebagai sebuah proses berkelanjutan yang didasarkan pada ecaluasi diri pada semangat perbaikan berkelanjutan (*continous improvemnt)*
7. BCP yang dibuat dapat digunakan dalam jangka waktu panjang	Perbaikan terus menerus yang dilakukan harus berorientasi pada kepentingan jangka

	pendek, menengah, panjang dan global dengan mengutamakan nilai-nilai idealistik, sistematis, terukur, keberlangsungan (sustainability), dan holistik

Untuk memastikan kesesuaian antara dokumen BCP dengan kebutuhan organisasi, maka peneliti akan mengajukan lembar verifikasi kepada manajemen STIE Perbanas. Lembar verifikasi ini akan dilampirkan pada A.

5.2.3 Proses formulasi Kerangka Kerja BCP STIE Perbanas

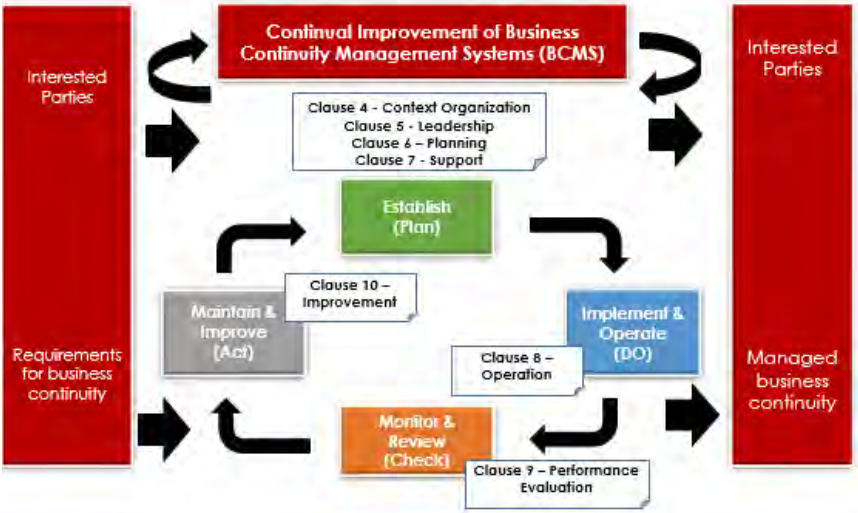
Dalam membuat kerangka kerja BCP, terlebih dahulu akan dilakukan formulasi kerangka kerja dengan melihat adanya kesesuaian pola kerangka keja BCP yang dijadikan acuan dan kerangka kerja tersebut nantinya juga akan disesuaikan dengan kebutuhan dari organisasi.

Penjelasan detail untuk masing masing kerangka kerja BCP yang menjadi acuan dalam penelitian ini dijelaskan pada bagian BAB II Tinjauan Pustaka. Formulasi kerangka kerja ini nantinya akan dilakukan dengan mengacu pada dua standar yaitu standar ISO 22301:2012 *business continuity management systems* dan kerangka kerja BCP Griffith University. Berikut merupakan hasil analisis dari masing masing kerangka BCP.

5.2.3.1 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 menggunakan model berupa siklus PDCA (*Plan-Do-Check-Act)* dalam menerapkan pengelolaan keberlangsungan

bisnisnya. Dalam model PDCA yang digunakan oleh ISO 22301:2012 ini organisasi dapat memulai merencanakan, mengimplementasikan, memonitor hingga meningkatkan kembali secara terus menerus perencanaan keberlangsungan bisnisnya dengan *continuous improvement.* Untuk ISO 22301:2012, pelaksanaan BCP dijabarkan pada klausa 4 hingga kalusa 10. Berikut merupakan pemetaan tiap fasenya.



Gambar 5.2 Pemetaan Klausa ke Bagan PDCA ISO 22301:2012

Berikut adalah bagan yang mejelaskan klausa-klausa dari masing masing fase model PDCA berdasarkan ISO 22301:2012 yang dapat digunakan dalam implementasi BCP pada STIE Perbanas.

Gambar 5.3 Rincian Klausa untuk Masing - Masing Fase PDCA

Berikut merupakan klasifikasi warna pada setiap fase PDCA (*plan – do – check – act)*

Gambar 5.4 Klasifikasi Warna pada Fase PDCA

Kerangka *Business Continuity Management Systems* (BCMS) ISO 22301:2012 memiliki kelebihan maupun kekurangan. Kelebihan dari penerapan kerangka kerja BCMS ini adalah ISO 22301:2012 merupakan suatu kerangka yang dapat mencakup semua aktifikas dan proses – proses dalam keberlanjutan bisnis pada organisasi. Kerangka ini juga bersifat dinamis dan dapat terus menerus diperbarui.

Kekurangan yang ada pada kerangka BCMS ini adalah kerangka ini bersifat sangat umum dan tidak benar – benar mendetail. Kerangka BCMS ini tidak dapat diterapkan sendiri pada STIE Perbanas karena kompleksitasnya yang tinggi dan konteksnya yang sangat umum dan teoritis.

5.2.3.2 Kerangka Kerja BCM Griffith University

Griffith University membuat suatu kerangka kerja *business continuity management* (BCM) yang mana telah disesuaikan dengan kondisi universitas atau organisasi pendidikan. Kerangka kerja Griffith University sifatnya operasional dan mudah diimplementasikan pada penelitian ini dikarenakan telah sesuai dengan kondisi organisasi pendidikan pada umumnya. Berikut merupakan fase dari kerangka BCM Griffith University.

Gambar 5.5 Tahapan dalam Kerangka Kerja Griffith University

Apabila dibandingkan dengan kerangka kerja ISO 22301:2012, kerangka kerja Griffith University ini bersifat lebih detail dan teknis apabila dibandingkan dengan ISO 22301:2012 yang bersifat lebih teoritis.

Kekurangan dari kerangka kerja BCM ini adalah kerangka ini adalah dikarenakan memiliki sifat yang sangat operasional dan teknis, hal ini menjadikannya kurang dinamis dan komprehensif. Selain itu, kerangka ini hanya mencakup fase perencanaan (*plan)*, implementasi (*do)* dan pengawasan (*check)*, namun tidak

mencakup fase tindakan (*act)* yang mana dilakukan untuk melakukan peningkatan secara terus menerus (*continuous improvement)* agar menjaga BCP tetap relevan dengan kondisi dan kebutuhan organisasi.

Kerangka Kerja BCMS ISO 22301:2012 dan Kerangka Kerja BCM Griffith University masing masing memiliki kekurangan dan kelebihan. Untuk itu, agar dapat menghasilkan kerangka BCP yang sesuai dan tepat guna maka peneliti akan menyusun kerangka sesuai dengan hasil formulasi dari kedua standar tersebut. Selain itu kerangka juga akan disesuaikan dengan kebutuhan dan keinginan organisasi terkait perencanaan keberlangsungan bisnis yang telah diidentifikasi sebelumnya.

Kedua standar yang digunakan pada penelitian ini memiliki tahapan yang sama yaitu pengembangan BCP dengan melihat aspek penilaian risiko dan analisis dampak bisnis. Walaupun begitu banyak bagian – bagian dari ISO 22301:2012 yang tidak tercakup pada kerangka kerja Griffith University.

Dari kedua standar kerangka BCP yang menjadi acuan di penelitian ini, peneliti menghasilkan kesimpulan bahwa berdasarkan ISO 22301:2012, hal yang diimplementasikan adalah penerapan siklus PDCA, sehingga didapatkan urutan yang komprehensif. Selain itu pada kerangka kerja. 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 dengan Kebutuhan dan Keinginan STIE Perbanas

Pada penelitian ini model BCP yang digunakan adalah menggunakan model *deming cycle* atau siklus deming yang dibuat oleh W. Edward Deming. Model *Deming cycle* ini memiliki nama lain yaitu Model PDCA (*plan-do-check-act)*. Alasan menggunakan model ini pada penelitian adalah karena model PDCA cocok diterapkan untuk kerangka BCP yang kebutuhannya bisa terus menerus berubah sehingga dibutuhkan model yang dapat terus meneurus dapat meningkatkan kerangka BCP agar relevan dengan

perkembangan teknologi informasi yang diterapkan oleh organisasi.

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 5.4 Pemetaan Kerangka Kerja BCP dengan Kebutuhan dan Keinginan Organisasi

FASE	KEBUTUHAN DAN KEINGINAN STIE PERBANAS	KERANGKA BCP
PLAN	BCP yang dibuat harus disesuaikan dengan *blueprint* teknologi informasi	Profil Organisasi
		Tujuan
		Ruang Lingkup
	BCP dibuat dengan melihat kondisi Sumber Daya Manusia di organisasi	Peran dan Tanggung Jawab
		Sumber Daya
		Alur Komunikasi
DO	BCP yang dibuat dapat membantu organisasi dalam menghadapi risiko dan bencana di bidang TIK	Analisis Risiko
		Analisis Dampak Bisnis
	BCP yang dibuat dapat membantu organisasi dalam	Strategi BCP
		Pembuatan Prosedur BCP

	keamanan teknologi informasi	
	BCP yang dibuat sesuai dengan operasional proses bisnis porganisasi	Pelatihan dan Pengujian
CHECK	BCP yang dibuat dapat dilakukan pembaharuan dari waktu ke waktu	Audit Internal
		Peninjauan Manajemen
ACT	BCP yang dibuat dapat digunakan dalam jangka waktu panjang	Peningkatan secara terus menerus

Setelah dilakukan penyesuaian kebutuhan organisasi, peneliti juga akan melakuan formulasi antara kerangka kerja dengan standar kerangka kerja BCP yang digunakan. Disini nantinya peneliti akan mengambil bagian – bagian yang memang sesuai dengan kebutuhan dan keinginan perusahaan sehingga tidak semua bagian dari kerangka kerja standar BCP akan digunakan. Sehingga akan terbentuk formulasi kerangka BCP yang unik dan sesuai dengan keinginan dan kebutuhan organisasi.

Gambar 5.6 Formulasi Kebutuhan dengan Kerangka Kerja BCP

5.3 Kerangka Kerja BCP STIE Perbanas

Kerangka Kerja BCP STIE Perbanas dihasilkan dari formulasi antara kebutuhan dan keinginan perusahaan serta hasil analisis formulasi dari 2 standar acuan kerangka kerja BCP yaitu ISO 22301:2012 dan Kerangka Kerja Griffith University. Berikut merupakan gambar kerangka kerja dari BCP STIE Perbanas.

Gambar 5.7 Kerangka Kerja BCP STIE Perbanas

Setiap tahapan yang ada pada Kerangka BCP STIE Perbanas merupakan hasil formulasi dari kebutuhan dan keinginan organisasi serta mengacu pada standar acuan yaitu kerangka kerja BCMS ISO 22301:2012 dan Kerangka Kerja Griffith University. Berikut merupakan pemetaan fase dan tahapan kerangka kerja BCP STIE Perbanas dengan standar acuan yang digunakan.

Tabel 5.5 Pemetaan Kerangka Kerja BCP STIE Perbanas dengan Standar Acuan

FASE	SUB-FASE	ACUAN
PLAN (PERENCANAAN)	Profil Organisasi	ISO 22301:2012
	Tujuan BCP	ISO 22301:2012

FASE	SUB-FASE	ACUAN
	Ruang Lingkup	ISO 22301:2012
	Peran dan Tanggung Jawab	ISO 22301:2012 Griffith University
	Sumber Daya	ISO 22301:2012
	Alur Komunikasi	ISO 22301:2012 Griffith University
DO (PENGERJAAN)	Analisis Risiko	ISO 22301:2012 Griffith University
	Analisis Dampak Bisnis	ISO 22301:2012 Griffith University
	Strategi BCP	ISO 22301:2012 Griffith University
	Pelatihan dan Pengujian	ISO 22301:2012 Griffith University
CHECK (PEMERIKSAAN)	Audit Internal TI	ISO 22301:2012 Griffith University
	Peninjauan Manajemen	ISO 22301:2012
ACT (TINDAKAN)	Peningkatan Secara Terus-Menerus	ISO 22301:2012

5.4 Hasil Validasi BCP

Berikut merupakan tabel rencana validasi yang akan diajukan oleh peneliti kepada pihak STIE Perbanas.

Tabel 5.6 Tabel Keterangan Validasi

No	Nama Validasi	Deskripsi Verifikasi
1.	Validasi kesesuaian formulasi kerangka BCP pada STIE Perbanas	Validasi ini berbentuk surat konfirmasi kesesuaian kepada Kasie Bagian TIK STIE Perbanas. Surat konfirmasi akan dilampirkan pada Lampiran A.
2.	Validasi kesesuaian analisis risiko STIE Perbanas	Validasi ini berbentuk surat konfirmasi kesesuaian kepada Kasie Bagian TIK STIE Perbanas. Surat konfirmasi ini akan dilampirkan pada Lampiran B.
3.	Validasi kesesuaian analisis dampak bisnis STIE Perbanas	Validasi ini berbentuk surat konfirmasi kesesuaian kepada Kasie Bagian TIK STIE Perbanas. Surat konfirmasi ini akan dilampirkan pada Lampiran C.
4.	Validasi Dokumen akhir BCP pada STIE Perbanas	Validasi ini berbentuk surat konfirmasi kesesuaian kepada Wakil Ketua Perbanas. Surat konfirmasi ini akan dilampirkan pada Lampiran D.

5.5 Hambatan dan Rintangan

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

1. Proses pengumpulan dan pengolahan data cukup lama sebelum peneliti bisa membuat BCP, hal ini dikarenakan peneliti harus melalui beberapa tahapan seperti analisis risiko serta analisis dampak bisnis.
2. Diperlukannya validasi di beberapa tahapan dalam penelitian untuk memastikan integritas dari hasil penelitian. Hal ini juga membutuhkan waktu yang relatif lama karena organisasi harus meninjau hasil dari tahapan yang telah dibuat oleh peneliti.

Walaupun terdapat beberapa hambatan dan rintangan, namun penelitian ini tetap berjalan dengan lancar berkat bantuan dari pihak STIE Perbanas yang terlibat dalam membantu berjalannya penelitian. Pihak STIE Perbanas juga sangat terbuka dan membantu penelitian dengan memberikan respon yang cepat dan bersedia meluangkan waktu untuk melakukan wawancara dan konsultasi.

Halaman ini sengaja dikosongkan

BAB VI
HASIL DAN PEMBAHASAN

Bab ini menjelaskan proses penyusunan dan pembahasan dokumen BCP STIE Perbanas yang telah dibuat pada bab sebelumnya.

6.1 Pembahasan Dokumen BCP STIE Perbanas

Bagian ini akan menjelaskan model BCP yang dirancang untuk STIE Perbanas Surabaya. Fase yang terdapat pada model ini merupakan fase PDCA yaitu yang terdiri dari *plan* (perencanaan), *do* (pengerjaan), *check* (pemeriksaan) dan *act* (tindakan).

6.1.1 Plan (Perencanaan)

Pada fase perencanaan, organisasi diharapkan dapat menyusun BCP sesuai dengan kebijakan, kebutuhan dan tujuan dari organisasi. Dalam fase ini, organisasi akan menentukan latar belakang dari organisasi sendiri, tujuan, ruang lingkup, peran dan tanggung jawab, sumber daya yang dibutuhkan dan alur komunikasi selama pengelolaan keberlangsungan bisnis.

6.1.1.1 Profil Perusahaan

Bagian ini menjelaskan mengenai informasi perusahaan yang terlibat dalam penyusunan BCP serta keinginan dan kebutuhan perusahaan terkait dengan proses keberlanjutan bisnis.

PROFIL STIE PERBANAS

STIE Perbanas Surabaya merupakan suatu lembaga pendidikan yang dibentuk dan berada di bawah naungan Perhimpunan Bank-bank Umum Nasional (Perbanas) Jawa Timur. Didirikan pada tahun 1970, STIE Perbanas telah memiliki dua kampus utama yang berada di Surabaya. STIE Perbanas telah memperoleh berbagai sertifikasi, penghargaan, dan dana hibah

merupakan bentuk pengakuan atas komitmen dan kerja keras dalam peningkatan mutu layanan pendidikan

Berikut merupakan tabel identitas dari STIE Perbanas Surabaya yang akan menjadi subyek untuk untuk perencanaan keberlanjutan bisnis dalam dokumen BCP ini.

Tabel 6.1 Profil STIE Perbanas

PROFIL PERUSAHAAN	
Nama Perusahaan	STIE Perbanas
Lokasi Perusahaan	Surabaya, Jawa Timur Kampus 1 : Jalan Nginden Semolo, Surabaya Kampus 2 : Jalan Wonorejo Indah Timur, Surabaya
Tahun Berdiri	1970
Jenis Usaha	Organisassi Pendidikan - Sekolah Tinggi Ilmu Ekonomi
Jumlah Kampus	2 Kampus Utama Kampus 1 : Jalan Nginden Semolo, Surabaya Kampus 2 : Jalan Wonorejo Indah Timur, Surabaya
Logo Perusahaan	

Untuk profil selengkapnya tentang STIE Perbanas Surabaya dapat kembali dilihat pada Bab IV, sub-bab 4.1.

Kebutuhan dan Keinginan BCP STIE Perbanas

Dokumen BCP STIE Perbanas nantinya harus sesuai dengan kebutuhan dan keinginan dari STIE Perbanas. Penggalian kebutuhan dilakukan agar rancangan kerangka kerja BCP yang nantinya dibuat dapat sesuai kondisi dan keinginan manajemen STIE Perbanas. Daftar kebutuhan dan keinginan organisasi akan diverifikasi oleh pihak STIE Perbenas. Untuk verifikasi kesesuaian BCP dengan kebutuhan dan keinginan organisasi, lihat Lampiran A.

Berikut merupakan daftar penggalian kebutuhan dan keinginan STIE Perbanas untuk dokumen BCP yang telah diverifikasi.

Tabel 6.2 Kebutuhan dan Keinginan STIE Perbanas

KEBUTUHAN DAN KEINGINAN STIE PERBANAS	STATUS
1. BCP yang dibuat dapat membantu organisasi dalam menghadapi risiko dan bencana di bidang TIK	Terverifikasi
2. BCP yang dibuat harus disesuaikan dengan *blueprint* teknologi informasi	Terverifikasi
3. BCP yang dibuat sesuai dengan operasional proses bisnis porganisasi	Terverifikasi
4. BCP yang dibuat dapat membantu organisasi dalam keamanan teknologi informasi	Terverifikasi
5. BCP dibuat dengan melihat kondisi Sumber Daya Manusia di organisasi	Terverifikasi

6. BCP yang dibuat dapat dilakukan pembaharuan dari waktu ke waktu	Terverifikasi
7. BCP yang dibuat dapat digunakan dalam jangka waktu panjang	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. Dapat menghasilkan dokumen BCP (*Business Continuity Plan*) yang sesuai dengan tujuan dan kebutuhan dari STIE Perbanas.
2. Menghasilkan dokumen BCP yang dapat mendukung proses pengelolaan keberlangsungan bisnis dapat diimplementasikan secara menyeluruh kepada bagian organisasi yang memiliki ketergantungan terhadap teknologi informasi.
3. Dapat membantu organisasi dalam meminimalisir risiko teknologi informasi yang dapat muncul dan menghambat operasional bisnis organisasi.
4. Dapat membantu organisasi dalam mengetahui dampak bisnis teknologi informasi terhadap keberlangsungan operasional bisnis organisasi.
5. Meningkatkan kesadaran dari seluruh pegawai STIE Perbanas atas pentingnya pengelolaan risiko dan pengelolaan keberlangsungan bisnis di organisasi.
6. Dapat membantu perusahaan mengelola layanan teknologi informasi dan menjaga citra baik dari organisasi.

6.1.1.3 Ruang Lingkup

Pada penyusunan dokumen BCP pada STIE Perbanas, terdapat beberapa fungsional bisnis dan proses bisnis yang terlibat. Fungsional bisnis dan proses bisnis yang terlibat merupakan yang menggunakan dan memiliki ketergantungan terhadap teknologi dan informasi dalam melakukan aktivitasnya.

Fungsional Bisnis dan Proses Bisnis yang Terlibat

Dilihat dari struktur organiasinya, Ketua STIE Perbanas memiliki 3 pembantu ketua (Puket), yaitu Pembantu Ketua I – bidang akademik, Pembantu Ketua 2 – bidang keuangan & umum dan Pembantu Ketua 3 – bidang kemahasiswaan dan kerjasama. Masing masing dari pembantu ketua membawahi beberapa bagiannya masing masing. Dalam fungsional bisnis yang dimiliki oleh STIE Perbanas, terdapat 4 fungsional bisnis yang terkait dengan penelitian ini. Keempat fungsional bisnis ini dianggap sebagai fungsional bisnis yang proses bisnisnya berjalan dengan dukungan teknologi informasi. Fungsional bisnis yang terkait dengan penelitian ini adalah bagian akademik, bagian kemahasiswaan, bagian teknologi informasi dan komunikasi dan bagian keuangan.

Selain fungsional bisnis yang ada pada STIE Perbanas, proses bisnis yang dibahas pada penelitian ini pun juga tidak semuanya dimasukkan. Proses bisnis yang dipilih hanyalah proses bisnis yang memiliki kaitan dan ketergantungan terhadap layanan teknologi informasi organisasi. Berikut merupakan penjabaran dari fungsional bisnis dan proses bisnis yang terlibat dalam proses BCP.

Tabel 6.3 Fungsional Bisnis dan Proses Bisnis Terkait Sistem

FUNGSIONAL BISNIS	PROSES BISNIS TERKAIT SISTEM
Akademik	Proses KRS
	Pengelolaan Data Perpustakaan

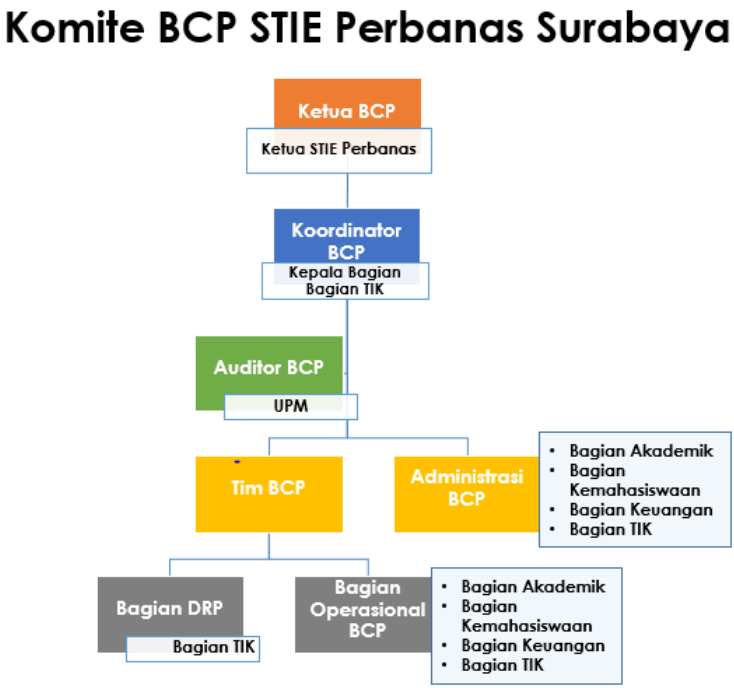
FUNGSIONAL BISNIS	PROSES BISNIS TERKAIT SISTEM
	Pengelolaan Nilai Mahasiswa
	Proses Wisuda
	Proses Pengajaran melalui E-Learning
Kemahasiswaan	Pendaftaran Mahasiswa Baru
	Proses Pengelolaan *Softskill* Mahasiswa
TIK	Melakukan Pemantauan Teknologi
	Melakukan Pengelahan Data Elektronik
	Melakukan Pengelolaan Konfigurasi Perangkat
	Menyediakan Layanan SI/TI untuk Mendukung Proses Pengajaran
	Disaster Recovery Planning
Keuangan	Pengelolaan Pembayaran Biaya Kuliah
	Penggajian Honor Mengajar
	Pengajuan Anggaran

6.1.1.4 Peran dan Tanggung Jawab

Dalam pembentukan BCP, Sumber Daya Manusia (SDM) merupakan suatu hal yang harus diperhatikan. Dengan adanya pembagian peran dan tanggung jawab SDM yang jelas, maka BCP dapat berjalan secara optimal. Oleh karena itu diperlukan adanya suatu pembentukan struktur komite BCP untuk dapat memastikan masing – masing peran dan tanggung jawab tiap bagian terhadap adanya perencanaan keberlangsungan bisnis. Identifikasi usulan sumber struktur komite BCP ini dilakukan dengan melakukan konsultasi pada pihak manajemen dan observasi pada kondisi STIE Perbanas.

Komite BCP ini juga nantinya akan berhubungan dengan Tim DRP, yang mana tim DRP ini merupakan bagian TIK STIE Perbanas. Tim DRP memiliki tanggung jawab untuk menangani semua gangguan pada teknologi informasi di STIE Perbanas.

Berikut merupakan bentuk usulan komite BCP STIE Perbanas Surabaya.



Gambar 6.1 Komite BCP STIE Perbanas Surabaya

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

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

B. Koordinator BCP
   - Bertanggung jawab dalam pengembangan BCP

- Melaksanakan rapat koordinasi saat adanya gangguan kritis
- Melakukan pelatihan dan pengujian sesuai dengan BCP

C. 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
- Menyiapkan
- 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

6.1.1.5 Sumber Daya

Dalam pelaksanaan BCP diperlukan dukungan dari sumber daya untuk dapat memastikan bahwa proses berjalan dengan lancar dan sesuai dengan perencanan. Untuk itu organisasi perlu mengidentifikasi sumber daya perangkat dan ketersediaan infrastruktur yang dapat menunjang operasional saat terjadinya gangguan maupun bencana. Sehingga nantinya diharapkan proses BCP dapat berjalan lancar dengan ketersediaan perangkat – perangkat ini. Identifikasi sumber daya ini dilakukan dengan melakukan konsultasi pada pihak manajemen dan observasi pada kondisi STIE Perbanas.

Berikut merupakan perangkat keras kritikal yang dibutuhkan dalam melakukan perencanaan keberlangsungan bisnis teknologi informasi pada STIE Perbanas.

a. Server Utama
b. Genset dan UPS
c. *Fire extinguisher*
d. NAS (*Network Attached Storage)*
e. Printer
f. Alat telepon PABX
g. Alat komunikasi dan modem di masing masing bagian

Berikut adalah perangkat perencanaan keberlanjutan bisnis terkait aplikasi teknologi informasi.

a. Dokumen informasi mengenai sistem yang memiliki kaitan dengan proses operasional organisasi
b. Perencanaan *back up* data harian agar dapat dilakukan *restore* apabila diperlukan.

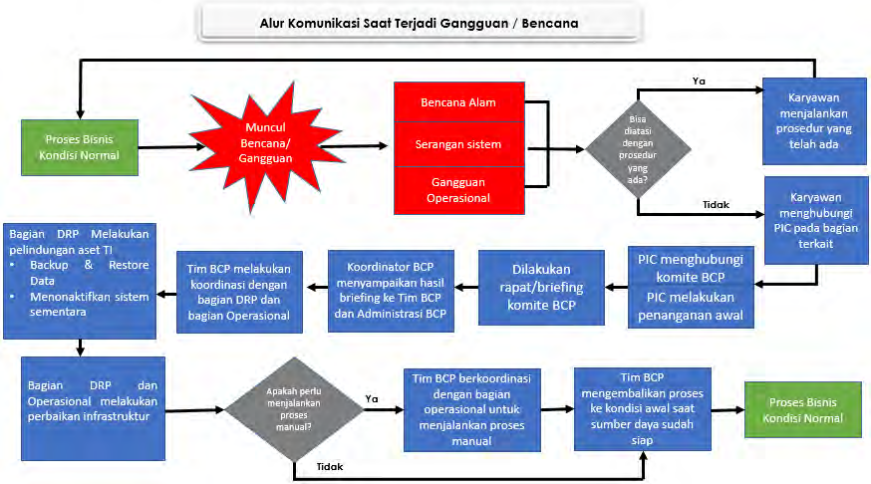
Berikut adalah dokumentasi serta perangkat penunjang lain yang dibutuhkan dalam perencanaan keberlangsungan bisnis teknologi informasi pada STIE Perbanas.

a. *Checklist* laporan kondisi layanan TI
b. Laporan hasil *backup*

c. Daftar Vendor Hardware/Software
d. Daftar kontak darurat
e. SOP (*Standard Operating Procedure*)

6.1.1.6 Alur Komunikasi

Pada dokumen BCP akan ditetapkan alur komunikasi untuk dapat menjamin kelancaran proses BCP yang telah direncanakan. Alur komunikasi ini merupakan gambaran proses komunikasi yang harus dilakukan untuk masing masing peran. Selain itu diperlukan adanya pengaturan struktur pemberian perintah dan tugas antar peran. adalah alur komunikasi saat terjadi gangguan atau bencana.



Gambar 6.2 Alur Komunikasi saat Terjadi Gangguan/Bencana

Berikut merupakan penjelasan mengenai alur komunikasi pada saat terjadi gangguan/bencana.

1. Alur komunikasi ini mulai dilakukan saat terjadi bencana atau gangguan kepada teknologi informasi organisasi yang

menyebabkan proses bisnis tidak dapat berjalan pada kondisi normal. Gangguan atau bencana ini dikategorikan menjadi 3 hal, yang pertama adalah bencana alam seperti kebakaran, banjir atau badai. Kedua adalah serangan terhadap sistem seperti serangan terhadap keamanan sistem maupun jaringan. Sedangkan yang terakhir merupakan gangguan operasional pada proses bisnis.

2. Apabila gangguan atau bencana dapat diatasi dengan prosedur yang telah ada, maka karyawan yang mengalami gangguan akan menjalankan prosedur hingga proses bisnis kembali ke kondisi normal. Apabila gangguan atau bencana tidak dapat diatasi dengan prosedur yang ada maka terlebih dahulu karyawan yang mengalami gangguan menghubungi PIC (*Person in Charge)* pada bagiannya.
3. Setelah itu, PIC akan menghubungi komite BCP dan apabila memungkinkan maka PIC akan mencoba melakukan penanganan awal terlebih dahulu. Dilakukan rapat/*briefing* komite BCP yang dipimpin oleh Koordinator BCP untuk membahas penanganan bencana atau gangguan yang terjadi. Rapat /*briefing* ini dilakukan untuk dapat merumuskan penyelesaian gangguan dan langkah – langkah yang harus diambil.
4. Setelah itu koordinator BCP akan menyampaikan hasil briefing kepada Tim BCP dan juga Administrasi BCP, Kemudia tim BCP akan melakukan koordinasi langkah teknis kepada bagian DRP dan juga Bagian Operasional.
5. Bagian DRP akan melakukan langkah-langkah perlindungan aset TI seperti pengamanan data dengan melakukan *backup* atau *restore*, serta menonaktifkan sistem sementara apabila diperlukan. Selain itu Bagian DRP akan berkoordinasi dengan

bagian operasional untuk dapat melakukan perbaikan infrastruktur.

6. Apabila dalam jangka waktu terjadinya gangguan atau bencana bagian operasional merasa perlu menjalankan proses bisnis sementara secara manual, maka tim BCP akan berkoordinasi dengan bagian operasional untuk menjalankan proses bisnis darurat secara manual. Proses manual harus diambil dengan adanya keputusan dari ketua komite BCP. Apabila semua sumber daya sudah dapat berjalan, maka tim BCP akan mengembalikan proses ke kondisi awal dan proses bisnis akan kembali berjalan dengan normal dan sebagaimana mestinya.

Daftar Alat Komunikasi Darurat

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

Tabel 6.4 Daftar Alat Komunikasi Darurat

DAFTAR ALAT KOMUNIKASI DARURAT
1. *Fixed Line Telephone*
2. Telepon genggam (*mobile*)
3. *E-mail*
5. *Handy Talkie (HT)*

. Alat komunikasi darurat diatas diharapkan dapat menjadi media penghubung antara pihak pihak yang bertanggung jawab

dalam proses BCP untuk dapat menginformasikan gangguan atau bencana yang terjadi maupun proses penanggulangan yang dilakukan. Diharapkan alat komunikasi diatas dapat selalu tersedia, sehingga dapat segera digunakan apabila diperlukan

6.1.2 Do (Pengerjaan)

Pada 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

Dalam tahapan analisis risiko, metode yang akan digunakan adalah dengan menggunakan metode OCTAVE dan FMEA.

Identifikasi Risiko dengan OCTAVE

Metode OCTAVE digunakan untuk dapat mengidentifikasi kemungkinan ancaman dan risiko yang dapat terjadi. Tahapan dalam metode OCTAVE antara lain 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 6.5 Output OCTAVE

Fase	Output
Fase 1 – Membangun profil ancaman berbasis aset	Daftar Aset Kritis
	Daftar Kebutuhan Keamanan untuk Aset Kritis
	Daftar Ancaman untuk Aset Kritis

Fase	Output
	Daftar Praktik Keamanan yang Dlakukan
	Daftar Kelemahan Organisasi
Fase 2 – Mengidentifikasi kelemahan infrastruktur	Daftar Komponen Utama
	Daftar Kerentanan Teknologi
Fase 3 – Membangun Perencanaan dan Strategi Keamanan	Daftar Risiko untuk Aset Kritis
	Pengukuran Risiko

Masing masing tahapan ini didapatkan dari hasil wawancara yang dilampirkan pada Lampiran E dan telah dilakukan verifikasi hasil risiko yang dilampirkan pada Lampiran B.

Fase 1 – Membangun Profil Ancaman Berbasis Aset

Pada fase ini akan dilakukan identifikai aset dan ancaman berbasis aset degan menggunakan informasi yang didapat dari senior manajemen dan bagian operasional. Hal ini diperlukan agar nantinya didapatkan suatu profil ancaman yang lengkap dari sisi manajemen maupun dari sisi teknis. Diharapkan nantinya analisis ini dapat melihat aset mana yang dianggap kritis dan apa saja langkah proteksi yang saat ini telah dilakukan. Selain itu organisasi nantinya juga dapat melihat apakah masing masing aset kritis telah memiliki tingkat keamanan sesuai dengn kebutuhanya.

Output yang dihasilkan dari fase ini nantinya adalah tabel aset kritis, tabel kebutuhan keamanan untuk aset kritis, ancaman untuk aset kritis, praktik keamanan yang sekarang dilakukan dan kelemahan organiisasi.

Untuk dapat membangun profil ancaman berbasis aset terlebih dahulu organisasi perlu mengidentifikasi aset kritis TI. Aset Kritis ini merupakan suatu barang yang memberikan nilai (*value)* tinggi untuk organisasi dalam melakukan proses bisnisnya. Selain itu, identifikasi aset kritis juga dilihat dari apabila tanpa

adanya aset ini, proses bisnis pada STIE Perbanas tidak dapat berjalan dengan lancar dan dalam kondisi normal. Berikut merupakan daftar aset kritis TI organisasi.

Tabel 6.6 Daftar Aset Kritis TI

Daftar Aset Kritis	
Hardware	Server
	PC
Software	SIMAS (bajol.perbanas.ac.id)
	E-Learning (kuliah.perbanas.ac.id)
	SPMB (spmb.perbanas.ac.id)
	Perpustakaan
Data	Data Demografi Mahasiswa
	Data Akademik
	Data File Server
Jaringan	Wifi
	Kabel
	Router
Sumber Daya Manusia	Dosen
	Mahasiswa
	Pegawai Non TI
	Pegawai TI

Dari aset kritis yang telah teridentifikasi tersebut, setelah itu akan dilakukan identifikasi kebutuhan keamanan untuk masing masing aset tersebut. Hal ini dilakukan nantinya untuk dapat mengetahui apa saja yang dibutuhkan organisasi Berikut merupakan kebutuhan keamanan aset kritis organisasi.

Tabel 6.7 Contoh Daftar Kebutuhan Keamanan Aset

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset
Hardware	Server	• Dapat diakses 24 jam dalam 7 hari

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset
		• Adanya sumber listrik cadangan • Adanya kontrol keamanan untuk ruang fisik server • Adanya pembatasan hak akses • Konfigurasi server dilakukan dengan benar
	PC	• Dapat berfungsi selama jam kerja organisasi • Adanya sumber listrik cadanagn • Adanya pembatasan hak akses • Adanya Antivirus
Software	SIMAS (simas.perbanas.ac.id)	• Dapat diakses 24 jam dalam 7 hari • Adanya pembatasan hak akses • Adanya pengamanan terhadap data
	E-Learning (kuliah.perbanas.ac.id)	
	Perpustakaan	

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset
Data	Data Demografi Mahasiswa	• Data dapat diakses 24 jam dalam 7 hari • Adanya *backup data* secara rutin • Adanya pengamanan terhadap data • Adanya pembatasan hak akses pegawai pada data
	Data Akademik	
	Data File Server	
Jaringan	Wifi	• Tersedia selama jam operasional kerja organisasi • Terdapat sumber listrik cadangan • Adanya kontrol rutin • Adanya anti netcut
	Kabel	• Tersedia selama jam operasional kerja organisasi • Adanya kontrol rutin • Kabel dilakukan pelabelan untuk mempermudah pengorganisasian

Kategori Aset	Nama Aset	Kebutuhan Keamanan Aset
	Router	• Tersedia selama jam operasional kerja organisasi • Adanya kontrol rutin

Setelah itu akan dilakukan identifikasi ancaman yang dikategorikan berdasarkan linkungan, manusia dan infrastruktur. Berikut merupakan daftar ancaman TI yang dapat menyerang organisasi.

Tabel 6.8 Daftar Ancaman pada Teknologi Informasi

Ancaman dari Lingkungan	
1.	Gempa Bumi
2.	Tsunami dan Badai
3.	Banjir
4.	Kebakaran
5.	Kebocoran dan Kerusakan Pada Bangunan
6.	Perubahan Regulasi
Ancaman dari Manusia	
7.	Kesalahan input data
8.	Pembobolan Sistem
9.	Pencurian Data
10.	Sharing Password
11.	Sabotase Jaringan Internet
12.	Penurunan Kompetensi Karyawan
Ancaman dari Infrastruktur	
Hardware	
13.	Kerusakan Komputer
14.	Kerusakan Server
15.	Kerusakan pada Genset dan UPS
16.	Kesalahan Konfigurasi Hardware

17.	Pencurian Peralatan Hadware
Software	
18.	Bug pada Software
19.	Virus/Worm
20.	Kesalahan Konfigurasi Sistem
21.	Data Corrupt/Rusak
Jaringan	
22.	Gangguan pada Router
23.	Kerusakan Kabel
24.	Gangguan Koneksi Internet

Praktik keamanan perlu diidentifikasi terlebih dahulu untuk dapat melihat sejauh apa organisasi telah mempersiapkan diri dari ancaman yang dapat terjadi. Hal ini juga dapat membantu dalam penentuan nilai deteksi pada penilaian risiko. Berikut merupakan daftar praktik keamanan yang telah diterapkan oleh organisasi.

Tabel 6.9 Daftar Praktik Keamanan Organisasi

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
Adanya antivirus (e-scan) dan diupdate terus menerus	Bagian TIK
Telah dipasang anti netcut untuk keamanan Wifi	Bagian TIK
Pada Lab tidak bisa memasang USB	Bagian TIK
Pada Lab tidak bisa menginstall aplikasi dari luar	Bagian TIK
Telah dipasang Smoke Detector pada ruang server untuk memberi peringatan apabila terjadi kebakaran	Bidang Keuangan dan Umum

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
Telah ada *fire extinguisher* untuk memadamkan api saat terjadi kebakaran	Bidang Keuangan dan Umum
Telah dilakukan sosialisasi kepada mahasiswa dan dosen untuk praktik keamanan TI	Bagian TIK
Telah dilakukan backup server dan NAS setiap hari pukul 19.00	Bagian TIK
Ada penguncian/penggembokan pada ruang server sehingga tidak dapat sembarang orang bisa masuk	Bagian TIK
Data hanya bisa dimasukkan, diganti atau dihapus oleh *database administrator* saja	Bagian TIK
Dilakukan *maintenance* rutin setiap 6 bulan sekali (diawal semester) untuk kelas dan lab	Bagian TIK
Dilakukan *maintenance* setiap sebelum UTS dan UAS hanya untuk lab saja	Bagian TIK
Dilakukan *maintenance* Wifi setiap 2 minggu sekali	Bagian TIK
Membedakan *role* atau hak akses untuk masing masing pegawai sesuai dengan fungsinya	Bagian TIK
Pengaturan kabel dengan melakukan pelabelan untuk masing masing fungsi kabel	Bagian TIK
Pembuatan dan pelaksanaan beberapa SOP mengenai SI/TI di organisasi	Bagian TIK

Setelah itu dari hasil *interview,* didapatkan beberapa kelemahan organisasi dedapatkan kelemahan organisasi terhadap keamanan teknologi informasi. Kelemahan ini nantinya menjadi masukan untuk dapat menganalisa risiko maupun penyebab risiko yang dapat terjadi. Berikut merupakan daftar kelemahan organisasi.

Tabel 6.10 Daftar Kelemahan Organisasi

Kelemahan Organisasi
Tata Kelola (SOP) untuk SI/TI belum lengkap dan belum sepenuhnya dijalankan
Belum menerapkan standar keamanan sepenuhnya untuk SI/TI organisasi
Adanya rolling peran pegawai sehingga hak akses terus menerus berubah
Belum adanya BCP maupun DRP
Untuk proses 'Reset Password' masih belum bisa pada sistem atau manual
Backup data masih dilakukan pada satu media yang sama
Belum ada *mirroring database*

Fase 2 – Identifikasi Kelemahan Infrastruktur

Pada fase ini akan dilakukan identifiksai kelemahan infrastruktur dengan menggunakan informasi yang didapat dari senior manajemen dan bagian operasional. Pada fase ini akan dilakukan evaluasi terhadap komponen utama dari sistem yang bersifat mendukung aset kritis, setelah didapat komponen utama maka dari itu akan ditinjau kelemahannya.

Output yang dihasilkan dari fase ini nantinya adalah tabel komponen utama dan tabel kerentanan teknologi

Komponen utama merupakan suatu komponen yang mana berkaitan dan berperan penting pada suatu aset. Komponen utama ini terlebih dahulu harus diidentifikasikan agar dapat terlihat gambaran besar dari keseluruhan ancaman. Untuk informasi selengkapnya terkait daftar komponen utama dapat dilihat pada

dokumen produk. Berikut merupakan daftar komponen utama dari masing masing aset kritis TI organisasi.

Tabel 6.11 Contoh Daftar Komponen Utama dari Aset Kritis

Server	
System of Interest	Server yang menyimpan Data Penting
Komponen Utama	• Sistem Operasi • Processor • RAM • Harddisk • Listrik • Keamanan Jaringan • Genset • UPS • Kabel • Smoke Detector
PC	
System of Interest	PC yang ada pada kampus I dan II STIE Perbanas
Komponen Utama	• CPU • Monitor, Keyboard dan Mouse • Kabel LAN • Antivirus • Sistem Operasi • Software • Listrik • UPS • Genset • Firewall
Data	

System of Interest	Data Demografi Mahasiswa, Data Akademik dan Data File Server
Komponen Utama	• Database • Server • Listrik • PC • Firewall • *Database Administrator* (DBA)
Perangkat Lunak	
System of Interest	SIMAS, E-learning dan Perpustakaan
Komponen Utama	• Firewall • Server • Antivirus
Wifi	
System of Interest	18 Wifi yang terpasang pada kampus I STIE Perbanas dan 3 Wifi yang terpasang pada kampus II STIE Perbanas
Komponen Utama	• Listrik • Kabel • Keamanan Jaringan
Router	
System of Interest	Router
Komponen Utama	• Listrik • Kabel • Keamanan Jaringan

Setelah dilakukan identifikasi komponen utama, maka akan dilakukan identifikasi ancaman untuk masing-masing komponen utama. Hal ini dilakukan untuk dapat melihat kerentanan teknologi yang ada. Ancaman yang menyerang komponen utama

tentunya juga akan mengancam aset kritis, oleh karena itu hal ini dapat membantuk dalam melihat keseluruhan ancaman yang dapat mengganggu aset kritis.

Untuk informasi selengkapnya terkait daftar kerentanan teknologi dapat dilihat pada dokumen produk. Berikut merupakan daftar kerentanan teknologi dari masing-masing komponen utama aset kritis TI organisasi.

Tabel 6.12 Contoh Daftar Kerentanan Teknologi dari Komponen Utama

Server	
System of Interest	Server yang menyimpan Data Penting
Komponen Utama	**Kemungkinan Ancaman**
• **Sistem Operasi** • **Processor** • **RAM** • **Harddisk** • **Listrik** • **Keamanan Jaringan** • **Genset** • **UPS** • **Kabel** • **Smoke Detector** • **Ruang Server**	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Genset tidak dapat berfungsi karena mengalami kerusakan • RAM mengalami kelebihan memori • Kinerja Procesor menurun akibat terlalu banyak kapasitas data • Tempat penyimpanan (*Harddisk)* penuh • Keamanan jaringan dapat ditembus • UPS tidak berfungsi • Ruang Server kurang diberi pengamanan

Fase 3 – Mengembangkan Perencanaan dan Strategi Keamanan

Fase ini dilakukan dengan tujuan untuk melakukan evaluasi risiko dari aset kritis berdasarkan output yang telah didapatkan dari fase 1 dan fase 2. Namun fase ini dibatasi tidak hingga mengembangkan strategi keamanan, oleh karena strategi keamanan nantinya akan dijabarkan pada bagian strategi BCP untuk risiko yang dinilai tinggi. Berikut merupakan hasil daftar risiko yang didapatkan dari analisis OCTAVE.

Tabel 6.13 Daftar Risiko

No	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
41	Hardware	Server	Kerusakan pada Server	Gempa bumi	1
				Badai dan Petir	2
				Banjir	3
				Kebakaran	4
				Kebocoran dan Kerusakan pada Bangunan	5
			Server berhenti	Kerusakan pada Genset dan UPS	6
				Listrik Mati	7
			Kinerja server menurun	RAM mengalami kelebihan memori	8
				Kinerja Procesor menurun akibat	9

No	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
				terlalu banyak kapasitas data	
				Tempat penyimpanan (*Harddisk)* penuh	10
			Pencurian data	Ruang Server kurang diberi pengamanan	11
				Kesalahan Konfigurasi Server	12
			Data Hilang	Kesalahan DBA	13
				Virus	14
		PC	Kerusakan pada PC	Gempa Bumi	15
				Badai dan Petir	16
				Banjir	17
				Kebakaran	18
				Kebocoran dan Kerusakan pada Bangunan	19
				Keyboard, mouse atau monitor mengalami kerusakan	20

No	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
				karena pemakaian berlebih	
			PC tidak dapat menyala	Kerusakan pada Genset dan UPS	21
				Listrik Mati	22
			PC terkena virus	Antivirus tidak update	23
2	Software	SIMAS, E-Learning, Perpustakaan	Aplikasi tidak dapat diakses	Listrik Mati	24
				Server Down	25
			Aplikasi diakses oleh pihak yang tidak berwenang	Kesalahan dalam pemberian hak akses	26
43	Data	Data demografi mahasiswa, Data Akademik dan Data File Server	Data tidak dapat diakses	Listrik Mati	27
				Server Down	28
			Pencurian data	Terdapat hacker yang mencuri data	29
			Manipulasi data	Username dan password ketahui oleh pengguna lain	30
				Terdapat hacker yang	31

No	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
				memanipulasi data	
			Backup data gagal	Kapasitas media penyimpanan overload	32
			Data hilang	Server Rusak	33
4	Jaringan	Kabel	Kurangnya kontrol pengamanan kabel	Kabel rusak	34
		Wifi dan Router	Internet Mati	Listrik Mati	35
				Wifi rusak	36
				Genset mati	37
				Kabel Rusak	38
			Akses internet lambat	Kesalahan Konfigurasi	39

No	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
				Ada yang melakukan netcut	40
5	Sumber Daya Manusia	Pegawai Non - TI	Penyalahgunaan data organisasi	Penurunan Kompetensi Karyawan Pegawai Non-TI	41
				Adanya praktik KKN di perusahaan	42
			Data yang ada tidak valid	Kesalahan dalam input data	43
			Pelanggaran regulasi hak akses	Penyalahgunaan akses regulasi	44
		Pegawai TI	Penyalahgunaan data organisasi	Penurunan Kompetensi Pegawai TI	45

No	Kategori Aset	Aset	Potensi Mode Kegagalan	Penyebab Potensi Kegagalan	ID Risiko
				Adanya praktik KKN di perusahaan	46
			Data yang ada tidak valid	Kesalahan dalam input data	47
			Pelanggaran regulasi	penyelahgunaan akses regulasi	48
		Dosen	Penyalahgunaan data organisasi	Penurunan Kompetensi Dosen	49
				Adanya praktik KKN di perusahaan	50
			Data yang ada tidak valid	Kesalahan dalam input data nilai	51
		Mahasiswa	Sharing Password Mahasiswa/i	Manipulasi Data	52

Penilaian Risiko dengan FMEA

Setelah melakukan identifikasi risiko, maka selanjutnya akan dilakukan penilaian risiko dengan memberikan skor dampak, kemungkinan dan deteksi. Untuk skala pemberian skor dapat melihat Bab 4 di bagian Pengolahan Data dan Informasi.

Untuk setiap risiko yang muncul akan dilakukan perhitungan nilai nilai RPN (*rish priority number)*, RPN nantinya merupakan skala untuk dapat menilai tingkat prioritas risiko. Skala RPN dapat dilihat pada Bab 4 di bagian Pengolahan Data dan

Informasi dan penilaian risiko dapat dilihat pada Lampiran G. Berikut merupakan tabel hasil penilaian risiko.

Tabel 6.14 Daftar Nilai RPN Risiko

Level Risiko	Potensi Mode Kegagalan	ID Risiko	Potensi Penyebab Kegagalan	RPN	Jumlah
Very High	Manipulasi Data	52	Sharing password oleh Mahasiswa/i	210	3
		30	Username dan password diketahui oleh pengguna lain	200	
	Kerusakan pada Server	5	Kebocoran dan kerusakan pada bangunan	200	
High	Manipulasi Data	31	Terdapat hacker yang memanipulasi data	160	4
	Data Hilang	34	Virus/bug	160	
	Pencurian Data	29	Terdapat hacker yang mencuri data	140	
	Kerusakan pada server	1	Gempa bumi	120	
Medium	Data Hilang	14	Virus	112	12
		33	Server rusak	96	
		13	Kesalahan DBA	84	
	Pencurian Data	11	Ruang server kurang diberi pengamanan	100	
		12	Kesalahan konfigurasi server	100	
		2	Badai dan Petir	80	

Level Risiko	Potensi Mode Kegagalan	ID Risiko	Potensi Penyebab Kegagalan	RPN	Jumlah
	Kerusakan pada Server	3	Banjir	80	
	Kerusakan pada PC	19	Kebocoran dan Kerusakan pada Bangunan	80	
	Aplikasi diakses oleh pihak yang tidak berwenang	26	Kesalahan dalam pemberian hak akses	108	
	Akses internet lambat	39	Kesalahan Konfigurasi	100	
	Internet mati	37	Genset mati	80	
	Data tidak valid	47	Kesalahan dalam input data oleh pegawai tI	108	
Low	Kerusakan pada Server	4	Kebakaran	48	33
	Server Berhenti	6	Kerusakan pada Genset dan UPS	56	
		7	Listrik Mati	70	
		8	RAM mengalami kelebihan memori	48	

Level Risiko	Potensi Mode Kegagalan	ID Risiko	Potensi Penyebab Kegagalan	RPN	Jumlah
	Kinerja Server Menurun	9	Kinerja Procesor menurun akibat terlalu banyak kapasitas data	36	
		10	Tempat penyimpanan (*Harddisk)* penuh	48	
	Kerusakan pada PC	15	Gempa Bumi	60	
		16	Badai dan Petir	40	
		17	Banjir	40	
		18	Kebakaran	24	
		20	Keyboard, mouse atau monitor mengalami kerusakan karena pemakaian berlebih	24	
	PC tidak dapat menyala	21	Kerusakan pada Genset dan UPS	48	
		22	Listrik Mati	42	
	PC terkena virus	23	antivirus tidak update	60	
	Aplikasi tidak dapat diakses	24	Listrik Mati	70	
		25	Server Down	75	
	Data tidak dapat diakses	27	Listrik Mati	70	
		28	Server Down	75	

Level Risiko	Potensi Mode Kegagalan	ID Risiko	Potensi Penyebab Kegagalan	RPN	Jumlah
	Backup data gagal	32	Kapasitas media penyimpanan *overload*	48	
	Kurangnya kontrol pengamanan kabel	34	Kabel rusak	50	
	Internet mati	35	Listrik Mati	70	
		36	Wifi rusak	30	
		38	Kabel rusak	50	
	Akses internet lambat	40	Ada yang melakukan netcut	70	
	Penyalahgunaan data organisasi	41	Penurunan Kompetensi Karyawan Pegawai Non-TI	60	
		42	Adanya praktik KKN di perusahaan	30	
	Pelanggaran regulasi hak akses	44	Penyalahgunaan akses regulasi	27	
	Penyalahgunaan data organisasi	45	Penurunan Kompetensi Pegawai TI	60	
		46	Adanya praktik KKN di perusahaan	45	

Level Risiko	Potensi Mode Kegagalan	ID Risiko	Potensi Penyebab Kegagalan	RPN	Jumlah
	Pelanggaran regulasi	48	Penyalahgunaan akses regulasi	36	
	Penyalahgunaan data organisasi	49	Penurunan Kompetensi Dosen	60	
		50	Adanya praktik KKN di perusahaan	30	
	Data yang ada tidak valid	43	kesalahan dalam Input data oleh pegawai Non-TI	75	
		51	Kesalahan dalam Input data oleh dosen	75	

6.1.2.2 Analisis Dampak Bisnis

Analisis dampak bisnis bertujuan untuk menentukan dan melakukan prioritisasi proses operasional bisnis yang paling dianggap kritis pada suatu organisasi. Dalam melakukan analisis dampak bisnis, peneliti mengacu pada ISO 22317:2015 – *business impact analysis*. Selain itu, analisis dampak bisnis juga dapat membantu perusahaan untuk melihat dampak yang ditimbulan terhadap suatu gangguan. Analisis dampak bisnis dapat membantu organisasi untuk dapat mengetahui batas waktu toleransi gangguan terjadi pada suatu proses bisnis.

Tahapan pada analisis dampak bisnis adalah Masing masing tahapan ini didapatkan dari hasil wawancara yang dilampirkan pada Lampiran F dan telah dilakukan verifikasi hasil analisis bisnis yang dilampirkan pada Lampiran C.

Prioritisasi Layanan TI

Organisasi perlu melakukan identifikasi layanan SI/TI beserta dengan melakukan prioritisasi tingkat kritis masing masing layanan. Berikut merupakan prioritisasi tingkat kritis untuk masing masing layanan TI yang dimiliki oleh organisasi.

Tabel 6.15 Prioritisasi Layanan TI

Layanan TI	Tingkat Kritis	Keterangan
SIMAS (bajol.perbanas.ac.id)	Kritis	SIMAS merupakan layanan TI utama organisasi. Semua sistem dari kepegawaian, keuangan, kemahasiswaan dan akademik terdapat disana. Apabila sistem ini terkena gangguan maka akan berdampak sangat besar terhadap operasional organisasi.
Sistem Pendaftaran Mahasiswa Baru (spmb.perbanas.ac.id)	Kritis	Sistem SPMB merupakan sistem pendaftaran mahasiswa baru. Apabila sistem terganggu maka mahasiswa baru yang akan mendaftar akan kesulitan untuk mengakses sistem.
Layanan E-learning (kuliah .perbanas.ac.id)	Penting	Layanan E-learning merupakan layanan untuk mendukung sistem pembelajaran. Apabila layanan terganggu maka

Layanan TI	Tingkat Kritis	Keterangan
		pembelajarn melalui e-learning tidak dapat dilakukan
Wifi, File Server, Email, Lab	Penting	Fasilitas layanan TI yang diberikan organisasi kepada mahasisnya adalah Wifi, File Server, E-mail dan Lab. Apabila terjadi gangguan pada layanan ini maka akan ada komplain dari civitas akademik.

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 6.16 Daftar Fungsional Bisnis yang Terlibat

Fungsional Bisnis	Keterangan
Bagian Akademik	Bagian akademik merupakan bagian yang melakukan pengelolaan seluruh program dan aktivitas akademik yang dilakukan oleh organisasi. Aktivitas akademik merupakan aktivitas seputar akademik dari mahasiswa masuk hingga mahasiswa lulus dari STIE Perbanas

	yang mana hal ini meliputi KRS, kegiatan perkuliahan, UTS/UAS hingga wisuda.
Bagian Kemahasiswaan	Bagian kemahasiswaan merupakan bagian yang bertugas untuk melakukan kegiataan terkait kemahasiswaan seperti melakukan penerimaan mahasiswa baru dan juga memantau kegiatan- kegiatan yang meningkatkan *softskill* dari mahasiswa.
Bagian TIK	Bagian Teknologi Informaasi dan Komunikasi merupakan bagian yang berfungsi dalam menyediakan serta memelihara layanan Teknologi Informasi untuk mendukung keseluruhan proses bisnis yang ada di STIE Perbanas. Bagian TIK juga bertanggung jawab dalam pengembangan layanan teknologi dan sistem informasi dan memastikan bahwa layanan TIK yang dimiliki oleh organisasi berjalan dengan lancar.
Bagian Keuangan	Bagian Keuangan merupakan bagian yang mengelola akuntansi dan administrasi dari keuangan organisasi. Proses pengelolaan ini meliputi proses pembayaran biaya sekolah, proses penggajian dan juga proses pengelolaan anggaran biaya.

Identifikasi Proses Bisnis dan Aktivitas 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 6.17 Contoh Daftar Proses Bisnis dan Aktivitas yang Terlibat

Fungsional Bisnis	Proses Bisnis Terkait Layanan TI	Aktivitas Terkait Layanan TI	Sistem Dan Layanan TI
Akademik	Proses KRS	• Set-up awal dari akademik • Pemilihan KRS untuk Mahasiswa • Verifikasi dari dosem pembimbing	SIMAS (bajol.perbanas.ac.id)
	Pengelolaan Nilai Mahasiswa	• Setp up awal nilai • Memasukkan nilai oleh dosen • Filterisasi nilai dari akademik • Pengisian kuesioner untuk mahasiswa • Mahasiswa dapat melihat nilai	SIMAS (bajol.perbanas.ac.id)

Fungsional Bisnis	Proses Bisnis Terkait Layanan TI	Aktivitas Terkait Layanan TI	Sistem Dan Layanan TI
	Proses kelulusan wisuda	• Rapat evaluasi • Pegelolaan yudisium	SIMAS (bajol.perbanas.ac.id)
	Proses Pengajaran melalui E-Learning	• Share materi dan modul • Group discussion • Kuliah via E-learning • Quiz	Layanan E-learning (kuliah.perbanas.ac.id)

Melakukan Prioritisasi Proses Bisnis

Prioritisasi proses bisnis dilakukan 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 6.18 Contoh Prioritisasi Proses Bisnis

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Tingkat Kritis	Keterangan
Akademik	Proses KRS	Kritis	Proses KRS akan terhambat dan harus dilakukan secara manual apabila terjadi gangguan pada sistem

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Tingkat Kritis	Keterangan
	Pengelolaan Nilai Mahasiswa	Kritis	Mahahasiswa tidak akan dapat melihat nilai & dosen tidak akan dapat menginputkan nilai apabila terjadi gangguan pada sistem
	Proses Kelulusan Mahasiswa	Penting	Rapat evaluasi wisuda dan pengelolaan yudisium akan ikut terganggu apabila terjadi gangguan pada sistem
	Proses Pengajaran melalui E-Learning	Penting	Mahasiswa tidak dapat melakukan pembelajaran di e-learning seperti mengambil modul, kuis maupun tugas apabila terjadi gangguan pada sistem

Analisis Waktu Pemulihan

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

- ***Maximum Tolerable Downtime*** **(MTD)** merupakan jumlah waktu maksimal yang dapat ditoleransi oleh perusahaan terhadap kegagalan proses bisnis
- ***Recovery Time Objective*** **(RTO)** adalah jumlah waktu lumpuh maksimal untuk seluruh sumber daya sistem yang ada, sebelum terjadi dampak lain kepada sumber daya lainnya.

- ***Recovery Point Objective*** **(RPO)** adalah jumlah waktu yang diperlukan setelah terjadinya gangguan, untuk memulihkan data setelah terjadinya gangguan.

Berikut merupakan contoh hasil analisis waktu pemulihan untuk proses bisnis tertentu

Tabel 6.19 Contoh Hasil Analisis Waktu Pemulihan

Fungsional Bisnis	Proses Bisnis Terkait Sistem	MTD	RTO	RPO
Akademik	Proses KRS	≤12jam	≤6jam	≤12jam
	Pengelolaan Nilai Mahasiswa	≤12jam	≤6jam	≤12jam
	Proses Kelulusan Mahasiswa	≤24jam	≤12jam	≤24jam
	Proses Pengajaran melalui E-Learning	≤24jam	≤12jam	≤24jam

Analisis Dampak Gangguan

Analisis dampak gangguan merupakan proses penilaian dampak dari masing masing proses bisnis apabila terjadi risiko yang tidak diinginkan. Dampak ini dibagi menjadi tiga, dampak ditinjau dari aspek finansial, dampak ditinjau dari reputasi dan juga dampak ditinjau dari target teknis. Berikut merupakan contoh hasil analisis dampak gangguan terhadap proses bisnis. Untuk informasi selengkapnya dapat melihat lampiran H atau lihat dokumen produk.

Tabel 6.20 Contoh Hasil Analisis Dampak Gangguan

Risiko :	Kerusakan pada Server

Penyebab risiko :		• Gempa Bumi • Banjir • Kebakaran • Kebocoran dan Kerusakan pada Gedung		
Fungsional bisnis	**Proses bisnis terkait Sistem**	**Dampak**		
		Finansial	**Reputasi**	**Target Teknis**
Akademik	Proses KRS	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Menggan ggu <15% target teknis dari proses bisnis
	Pengelolaan Data Perpustakaan	Tidak ada dampak secara finansial kepada perusahaan	Berdampak kecil pada reputasi perusahaan	Menggan ggu <10% target teknis dari proses bisnis
	Pengelolaan Nilai Mahasiswa	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Menggan ggu <15% target teknis dari proses bisnis
	Proses wisuda	Tidak ada dampak secara finansial	Tidak berdampak langsung pada	Menggan ggu <3% target teknis

		kepada perusahaan	reputasi perusahaan	dari proses bisnis
	Proses Pengajaran melalui E-Learning	Tidak ada dampak secara finansial kepada perusahaan	Berdampak sedang pada reputasi perusahaan	Menggan ggu <10% target teknis dari proses bisnis

6.1.2.3 Strategi BCP

Strategi BCP akan ditentukan berdasarkan hasil analisis yang telah dilakukan pada tahapan analisis risiko dan juga analisis dampak bisnis. Strategi BCP dibuat untuk dapat menjaga keberlangsungan dari proses bisnis yang diprioritaskan oleh organisasi dan juga melakukan pengelolaan mitigasi dari risiko. Strategi yang dibuat nantinya merupakan strategi preventif, strategi DRP, strategi saat terjadi gangguan dan strategi pemulihan. Dalam menentukan strategi ini akan dilihat berdasarkan risiko dan penyebab risiko.

Risiko yang diambil untuk strategi BCP adalah risiko yang memiliki nilai RPN *Very High* pada tabel 6.14, yaitu risiko kerusakan server dan juga risiko 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 kerusakan server.

Tabel 6.21 Contoh Strategi Preventif

	Risiko : Kerusakan Server
	Penyebab : Kebakaran
Strategi Preventif	Keterangan
Pengaturan hak akses untuk ruang server	Strategi pengaturan hak akses untuk ruang server perlu dilakukan agar nantinya otoritas dan kewenangan terhadap akses ruang server dapat terjaga.
Instalasi dan *monitoring* ketersediaan perangkat untuk pencegahan kebakaran	Untuk dapat melakukan pencegahan kebakaran dengan cepat, maka perlu dilakukan instalasi dan *monitoring* terhadap ketersediaan perangkat untuk mencegah kebakaran seperti alat pemadam kebakaran, alat komunikasi darurat dan juga *smoke detector*. Diharapkan nantinya perangkat dapat tersedia dan berfungsi dengan baik saat terjadinya bencana.
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	Bagian TIK diharapkan dapat memiliki pengetahuan untuk dapat melakukan restore data dengan benar saat adanya kehilangan data. Sehingga nantinya diharapkan hal ini

	dapat mempercepat pemulihan sistem operasional saat terjadi bencana.
Pelatihan untuk kebakaran	Strategi pelatihan untuk kebakaran meupakan strategi yang dilakukan kepada semua pegawai agar masing – masing pegawai mendapatkan pengetahuan mendasar terhadap tindakan yang harus dilakukan saat bencana. Hal ini termasuk cara penggunaan *fire extinguisher*, kontak darurat yang harus dihubungi dan jalur evakuasi.

Berikut merupakan contoh strategi DRP untuk risiko kerusakan server.

Tabel 6.22 Contoh Strategi DRP

	Risiko : Kerusakan Server
	Penyebab : Kebakaran
Strategi DRP	
Berikut merupakan langkah – langkah yang perlu dilakukan saat terjadinya kebakaran : • Identifikasi situasi dan melakukan pelaporan gangguan terhadap Tim BCP • Untuk kebakaran dengan kondisi minor,tim DRP akan melakukan pemadaman dengan menggunaan fire extinguisher oleh pegawai yang terlatih dan tim keamanan.	

• Untuk kebakaran dengan kondisi major,Tim DRP akan menghubungi pemadam kebakaran setempat dan melakukan evakuasi area • Apabila api telah padam, Tim DRP akan melakukan peninjauan terhadap area

Berikut merupakan contoh strategi saat terjadi gangguan untuk risiko kerusakan server.

Tabel 6.23 Contoh Strategi Saat Terjadi Gangguan

	Risiko : Kerusakan Server
Strategi Saat Terjadi Gangguan	Keterangan
Identifikasi penyebab bencana	Organisasi perlu tau penyebab dari kebakaran untuk nantinya bisa ditinjau lebih jauh. Apabila bencana terjadi diluar kesalahan manusia, maka organisasi dapat melakukan langkah perbaikan terhadap kondisi lingkungan. Apabila bencana terjadi karena kesalahan manusia, maka akan dilakukan antisipasi lebih lanjut kepada pihak yang bertanggung jawab.
Pengamanan aset SI/TI	Pada saat terjadi kebakaran maka tim BCP harus terlebih dahulu

	melakukan pengamanan terhadap aset TI kritis, terutama server utama. Diharapkan dengan melakukan pengamanan saat terjadi gangguan, kemungkinan dampak bencana terhadap proses bisnis TI dapat berkurang.
Pemindahan proses dari sistem ke manual	Apabila server tidak dapat berjalan, maka tim BCP akan menginstruksikan untuk melakukan pemindahan proses – proses penting yang awalnya dilakukan dengan penggunaan sistem menjadi manual untuk sementara.
Restore Data	Saat server mengalami kerusakan dan diidentifikasi terdapat kehilangan data pada server, maka dapat dilakukan strategi *restore data.* Data dapat di*restore* kembali dengan menggunakan hasil *back-up* terbaru yang dilakukan. Restore data dilakukan dengan memprioritaskan data kritis terlebih dahulu.
Penyuluhan terhadap tiap bagian yang terkena dampak dari gangguan	Strategi penyuluhan terhadap bagian yang terkena dampak dari gangguan akan mempermudah alur komunikasi organisasi. Strategi ini juga dijalankan agar nantinya tidak terjadi kesalahpahaman dan mempercepat proses penanggulangan bencana

Menonaktifkan Sistem	Strategi menutup atau menonaktifkan sistem sementara akan mempermudah tim BCP dalam melakukan penanggulangan dari dampak bencana

Berikut merupakan contoh korektif untuk risiko kerusakan server.

Tabel 6.24 Contoh Strategi Korektif

	Risiko : Kerusakan Server
Strategi Korektif	Keterangan
Evaluasi dari dokumentasi hasil insiden	Strategi evaluasi ini akan dilakukan dengan melihat hasil dokumentasi dari insiden yang terjadi dan penanganan yang dilakukan. Sehingga nantinya ditentukan aksi tindakan korektif dan perbaikan yang sesuai.
Perbaikan terhadap sistem keamanan dan lingkungan ruang server	Apabila penyebab dari kebakaran dikarenakan kurangnya keamanan pada ruang server maka diperlukan adanya strategi perbaikan keamanan pada ruang server untuk memastikan

	bahwa bencana tidak akan terulang kembali

Untuk informasi selengkapnya dapat dilihat pada Buku Produk BCP STIE Perbanas.

6.1.2.3 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 I.

Tabel 6.25 Contoh Modul Pelatihan *Backup* dan *Restore*

	GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS
Nama Pelatihan	Pelatihan *Back up* dan *Restore Data*
Jenis Pelatihan	Pemberian materi in-door dan praktik
Deskripsi Pelatihan	
Pelatihan ini bertujuan untuk memberi pengetahuan umum dan teknis mengenai *back up* dan *restore* data, hal ini termasuk tipe *back up* dan *restore*, penjadwalan *back* up dan tata cara dalam melakukan *back up* dan *restore* . Diharapkan dengan adanya pelatihan ini maka akan memberi wawasan kepada obyek penelitian mengenai tata cara melakukan *back up* dan *restore* dengan benar.	

Sasaran Pelatihan	Seluruh Staf Bagian TIK
Materi Umum	
Dalam pelatihan ini akan memberikan materi kepada karyawan yaitu sebagai berikut : • Pengetahuan umum dan jenis dari *back up* dan *restore* • Prioritisasi data dalam melakukan *back up* • Prosedur dalam melakukan *back up* dan *restore* • Penjadwalan dari proses *back up* dan *restore*	

Tahapan pengujian dilakukan untuk dapat melihat keefektifan perencanaan keberlangsungan bisnis dalam penerapannya di organisasi. Pengujian yang dilakukan nantinya adalah pengujian parsial yang hanya difokuskan pada risiko tertinggi saja. Berikut merupakan contoh skenario pengujian terhadap perencanaan keberlangsungan bisnis. Pada tahap pengujian nantinya peneliti akan mendokumentasikan hasil pengujian BCP

Skenario pengujian BCP yang dilakukan nantinya adalah dengan melakukan proses *backup* dan *restore* serta melakukan proses pengelolaan server. Pengujian ini dilakukan menggunakan metode *walthrough* yang mana pegawai TIK nantinya akan menjalankan prosedur – prosedur terkait BCP untuk melakukan hal tersebut.

Tabel 6.26 Contoh Hasil Skenario Pengujian BCP untuk Proses Backup dan Restore data

Hasil Pengujian BCP untuk Proses *Backup* dan *Restore* Data	
Waktu Pengujian	4 Januari 2016
Tempat Pengujian	Ruang ICT Kampus I PERBANAS

Hasil Pengujian BCP untuk Proses *Backup* dan *Restore* Data		
Pelaku dan pembagian peran	1. Staf TIK 1 sebagai yang melakukan backup dan restore data 2. Kepala Bagian TIK sebagai pengawas berjalannya pengujian 3. Peneliti sebagai Dokumentator	
Proses	1. Staf TIK 1 sebagai mencoba melakukan *backup data* untuk data mahasiswa keseluruhan dengan prosedur *backup data*	Status Proses Berhasil
	2. Kepala Bagian TIK melihat kesesuaian data hasil *backup*	Status Proses Berhasil
	3. Staf TIK 1 sebagai mencoba melakukan restore data dari hasil backup tadi pada dengan prosedur *restore data*	Status Proses Berhasil
	4. Kepala Bagian TIK melihat kesesuaian data hasil restore dengan data awal	Status Proses Berhasil
	5. Peneliti mendokumentasikan hasil pengujian BCP.	Status Proses Berhasil

Untuk informasi lebih lengkapnya mengenai modul pelatihan dan skenario pengujian BCP dapat melihat Lampiran J atau pada buku produk STIE Perbanas.

6.1.3 Check (Pemeriksaan)

Fase *check (*pemeriksaan) bertujuan untuk melakukan peninjauan kembali terhadap keseluruhan proses yang terdapat pada BCP dengan kebutuhan dan tujuan utama organisasi. Pada fase ini akan dilakukan audit internal BCP dan peninjauan manajemen sebagai bentuk kontrol organisasi terhadap BCP. Selain itu fase ini juga bertujuan untuk melihat adanya ketidaksesuaian atau berkurangnya relevansi BCP terhadap kondisi kekinian organisasi.

6.1.3.1 Audit Internal

Proses audit internal BCP merupakan suatu proses yang bertujuan untuk melakukan pemeriksaan terhadap tingkat keefektifan dari implementasi BCP yang telah dibuat. Dalam tahapan ini auditor akan melakukan penilaian terhadap tingkat kesesuaian BCP yang telah berjalan dan mengukur sejauh apa efektifitas BCP dalam menangani gangguan.. Audit internal BCP dilakukan oleh auditor BCP yang telah ditunjuk dengan pengawasan dari komite BCP.

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

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

a) Memastikan kesesuaian dokumen BCP dengan kebutuhan organisasi
b) Memastikan kesesuaian dokumen BCP dengan kerangka standar yang digunakan
c) Memastikan keefektifan dari implementasi BCP
d) Kesesuaian peran dan tanggung jawab dalam struktur Komite BCP
e) Menjalankan proses audit sesuai dengan perencanaan dengan menjaga obyektifitas
f) Mendokumentasikan proses implementasi audit dan hasil audit

6.1.3.2 Peninjauan Manajemen

Tahapan peninjauan manajemen (*management review)* dilakukan untuk memastikan bahwa BCP telah sesuai dengan kondisi, tujuan dan kebutuhan organisasi. Berikut adalah cakupan hal yang perlu ditinjau oleh pihak manajemen:

1. Status dari tindakan yang ditinjau pada proses peninjauan sebelumnya.
2. Adanya perubahan dari internal dan eksternal yang berkaitan dengan BCP.

3. Informasi terkait dengan kinerja BCP seperti adanya ketidak sesuaian yang terjadi dan langkah korektif yang telah dilakukan serta hasil audit.
4. Kebutuhan untuk melakukan perubahan terhadap BCP untuk kebijakan maupun prosedur.
5. Kebutuhan untuk membuat prosedur baru yang dapat meningkatkan kinerja dan keefektifan BCP.
6. Status dari aksi perbaikan yang telah dilakukan.
7. Rekomendasi untuk peningkatan BCP.
8. Hasil pembelajaran dan tindakan yang dilakukan dari insiden yang pernah terjadi sebelumnya.
9. Hasil dari pengujian BCP.

Sebagai media bantu untuk proses peninjauan manajemen, terdapat formulir rapat peninjauan manajemen yang tertera pada dokumen produk dan pada Lampiran K.

6.1.4 Act (Tindakan)

Fase *Act* (Tindakan) merupakan fase dimana organisasi melakukan peningkatan terhadap kinerja BCP dengan cara melakukan tindakan korektif berdasarkan hasil tinjauan manajemen. Selain itu pada fase ini organisasi juga dapat menilai kembali ruang lingkup dari BCP dan juga kebijakan serta prosedur yang berlaku. Hal ini dilakukan dengan harapan dokumen BCP dapat bersifat dinamis dan relevan dengan tujuan dan kebutuhan organisasi.

6.1.4.1 Peningkatan Terus Menerus (*Continuous Improvement)*

Untuk dapat menjaga tingkat relevansi BCP dengan perubahan kondisi internal maupun eksternal organisasi, BCP harus selalu terus menerus diperbaiki dan ditingkatkan. Untuk itulah organisasi perlu melakukan tahapan peningkatan terus menerus (*continous improvement)*. Dalam tahapan peningkatan terus menerus ini organisasi harus melihat dari dua sisi, yaitu dari sisi internal dan eksternal. Sisi internal merupakan proses yang dilakukan dalam cakupan kerangka BCP yang telah dilakukan

pada fase sebelumnya (*check)*, hal – hal tersebut antara lain adalah sebagai berikut :

1. Hasil audit internal
2. Hasil peninjauan manajaemen

Selain dari sisi internal, organisasi juga perlu untuk memperhatikan sisi eksternal, yaitu bagian yang ada diluar cakupan dari kerangka BCP. Bagian tersebut antara lain adalah sebagai berikut :

1. Regulasi pemerintah di bidang pendidikan tinggi yang sudah diimplementasikan, seperti berikut :
   - Undang-Undang Republik Indonesia No.20 tahun 2003 tentang Sistem Pendidikan Nasional
   - Undang-Undang Republik Indonesia No. 12 tahun 2012 tentang Pendidikan Tinggi
   - Peraturan Pemerintah Republik Indonesia No. 17 tahun 2010 tentang Pengelolaan dan Penyelenggaraan Pendidikan
   - Statuta STIE Perbanas
2. Regulasi pemerintah di bidang pendidikan tinggi yang nantinya akan diimplementasikan
3. Regulasi dari Yayasan Pendidikan Perbanas Jawa Timur
4. Hasil rapat manajemen periodik STIE Perbanas

Untuk dapat menjaga tingkat relevansi BCP diharapkan organisasi melakukan proses peningkatan terus menerus secara periodik.

Halaman ini sengaja dikosongkan

BAB VII
KESIMPULAN DAN SARAN

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

7.1 Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut.

Kesimpulan Pertama

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 52 risiko yang didapatkan dari hasil analisis OCTAVE.
    - Terdapat 3 risiko dengan level *very high* yaitu manipulasi data karena sharing password oleh mahasiswa/i, manipulasi data karena username dan password diketahui pengguna lain dan kerusakan server karena kebocoran dan kerusakan pada bangunan
    - Terdapat 4 risiko dengan level *high* yaitu manipulasi data karena hacker, data hilang karena virus/bug, pencurian data karena hacker dan kerusakan server karena gempa bumi
    - Selain itu terdapat pula 12 risiko dengan level *medium* dan juga 33 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 kritis pada STIE Perbanas yaitu SIMAS dan Sistem Pendaftaran Mahasiswa Baru (SPMB) dan juga terdapat 5 layanan TI yang bersifat penting yaitu E-learning, Wifi, File Server, Email dan Labarotorium.
- Terdapat 10 proses bisnis dengan tingkat kritis yaitu proses KRS, pengelolaan nilai mahasiswa, proses kelulusan mahasiswa, pendaftaran mahasiswa baru, pemantauan tenologi, pengolahan data elektronik, penyediaan layanan SI/TI, *disaster recovery planning,* pengelolaan pembayaran biaya kuliah dan penggajian honor mengajar
- Terdapat 4 proses bisnis dengan tingkat penting yaitu pengelolaan *softskill*, pengajaran melalui e-learning, pengelolaan konfigurasi perangkat dan pengajuan anggaran
- Terdapat identifikasi nilai MTD (*Maximum Tolerable Downtime)*, RPO (*Recovery Point Objective)* 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.

Kesimpulan Kedua

Masing - masing organisasi membutuhkan *Business Continuity Plan* (BCP) yang berbeda dari satu dengan yang lain. Hal ini lah yang membuat BCP menjadi sesuatu hal yang unik.

Hal ini dikarenakan semua organisasi pasti memiliki kondisi serta kebutuhan yang berbeda beda. Oleh karena itulah rancangan BCP pada penelitian ini merupakan hasil formulasi dari

kebutuhan organisasi dengan hasil analisis dari acuan standar yang ada.

7.2 Saran

Saran pada penelitian ini merupakan perbaikan untuk keberlanjutan penelitian, maupun penelitian selanjutnya. Berikut merupakan saran dari penelitian ini.

Saran untuk keberlanjutan penelitian ini

Untuk keberlanjutan penelitian ini, diharapkan nantinya rancangan BCP dari penelitian ini dapat terus berkembang. Rancangan BCP ini sendiri telah disesuaikan oleh kebutuhan perusahaan, kebutuhan ini dapat berubah dengan adanya perkembangan kondisi organisasi maupun perkembangan dari teknologi informasi sendiri. Untuk itulah diperlukan adanya peningkatan terus – menerus agar rancangan BCP nantinya akan menjadi lebih baik lagi kualitasnya.

Saran untuk penelitian selanjutnya

Diharapkan nantinya rancangan BCP ini dapat di implementasikan pada organisasi pendidikan lainnya sesuai dengan langkah – langkah yang telah dijabarkan. Sehingga nantinya dapat dilihat kesesuaian dari hasil rancangan yang telah dibuat.

LAMPIRAN

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

KODE LAMPIRAN	LAMPIRAN
A	Lampiran Dokumen Konfirmasi Kesesuaian Kerangka Kerja BCP STIE Perbanas
B	Lampiran Dokumen Konfirmasi Kesesuaian Hasil Analisis Risiko STIE Perbanas
C	Lampiran Dokumen Konfirmasi Kesesuaian Hasil Analisis Dampak Bisnis STIE Perbanas
D	Lampiran Dokumen Konfirmasi Kesesuaian Hasil Dokumen BCP STIE Perbanas
E	Lampiran Interview Protokol Analisis Risiko
F	Lampiran Interview Protokol Anaalisis Dampak Bisnis
G	Lampiran Analisis Risiko
H	Lampiran Analisis Dampak Bisnis
I	Lampiran Gambaran Umum Modul Pelatihan & Skenario Pengujian BCP
J	Lampiran Formulir Audit Internal BCP
K	Lampiran Formulir Peninjauan Manajemen
L	Dokumentasi

LAMPIRAN A

Lampiran Dokumen Konfirmasi Kesesuaian Kerangka Kerja BCP STIE Perbanas

SURAT KONFIRMASI
Kesesuaian Kerangka Kerja *Business Continuity Plan* (BCP)
untuk STIE Perbanas

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Sabrina Leviana Putri
NRP : 5212100050
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian kerangka kerja *Business Continuity Plan* (BCP) untuk STIE Perbanas kepada Pembantu Ketua 1 Bidang Akademik STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan validasi hasil kesesuaian kerangka kerja *Business Continuity Plan* untuk STIE Perbanas, telah sesuai dengan kebutuhan dan keinginan STIE Perbanas.

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

PERSETUJUAN KONFIRMASI Surabaya, 4 November 2015	
Mengetahui, Pembantu Ketua 1 Bidang Akademik STIE Perbanas	Peneliti
Dr. Drs. Emanuel Kristjadi, MM	Sabrina Leviana Putri

LAMPIRAN B

Lampiran Dokumen Konfirmasi Kesesuaian Hasil Analisis Risiko STIE Perbanas

SURAT KONFIRMASI
Kesesuaian Hasil Analisis Risiko untuk STIE Perbanas Surabaya

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Sabrina Leviana Putri
NRP : 5212100050
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis risiko TI untuk STIE Perbanas kepada Kasie Teknologi Informasi dan Komunikasi (TIK) TIK STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis risko TI untuk STIE Perbanas yang dibuat secara khusus, sesuai dengan kebutuhan STIE Perbanas.

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

PERSETUJUAN KONFIRMASI Surabaya, 6 November 2015	
Mengetahui, Kasie Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas	Peneliti
Hariadi Yutanto, S.Kom, M.Kom	Sabrina Leviana Putri

LAMPIRAN C

Lampiran Dokumen Konfirmasi Kesesuaian Hasil Analisis Bisnis STIE Perbanas

SURAT KONFIRMASI

Kesesuaian Hasil Analisis Dampak Bisnis untuk STIE Perbanas Surabaya

Dengan hormat,

Saya yang bertanda tangan di bawah ini :

Nama : Sabrina Leviana Putri
NRP : 5212100050
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis dampak bisnis untuk STIE Perbanas kepada Kasie Teknologi Informasi dan Komunikasi (TIK) TIK STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis dampak bisnis untuk STIE Perbanas yang dibuat secara khusus, sesuai dengan kebutuhan STIE Perbanas.

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

PERSETUJUAN KONFIRMASI Surabaya, 6 November 2015	
Mengetahui, Kasie Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas	Peneliti
Hariadi Yutanto, S.Kom, M.Kom	Sabrina Leviana Putri

LAMPIRAN D

Lampiran Dokumen Konfirmasi Kesesuaian Hasil Dokumen Akhir BCP STIE Perbanas

SURAT KONFIRMASI
Kesesuaian Dokumen Akhir *Business Continuity Plan* (BCP)
untuk STIE Perbanas

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Sabrina Leviana Putri
NRP : 5212100050
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian dokumen akhir *Business Continuity Plan* (BCP) untuk STIE Perbanas kepada Pembantu Ketua 1 Bidang Akademik STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan validasi bukti dokumen akhir *Business Continuity Plan* (BCP) untuk STIE Perbanas, sesuai dengan kebutuhan dan keinginan STIE Perbanas.

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

PERSETUJUAN KONFIRMASI Surabaya, 4 Januari 2016	
Mengetahui, Pembantu Ketua 1 Bidang Akademik STIE Perbanas	Peneliti
Dr. Drs. Emanuel Kristijadi, MM	Sabrina Leviana Putri

Lampiran Dokumen Konfirmasi Kesesuaian Hasil Pengujian BCP

SURAT KONFIRMASI
Validasi Hasil Pengujian *Business Continuity Plan* Teknologi Informasi STIE Perbanas

Dengan hormat,

Saya yang bertanda tangan di bawah ini :
Nama : Sabrina Leviana Putri
NRP : 5212100050
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas hasil pengujian *Business Continuity Plan* yang telah dilakukan pada Teknologi Informasi STIE Perbanas.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan validasi bahwa hasil pengujian *Business Continuity Plan* telah benar dan *Business Continuity Plan* telah sesuai dengan kebutuhan STIE Perbanas.

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

PERSETUJUAN KONFIRMASI Surabaya, 04 Januari 2016	
Mengetahui, Staf Fungsional Bagian Teknologi Informasi dan Komunikasi (TIK) STIE Perbanas	Peneliti
Yusuf Effendi (36120268)	Sabrina Leviana Putri

LAMPIRAN E

Lampiran Interview Protokol Analisis Risiko

Informasi Narasumber	
Nama Narasumber	Dr. Drs. Emanuel Kritijadi, MM
Nama Organisasi	STIE Perbanas
Jabatan	Pembantu ketua Bidang Akademik
Waktu	Jumat, 30 Oktober 2015
Tempat	STIE Perbanas Kampus II
Media	Wawancara

Fase 1 Membangun aset berdasarkan ancaman profil	
Obyektif 1 : Menggali informasi aset kritis teknologi dan sistem informasi yang telah diterapkan organisasi	
Pertanyaan	Jawaban
Bagaimana proses umum penerapan teknologi informasi di organisasi?	Proses umum TI pada yang ada di organisasi untuk mahasiswa dimulai dari masuknya mahasiswa baru, proses KRS, proses pembelajaran yang didalamnya terdapat UTS dan UAS, Tugas Akhir lalu Kelulusan atau Wisuda.
Apa sajakah fungsional organisasi yang mendukung penggunaan teknologi dan sistem informasi?	Semua prose bisnis semua sudah tercakup oleh sistem informasi organisasi dari akademik, keuangan, kemahasiswaan, kepegaawaian dan lain sebagainya. Yang belum tercakup hanyalah proses wisuda yang harus menginputkan SKPI secara manual.
Aset teknologi apa sajakah yang dapat memberikan ancaman pada proses bisnis organisasi?	Aset teknologi kritis anatara lain adlaah server, komunikasi jaringan yang mana ada yang menggunakan kabel dan wireless, PC untuk masing-masing unit, database, genset, dan juga UPS.
Obyektif 2 : Menggali informasi kebutuhan keamanan sistem organisasi	
Pertanyaan	Jawaban
Bagaimana usaha yang telah dilakukan organisasi dalam	Dengan melakukan backup data dan memasang sistem keamanan. Untuk kebakaran DRP belum ada karena pembuatannya masih tertunda. Namun telah dipasang

menghadapi ancaman yang ada?	smoke detector untuk mengantisipasi terjadinya ancaman tersebut.
Berapa kali organisasi melakukan backup data pada area fungsional bisnis kritis?	Backup dilakukan setiap hari (jam 7 malam). Namun kelemahannya adalah backup masih dilakukan di media yang sama.
Berapa kali organisasi melakukan *maintenance* terhadap aset teknologi informasi yang mendukung fungsional bisnis kritis organisasi?	Maintenance dilaksanakan oleh unit TIK biasanya untuk maintenance penuh akan dilakukan setiap awal semester (6 bulan sekali) dan nantinya akan menghasilkan laporan untuk melakukan tindakan lebih lanjut
Apakah terdapat mekanisme proteksi keamanan aset teknologi dan informasi pada fungsional bisnis kritis organisasi?	Pengamanan hardware sudah dilakukan dan juga pengaturan keamanan untuk lingkungan sistem SI/TI juga sudah ada. Backup data rutin dilakukan. Penataan kabel juga sudah dilakukan sekarang.
Obyektif 3 : Menggali Informasi mengenai identifikasi ancaman terhadap aset teknologi dan informasi	
Pertanyaan	Jawaban
Bencana alam apa saja yang mungkin dapat terjadi dan mengancam aset teknologi dan sistem informasi di fungsional kritis perusahaaan?	Bencana alam yang mungkin mengancam adalah kebakaran,. Hujan lebat juga dapat mengancam karena dapat menyebabkan kebocoran ruangan (saat ini telah terdapat beberapa kebocoran diruangan namun bukan ruang server), selain itu petir juga dapat menjadi ancaman walaupun telah diantisipasi dengan penangkal petir. Kelembapan ruangan juga perlu diperhatikan.
Gangguan apa sajakah yang pernah terjadi pada aset	Kebakaran adalah gangguan paling besar yang pernah terjadi, selain itu ada gangguan krusial lainnya yaitu adanya nilai yang berubah tiap semesternya (Tiap semester ada <5 kasus), namun belum diketahui

teknologi dan informasi?	penyebabnya apakah ada yang membobol ataukah hanya bug pada sistem.
Apakah pernah terjadi gangguan akibat manusia misalnya pembobolan data?	Belum diketahui apakah pernah ada pencurian data karena belum pernah dilakukan pelacakan. Namun pernah ada siswa yang membobol sistem namun tidak mengambil data apapun.
Obyektif 4 : Menggali informasi mengenai praktik keamanan terkini yang telah dilakukan oleh organisasi	
Pertanyaan	Jawaban
Apakah setiap *user* sistem memiliki hak akses yang berbeda?	Setiap orang memiliki hak akses yang berbeda beda sesuai dengan role atau peran mereka dan sesuai dengan waktu atau situasinya. Pegawai, dosen maupun mahasiswa tentunya hak akses pada sistemnya akan berbeda. Selain itu ada juga yang tergantung pada situasi, contohnya dosen hanya memiliki hak akses untuk input data nilai UTS 3 minggu setelah UTS, setelah itu hak input data mereka akan dicabut.
Apakah organisasi menerapkan standar keamanan untuk melindungi aset teknologi dan sistem informasi?	Keamnaan TI organisasi belum mengacu pada standar keamanan tertentu. Namun memang sudah ada beberapa prosedur untuk melakukan proses TI dan menjaga keamanan TI.
Obyektif 5 : Mengidentifikasikan kelemahan organisasi	
Pertanyaan	Jawaban
Apakah terdapat SOP terkait keamanan teknologi dan informasi organisasi?	Sudah ada beberapa SOP terkait proses TI dan juga keamanan TI namun belum mencakup semuanya dan masih tergolong general
Apakah terdapat permasalahan organisasi apabila terjadi gangguan pada aset teknologi dan informasi?	Terhadi permasalahan apabila terjadi gangguan pada data contohnya kehilangan data. Karena proses bisnis sangat bergantung pada data – data tersebut khususnya data mahasiswa dan juga data akademik.
Fase 2 Identifikasi Kelemahan Infrastruktur	

Obyektif 1 : Mengidentifikasikan komponen aset teknologi dan informasi yang diterapkan	
Pertanyaan	Jawaban
Apa sajakah komponen TI yang digunakan pada funngsional kritis organisasi?	Komponen TI yang paling kritis sendiri adalah data. Data yang paling kritis adalah data demografi mahasiswa dan juga data akademik, contohnya data nilai mahasiswa. Selain itu server dan database juga kritis karena memastikan bahwa data dapat bisa selalu diakses dan apabila data hilang dapat segera dikembalikan.
Apakah sistem memiliki kebutuhan infrastruktur yang sama?	Setiap sistem memiliki kebutuhan insfrastruktur yang tidak sama karena kebutuhan dan fungsi merekapun berbeda – beda.
Obyektif 2 : Mengidentifikasikan kelemahan aset teknologi informasi yang diterapkan pada fungsional kritis organisasi	
Pertanyaan	Jawaban
Kelemahan teknis apa saja untuk aset teknologi informasi yang telah diterapkan pada organisasi	Kelemahan teknis yang dimiliki oleh organisasi antara lain adalah belum ada prosedur teknis dan detail untuk keamanan proses TI. Selain itu juga belum ada pembagian listrik yang mana apabila beban listrik terlalu berat hal ini dapat memicu kebakaran. Pada struktur bangunan pun perlu diperhatikan karena sudah ada kebocoran yang terjadi.
Berapa lama waktu yang dibutuhkan oleh server untuk melakukan *booting* setelah kondisi server mati? Bagaimana cara backup yang dilakukan?	Server jarang tidak pernah mati karena sudah ada UPS server. Backup dilakukan secara otomatis setiap harinya dan untuk backup sendiri blm pernah mengalami kegagalan.
Bagaimana penataan kabel yang digunakan oleh organisasi?	Penataan kabel sudah ada sekarang, dulunya belum. Masing masing kabel telah ditata sehingga mempermudah pengaturan.

Informasi Narasumber	
Nama Narasumber	Hariadi Yutanto, S.Kom, M.Kom
Nama Organisasi	STIE Perbanas
Jabatan	Kasie TIK (Manajemen Jaringan dan Technical Support)
Waktu	Kamis, 21 Oktober 2015
Tempat	STIE Perbanas Kampus II
Media	Wawancara

Fase 1 Membangun aset berdasarkan ancaman profil	
Obyektif 1 : Menggali informasi aset kritis teknologi dan sistem informasi yang telah diterapkan organisasi	
Pertanyaan	Jawaban
Bagaimana proses umum penerapan teknologi informasi di organisasi?	Proses umum di STIE Perbanas yang tercakup oleh TI adalah diawali dengan pendaftaran siswa baru dengan menggunakan SPMB Online. Setelah itu data mahasiswa akan disimpan di bagian kemahasiswaan. Selain itu ada SIMAS (bajol.perbanas.ac.id) yang didalamnya terdapat sistem akademik, kemahasiswaan, keuangan, kepegawaian, kesekretariatan dan lain sebagainya. Dalam sistem Akademik mahasiswa dan dosen dapat melakukan proses KRS, memasukkan dan melihat nilai, dan berbagai aktivitas akademik lainnya. Didalamnya juga ada sistemi kepegawaian untuk para pegawai. Selain itu STIE Perbanas juga memiliki E-Learning untuk membantu proses mengajar (kuliah.perbanas.ac.id). Selain itu ada juga aplikasi perpustakaan untuk dapat mengakses penelitiaan dan tugas akhir mahasiswa. Layanan TI lainnya yang diberikan kepada mahasiswa adalah email, hotspot dan File Server.
Apa sajakah fungsional organisasi yang mendukung	Semua proses bisnis yang ada pada fungsional organisasi telah tercakup oleh TI. Dari semua proses bisnis yang kritis adalah pada fungsional akademik karena disana terdapat data kritis seperti dari SIMAS.

penggunaan teknologi dan sistem informasi?	
Aset teknologi apa sajakah yang dapat memberikan ancaman pada proses bisnis organisasi?	Aset kritis yang mampu memberi ancaman antara lain ada database yang berisi semua data penting organisasi. Kerusakan pada server dan juga hardware juga dapat menjadi ancaman terhadap hilangnya data. Selain dari hardware dan software, jaringan juga memiliki peran penting pada proses bisnis organisasi. Apabila mati lampu atau tidak adanya listrik, maka organisasi juga membutuhkan aset yaitu genset dan UPS.
Obyektif 2 : Menggali informasi kebutuhan keamanan sistem organisasi	
Pertanyaan	Jawaban
Bagaimana usaha yang telah dilakukan organisasi dalam menghadapi ancaman yang ada?	Usaha yang dilakukan oleh organisasi antara lain adalah dengan memasang firewall untuk keamanan sistem dan menggunakan anti-netcut untuk keamanan Wifi. Selain itu organisasijuga memasang antivirus dan memasang login untuk portal, wifi dan server. Selain itu organisasi juga giat melakukan sosialisasi keamanan kepada mahasiswa dan juga membuat beberapa peraturan untuk menjaga keamanan TI.
Berapa kali organisasi melakukan backup data pada area fungsional bisnis kritis?	Organisasi melakukan backup pada database setiap hari, biasanya pada malam hari. Selain itu juga dilakukan backup server dan NAS (Network-Attached Storage)
Berapa kali organisasi melakukan *maintenance* terhadap aset teknologi informasi yang mendukung fungsional bisnis kritis organisasi?	Pada awal semester (6 bulan sekali) organisasi melakukan maintenance keseluruhan untuk setiap kelas dan lab yang kemudian akan menghasilkan laporan. Apabila ada kerusakan maka akan diserahkan kebagian Umum yang kemudian bertugas memanggil orang untuk memperbaiki atau mengganti aset. Selain itu maintenance untuk lab juga dilakukan sebelum aktivitas UAS dan UTS dan juga nantinya akan menghasilkan laporan.
Apakah terdapat mekanisme proteksi	Organisasi telah memasang firewall dan antivirus untuk keamanan sistem. Selain itu untuk keamanan Wifi juga

keamanan aset teknologi dan informasi pada fungsional bisnis kritis organisasi?	telah dipasang *anti-netcut*. Organisasi juga telah menerapkan beberapa peraturan untuk menjaga keamanan dari aset TI. Selain itu organisasi juga berencana akan membuat DRP untuk keamanan saat terjadi bencana.
Obyektif 3 : Menggali Informasi mengenai identifikasi ancaman terhadap aset teknologi dan informasi	
Pertanyaan	Jawaban
Bencana alam apa saja yang mungkin dapat terjadi dan mengancam aset teknologi dan sistem informasi di fungsional kritis perusahaaan?	Bencana alam yang mungkin mengancam adalah kebakaran dan mungkin gempa bumi. Apabila banjir mungkin tidak seberapa mengancam karena letak fungsi TI sudah berada di lantai dua kecuali ada badai hebat atau terjadi tsunami.
Gangguan apa sajakah yang pernah terjadi pada aset teknologi dan informasi?	Gangguan yang paling besar terjadi pada STIE Perbanas adalah kebakaran yang terjadi di ruang server pada awal tahun 2015 lalu. Selain itu gangguan lainnya adalah biasanya wifi sering di *netcut*. Hal lain yang mengganggu adalah mahasiswa seringkali menyebarkan password mereka keteman terdekat mereka, hal ini menyebabkan banyak komplain saat KRS dimana data mereka dirubah oleh teman mereka.
Apakah pernah terjadi gangguan akibat manusia misalnya pembobolan data?	Pernah ada mahasiswa yang mengambil soal dengan membobol data, hal ini terjadi satu kali. Namun saat ini sistem telah diamankan. Selain itu mungkin pembobolan data juga terjadi karena mahasiswa masih sering memberikan password ke teman terdekat mereka.
Obyektif 4 : Menggali informasi mengenai praktik keamanan terkini yang telah dilakukan oleh organisasi	
Pertanyaan	Jawaban
Apakah setiap *user* sistem memiliki hak akses yang berbeda?	Setap user sistem tentu saja memiliki hak akses yang berbeda. Untuk file server dan email user telah diberi login masing – masing. Sedangkan untuk wifi juga dibedakan melalui login sehingga mahasiswa dan

	dosen memiliki akses berbeda. Untuk bagian lainnya tiap role pegawai akan memiliki hak akses yang berbeda sesuai dengan fungsional yang sedang dia jalani. Sehingga masing masing pegawai hanya terbatas dalam mengakses sistem TI sesuai kebutuhan saja.
Apakah organisasi menerapkan standard keamanan untuk melindungi aset teknologi dan sistem informasi?	Organisasi belum menerapkan standard keamanan tertentu hanya ada beberapa prosedur yang dibuat mengenai pengelolaan SI/TI.
Obyektif 5 : Mengidentifikasikan kelemahan organisasi	
Pertanyaan	Jawaban
Apakah terdapat SOP terkait keamanan teknologi dan informasi organisasi?	Ada beberapa SOP yang telah ada namun ada yang telah dijalankan dan ada juga yang belum. Contoh SOP yang telah dijalankan adalah mengenai SLA, jaringan LAN, Maintenance, jaringan Internet dan pembuatan Email. Salah satu SOP yang belum dijalankan adalah SOP mengenai pengelolaan komplain. Selain itu SOP mengenai penanganan bencana belum ada.
Apakah terdapat permasalahan organisasi apabila terjadi gangguan pada aset teknologi dan informasi?	Permasalahan organisasi apabila terjadi gangguan tadi mungkin karena belum semua SOP dijalankan dan semua SOP ada maka mungkin akan terjadi kebingungan untuk menjalankan beberapa aktivitas TI. Selain itu juga pegawai secara rutin dilakukan *rolling* untuk fungsionalnya sehingga hal ini akan menyebabkan hak akses harus terus menerus dirubah dan di*update.*
Fase 2 Identifikasi Kelemahan Infrastruktur	
Obyektif 1 : Mengidentifikasikan komponen aset teknologi dan informasi yang diterapkan	
Pertanyaan	Jawaban
Apa sajakah komponen TI yang digunakan	Komponen TI untuk fungsional kritis ada banyak. Contohnya untuk data yang kritis adalah data SIMAS dan data File Server. Selain itu sistem yang

pada funngsional kritis organisasi?	kritis ada sistem SIMAS dan juga E-learning. Sedangkan server dan hardware lainnya sendiri juga komponen yang penting karena mendukung proses kritis organisasi.
Apakah sistem memiliki kebutuhan infrastruktur yang sama?	Setiap sistem memiliki kebutuhan insfrastruktur yang tidak sama karena kebutuhan dan fungsi merekapun berbeda – beda.
Obyektif 2 : Mengidentifikasikan kelemahan aset teknologi informasi yang diterapkan pada fungsional kritis organisasi	
Pertanyaan	Jawaban
Kelemahan teknis apa saja untuk aset teknologi informasi yang telah diterapkan pada organisasi	Kelemahan teknis yang dimiliki oleh organisasi antara lain adalah firewall yang digunakan hanya microtix, belum ada mirroring untuk database selain itu mahasiswa juga belum bisa reset password sendiri harus manual melalui admin TI.
Berapa lama waktu yang dibutuhkan oleh server untuk melakukan *booting* setelah kondisi server mati? Bagaimana cara backup yang dilakukan?	Server jarang sekali mati karena sudah ada UPS. Backup dilakukan secara otomatis setiap malam hari.
Bagaimana penataan kabel yang digunakan oleh organisasi?	Penataan kabel sudah ada. Masing – masing kabel sudah ditata sendiri-sendiri dan masing masing kabel telah memiliki label untuk mempermudah pengaturan.

LAMPIRAN F

Lampiran Interview Protokol Analisis Dampak Bisnis

Informasi Narasumber	
Nama Narasumber	Dr. Drs. Emanuel Kritijadi, MM
Nama Organisasi	STIE Perbanas
Jabatan	Pembantu ketua Bidang Akademik
Waktu	Jumat, 30 Oktober 2015
Tempat	STIE Perbanas Kampus II
Media	Wawancara

Pertanyaan	**Jawaban**
Apa saja layanan TI yang ada pada organisasi dan bagaimana tingkat prioritas untuk masing masing layanan?	Kalau layanan TI yang paling kritis ada dan utama SIMAS yang ada pada bajol.perbanas.ac.id, lalu ada e-learning dan juga ada SPMB Online untuk penerimaan mahasiswa baru.
Apa saja proses bisnis yang berlangsung pada layanan kritis yang dimiliki organisasi? Bagaimana prioritisasi proses tersebut?	Kalau misalnya pada SIMAS, ada banyak karena didalam SIMAS ada sistem informasi kepegawaian, keuangan, kemahasiswaan dan lain sebagainya.Untuk akademik yang kritis pada SIMAS disana ada proses KRS dan proses pengolahan nilai. Kalau untuk kemahasiswaan yang kritis adalah pada proses SPMB.
Apa saja aktivitas yang berlangsung pada proses bisnis kritis yang dimiliki organisasi? Bagaimana prioritisasi aktivitas tersebut?	Proses KRS didalamnya ada aktivitas set up, pengambilan mata kuliah dan juga verifikasi dari dosen wali seperti biasanya. Sedangkan untuk pengolahan nilai biasanya dosen mengatur set up awal penilaian dan menginputkan nilai sesuai dengan jadwal.

	Selain itu untuk SPMB Online bisa dilihat di websitenya disitu ada aktivitas-aktivitas yang tertera. Selain itu kalau e-learning sendiri disana ada fitur group discussion, pengambilan kuis online dan juga *share* modul.
Apakah dampak yang terjadi pada layanan bila terjadi gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis)	Dampaknya sebenarnya paling besar di reputasi, karena apabila layanan TI terkena gangguan maka akan menimbulkan komplain dan citra buruk. Namun juga bisa dilihat dari segi finansial, terutama apabila ada perubahan data pada keuangan.
Apabila terjadi gangguan bagaimana waktu yang ditoleransi organisasi terkait gangguan tersebut?	Sebenarnya selama ini belum ada toleransi waktu tertentu. Biasanya apabila terjadi gangguan di pada proses bisnis kritis seperti waktu itu pada proses SPMB, besoknya kami langsung melakukan proses secara manual. Biasanya untuk yang kritis secepatnya, selain itu mungkin sekitar 1 hari keatas.
Apakah organisasi memiliki toleransi waktu dalam tahap pemulihan sistem apabila terjadi gangguan?	Sebenarnya belum ada peraturan untuk toleransi waktu dalam pemulihan sistem.
Apakah organisasi memperhitungkan kegagalan proses bisnis bila terjadi gangguan?	Iya organisasi akan memperhitungkan kegagalan apabila terjadi gangguan.

Apakah setiap layanan dan proses bisnis memiliki aspek kritis yang berbeda-beda?	Iya tentu saja, setiap layanan memiliki tingkat kekritisan yang berbeda-beda tergantung dengan nilai yang diberikan kepada organisasi
Apa yang dilakukan organisasi terhadap proses bisnis kritis bila terjadi gangguan?	Biasanya apabila terjadi gangguan pada aspek kritis maka akan langsung dirapatkan dan dilakukan tindakan untuk mengatasinya.

Informasi Narasumber	
Nama Narasumber	Hariadi Yutanto, S.Kom, M.Kom
Nama Organisasi	STIE Perbanas
Jabatan	Kasie TIK (Manajemen Jaringan dan Technical Support)
Waktu	Kamis, 21 Oktober 2015
Tempat	STIE Perbanas Kampus II
Media	Wawancara

Pertanyaan	**Jawaban**
Apa saja layanan TI yang ada pada organisasi dan bagaimana tingkat prioritas untuk masing masing layanan?	Layanan TI sendiri untuk sistem informasi ada SIMAS, SPMB Online, Perpustakaan. Selain itu untuk fasilitas kepada mahasiswa kita juga menyediakan e-learning, wifi, file server, email dan lab. Untuk layanan yang kritis ada pada SIMAS, SPMB Online juga kritis apabila sedang waktunya pendaftaran mahasiswa baru.
Apa saja proses bisnis yang berlangsung pada layanan kritis	Kalau misalnya pada sistem informasi keuangan ada ada proses penggajian

yang dimiliki organisasi? Bagaimana prioritisasi proses tersebut?	honor mengajar, pengajuan anggaran dan pembayaran biaya. Penggajian dan pembayaran dapat dibilang kritis karena menyangkut masalah uang. Selain itu untuk sistem informasi bagian kemahasiswaan dapat mengelola *softskill*, ini cukup penting karena juga sebagai persyaratan wisuda. Namun pengelolaan kelulusan wisuda sendiri dikelola oleh akademik.
Apa saja aktivitas yang berlangsung pada proses bisnis kritis yang dimiliki organisasi? Bagaimana prioritisasi aktivitas tersebut?	Untuk pendaftaran mahasiswa baru sendiri ada aktivitas registrasi dan daftar ulang yang menggunakan sistem. Sedangkan untuk pengelolaan softskill sendiri mahasiswa dapat upload softskill yang nantinya diverifikasi melalui sistem. Sedangkan untuk bagian keuangan, pengajuan anggaran dilakukan menggunakan sistem dan dilakukan verifikasi pula pada sistem.
Apakah dampak yang terjadi pada layanan bila terjadi gangguan pada aset SI/TI? (ditinjau dari finansial, reputasi, regulasi, kontraktual dan tujuan bisnis)	Dampaknya yang terasa pasti pada terhambatnya proses bisnis. Selain itu juga terdapat dampak dari reputasi apabila ada gangguan pada proses bisnis yang kritis.
Apabila terjadi gangguan bagaimana waktu yang ditoleransi organisasi terkait gangguan tersebut?	Toleransi waktu yang paten belum ditentukan oleh organisasi. Kebanyakan untuk yang proses bisnisnya kritis sekitar 12 jam kebawah harus segera diatasi.
Apakah organisasi memiliki toleransi waktu dalam tahap pemulihan sistem apabila terjadi gangguan?	Sebenarnya belum ada peraturan untuk toleransi waktu dalam pemulihan sistem. Namun apabila diperhitungkan mungkin ½ dari toleransi waktu maksimal gangguan perusahaan.

Apakah organisasi memperhitungkan kegagalan proses bisnis bila terjadi gangguan?	Betul, organisasi akan memperhitungkan kegagalan dari proses bisnis karena hal ini pasti akan membawa dampak bagi organisasi.
Apakah setiap layanan dan proses bisnis memiliki aspek kritis yang berbeda-beda?	Benar, setiap layanan memiliki tingkat kekritisan yang berbeda-beda dan kebutuhan yang berbeda-beda pula
Apa yang dilakukan organisasi terhadap proses bisnis kritis bila terjadi gangguan?	Tergantung pada tingkat kekritisannya, apabila gangguan terjadi pada proses bisnis yang sangat kritis maka akan sesegera mungkin dilakukan tindakan.

LAMPIRAN G

Lampiran Analisis Risiko

G.1 Penilaian Risiko

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
Hardware	Server	1	Kerusakan pada Server	Proses bisnis terhambat	8	Gempa bumi	3	Letak lokasi ruang server di lantai 2	5	**120**	High
						Badai dan Petir	5	Terdapat penangkal petir	2	**80**	Medium
						Banjir	5	Letak lokasi ruang server di lantai 2	2	**80**	Medium
				Penurunan citra organisasi		Kebakaran	2	Terdapat smoke detector dan *fire extinguisher*	3	**48**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
				Organisasi mengalami kerugian secara finansial		Kebocoran dan Kerusakan pada Bangunan	5	Terdapat maintenance yang dilakukan 6 bulan sekali	5	**200**	Very High
		2	Server berhenti	Proses bisnis terhambat	7	Kerusakan pada Genset dan UPS	4	Lokasi genset dan UPS terdapat pada lokasi aman dan terdapat maintenance yang dilakukan 6 bulan sekali	2	**56**	Low
						Listrik Mati	7	Sudah terdapat genset dan UPS saat listrik mati	2	**70**	Low
		3	Kinerja server menurun	Berkurangnya kepercayaan	3	RAM mengalami	4	Maintenance dilakukan 6 bulan sekali	4	**48**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
				civitas akademika		kelebihan memori					
				Menurunnya prouktivitas		Kinerja Procesor menurun akibat terlalu banyak kapasitas data	3	Maintenance dilakukan 6 bulan sekali	4	**36**	Low
						Tempat penyimpanan (*Harddisk)* penuh	4	Maintenance dilakukan 6 bulan sekali	4	**48**	Low
		4	Pencurian data	Penurunan citra organisasi	5	Ruang Server kurang diberi pengamanan	5	Ruang server dikunci dan tidak semua dapat masuk ke dalam ruangan	4	**100**	Medium

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
				Penyalahgunaan data		Kesalahan Konfigurasi Server	4	Terdapat pelatihan terhadap staf bagian TIK	5	**100**	Medium
		5	Data Hilang	Berkurangnya kepercayaan civitas akademika	7	Kesalahan DBA	4	Melakukan pelatihan pada DBA	3	**84**	Medium
				Proses bisnis terhambat		Virus	4	Memasang antivirus E-scan	4	**112**	Medium
	PC	6	Kerusakan pada PC	Menurunnya produktivitas	4	Gempa Bumi	3	Letak lokasi ruang kerja di lantai 2	5	**60**	Low
				Organisasi mengalami		Badai dan Petir	5	Terdapat penangkal petir	2	**40**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
				kerugian secara finansial		Banjir	5	Letak lokasi ruang server di lantai 2	2	**40**	Low
				Proses bisnis terhambat		Kebakaran	2	Terdapat smoke detector dan *fire extinguisher*	3	**24**	Low
						Kebocoran dan Kerusakan pada Bangunan	5	Terdapat maintenance yang dilakukan 6 bulan sekali	4	**80**	Medium
						Keyboard, mouse atau monitor mengalami kerusakan karena pemakaian berlebih	3	Terdapat maintenance yang dilakukan 6 bulan sekali	2	**24**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
		7	PC tidak dapat menyala	Menurunnya produktivitas	3	Kerusakan pada Genset dan UPS	4	Terdapat maintenance yang dilakukan 6 bulan sekali	4	**48**	Low
						Listrik Mati	7	Sudah terdapat genset saat listrik mati	2	**42**	Low
		8	PC terkena virus	Menurunnya produktivitas	3	antivirus tidak update	4	Terdapat antivirus e-scan	5	**60**	Low
Software	SIMAS, E-Learni	9	Aplikasi tidak dapat diakses	Proses bisnis terhambat	5	Listrik Mati	7	Sudah terdapat genset dan UPS saat listrik mati	2	**70**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
	ng, Perpustakaan			Menurunnya produktivitas		Server Down	5	Adanya perawatan maintenance pada server 6 bulan sekali	3	**75**	Low
		10	Aplikasi diakses oleh pihak yang tidak berwenang	Tersebarluasnya data orgnisasi	9	Kesalahan dalam pemberian hak akses	3	Adanya peraturan dalam pembatasan hak akses	4	**108**	Medium
Data	Data demografi mahasiswa,	11	Data tidak dapat diakses	Menurunnya produktivitas	5	Listrik Mati	7	Sudah terdapat genset dan UPS saat listrik mati	2	**70**	Low
				Proses bisnis terhambat		Server Down	5	Adanya perawatan	3	**75**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
	Data Akademik dan Data File Server			Berkurangnya kepercayaan civitas akademika				maintenance pada server 6 bulan sekali			
		12	Pencurian data	Berkurangnya kepercayaan civitas akademika	7	Terdapat hacker yang mencuri data	4	Adanya firewall dan pengamanan jaringan	5	**140**	High
		13	Manipulasi data	Komplain dari civitas akademika	8	Username dan password ketahui oleh pengguna lain	5	Diadakan sosialisasi kepada civitas akademika	5	**200**	Very High
				Berkurangnya kepercayaan		Terdapat hacker yang	4	Adanya firewall dan sosialisasi	5	**160**	High

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
				civitas akademika		memanipulasi data		dari Bagian TIK ke civitas			
		14	Backup data gagal	Informasi yang ditampilkan tidak terbaru/terkini	4	Kapasitas media penyimpanan overload	4	Maintenance oleh DBA	3	**48**	Low
		15	Data hilang	Berkurangnya kepercayaan civitas akademika Komplain dari civitas akademika	8	Server Rusak	3	Melakukan maintenance yang dilakukan 6 bulan sekali serta backup data setiap harinya	4	**96**	Medium

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
				Proses bisnis terhambat		Virus/Bug	5	Adanya antvirus e-scan	4	**160**	High
Jaringan	Kabel	16	Kurangnya kontrol pengamanan kabel	Proses bisnis terhambat	5	Kabel rusak	5	Sudah ada pelabelan dan pengaturan kabel	2	**50**	Low
	Wifi dan Router	17	Internet Mati	Produktivitas menurun	5	Listrik Mati	7	Sudah terdapat genset dan UPS saat listrik mati	2	**70**	Low
						Wifi rusak	3	Melakukan maintenance yang dilakukan 2 minggu sekali	2	**30**	Low
				Komplain dari civitas akademika		Genset mati	4	Melakukan maintenance yang dilakukan 6 bulan sekali	4	**80**	Medium

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
						Kabel Rusak	5	Sudah ada pelabelan dan pengaturan kabel	2	**50**	Low
		18	Akses internet lambat	Komplain dari civitas akademika	5	Kesalahan Konfigurasi	5	Melakukan maintenance 6 bulan sekali	4	**100**	Medium
				Produktivitas menurun		Ada yang melakukan netcut	7	Memasang anti netcut	2	**70**	Low
Sumber Daya Manusia	Pegawai Non - TI	19	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Penurunan Kompetensi Karyawan	3	Adanya pelatihan untuk Pegawai Non-TI	4	**60**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
						Pegawai Non-TI					
						Adanya praktik KKN di perusahaan	2	Adanya kebijakan dan prosedur serta sosialisasi dari Bagian TIK ke civitas	3	**30**	Low
		20	Data yang ada tidak valid	Penurunan citra organisasi Komplain dari civitas akademika	5	Kesalahan dalam input data	5	Adanya pelatihan untuk karyawan	3	**75**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
		21	Pelanggaran regulasi hak akses	Berkurangnya kepercayaan civitas akademika	3	Penyalahgunaan akses regulasi	3	Adanya kebijakan dan prosedur regulasi	3	**27**	Low
	Pegawai TI	22	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Penurunan Kompetensi Pegawai TI	3	Adanya pelatihan untuk Pegawai TI	4	**60**	Low
						Adanya praktik KKN di perusahaan	3	Adanya kebijakan dan prosedur serta sosialisasi dari Bagian TIK ke civitas	3	**45**	Low
		20	Data yang ada tidak valid	Komplain dari civitas akademika	6	Kesalahan dalam input data	6	Adanya pelatihan untuk karyawan	3	**108**	Medium

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
		23	Pelanggaran regulasi	Penurunan citra organisasi	3	penyelahgunaan akses regulasi	4	Adanya kebijakan dan prosedur regulasi	3	**36**	low
	Dosen	24	Penyalahgunaan data organisasi	Tersebarluasnya data orgnisasi	5	Penurunan Kompetensi Dosen	3	Adanya pelatihan untuk dosen	4	**60**	Low
						Adanya praktik KKN di perusahaan	2	Adanya kebijakan dan prosedur serta sosialisasi dari Bagian TIK ke civitas	3	**30**	Low
		25	Data yang ada tidak valid	Komplain dari civitas akademika	5	Kesalahan dalam input data nilai	5	Adanya pelatihan untukdosen	3	**75**	Low

Kategori Aset	Aset	ID Risiko	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Penyebab Potensi Kegagalan	Occ	Proses Kontrol Saat ini	Det	RPN	Level
	Mahasiswa	26	Sharing Password Mahasiswa/i	Komplain dari civitas akademika Penurunan citra organisasi	7	Manipulasi Data	6	Sosialisasi kepada mahasiswa/i	5	**210**	Very High

LAMPIRAN H

Lampiran Analisis Dampak Bisnis

H.1 Tingkat Kritis Proses Bisnis

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Tingkat Kritis	Keterangan
Akademik	Proses KRS	Kritis	Proses KRS akan terhambat dan harus dilakukan secara manual apabila terjadi gangguan pada sistem
	Pengelolaan Nilai Mahasiswa	Kritis	Mahahasiswa tidak akan dapat melihat nilai & dosen tidak akan dapat menginputkan nilai apabila terjadi gangguan pada sistem
	Proses kelulusan mahasiswa	Penting	Rapat evaluasi wisuda dan pengelolaan yudisium akan ikut terganggu apabila terjadi gangguan pada sistem
	Proses Pengajaran melalui E-Learning	Penting	Mahasiswa tidak dapat melakukan pembelajaran di e-learning seperti mengambil modul, kuis maupun tugas apabila terjadi gangguan pada sistem
Kemahasiswaan	Pendaftaran Mahasiswa Baru	Kritis	Mahasiswa baru akan kesulitan untuk mendaftar dan pendaftaran harus diganti secara manual apabila terjadi gangguan pada sistem
	Proses Pengelolaan *Softskill*	Penting	Mahasiswa tidak akan dapat memasukkan data *softskill* melalui sistem apabila terjadi

Fungsional Bisnis	Proses Bisnis Terkait Sistem	Tingkat Kritis	Keterangan
			gangguan. Pengelolaan *softskill* akan dilakukan secara manual apabila terjadi gangguan
TIK	Melakukan Pemantauan Teknologi	Kritis	Apabila terjadi gangguan maka tidak dapat dilakukan pemantauan teknologi indormasi
	Melakukan Pengolahan Data Elektronik	Kritis	Apabila terjadi gangguan maka data elektronik miliki organisasi akan terkena risiko ancaman.
	Melakukan Pengelolaan Konfigurasi Perangkat	Penting	Pengelolaan konfigurasi perangkat tidak dapat dilakukan apabila terjadi gangguan
	Menyediakan Layanan SI/TI untuk Mendukung Proses Pengajaran	Kritis	Layanan SI/TI seperti wifi, e-learning dan file server tidak akan bisa berjalan apabila terjadi gangguan
	Disaster Recovery Planning	Kritis	Pemulihan sistem harus secepatnya dilakukan apabila terjadi bencana
Keuangan	Pengelolaan Pembayaran Biaya Kuliah	Kritis	Pemantauan dan pengelolaah biaya kuliah harus dilaukan manual apabila sistem terjadi gangguan
	Penggajian Honor Mengajar	Kritis	Pengelolaan gaji honor mengajar harus dilakukan secara manual apabila sistem terjadi gangguan
	Pengajuan Anggaran	Penting	Pengajuan anggaran harus manual apabila sistem terjadi gangguan

H.2 Analisis Dampak Gangguan

Penyebab				Dampak		
Risiko		**Fungsional bisnis**	**Proses bisnis terkait sistem**	**Finansial**	**Reputasi**	**Target Teknis**
Kerusakan pada Server	• Gempa Bumi • Banjir • Kebakaran • Kebocoran dan Kerusakan pada Gedung	Akademik	Proses KRS	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Mengganggu <15% target teknis dari proses bisnis
			Pengelolaan Nilai Mahasiswa	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Mengganggu <15% target teknis dari proses bisnis
			Proses Kelulusan Mahasiswa	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak besar pada reputasi perusahaan	Mengganggu <3% target teknis dari proses bisnis
			Proses Pengajaran melalui E-Learning	Tidak ada dampak secara finansial kepada perusahaan	Berdampak sedang pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis

Penyebab				Dampak		
Risiko		**Fungsional bisnis**	**Proses bisnis terkait sistem**	**Finansial**	**Reputasi**	**Target Teknis**
		Kemahasiswaan	Pendaftaran Mahasiswa Baru	Menimbulkan kerugian finansial/biaya ekstra <15%	Berdampak besar pada reputasi perusahaan	Mengganggu <15% target teknis dari proses bisnis
			Proses Pengelolaan *Softskill*	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak kecil pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis
		TIK	Melakukan Pemantauan Teknologi	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis
			Melakukan Pengelahan Data Elektronik	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak besar pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis
			Melakukan Pengelolaan	Menimbulkan kerugian	Berdampak sedang pada reputasi perusahaan	Mengganggu <10% target

Penyebab				Dampak		
Risiko		**Fungsional bisnis**	**Proses bisnis terkait sistem**	**Finansial**	**Reputasi**	**Target Teknis**
			Konfigurasi Perangkat	finansial/biaya ekstra <5%		teknis dari proses bisnis
			Menyediakan Layanan SI/TI untuk Mendukung Proses Pengajaran	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak besar pada reputasi perusahaan	Mengganggu <15% target teknis dari proses bisnis
			Disaster Recovery Planning	Menimbulkan kerugian finansial/biaya ekstra <20%	Berdampak besar pada reputasi perusahaan	Mengganggu <15% target teknis dari proses bisnis
		Keuangan	Pengelolaan Pembayaran Biaya Kuliah	Menimbulkan kerugian finansial/biaya ekstra <15%	Berdampak besar pada reputasi perusahaan	Mengganggu <15% target teknis dari proses bisnis
			Penggajian Honor Mengajar	Menimbulkan kerugian finansial/biaya ekstra <10%	Berdampak kecil pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis

Penyebab				Dampak		
Risiko		**Fungsi onal bisnis**	**Proses bisnis terkait sistem**	**Finansial**	**Reputasi**	**Target Teknis**
			Pengajuan Anggaran	Menimbulkan kerugian finansial/biaya ekstra <5%	Tidak berdampak langsung pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis

Risiko	Penyebab	Fungsional bisnis	Proses bisnis terkait sistem	Dampak		
				Finansial	Reputasi	Teknis
Manipulasi data	• Username dan password ketahui oleh penggun a lain • Terdapat hacker yang memanip ulasi data	Akade mik	Proses KRS	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis
			Pengelolaan Data Perpustakaan	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis
			Pengelolaan Nilai Mahasiswa	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak besar pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis
			Proses wisuda	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Mengganggu <3% target teknis dari proses bisnis

Risiko	Penyebab	Fungsional bisnis	Proses bisnis terkait sistem	Dampak		
				Finansial	Reputasi	Teknis
			Proses Pengajaran melalui E-Learning	Tidak ada dampak secara finansial kepada perusahaan	Berdampak sedang pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis
		Kemahasiswaan	Pendaftaran Mahasiswa Baru	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak besar pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis
			Proses Pengelolaan *Softskill*	Tidak ada dampak secara finansial kepada perusahaan	Berdampak sedang pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis
		TIK	Melakukan Pemantauan Teknologi	Menimbulkan kerugian finansial/biaya ekstra <3%	Berdampak sedang pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis
			Melakukan Pengelahan Data Elektronik	Menimbulkan kerugian	Berdampak sedang pada reputasi perusahaan	Mengganggu <10% target

Risiko	Penyebab	Fungsional bisnis	Proses bisnis terkait sistem	Dampak		
				Finansial	Reputasi	Teknis
				finansial/biaya ekstra <3%		teknis dari proses bisnis
			Melakukan Pengelolaan Konfigurasi Perangkat	Menimbulkan kerugian finansial/biaya ekstra <3%	Berdampak kecil pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis
			Menyediakan Layanan SI/TI untuk Mendukung Proses Pengajaran	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis
			Disaster Recovery Planning	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak sedang pada reputasi perusahaan	Mengganggu <10% target teknis dari proses bisnis
		Keuangan	Pengelolaan Pembayaran Biaya Kuliah	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak besar pada reputasi perusahaan	Mengganggu <15% target teknis dari proses bisnis

Risiko	Penyebab	Fungsi onal bisnis	Proses bisnis terkait sistem	Dampak		
				Finansial	Reputasi	Teknis
			Penggajian Honor Mengajar	Menimbulkan kerugian finansial/biaya ekstra <5%	Berdampak besar pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis
			Pengajuan Anggaran	Tidak ada dampak secara finansial kepada perusahaan	Berdampak besar pada reputasi perusahaan	Mengganggu <5% target teknis dari proses bisnis

LAMPIRAN I

Lampiran Gambaran Umum Modul Pelatihan BCP & Skenario Pengujian

	GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS
Nama Pelatihan	Pelatihan *Back up* dan *Restore Data*
Jenis Pelatihan	Pemberian materi in-door dan praktik
Deskripsi Pelatihan	
Pelatihan ini bertujuan untuk memberi pengetahuan umum dan teknis mengenai *back up* dan *restore* data, hal ini termasuk tipe *back up* dan *restore*, penjadwalan *back* up dan tata cara dalam melakukan *back up* dan *restore* . Diharapkan dengan adanya pelatihan ini maka akan memberi wawasan kepada obyek penelitian mengenai tata cara melakukan *back up* dan *restore* dengan benar.	
Sasaran Pelatihan	Seluruh Staf Bagian TIK
Materi Umum	
Dalam pelatihan ini akan memberikan materi kepada karyawan yaitu sebagai berikut : • Pengetahuan umum dan jenis dari *back up* dan *restore* • Prioritisasi data dalam melakukan *back up* • Prosedur dalam melakukan *back up* dan *restore* • Penjadwalan dari proses *back up* dan *restore*	

	GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS

Nama Pelatihan	Pelatihan dan sosialisasi mengenai keamanan data
Jenis Pelatihan	Pemberian materi *in-door*
Deskripsi Pelatihan	
Pelatihan ini bertujuan untuk memberi pengetahuan umum mengenai pentingnya keamanan data kepada para civitas kampus STIE Perbanas, yaitu dosen, karyawan maupun mahasiswa/i. Diharapkan penelitian ini dapat meningkatkan kesadaran civitas akademik dalam hal keamanan data.	
Sasaran Pelatihan	Seluruh Civitas Kampus STIE Perbanas
Materi Umum	
Dalam pelatihan ini akan memberikan materi kepada seluruh civitas kampus yaitu sebagai berikut : • Pengetahuan umum mengenai keamanan data • Pengelolaan keamanan password dan prosedur manajemen password • Keamanan pada jaringan dan internet • Dampak dari kurangnya implementasi keamanan data	

	GAMBARAN UMUM MODUL PELATIHAN KEBERLANJUTAN BISNIS
Nama Pelatihan	Pelatihan penanganan sistem dari penyerangan *hacker*
Jenis Pelatihan	Pemberian materi *in-door* dan praktik
Deskripsi Pelatihan	
Pelatihan ini bertujuan untuk memberi pengetahuan umum serta teknis mengenai penanganan sistem apabila terjadi penyerangan *hacker*. Diharapkan penelitian ini dapat meningkatkan kemampuan bagian TIK dalam menangani insiden tersebut.	
Sasaran Pelatihan	Staf Bagian TIK
Materi Umum	

Dalam pelatihan ini akan memberikan materi kepada seluruh civitas kampus yaitu sebagai berikut :

- Pengetahuan umum mengenai penyeranganan hacker
- Prosedur manajemen insiden
- Prosedur keamanan data
- Pembagian tanggung jawab saat terjadi insiden
- Langkah – langkah penanganan sistem dari penyerangan hacker

SKENARIO PENGUJIAN BCP	
Pelaku dan Pembagian Peran	1. Staf TIK 1 sebagai *hacker* 2. Staf TIK 2 sebagai dokumentator 3. Kepala Bagian TIK sebagai pengawas berjalannya proses pengujian 4. Kasie TIK Bidang Jaringan sebagai pihak yang mengatasi serangan
Skenario	1.Staf TIK 1 sebagai *hacker* yang mencoba masuk dan melakukan manipulasi data organisasi 2. Kasie Bidang Jaringan mengidentifikasi serangan dan melaporkan kepada kepala bidang TIK dengan melihat prosedur manajemen insiden. 3. Kasie Bidang jaringan melakukan perbaikan pada sistem dan mengembalikan integritas data 4. Kepala Bidang TIK melakukan pengawasan tindakan perbaikan 4. Staf TIK 2mendokumentasikan hasil pengujian BCP.

SKENARIO PENGUJIAN BCP	
Pelaku dan pembagian peran	1. Staf TIK 1 sebagai yang melakukan backup dan restore data 2. Staf TIK 2 sebagai dokumentator 3. Kepala Bagian TIK sebagai pengawas berjalannya pengujian
Skenario	1.Staf TIK 1 sebagai mencoba melakukan backup data kepada sistem sesuai dengan prosedur *backup data* Kepala Bagian TIK menghapus data yang telah dibackup pada sistem.

	3. Staf TIK 1 sebagai mencoba melakukan restore data dari hasil backup tadi pada dengan prosedur *restore data* 3. Staf TIK 1 melihat kesesuaian data hasil restore dengan data awal 4. Kepala Bidang TIK melakukan pengawasan pengujian 4. Staf TIK 2 mendokumentasikan hasil pengujian BCP.

LAMPIRAN J

Lampiran Formulir Audit Internal BCP

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

2.4	Apakah organisasi telah melakukan prioritisasi terhadap layanan dan proses yang memiliki ketergantungan terhadap TI?				
2.5	Apakah organisasi telah menentukan toleransi waktu pemulihan terhadap gangguan dan telah disetujui oleh manajemen senior?				
2.6	Apakah organisasi telah melakukan perhitungan dampak bisnis terhadap proses bisnis apabila terjadi gangguan?				
3. Pengelolaan Strategi BCP					
3.1	Apakah organisasi telah mendokumentasikan strategi pencegahan apabila tehadapbencana atau gangguan?				
3.2	Apakah organisasi telah mendokumentasikan strategi pemulihan terjadi bencana atau gangguan?				
3.3	Apakah organisasi telah mendokumentasikan strategi korektif setelah terjadi bencana atau gangguan?				
3.4	Apakah strategi tersebut telah secara formal disetujui oleh manajemen senior?				
3.5	Apakah telah ada prosedur yang mendukung strategi – strategi BCP?				
3.6	Apakah strategi BCP telah dikomunikasikan kepada keseluruhan organisasi?				

3.7	Apakah prosedur terkait BCP telah dikomunikasikan kepada pegawai?				
3.8	Apakah keseluruhan risiko kritis telah dicakup pada BCP?				
3.9	Apakah BCP juga telah mencakup perencanaan komunikasi yang efektif antar bagian?				
4.	Pelatihan dan Pengujian BCP				
4.1	Apakah telah dilakukan pelatihan formal terhadap tim BCP?				
4.2	Apakah terdapat pengujian BCP secara keseluruhan (*full test*) maupun sebagian (*partial test*)?				
4.3	Apakah semua aspek perencanaan telah di uji pada 1 tahun terakhir ini?				
4.4	Apakah pengujian dilakukan oleh staf yang memang terkait dengan perencanaan?				
4.5	Apakah hasil pengujian telah sepenuhnya terdokumentasi?				
5.	Pemeliharaan dan Peninjauan BCP				
5.1	Apakah terdapat proses peninjauan terhadap BCP Proses?				
5.2	Apakah proses BCP telah dibuat dengan tipe siklus yang mana terdapat proses *continous improvement?*				
5.3	Apakah terdapat proses untuk mengukur keefektifan BCP?				
5.4	Apakah terdapat proses untuk melakukan tindakan perbaikan dengan tujuan untuk meningkatkan BCP?				

LAMPIRAN K

Lampiran Formulir Peninjauan Manajemen

Masukan	Pemimpin Rapat :	❑ Ketua Komite BCP		
	Tanggal dan Waktu Rapat:	❑		
	Peserta Rapat yang Hadir:	❑ ❑		
	Peserta Rapat yang Tidak Hadir	❑ ❑		
	Sumber Daya yang Dibutuhkan	❑ Laporan Hasil Tinjauan Manajemen Sebelumnya ❑ Laporan Hasil Internal Audit ❑ Hasil Pengujian BCP		
Analisis	**Topik Diskusi**	**Keputusan/Tindakan**	**Batas Waktu**	**Penanggung Jawab**
	Status dari tindakan yang ditinjau pada Tinjauan Manajemen Sebelumnya			

	Perubahan internal dan eksternal yang berikaitan dengan BCP			
	Hasil audit BCP dan langkah korektif yang dilakukan			
	Kebutuhan untuk melakukan perubahan terhadap BCP untuk kebijakan maupun prosedur			

	Kebutuhan untuk membuat prosedur baru yang dapat meningkatkan kinerja dan keefektifan BCP			
	Rekomendasi untuk peningkatan BCP			
	Hasil pembelajaran dan tindakan yang dilakukan dari insiden yang pernah terjadi sebelumnya			

	Hasil dari pengujian BCP			
Keluaran	Daftar Hadir	❑ ❑		
	Daftar tindakan dan Aksi	❑ ❑		

LAMPIRAN L

Dokumentasi

Lampiran ini akan menunjukkan dokumentasi saat proses penyusunan BCP di STIE Perbanas

Penyerahan Dokumen BCP kepada Kasie TIK Perbanas Bapak Hariadi Yutanto, S.Kom, M.Kom

DAFTAR PUSTAKA

1. Alberts, C., Dorofee, A., Stevens, J. & Woody, C., 2003. *Introduction to the OCTAVE Approach,* Pittsburgh: Carnegie Mellon University.
2. Alijoyo, A., 2006. *Enterprise Risk Management.* Jakarta: PT. Ray Indonesia.
3. Ali, M., 2009. *Pendidikan untuk Pembangunan Nasional.* Jakarta: GRASINDO (PT Gramedia Widiasarana Kompas Gramedia Building).
4. Amanda, A. A., 2014. *Business Continuity Plan pada Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara.* Surabaya: Institut Teknologi Sepuluh Nopember.
5. Arnold, E. P., 1986. *Series on Seismology.* Malaysia: S,E Assian Assoc. Seismology & Earthquake.
6. Australian National Audit Office (ANAO), 2009. *Business Continuity Management : Buiding Resilience in Public Sector Entities.* s.l.:s.n.
7. Awad, H. A. H. & Battah, F. M., 2011. Enhancing Information Systems Security in Educational Organizations. *International Journal of Computer Science Issues,* 8(5).
8. Becker, G. S., 1976. *Economic Theory.* s.l.:Transaction Publishers.
9. Botha, J. & Solms, R. V., 2004. A cyclic approach to business continuity planning. *Information Management & Computer Security,* 12(4), pp. 328-337.
10. Brooks, C., Bedernjak, M., Juran, I. & Merryman, J., 2002. *Disaster Recovery Strategy with Tivoli Storage Management.* s.l.:IBM.

11. COMDISCO, 1997. *The Vulnerability Index,* s.l.: COMDISCO.
12. Djohanputro, B., 2008. *Manajemen Risiko Korporat.* Jakarta: Pendidikan dan Pembinaan Manajemen.
13. Doughty, K., 2000. *Business Continuity Planning: Protecting Your Organization's Life.* s.l.:Auerbach.
14. George, W. & Hunter, R., 2007. *IT Risk : Turning Business Threats into Competitive Advantage.* Boston, Massachusetts: Harvard Business School Press.
15. Griffith University, 2013. *Business Continuity Framework,* s.l.: Griffith University.
16. Hiles, A., 2007. *The Definitive Handbook of Business Continuity Management.* Second Edition ed. England: John Wiley & Sons, Ltd.
17. IBM, 2009. *IBM survey of 224 Business Leaders,* s.l.: IBM.
18. ISO 22301:2012, *Societal Security-Business Continuity Management Systems-Requirements*.
19. ISO 22317:2015, *Societal Security - Business Continuity Management Systems - Business Impact Analysis*.
20. ISO 31000:2009, *Risk Management - Principles and Guidelines*
21. Merna, T. & Al-Thani, F. F., 2008. *Corporate Risk Management.* 2nd Edition ed. s.l.:s.n.
22. NIST, 2008. *Disaster Recovery Plan,* USA: Elthister.
23. NIST, 2010. *Contingency Planning Guide for Federal Information Systems,* s.l.: s.n.
24. Panda, P., 2005. The OCTAVE Approach to Information Security Risk Assessment. *ISACA Journal,* Volume 4.

25. Rosenbeerg, N. A., 2006. *10 Steps to Implement a Disaster Recovery Plan,* s.l.: Quality Technology Solutions, Inc.
26. SANS Institute, 2002. *Introduction to Business Continuity Planning.* [Online] Available at: https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559 [Accessed 20 September 2015].
27. Schultz, T., 1965. *The Economic Value of Education.* s.l.:John Wiley.
28. Snedaker, S., 2014. *Business Continuity and Disaster Recovery For IT Professional.* USA: Elsevier,Inc.
29. Yisa, V. L. & Baba, M., 2014. Evaluation of Business Continuity and Information Disaster Recovery Mechanism in Top Universities in North Cyprus. *International Journal of Emerging Science and Engineering,* 2(11), pp. 19-27.

BIODATA PENULIS

Penulis dilahirkan di Surabaya, 5 November 1994. Penulis telah menempuh pendidikan formal di SD Al-Falah Tropodo 1 Sidoarjo, SMP Al-Falah Deltasari Sidorjo, serta SMA 15 Surabaya. Setelah lulus dari sekolah menengah, penulis meneruskan pendidikan di Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya dan terdaftar dengan NRP 5210100050. Di Jurusan Sistem Informasi penulis mengambil bidang studi Manajemen Sistem Informasi (MSI).

Selama perkuliahan penulis aktif dibidang akademik dan non akademik. Pada bidang akademik penulis tercatat sebagai asisten praktik mata kuliah Sistem Fungsional Binis I dan asisten dosen mata kuliah Matematika Diskrit.Selain itu penulis juga mengikuti organisasi Srikandi Project Surabaya dan juga mengikuti beberapa kepanitian pada tingkat jurusan, fakultas dan institut. Pada pertengahan tahun 2015, penulis melaksanakan kerja praktik di perusahaan minyak dan gas SKK Migas Jakarta selama 1,5 bulan.

Penulis memiliki hobi memasak dan membaca. Penulis juga memiliki mimpi untuk dapat memiliki perusahaan sendiri dan berjalan – jalan ke berbagai penjuru dunia. Penulis dapat dihubungi melalui e-mail sabrinaputri5@gmail.com.