TUGAS AKHIR – KS141501

Implementasi Metodologi Business Continuity Planning pada Pembuatan Dokumen Perencanaan Keberlangsungan Bisnis Divisi Teknologi Informasi (Studi Kasus Bank Pembangunan Daerah Jawa Timur)

IMPLEMENTATION OF BUSINESS CONTINUITY PLANNING METHODOLOGY ON BUSINESS CONTINUITY PLAN DOCUMENTATION IN INFORMATION TECHNOLOGY DEPARTMENT (CASE STUDY: EAST JAVA REGIONAL DEVELOPMENT BANK)

RACHEL CAROLINA
NRP 05211440000104

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

DEPARTEMEN SISTEM IN*FORMA*SI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember

TUGAS AKHIR – KS141501

IMPLEMENTASI METODOLOGI BUSINESS CONTINUITY PLANNING PADA PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS PADA DIVISI TEKNOLOGI INFORMASI (STUDI KASUS BANK PEMBANGUNAN DAERAH JAWA TIMUR)

RACHEL CAROLINA
NRP 05211440000104

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

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

FINAL PROJECT – KS141501

IMPLEMENTATION OF BUSINESS CONTINUITY PLANNING METHODOLOGY ON BUSINESS CONTINUITY PLAN DOCUMENTATION IN INFORMATION TECHNOLOGY DEPARTMENT (CASE STUDY: EAST JAVA REGIONAL DEVELOPMENT BANK)

RACHEL CAROLINA
NRP 05211440000104

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

INFORMATION SYSTEMS DEPARTMENT
Faculty of Information and Communication Technology (ICT)
Institut Teknologi Sepuluh Nopember
Surabaya 2018

LEMBAR PENGESAHAN

IMPLEMENTASI METODOLOGI BUSINESS CONTINUITY PLANNING PADA PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS PADA DIVISI TEKNOLOGI INFORMASI (STUDI KASUS BANK PEMBANGUNAN DAERAH JAWA TIMUR)

TUGAS AKHIR

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

Oleh:

RACHEL CAROLINA
NRP. 05211440000104

Surabaya, Juli 2018

KEPALA
DEPARTEMEN SISTEM INFORMASI

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

IMPLEMENTASI METODOLOGI BUSINESS CONTINUITY PLANNING PADA PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS PADA DIVISI TEKNOLOGI INFORMASI (STUDI KASUS BANK PEMBANGUNAN DAERAH JAWA TIMUR)

TUGAS AKHIR

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

Oleh :
RACHEL CAROLINA
05211440000104

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

Dr. Apol Pribadi S.,S.T.,M.T. **(Pembimbing1)**

Eko Wahyu Tyas D, S.Kom, MBA **(Penguji 1)**

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

IMPLEMENTASI METODOLOGI BUSINESS CONTINUITY PLANNING PADA PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS PADA DIVISI TEKNOLOGI INFORMASI (STUDI KASUS BANK PEMBANGUNAN DAERAH JAWA TIMUR)

Nama Mahasiswa : Rachel Carolina
NRP : 05211440000104
Departemen : Sistem Informasi FTIF-ITS
Pembimbing 1 : Dr. Apol Pribadi S.,S.T.,M.T.

ABSTRAK

Penerapan teknologi oleh peruaaan memiliki risiko yang harus bisa dikendalikan oleh perusahaan. Jika risiko dari teknologi informasi tidak dapat dikelola maka dampaknya dapat mengganggu aktivitas dalam proses bisnis perusahaan bahkan dapat melumpuhkan proses bisnis yang ada. Sehingga setiap perusahaan yang menerapkan teknologi informasi membutuhkan perencanaan untuk dapat mengantisipasi risiko yang timbul akibat teknologi informasi serta mengantisipasi gangguan yang terjadi pada teknologi informasi yang dapat mempengaruhi berlangsungnya proses bisnis. Perencanaan yang dibuat adalah berupa perencanaan keberlangsungan bisnis atau Business Continuity Plan.

Penelitian ini bertujuan untuk mengetahui kesesuaian metodologi Business Continuity Planning yang disusun oleh Yusrida Muflihah jika diterapkan dalam industri perbankan. Industri perbankan dipilih karena industri ini sangat bergantung kepada Teknologi Informasi, selain itu karena adanya kebijakan Otoritas Jasa Keuangan yang mewajibkan pelaku industri perbankan untuk menerapkan manajemen risiko. Metodologi Business Continuity Plan disintesis dari beberapa standart yang ada hingga detil kepada langkah-

langkah pembuatan dokumen BCP. Standart-standart tersebut seperti ISO 22301:2012, COBIT 5 (DSS04: Manage Continuity) serta ITIL *(Service Design - IT Service Continuity Management).*

Hasil dari penelitian yang adalah adanya temuan-temuan dalam implementasi metodologi Business Continuity Plan pada Bank Pembangunan Daerah Jawa Timur. Temuan dari implementasi untuk mengetahui kesesuaian metodologi jika diimplementasikan dalam industri perbankan serta untuk menjadi peluang bagi keberlanjutan penelitian metodologi Business Continuity Plan di masa yang akan datang.

***Kata kunci**: Perencanaan Keberlangsungan Bisnis, Metodologi Business Continuity Plan, Analisis Risiko, Analisis Dampak Bisnis*

IMPLEMENTATION OF BUSINESS CONTINUITY PLANNING METHODOLOGY ON BUSINESS CONTINUITY PLAN DOCUMENTATION IN INFORMATION TECHNOLOGY DEPARTMENT (CASE STUDY: EAST JAVA REGIONAL DEVELOPMENT BANK)

Nama Mahasiswa : Rachel Carolina
NRP : 05211440000104
Departemen : Sistem Informasi FTIF-ITS
Pembimbing 1 : Dr. Apol Pribadi S.,S.T.,M.T.

ABSTRACT

The application of technology by the company has risks that must be controlled by the company. If the risks of information technology can not be managed then the impact can disrupt the activities in the company's business processes can even cripple existing business processes. So that every company that applies information technology needs planning to anticipate risks arising from information technology and anticipate disruption that happened at information technology that can influence ongoing business process. Planning is in the form of business continuity planning or Business Continuity Plan.

This study aims to determine the suitability of Business Continuity Planning methodology compiled by Yusrida Muflihah if applied in the banking industry. The banking industry was chosen because the industry relied heavily on Information Technology, in addition to the policy of the Financial Services Authority which required banking industry actors to apply risk management. The Business Continuity Plan methodology is synthesized from some of the existing standards up to the details of the BCP document creation steps. Standards such as ISO 22301: 2012, COBIT 5 (DSS04: Manage Continuity) and ITIL (Service Design - IT Service Continuity Management).

The result of the research is the findings in the implementation of Business Continuity Plan methodology at East Java Regional Development Bank. Findings from the implementation to determine the suitability of the methodology if implemented in the banking industry as well as to become an opportunity for continuous research methodology Business Continuity Plan in the future.

Key Words: *Business Continuity Plan, Business Continuity Planning Methodology, Risk Analysis, Business Impact Analysis*

KATA PENGANTAR

Puji Syukur atas karunia, berkat, dan jalan yang telah diberikan Tuhan YME selama ini sehingga penulis mendapatkan kelancaran dalam menyelesaikan tugas akhir dengan judul:

IMPLEMENTASI METODOLOGI BUSINESS CONTINUITY PLANNING PADA PEMBUATAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS PADA DIVISI TEKNOLOGI INFORMASI (STUDI KASUS BANK PEMBANGUNAN DAERAH JAWA TIMUR)

Terima kasih atas pihak-pihak yang telah mendukung, memberikan saran, motivasi, semangat, dan bantuan baik materi maupun spiritual demi tercapainya tujuan pembuatan tugas akhir ini. Secara khusus penulis akan menyampaikan ucapan terima kasih yang sedalam-dalamnya kepada:

1. Bapak Dr. Ir. Aris Tjahyanto, M.Kom selaku Kepala Departemen Sistem Informasi ITS Surabaya
2. Bapak Dr. Apol Pribadi S.,S.T.,M.T. selaku dosen pembimbing yang meluangkan waktu, memberikan ilmu, petunjuk, dan motivasi untuk kelancaran tugas akhir ini.
3. Ibu Eko Wahyu Tyas D, S.Kom, MBA dan Ibu Anisah Herdiyanti, S.Kom, M.Sc selaku dosen penguji yang telah memberikan masukan untuk perbaikan tugas akhir ini.
4. Bapak M.Arief R. Dan Bapak Adimas Indra selaku pembimbing penelitian di Bank Pembangunan Daerah Jawa Timur.
5. Orang tua penulis, Ir. Haryono Setyo dan Endah Dwi Winarni, yang telah memberikan dukungan material dan spiritual kepada penulis.
6. Saudara kandung penulis, Michelle Florencia yang turut mendokan dan mendukung penyelesaian tugas akhir.
7. Kawan MARKITDON yaitu Septy, Fia, Cindy Patty, Depe, Opor, Roy, Ninda, Rara, Tatan, Risha, Nita, Nody, Dhira, dan Yunis,.yang selalu menemani penulis dalam suka dan duka dan atas dukungan, candaan, dan nasihat yang selalu diberikan kepada penulis.

8. Kawan-kawan OSIRIS yang telah mengisi hari-hari penulis selama berkuliah di Departemen Sistem Informasi ITS.
9. Seluruh dosen Departemen Sistem Informasi ITS yang telah memberikan ilmu yang sangat berharga bagi penulis.
10. Berbagai pihak yang membantu dalam penyusunan Tugas Akhir ini dan belum dapat disebutkan satu per satu dengan dukungan, semangat, dan kebersamaan.

Penyusunan laporan ini masih jauh dari sempurna, untuk itu saya menerima adanya kritik dan saran yang membangun untuk perbaikan di masa mendatang. Semoga buku tugas akhir ini dapat memberikan manfaat bagi pembaca.

Surabaya, Juni 2018
Penulis,

(Rachel Carolina)

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

(Halaman ini sengaja dikosongkan)

BAB I
PENDAHULUAN

Pendahuluan berisi hal-hal yang mendorong atau hal-hal yang melatar belakangi pentingnya dilakukan Tugas Akhir.

1.1 Latar Belakang

Dalam dunia bisnis, Teknologi Informasi semakin banyak digunakan. Hal tersebut dikarenakan Teknologi Informasi yang membawa banyak manfaat bagi perusahaan seperti meningkatkan produktivitas, memungkinkan persebaran informasi secara realtime hingga dapat mengurangi biaya. Namun penerapan teknologi juga memiliki risiko yang harus bisa dikendalikan oleh perusahaan. Jika risiko dari teknologi informasi tidak dapat dikelola maka dampaknya dapat mengganggu aktivitas dalam proses bisnis perusahaan bahkan dapat melumpuhkan proses bisnis yang ada. Berdasarkan penelitian 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 Oleh karena itu, perusahaan yang menggunakan teknologi informasi dalam proses bisnisnya sangatlah perlu membuat perencanaan untuk menjamin keberlangsungan bisnis.

Perencanaan keberlangsungan bisnis atau *Business Continuity Plan* (BCP) adalah metodologi yang digunakan membuat dan memvalidasi untuk memelihara keberlangsungan operasional bisnis sebelum, saat dan setelah bencana maupun gangguan [1]. *Business Continuity Plan* berhubungan dengan mengidentifikasi, memperoleh, mengembangkan, mendokumentasikan serta menguji sumber daya dan prosedur sehingga proses bisnis kritis suatu organisasi dapat terjaga saat terjadi bencana atau insiden apapun [2]. Dalam menyusun

Business Continuity Plan, perusahaan dapat menggunakan beberapa standart yang ada seperti ISO 22301 dan COBIT 5. Namun, berdasarkan penelitian yang dilakukan oleh Yusrida, standart yang telah ada masih belum ada yang menyediakan tahap-tahap dalam menyusun *Business Continuity Plan* [3]. Karena keterbatasan pada standart terkait BCP yang ada saat ini, Yusrida melakukan penelitian dan membuat metodologi Business Continuity Planning.

Metodologi *Business Continuity Planning* adalah metodologi yang berisi panduan dalam membuat Perencanaan Keberlangsungan Bisnis. Metodologi BCP mengadopsi dari siklus Plan-Do-Check-Act. Siklus PDCA merupakan model yang terkenal untuk perbaikan proses secara terus menerus (*continual improvement*). PDCA mengakomodasi organisasi untuk merencanakan sebuah tindakan (*plan*), melakukan (*do*), memeriksa untuk melihat bagaimana hal itu sesuai dengan rencana (*check*) dan bertindak berdasarkan apa yang telah dipelajari (*act*) [3]. Tahap-tahap yang ada pada metodologi *Business Continuity Planning* disintesis dari standart terkait dengan *business continuity* yaitu ISO 22301:2012, COBIT 5 DSS04: Manage Continuity dan ITIL *IT Service Continuity Management* serta standart lain yang dapat mendukung pendetilan proses yaitu ISO 22317:2015 untuk pendetilan aktivitas pada tahap analisis dampak bisnis dan penyusunan strategi keberlangsungan bisnis, ISO 31000 untuk pendetilan aktivitas pada tahap analisis risiko, ISO 24762:2012 untuk pedetilan aktivitas pada tahap rencana pemulihan bencana [3].

Metodologi *Business Continuity Planning* baru diimplementasi pada PT.PLN (Persero) Distribusi Jawa Timur. Sehingga belum diketahui apakah metodologi dapat diimplementasi dalam pembuatan dokumen BCP pada bidang industri lainnya. Oleh karena itu, pada Tugas Akhir ini akan diteliti apakah semua tahapan pada metodologi *Business Continuity Planning* dapat diterapkan pada bidang industri lainnya. Pada tugas akhir ini metodologi Business Continuity Plan akan di implementasi

pada pembuatan dokumen BCP Bank Pembangunan Daerah Jawa Timur. Setiap tahapan pada metodologi akan dilakukan dalam pembuatan dokumen BCP Bank Pembangunan Daerah. Sehingga nantinya akan diketahui tahap yang dapat dan tidak dapat dilakukan pada bidang perbankan. Hasil yang diharapkan dalam tugas akhir ini adalah dokumen BCP yang dibuat berdasarkan metodologi Buisness Continuity Planning serta mengetahui tahapan apa saja pada metodologi yang dapat dilakukan pada bidang perbankan.

1.2 Rumusan Masalah

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

1. Bagaimana hasil implementasi metodologi *Business Continuity Planning* pada pembuatan dokumen perencanaan keberlangsungan bisnis pada Bank Pembangunan Daerah di Jawa Timur?
2. Apakah semua tahap pada metodologi *Business Continuity Planning* dapat dilakukan pada pembuatan dokumen BCP Bank Pembangunan Daerah Jawa Timur?

1.3 Batasan Masalah

Dalam permasalahan yang ada pada bagian atas, batasan masalah yang ada dalam tugas akhir ini adalah:

1. Penelitian akan dilakukan pada Bank Pembangunan Daerah pada Jawa Timur pusat yang ada di Surabaya.
2. Pengerjaan BCP akan berfokus kepada proses bisnis yang kritis dan risiko TI yang tingkatannya tinggi.
3. Penelitian akan berfokus kepada divisi teknologi informasi pada Bank Pembangunan Daerah.
4. Pengujian BCP yang dilakukan berupa skenario pengujian.

5. Pemantauan dan review hanya berupa formulir kuisioner.

1.4 Tujuan Penelitian

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

1. Menghasilkan dokumen BCP yang sesuai dengan metodologi *Business Continuity Planning*.
2. Mengetahui tahap pada metodologi *Business Continuity Planning* yang dapat dan tidak dapat dilaksanakan.

1.5 Manfaat Penelitian

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

a. Manfaat bagi Bank Pembangunan Daerah Jawa Timur
   - Divisi teknologi informasi pada Bank Pembangunan Daerah di Jawa Timur dapat memiliki dokumen perencanaan keberlangsungan bisnis.
   - Divisi teknologi informasi pada Bank Pembangunan Daerah Jawa Timur dapat mengetahui proses bisnis yang bersifat kritis serta risiko yang tingkatannya tinggi.

b. Manfaat Akademis
   - Mengetahui apakah semua tahap metodologi *Business Continuity Planning* bisa diterapkan pada industri perbankan sehingga dapat dilakukan penelitian lebih lanjut terkait dengan metodologi Business Continuity Plan.
   - Penelitian ini diharapkan dapat menambah pengetahuan dan dapat dijadikan referensi dalam pengembangan dokumen *business continuity plan* (BCP) yang menggunakan metodologi *Business Continuity Planning*

1.6 Relevansi

Tugas akhir ini akan berkaitan dengan mata kuliah Manajemen Risiko Teknologi Informasi dan Perencanaan Keberlangsungan Bisnis.

1.7 Sistematika Penulisan

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

BAB I PENDAHULUAN

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

BAB II TINJAUAN PUSTAKA

Bab ini berisi definisi dan penjelasan pustaka yang dijadikan referensi dalam pembuatan tugas akhir. Teori yang dijelaskan antara lain Risiko, Manajemen Risiko, *Business Continuity Plan* serta konsep-konsep lain yang berkaitan dengan pembuatan tugas akhir.

BAB III METODOLOGI

Bab ini menggambarkan uraian serta urutan pekerjaan yang dilakukan dalam penyusunan tugas akhir.

BAB IV PERANCANGAN

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

BAB V IMPLEMENTASI

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

BAB VI HASIL DAN PEMBAHASAN

Bab ini berisi tentang bagaimana proses implementasi metodologi Business Continuity Planning pada Bank Jatim serta bagaimana evaluasi dari implementasi metodologi.

BAB VII PENUTUP

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

BAB II
TINJAUAN PUSTAKA

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

2.1 Penelitian Sebelumnya

Dalam pengerjaan tugas akhir ini, perlu adanya pedoman dan referensi dari penelitian terdahulu untuk mendapatkan dasar teori dan masukan sebagai bahan dasar yang akan dipakai. Berikut adalah penjelasan mengenai deskripsi, metodologi, hasil serta keterkaitan dari penelitian terdahulu dengan tugas akhir ini yang akan disajikan dalam bentuk tabel:

Tabel 2.1-1Penelitian Sebelumnya

Business Continuity Plan : Sebuah Usulan Metodologi, Empiris PT PLN (Persero) Distribusi Jawa Timur [3]	
Nama Penulis	Yusrida Muflihah
Tahun Penelitian	2017
Deskripsi Umum Penelitian	Penelitian membahas mengenai formulasi metodologi pembuatan BCP yang didapatkan dari gabungan beberapa standard yang ada yang terkait dengan Business Continuity Management seperti ISO 22301:2012, COBIT 5 DSS04: Manage Continuity dan ITIL Service Design-IT Service Continuity Management dan Standard lainnya.
Hasil Penelitian	Elemen utama dalam pembuatan dokumen Business Continuity Plan dan hasil formulasi metodologi BCP yang mencakup panduan teknis pembuatan dokumen BCP
Keterkaitan Penelitian	Metodologi yang dihasilkan dari penelitian tersebut akan diterapkan

	dalam pembuatan dokumen BCP dalam tugas akhir ini.

Konsep Penyusunan Kerangka Kerja Business Continuity Plan Teknologi dan Sistem Informasi [4]	
Nama Penulis	Anindita Alisia Amanda
Tahun Penelitian	2014
Deskripsi Umum Penelitian	Penelitian membahas mengenai penyusunan kerangka *Business Continuity Plan* yang sesuai dengan kebutuhan perusahaan. Dalam penelitian tersebut kerangka Business Continuity Plan tersebut disintesis dari kerangka kerja ISO 22301:2012 serta kajian empiris dari Bank Of Japan dan Dutch Financial Sector.
Hasil Penelitian	Kerangka BCP yang disesuaikan dengan studi kasus BPR Bank Surya Yudha Banjarnegara dan disintesis dari ISO 22301:2012 , Bank Of Japan dan Dutch Financial Sector.
Keterkaitan Penelitian	Hasil elemen BCP yang memberikan pandangan akan implementasi BCP pada bidang perbankan,

Formulasi Strategi Untuk Acuan Dokumen Perencanaan Keberlangsungan Bisnis (BCP) Berbasis Teknologi di PT. Pertamina Refinery Unit IV Cilacap [5]	
Nama Penulis	Ulvi Rahma Isnaini
Tahun Penelitian	2016
Deskripsi Umum Penelitian	Penelitian ini membahas mengenai pembuatan strategi pada dokumen BCP pada PT. Pertamina Refinery Unit IV Cilacap
Hasil Penelitian	Penelitian menghasilkan dokumen BCP pada PT. Pertamina RU IV yang telah mengacu kepada ISO 22301, ISO 27301 dan penelitian Kartini Selamet.

Keterkaitan Penelitian	Penelitian menjadi acuan dalam menyusun format dokumen BCP dan buku Tugas Akhir.

2.2 Dasar Teori

2.2.1 Risiko

Berdasarkan ISO 31000, risiko merupakan dampak dari ketidak pastian dari tujuan yang hendak dicapai [6]. Sedangkan menurut NIST atau National Institute of Standards and Technology, risiko merupakan peluang terjadinya kehilangan sebagai akibat dari ketidakmampuan atau kegagalan dalam merespon potensi ancaman[7]. Menurut William Heins, risiko adalah variansi dari hasil yang terjadi selama periode tertentu. Sehingga risiko tidak bisa dipastikan kapan akan terjadi, namun bisa diketahui peluang atau kemungkinan terjadinya [8]. Mario Sprermic berpendapat jika risiko adalah kemungkinan (*likelihood*), sumber ancaman (*threat-source*) yang mengeksploitasi kerentanan (*vulnerability*) potensial yang mengakibatkan dampak (*impact*) berupa kejadian yang dapat merugikan organisasi. Priti Sikdar berpendapat bahwa risiko merupakan penggabungan dari aset, ancaman (threats) dan kerentanan (vulnerability)[9]. Akan terjadi potensi kehilangan jika ancaman mengeksploitasi kerentanan dari aset[10].

2.2.1.1 Komponen Risiko

Risiko memiliki beberapa komponen yaitu terdiri dari *event, asset, outcome* dan *probability.* Berikut ini merupakan penjelasan dari setiap komponen:

1. Event

Event merupakan peluang atau situasi dimana hal tersebut mungkin terjadi, namun tidak dapat dipastikan terjadinya. Event dalam konteks penilaian risiko dilihat dari kejadian yang akan datang. Identifikasi *event* merupakan aktivitas kunci dalam proses menilai risiko. Dalam proses penilaian risiko, *event-event* risiko dapat berpotensi menjadi ancaman.

2. Asset

Aset merupakan sumberdaya ekonomi yang dikuasai atau dimiliki oleh organisasi sebagai akibat peristiwa masa lalu dan dari mana manfaat ekonomi dan sosial di masa depan diharapkan dapat diperoleh, baik dari pemerintah maupun masyarakat, serta dapat diukur dalam satuan uang, termasuk sumber daya non keuangan yang diperlukan untuk penyediaan jasa bagi masyarakat umum dan sumber-sumber daya yang dipelihara. Salah satu jenis aset adalah aset informasi. Aset informasi merupakan bagian inti dari aset teknologi informasi. Aset informasi berisikan data dan informasi yang relevan dengan proses bisnis pada suatu organisasi. Aset informasi pada penelitian ini meliputi komponen-komponen pendukung yang meliputi:

a. Orang *(people)*
   Dalam tugas akhir ini komponen yang akan diidentifikasi adalah pengguna aplikasi yang ada di proses bisnis organisasi tersebut.
b. Data
   Dalam dunia teknologi informasi, yang disebut data adalah individu dalam sebuah database, yang disimpan dalam basis data untuk keperluan penyediaan informasi dalam tujuannya untuk mendukung perusahaan dalam menjalankan proses operasional.
c. Perangkat Keras
   Mencakup perangkat fisik, seperti komputer, printer, dan monitor. Perangkat ini berperan sebagai media yang bertugas untuk menyimpan dalam sistem informasi. Setiap perushaaan yang memiliki teknologi informasi yang maju pasti memiliki perangkat keras dengan jumlah yang banyak.
d. Perangkat Lunak
   Merupakan sekumpulan instruksi yang mempengaruhi kinerja dari perangkat keras dan pemroses data. Tujuan dari perangkat lunak adalah untuk mengolah

menghitung, dan memanipulasi data agar menghasilkan informasi yang berguna.

e. Jaringan
Merupakan sistem penghubung yang memungkinkan untuk suatu sumber dapat digunakan secara bersamaan dalam waktu dan tempat yang berbeda-beda. Sehingga kemudian kelima komponen tersebut saling berinteraksi dan dapat berfungsi sebagai pendukung dan penyedia kebutuhan informasi

3. Outcome

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

4. Probability

Probability merupakan peluang terjadinya suatu risiko di masa depan. Tujuan dari penilaian risiko adalah untuk mengukur suatu kemungkinan atau *likelihood* dari event risiko yang akan terjadi di masa depan. Berikut merupakan keterkaitan hubungan dan interaksi antara keempat komponen risiko yang telah dijelaskan sebelumnya hingga menjadi risiko.

Gambar 2.2-1 Keterkaitan Komponen Risiko

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

2.2.1.2 Jenis-jenis Risiko

Menurut Spremic, Risiko memiliki beberapa jenis yang dapat dilihat dari sifat dan penyebabnya. Berikut ini merupakan jenis-jenis risiko berdasarkan sifatmya:

1. Risiko yang tidak disengaja (risiko murni)

Risiko yang apabila terjadi akan menimbulkan kerugian dan terjadi karena tidak sengaja, misalnya kebakaran, bencana alam.

2. Risiko yang disengaja (risiko spekulatif

Risiko yang sengaja ditimbulkan, untuk memperoleh keuntungan.

3. Risiko Fundamental

Risiko yang penyebabnya tidak dapat dilimpahkan kepada seseorang dan yang menderita tidak hanya satu atau beberapa orang, misalnya angina topan, banjir.

4. Risiko Khusus

Risiko yang bersumber pada peristiwa yang mandiri dan umumnya diketahui penyebabnya, misalnya kapal kandas, pesawat jatuh.

Selain menurut sifatnya, berikut ini merupakan risiko berdasarkan penyebabnya:

1. Risiko Intern

Risiko yang berasal dari dalam perusahaan, misalnya kecelakaan pekerja.

2. Risiko Eksternal

Risiko yang berasal dari luar pekerjaan misalnya penipuan, perubahan politik.

Risiko yang akan dihadapi perusahaan yang menerapkan Teknologi adalah Risiko Teknologi Informasi. Risiko Teknologi Informasi (TI) merupakan risiko sebagai akibat dari penerapan TI di perusahaan. Hughes berpendapat mengenai penerapan teknologi informasi yang menimbulkan risiko kehilangan informasi perusahaan dan upaya apa yang dapat dilakukan untuk melakukan pemulihan. Upaya tersebut diantaranya:

1. Keamanan

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

2. Ketersediaan

Resiko yang berupa ketidaktersediaannya informasi saat dibutuhkan oleh perusahaan

3. Daya Pulih

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

4. Performa

Permintaan akan informasi yang meningkat dalam satuan waktu sehingga mengganggu performa.

5. Daya Skala

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

6. Ketaatan

Pelanggaran penggunaan IT dari peraturan maupun kebijakan yang sudah ditetapkan oleh pihak pengelola.

2.2.1.3 Risiko Teknologi Informasi

Teknologi informasi adalah penggunaan mesin dan program elektronik yang digunakan untuk memproses, menyimpan, mengirim, dan menyajikan informasi [11]. Sedangkan sistem informasi adalah kombinasi dari orang, *hardware*, *software,* jaringan komunikasi, data, kebijakan dan prosedur yang menyimpan, mengambil, merubah, dan menyebarkan informasi dalam sebuah organisasi [12].

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

2.2.2 Manajemen Risiko

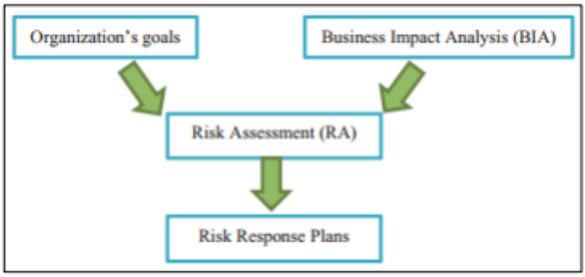
Manajemen risiko adalah ilmu dan seni untuk dapat mengenali keberadaan ancaman (*threats*), menentukan konsekuensinya terhadap sumber daya, dan menerapkan faktor modifikasi dengan biaya yang efektif untuk menjaga konsekuensi yang merugikan tetap dalam batas [13]. Menurut ISO 31000, manajemen risiko merupakan proses yang secara sistematik mengaplikasikan manajemen kebijakan, prosedur, dan praktek ke dalam kumpulan aktivitas dengan tujuan untuk membentukn mengkomunikasikan dan mengkonsultasikan dengan *stakeholder* dan mengidentifikasi, menganalisa, mengevaluasi, merespon, mengawasi dan mereview risiko.

Manajemen risiko mencakup tiga proses, yaitu penilaian risiko, mitigasi risiko dan evaluasi risiko. Penilaian risiko merupakan proses yang mencakup mengidentifikasi dan mencari dampak risiko serta membuat rekomendasi untuk meminimalisir risiko. Mitigasi risiko mencakup pada melakukan prioritisasi, implementasi dan pemeliharaan terhadap langkah-langkah untuk dapat mengurangi risiko yang direkomendasikan pada proses penilaian risiko. Evaluasi risiko merupakan tahap untuk melihat apakah risiko yang terjadi ada pada tingkat yang dapat diterima atau perlu dilakukan kontrol keamanan tambahan untuk mengurangi risiko [1]. Tahap-tahap yang perlu dilakukan dalam manajemen risiko menurut pendapat Spremic adalah sebagai berikut [9]:

1. Mengidentifikasi dan mengklarifikasi risiko.
2. Menilai setiap risiko.
3. Membuat langkah penanggulangan risiko.
4. Mendokumentasi dan mengimplementasi langkah penanggulangan risiko.
5. Melakukan pendekatan portfolio risiko TI.

6. Melakukan monitoring berkala terhadap tingkat risiko dan audit.

Salah satu tahapan yang dilakukan dalam manajemen risiko adalah penilaian risiko atau *risk assessment*. Penilaian risiko adalah metodologi dimana menggunakan informasi yang tersedia untuk mengetahui kemungkinan risiko yang terjadi serta bagimana risiko tersebut dapat mempengaruhi tujuan organisasi. Peniliaian risiko mencakup pada penilaian kemungkinan terjadinya risiko (*likelihood*) dan dampak risiko yang mengancam kegiatan organisasi serta mempersiapkan rencana respon terhadap risiko yang berdampak kritis bagi perusahaan. Menurut Torabi penilaian risiko memiliki hubungan dengan analisis dampak bisnis (*business impact analysis*) dan komponen BCMS [14].



Gambar 2.2-2 Keterkaitan antara penilaian risiko dengan BIA dan komponen BCMS [14]

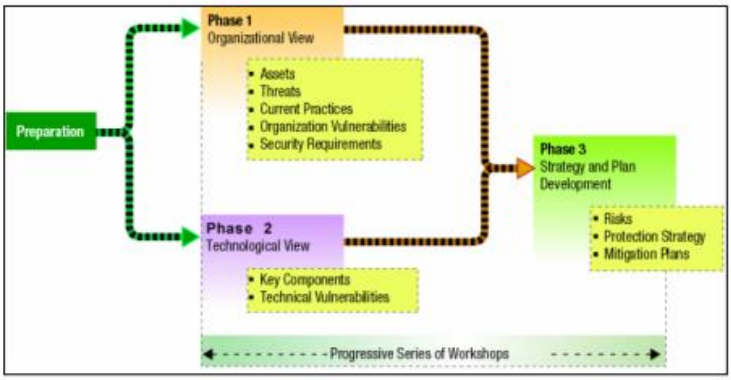
Penilaian risiko dan BIA memiliki keterkaitan dimana hasil dari keduanya digunakan untuk mengembangkan BCP yang sesuai untuk mengatasi risiko yang telah teridentifikasi. Selain itu luaran dari BIA seperti *minimum business continuity objective* (MBCO) dan *maximum tolerable period of disruption* (MTPD) bersama dengan hasil penilaian risiko digunakan untuk mempersiapkan respon dalam mengatasi risiko. Keterakitan penilaian risiko dengan tujuan organisasi yaitu penilaian risiko harus mampu memenuhi tujuan organisasi yaitu dalam hal mengetahui kemungkinan risiko akan terjadi serta respon terhadap risiko.

2.2.3 *Framework* OCTAVE

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) merupakan 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 [15]. Menurut Christoper, 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[16]. Metodologi ini memanfaatkan pengetahuan dari beberapa tingkat organisasi, fokus pada[17]:

1. Mengidentifikasi aset kritis dan ancaman pada aset
2. Mengidentifikasi kerentanan, baik dari segi organisasi dan teknologi yang dapat menjadi ancaman, dan membuat risiko kepada organisasi.
3. Mengembangkan strategi proteksi dan rencana mitigasi risiko untuk mendukung misi dan prioritas organisasi.

Metodologi OCTAVE menggunakan pendekatan dengan 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. Metodologi OCTAVE dibagi menjadi 8 proses : 4 proses terdapat di fase 1, 2 proses terdapat di fase 2 dan 2 proses lainnya terdapat di fase 3. Berikut merupakan tahapan dari metodologi OCTAVE [15].



Gambar 2.2-3 Tahapan OCTAVE

1. *Tahap Persiapan*
Dalam tahapan ini kegiatan persiapan yang harus dilakukan adalah menyusun jadwal, membentuk tim analisis, meminta dukungan dan menyiapkan logistic.

2. *Fase 1 : Membangun Aset Berbasis Profil Ancaman* Fase ini merupakan fase dari evaluasi dari pandangan organisasi (organizational view). Tim analisis akan menentukan apa saja aset yang penting bagi suatu organisasi serta apa saja yang dilakukan untuk menjaga aset tersebut. Setelah itu akan diidentifikasi masing masing ancaman untuk tiap aset kritis sehingga akan menghasilkan profil ancaman untuk aset. Proses - proses yang ada pada fase 1 adalah sebagai berikut.
- Proses 1 : Mengidentifikasi pengetahuan dari senior manajemen
- Proses 2 : Mengidentifikasi pengetahuan mengenai area operasional
- Proses 3 : Mengidentifikasi pengetahuan dari staf
- Proses 4 : Membuat profil ancaman

3. *Fase 2 : Mengidentifikasi Kerentanan Infrastruktur*
Fase ini merupakan fase yang melihat dari pandangan teknologi (technological view). Pada fase ini akan dilakukan evaluasi terhadap infrastruktur. Pada fase ini terdapat pemeriksaan jalur

akses jaringan, identifikasi masing masing kelas dari komponen TI yang berkaitan dengan aset kritis. Luaran dari tahapan ini adalah berupa komponen penting dalam aset kritis dan kelemahan infrastruktur TI yang ada saat ini. Proses - proses yang ada pada fase 2 adalah sebagai berikut.

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

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

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

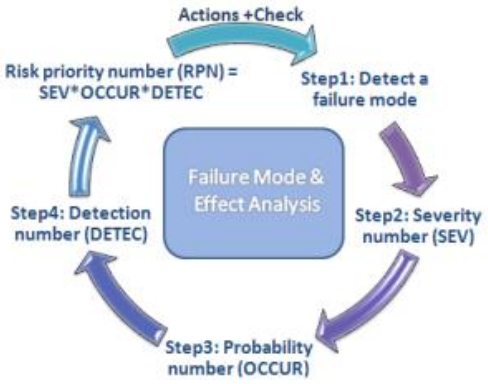
- Proses 8 : Menjalankan analisis risiko
- Proses 9 : Mengembangkan strategi perlindungan

2.2.4 Metodologi FMEA

FMEA (Failure Mode and Effects Analysis) merupakan metodologi sistematis yang digunakan untuk melakukan identifikasi 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. Metodologi ini di desain untuk dapat mengidentifikasi dan memahami secara penuh potensi kegagalan serta penyebabnya dan juga dampak kegagalan kepada sistem dan pengguna untuk produk dan proses, menilai risiko yang berasosiasi dengan identifikasi mode kegagalan, dampak dan penyebab serta prioritisasi masalah untuk tindakan korektif, dan mengidentifikasi dan melaksanakan tindakan korektif [18]. FMEA ini memiliki tujuan untuk menghindari terjadi kegagalan. FMEA mengidentifikasi tiga hal, yaitu [19]:

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

Proses yang dilakukan dalam penerapan FMEA adalah mengukur potensi terjadinya kegagalan tersebut melalui tiga komponen. Tahapan dari FMEA digambarkan pada diagram alur berikut [20]:



Gambar 2.2-4 Proses FMEA

Gambar tersebut merupakan alur yang menunjukkan tahapan dalam mengidentifikasi dari potensi kegagalan sistem atau proses, diantaranya:

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

Penilaan risiko dengan metodologi FMEA dilakukan dengan menentukan nilai severity, occurance, dan detection. Berikut ini penjelasan untuk setiap komponen:

1. *Severity* (tingkat keparahan) /*Impact*

Tingkat keparahan atau severity merupakan pengukuran dalam memperkirakan secara numerik dari seberapa parak akibat dari risiko yang terjadi pada para pekerja/pihak ketiga/pelanggan. Pengukuran nilai dampak akan dilihat seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek aspek penting dalam organisasi. Terdapat tiga aspek yang akan dijabarkan yaitu aspek jadwal, aspek biaya dan aspek teknis. Berikut merupakan penjelasan dari kriteria nilai dampak [21].

Tabel 2.2-1 Kriteria Penilaian Severity

Dampak	Dampak dari Efek	Ranking
Akibat Berbahaya	Melukai pelanggan atau karyawan	10
Akibat Serius	Aktivitas yang ilegal	9
Akibat Ekstrim	Mengubah produk atau jasa menjadi tidak layak untuk 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 diatasi tanpa kehilangan sesuatu	3
Akibat Sangat Ringan	Tanpa disadari terjadi gangguan kecil pada kinerja	2
Tidak Ada Akibat	Tanpa disadari dan tidak mempengaruhi kinerja	1

2. *Occurance* (Nilai Kemungkinan) Likelihood

Nilai kemungkinan atau *occurence* adalah pengukuran terhadap tingkat frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat mengakibatkan kegagalan. Berikut merupakan pejelasan dari kriteria kemungkinan [21].

Tabel 2.2-2 Kriteria Penilaian Occurance

Kemungkinan Kegagalan	Kemungkinan	Ranking
Very High: Kegagalan hampir/ tidak dapat dihindari	Lebih dari satu 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 sebulan	7
Moderately high: Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan	6
Moderate: Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan	5
Moderate Low: Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relatif kecil	Satu kali dalam 1-3 tahun	3
Very Low: Kegagalan terjadi relatif kecil	Satu kali dalam 3-6 tahun	2
Remote: Kegagalan tidak pernah terjadi	Satu kali dalam 6-50 tahun	1

3. *Detection* (deteksi) / Cause

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 [21].

Tabel 2.2-3 Kriteria Penilaian Detection

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

Nilai dari *severity*, *occurence*, dan *detection* kemudian dikalkulasikan hingga menghasilkan nilai RPN atau risk priority number. Berikut adalah rumus untuk menghitung RPN [19] .

RPN= Severity * Occurence * Detection

Skala Nilai RPN yang didapat dari perhitungan akan menghasilkan level resiko tertentu. Berikut merupakan skala penentuan level risiko berdasarkan nilai RPN.

Tabel 2.2-4 Skala Nilai RPN[19]

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

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

2.2.5 Business Impact Analysis

2.2.5.1 Faktor-faktor Dampak Bisnis

Dampak kehilangan dari gangguan *downtime* Teknologi Informasi pada bisnis dapat berupa tangible maupun intangible. Berikut ini merupakan dampak kerugian tangible [10]:

1. L*ost Revenue:* Kehilangan pendapatan dapat terjadi saat downtime terutama kepada aplikasi yang 24 jam mengandalkan sistem untuk melakukan penjualan. Cara untuk mengestimasi kehilangan adalah dengan mengkalkulasikan penjualan normal setiap jam dikalikan dengan jumlah *downtime*.
2. *Lost Productivity*: Terdapat waktu yang terhenti saat sistem sedang *down.* Pegawai harus dibayar saat waktu terhenti sehingga menimbulkan tambahan beban biaya.
3. *Late Fees and Penalties:* Ketika pengiriman terlambat, SLA yang ada memiliki kekuasaan untuk memberikan denda dan hukuman. Ketidaktaatan terhadap norma peraturan juga dapat menimbulkan denda.

Dalam bisnis terdapat beberapa jenis dampak yang ditimbulkan akibat gangguan, berikut ini merupakan jenis dampak dari gangguan[10]:

1. Dampak Finansial
    a. Kehilangan penjualan dan pendapatan
    b. Penambahan pengeluaran
    c. Denda
2. Dampak Operasional
    a. Ketidakpuasan customer
    b. Penundaan rencana bisnis
3. Dampak reputasi
4. Penurunan penjualan
5. Dampak hukum dan undang-undang

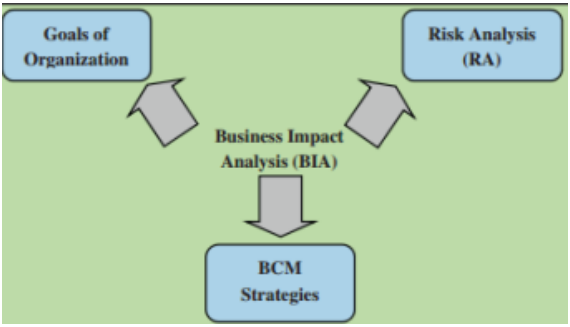
2.2.5.2 Definisi *Business Impact Analysis*

Business Impact Analysis (BIA) merupakan suatu dokumen yang mengidentifikasi proses bisnis kritikal, perkiraan dampak bencana terhadap unit bisnis, dan kebutuhan sumber daya yang diperlukan dalam pemulihan. Menurut Torabi, *business impact analysis* (BIA) merupakan langkah awal dalam proses perencanaan BCP [14]. Berdasarkan ISO 22301:2012, BIA merupakan suatu proses penilaian dari dampak yang terjadi pada aktivitas-aktivitas yang mendukung produk maupun layanan dari suatu organisasi atau perusahaan [22]. *Business Impact Analysis* juga meliputi tiga hal yaitu identifikasi fungsi bisnis yang penting dalam organisasi, menentukan dampak bisnis dari terhentinya fungsi bisnis serta memastikan implikasi biaya [23]. Dari perspektif Teknologi Informasi yang dilihat oleh NIST, BIA bertujuan untuk mengkorelasikan komponen spesifik dari sistem dengan layanan kritis yang disediakan, dan berdasarkan dari informasi tersebut untuk mengkarakteristikan akibat dari gangguan kepada komponen sistem [7].

Tujuan utama dari BIA adalah mengumpulkan dan menganalisis informasi yang diperlukan untuk mempersiapkan perencanaan keberlangsungan bisnis [10]. Menurut *National*

Institute of Standards and Technology (NIST) BIA merupakan salah satu aktivitas yang bertujuan untuk menkorelasikan sistem dengan proses bisnis maupun layanan yang tersedia dan dari informasi tersebut di dapat karakterisasi dari konsekuensi yang ada pada setiap [10]. *Business Impact Analysis* digunakan untuk melakukan identifikasi proses bisnis dan sumber daya yang mendukung proses yang sangat penting bagi perusahaan [24]. Beberapa tujuan lain dari *Business Impact Analysis*, diantaranya (1) identifikasi potensi risiko, (2) memperkirakan efek dari bencana pada organisasi secara keseluruhan, (3) menentukan kebutuhan untuk strategi pemulihan termasuk sumber daya yang diperlukan, (4) memberikan justifikasi keuangan atas bencana, (5) menentukan tingkat kritis setiap fungsi bisnis berdasarkan dampak keseluruhan organisasi, dan (6) menentukan jangka waktu pemulihan [23].

Business Impact Analysis (BIA) memiliki keterkaitan dengan tiga hal yaitu tujuan organisasi, analisis risiko dan strategi BCM seperti yang digambarkan pada gambar berikut [14].



Gambar 2.2-5 Keterkaitan BIA

Keterkaitan BIA dengan tujuan organisasi ditunjukkan dengan proses BIA yang tepat harus mempertimbangkan tujuan organisasi dan tidak bertentangan dengan tujuan tersebut. Keterkaitan antara BIA dengan analisis risiko dikarenakan hasil dari keduanya digunakan untuk mengembangkan rencana keberlangsungan bisnis yang sesuai. Sedangkan, keterkaitan

BIA dengan strategi BCM yaitu strategi BCM menjaga kelangsungan fungsi utama organisasi berdasarkan dengan hasil dari BIA, oleh karena itu validitas rencana keberlangsungan bisnis tergantung pada hasil BIA.

2.2.6 Business Continuity Plan

2.2.6.1 Definisi Business Continuity Plan

Berdasarkan 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 [22]. Menurut Venclova, *Business Continuity* adalah sebuah kegiatan yang dilakukan oleh organisasi untuk memastikan bahwa fungsi bisnis kritis akan tersedia untuk pelanggan, pemasok, dan entitas lain yang memiliki akses ke fungsi fungsi tersebut [25]. *Business Continuity Plan* adalah proses mengidentifikasi fungsi bisnis yang penting, memprioritaskan sumber daya untuk mendukung fungsi-fungsi, dan mengembangkan strategi untuk mempertahankan operasi sebelum gangguan bisnis atau peristiwa krisis [24]. BCP merupakan suatu proses berkelanjutan dalam melakukan identifikasi terhadap bencana dan kerentanan dari organisasi, kemungkinan terjadinya bencana, potensi konsekuensi terhadap tujuan dan keberhasilan strategi, keefektifan kontrol yang berlaku dan strategi untuk meningkatkan kinerja dan efisiensi [26]. *Business continuity planning* (BCP) adalah suatu proses identifikasi dan proteksi terhadap proses yang bisnis kritis serta 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 [27]. Selain itu, definisi *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 [28]. Menurut Snedaker BCP adalah suatu metodologi yang digunakan untuk membuat dan memvalidasi rencana untuk mempertahankan operasi bisnis secara terus menerus, sebelum, selama dan setelah bencana dan insiden yang mengganggu [29]. *Business Continuity Plan* berhubungan dengan mengidentifikasi, memperoleh, mengembangkan, mendokumentasikan serta menguji sumber daya dan prosedur sehingga proses bisnis kritis suatu organisasi dapat terjaga saat terjadi bencana atau insiden apapun [2].

2.2.7 Metodologi Busines Continuity Planning

2.2.7.1 Definisi Metodologi Business Continuity Planning

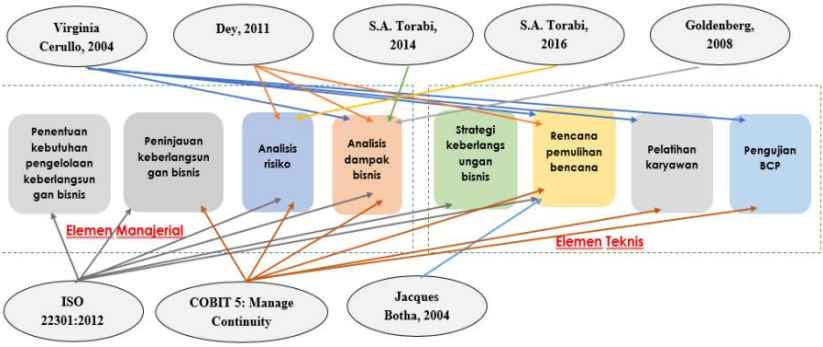
Metodologi Business Continuity Plan adalah metodologi untuk membuat dokumen perencanaan keberlangsungan bisnis. Metodologi Business Continuity Plan ini dikembangkan karena standar terkait dengan *Business Continuity Management* yaitu ISO 22301:2012, COBIT 5 DSS04: Manage Continuity, ITIL Service Design-IT Service Continuity Management masih belum dapat dijadikan sebagai panduan langsung untuk *Business Continuity Plan*, masih kurangnya pemahaman mengenai elemen utama dari perancangan *business continuity plan*, sehingga BCP yang dimiliki perusahaan masih mengalami kekurangan dalam kelengkapan strategi kelangsungan bisnis, penelitian terdahulu masih fokus pada metodologi BCP sesuai dengan objek penelitian masing-masing, tidak sampai mendetilkan mengenai elemen utama dari *Business Continuty Plan*, masih belum ada kecukupan panduan mengenai *Business Continuity Plan* serta *Business Continuity Plan* bersifat unik dan berbeda setiap perusahaan. Beberapa permasalahan tersebut mengarah pada penelitian mengenai metodologi *Business Continuity Plan* yang dapat dijadikan panduan dalam merencanakan kelangsungan bisnis [3].

Metodologi BCP mengadopsi dari siklus Plan-Do-Check-Act. Siklus PDCA merupakan model yang terkenal untuk perbaikan proses secara terus menerus (*continual improvement*). PDCA

mengakomodasi organisasi untuk merencanakan sebuah tindakan (*plan*), melakukan (*do*), memeriksa untuk melihat bagaimana hal itu sesuai dengan rencana (*check*) dan bertindak berdasarkan apa yang telah dipelajari (*act*). Untuk pendetilan aktivitas yang ada dari proses, metodologi BCP disintesis dari standart terkait dengan *business continuity* yaitu ISO 22301:2012, COBIT 5 DSS04: Manage Continuity dan ITIL *IT Service Continuity Management* serta standart lain yang dapat mendukung pendetilan proses yaitu ISO 22317:2015 untuk pendetilan aktivitas pada tahap analisis dampak bisnis dan penyusunan strategi keberlangsungan bisnis, ISO 31000 untuk pendetilan aktivitas pada tahap analisis risiko, ISO 24762:2012 untuk pedetilan aktivitas pada tahap rencana pemulihan bencana.

2.2.7.2 Elemen Metodologi BCP

Elemen yang ada pada metodologi BCP menggunakan beberapa literatur yang membahas mengenai elemen dari *Business Continuity Plan* serta beberapa standart terkait dengan Business Continuity seperti ISO 22301:2012 dan COBIT 5Domain: *Manage Continuity*. Berdasarkan fokusnya, elemen pada BCP dibagi menjadi dua, yaitu elemen manajerial dan elemen teknis[3]. Elemen manajerial terdiri dari penentuan kebutuhan keberlangsungan bisnis, peninjauan keberlangsungan bisnis, analisis risiko, analisis dampak bisnis. Sedangkan elemen teknis terdiri dari rencana pemulihan bencana, pelatihan karyawan dan pengujian BCP.



Gambar 2.2-6 Rangkuman elemen *BCP*

Berikut ini merupakan pembahasan dari setiap elemen BCP:

1. **Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis**

   Berdasarkan ISO/TC 233 organisasi perlu untuk menentukan kebutuhan dalam mengelola keberlangsungan bisnis[22]. Kebutuhan tersebut terkait dengan pendefisian dari peran manajemen, tujuan, ruang lingkup, dan komunikasi dengan pihak terkait. Sehingga pendetilan dari kebutuhan awal lingkup manajemen terkait dengan tujuan, ruang lingkup, peran manajemen, sumberdaya serta komunikasi menjadi fokusan elemen ini [3].

2. **Peninjauan Keberlangsungan Bisnis**

   Agar memastikan kemampuan keberlangsungan serta keefektivitasan dan pengaturan perubahan rencana yang disesuaikan dengan kontrol agar rencana keberlangsungan dapat diperbaharui sehingga sesuai dengan kebutuhan bisnis, maka diperlukan adanya peninjauan terhadap keberlangsungan bisnis yang telah ditetapkan[30]. Peninjauan keberlangsungan bisnis dilakukan dengan melakukan review terhadap keberlangsungan bisnis secara objektif dan melaporkan hasilnya kepada manajemen untuk menentukan tindakan dalam memperbaiki dan meningkatkan performa (Technical Committee ISO/TC 223, 2012). Peninjauan keberlangsungan bisnis yang dilihat dari kemampuan dan keefektifan keberlangsungan bisnis yang

ditetapkan dalam rencana keberlangsungan bisnis serta memberikan *feedback* dari ketidaksesuaian keberlangsungan bisnis yang digunakan untuk memperbaiki dan meningkatkan kinerja keberlangsungan menjadi fokus dari elemen ini [3].

3. **Analisis Risiko**

   Analisis risiko merupakan elemen yang dimana dilakukan identifikasi risiko dengan dampaknya terhadap perusahaan kemudian penilaian risiko juga melibatkan kemungkinan terjadinya risiko serta dampaknya yang mengancam bisnis organisasi juga mempersiapkan rencana respon terhadap risiko yang berdampak kritis untuk perusahaan[14]. Sehingga dapat diketahui bahwa fokus dari elemen ini adalah mengidentifikasi kemungkinan terjadinya risiko, menilai risiko dan dampak risiko.

4. **Analisis Dampak Bisnis**

   Analisis dampak bisnis mencakup pada proses mengidentifikasi, memprioritasi, klasifikasi fungsi bisnis kritis serta denfan asset dan menentukan jangka waktu maksimum toleransi gangguan. Analisis dampak bisnis melakukan tiga tahapan yaitu identifikasi fungsi bisnis, identifikasi risiko terhadap fungsi bisnis penting, serta identifikasi dampak risiko terhadap bisnis. Analisis dampak bisnis merupakan proses menganalisis fungsi operasional dan efek yang mungkin timbul dari adanya gangguan [22]. Sehingga elemen analisis dampak bisnis fokus kepada identifikasi dan prioritisasi fungsi bisnis dan aset, penentuan jangka waktu toleransi gangguan dan identifikasi dampak gangguan.

5. **Strategi Keberlangsungan Bisnis**

   Dalam keberlangsungan bisnis di organisasi, penentuan strategi keberlangsungan bisnis diperlukan. Strategi keberlangsungan bisnis dilakukan dengan menentukan pertanggungjawaban atas dampak gangguan yang mengganggu proses bisnis dan mengembangkan prosedur untuk mengelola kerusakan atau gangguan yang terjadi [22]. Sehingga, dapat disimpulkan bahwa elemen ini berfokus

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

6. **Rencana Pemulihan Bencana**

   Rencana pemulihan bencana dilakukan dengan menangani insiden, pemulihan kerusakan dan kerugian serta pengembalian kegiatan kepada keadaaan seperti sedia kala [31]. Rencana pemulihan bencana spesifik kepada prosedur yang diterapkan saat terjadi bencana, yang mencakup identifikasi anggota tim beserta perannya, proses menjaga dan memulihkan gangguan, daftar kontak penting, daftar vendor baik eksternal maupun internal maupun alternatif vendor [32]. Sehingga, dapat disimpulkan bahwa elemen ini fokus pada penanganan insiden, prosedur saat gangguan beserta detil mengenai pihak yang bersangkutan, pemulihan gangguan.

7. **Pelatihan Karyawan**

   Pelatihan dilakukan bagi internal maupun eksternal yang terkait dengan prosedur dan tanggung jawab ketika terjadi gangguan. Pelatihan yang dilakukan mencakup pra-pelatihan yaitu mekanisme penyampaian pelatihan, pelaksanaan pelatihan yang terdiri dari latihan dan ujian, serta pasca-pelatihan yaitu memantau kompetensi berdasarkan hasil latihan dan ujian[30]. Sehingga, dapat disimpulkan bahwa elemen pelatihan karyawan berfokus kepada proses pelatihan yang mencakup mekanisme penyampaian pelatihan, pelaksanaan pelatihan yang terdiri dari latihan dan ujian, dan pemantauan kompetensi berdasarkan hasil latihan dan ujian.

8. **Pengujian BCP**

   Pengujian meliputi pembuatan alur pengujian, pengujian dan perbaikan dari BCP [32]. Sehingga, dapat disimpulkan bahwa elemen pengujian BCP berdokus kepada pembuatan alur pengujian, pengujian dan perbaikan berdasarkan hasil pengujian yang dilakukan.

2.2.7.3 Tahap-tahap dalam metodologi BCP

Metodologi Business Continuity Planning atau metodologi BCP memiliki beberapa tahap dalam membuat BCP. Berikut ini merupakan fase-fase yang ada pada metodologi *Business Continuity Plan* [3] :

Gambar 2.2-7 Fase 1: Perencanaan

1. Penentuan Kebutuhan Keberlangsungan Bisnis

Penentuan kebutuhan pengelolaan keberlangsungan bisnis fokus pada pendetilan kebutuhan awal pada lingkup manajemen terkait dengan tujuan, ruang lingkup, peran manajemen, sumber daya dan komunikasi.

Aktivitas:

1. Menentukan tujuan dari adanya perencanaan keberlangsungan bisnis pada perusahaan.
2. Menentukan ruang lingkup yang akan menjadi bagian dari perencanaan keberlangsungan bisnis.
3. Melakukan pemebentukan komite BCP, komite BCP ini yang akan bertanggungjawab mengenai perencanaan keberlangsungan bisnis perusahaan.
4. Menentukan tanggungjawab dari tiap bagian dalam komite BCP.
5. Menentukan pihak internal atau eksternal yang berkaitan dengan kelangsungan bisnis perusahaan.

6. Menentukan sumber daya baik manusia maupun perangkat untuk dapat memastikan bahwa proses berjalan dengan lancar dan sesuai dengan perencanan.
7. Membuat alur komunikasi saat terjadi gangguan dalam perusahaan beserta dengan kontak dari pihak yang akan dihubungi.

Gambar 2.2-8 Fase 2: Implementasi

2. Analisis Risiko

Analisis risiko berfokus pada identifikasi kemungkinan terjadinya risiko, penilaian risiko dan dampak dari risiko.

Aktivitas:

1. Melakukan pendataan risiko yang mungkin dapat diterima oleh perusahaan berdasarkan komponen TI yaitu hardware, software, data, jaringan, prosedur dan manusia.
2. Melakukan analisis dari setiap risiko untuk mengetahui kemungkinan penyebab terjadinya risiko.
3. Memberikan nilai pada setiap risiko yang telah diidentifikasi berdasarkan aspek tingkat kemungkinan terjadinya risiko, tingkat dampak yang ditimbulkan dari

risiko, dan tingkat kemampuan perusahaan untuk mendeteksi terjadinya suatu risiko.

3. Analisis Dampak Bisnis

Analisis dampak bisnis berfokus pada identifikasi dan prioritisasi fungsi bisnis beserta dengan aset, penentuan jangka waktu toleransi gangguan, dan identifikasi dampak dari adanya gangguan.

Aktivitas:

1. Melakukan pendataan proses bisnis perusahaan beserta layanan TI yang mendukung.
2. Melakukan prioritisasi dari layanan TI sesuai dengan tingkat kritisnya yaitu sangat kritis, penting atau minor.
3. Melakukan prioritisasi proses bisnis perusahaan sesuai dengan tingkat kritisnya yaitu sangat kritis, penting atau minor.
4. Melakukan analisis dampak dari adanya gangguan, dengan melakukan analisis berdasarkan tiga aspek yaitu finansial, reputasi dan target teknis.
5. Menentukan waktu pemulihan pada tiap layanan TI, dimana terdapat tiga waktu yang ditentukan yaitu *Maximum Tolerable Downtime* (MTD), *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO).

4. Penyusunan Strategi Keberlangsungan Bisnis

Penyusunan strategi keberlangsungan bisnis fokus pada penentuan pertanggungjawaban atas dampak gangguan yang mengganggu proses bisnis dan pengembangan prosedur pengelolaan kerusakan atau gangguan.

Aktivitas:

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

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

5. Perencanaan Pemulihan Bencana

Perencanaan pemulihan bencana fokus pada penanganan insiden, prosedur saat bencana beserta detil mengenai pihak yang bersangkutan dan pemulihan bencana.

Aktivitas:

1. Melakukan pendataan asset TI yang dimiliki oleh perusahaan.
2. Melakukan pendataan vendor jasa atau produk yang dibutuhkan dan digunakan oleh perusahaan beserta dengan tanggung jawabnya.
3. Menentukan lokasi server atau asset TI yang aman terhadap bencana
4. Membuat bentuk kontrol dari bencana atau gangguan yang didasarkan pada kategori kontrol yaitu pencegahan sumber masalah (*preventive control*), pendeteksi sumber masalah saat bencana terjadi (*detective control*), dan pengurangan dampak (*corrective control*).
5. Menentukan bilamana akan dilakukan aktivasi pemulihan mulai dari deklarasi status sampai kepada de-aktivasi atau status dimana dapat beroperasi kembali.
6. Membuat skenario pengujian dan melakukan simulasi pengujian.
7. Melakukan evaluasi hasil pengujian dan merivisi bentuk kontrol dari rencana pemulihan bencana.

6. Pelatihan Karyawan

Pelatihan karyawan fokus pada proses pelatihan yang mencakup mekanisme penyampaian pelatihan, pelaksanaan

pelatihan yang terdiri dari latihan dan ujian, dan pemantauan kompetensi berdasarkan hasil latihan dan ujian.
Aktivitas:

1. Menentukan jenis pelatihan yang sesuai dengan kebutuhan perusahaan.
2. Menentukan mekanisme penyampaian pelatihan.
3. Merancang dan memenuhi sumber daya yang diperlukan dalam melaksanakan pelatihan.
4. Melaksanakan pelatihan sesuai dengan mekanisme yang telah ditentukan.

Gambar 2.2-9 Fase 3: Pemantauan & Review

7. Pengujian BCP

Pengujian BCP fokus pada pembuatan alur pengujian, pengujian dan perbaikan berdasarkan hasil pengujian yang dilakukan.
Aktivitas:

1. Merencanakan mekanisme pengujian termasuk metode pengujian dan menyusun alur pengujian.
2. Melakukan pengujian sesuai dengan metode dan rencana pengujian yang telah ditentukan.
3. Melakukan pencatatan temuan selama proses pengujian berlangsung.

4. Mendokumentasikan hasil pengujian untuk dijadikan masukan atau rekomendasi dalam peninjauan keberlangsungan bisnis.

Gambar 2.2-10 Fase 4: Pemeliharaan & Peningkatan

8. Peninjauan Keberlangsungan Bisnis

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

Aktivitas:

1. Menentukan periode waktu peninjauan keberlangsungan bisnis.
2. Melakukan peninjauan keberlangsungan bisnis secara berkala.
3. Melakukan analisis ulang terhadap adanya dampak, risiko, dan strategi baru terkait dengan rencana keberlangsungan bisnis yang telah diterapkan.
4. Melakukan pertimbangan terhadap perubahan dari rencana keberlangsungan bisnis yang telah ditetapkan

(Halaman ini sengaja dikosongkan)

BAB III
METODOLOGI

Pada bab ini akan menjelaskan bagaimana pelaksanaan penelitian untuk membuat dokumen perencanaan keberlangsungan bisnis di Bank Pembangunan Daerah Jawa Timur. Berikut adalah Penjelasan pelaksanaan yang disajikan dalam bentuk gambar alur proses secara runtut dan bertahap.

3.1 Tahapan Pelaksanaan Tugas Akhir

Gambar 3.1-1 Metodologi Penelitian

3.2 Penjabaran Metodologi Penelitian

Berikut ini merupakan penjelasan-penjelasan uraian dari metodologi pengerjaan tugas akhir:

3.2.1 Identifikasi Masalah

Pada tahap identifikasi masalah, dilakukan identifikasi terhadap permasalahan yang akan diangkat dalam penelitian tugas akhir. Input atau masukan untuk tahap identifikasi masalah ini adalah adanya kekurangan pada penelitian terdahulu. Penelitian dalam hal ini adalah metodologi BCP yang dibuat oleh Yusrida Muflihah. Hasil dari tahap identifikasi masalah ini adalah berupa latar belakang dan rumusan masalah.

3.2.2 Studi Literatur

Pada tahap studi literatur yang dilakukan adalah mempelajari jurnal, paper, penelitian TA dan buku-buku referensi lainnya untuk dapat memahami dan mengerti gambaran mengenai konsep BCP dan apa saja yang berhubungan dengan BCP.

3.2.3 Pengumpulan Data

Berdasarkan dari studi literatur dan permasalahan yang di definisikan dilakukan pengumpulan data pada Bank Pembangunan Daerah terkait dengan pembuatan dokumen BCP yang sesuai dengan metodologi BCP. Pengumpulan data dilakukan dengan observasi, wawancara maupun diskusi dengan pihak terkait pada departemen Teknologi Informasi Bank Pembangunan Daerah. Proses pengumpulan data dilakukan selama tahapan implementasi metodologi BCP.

3.2.4 Pembuatan Dokumen BCP

Jika data-data yang dibutuhkan telah terkumpul, maka data diolah menjadi dokumen BCP. Metodologi *Business Continuity Planning* diimplementasi dalam pembuatan dokumen BCP. Dalam membuat dokumen BCP dengan menggunakan metodologi *Business Continuity Planning* terdapar beberapa

langkah yang harus dilakukan. Berikut ini langkah-langkah pada metodologi *Business Continuity Planning*.

3.2.4.1 Menentukan Kebutuhan Perencanaan Keberlangsungan Bisnis

Tahap ini merupakan tahapan awal dari metodologi BCP. Penentuan kebutuhan perencanaan keberlangsungan bisnis berfokus kepada pendetilan dari kebutuhan awal pada lingkup manajemen terkait dengan tujuan, ruang lingkup, peran manajemen, sumberdaya dan komunikasi. Adapun berikut ini merupakan aktivitas dari tahap ini:

1. Menentukan tujuan dari adanya perencanaan keberlangsungan bisnis pada perusahaan.
2. Menentukan ruang lingkup yang akan menjadi bagian dari perencanaan keberlangsungan bisnis.
3. Melakukan pemebentukan komite BCP, komite BCP ini yang akan bertanggung jawab mengenai perencanaan keberlangsungan bisnis perusahaan.
4. Menentukan tanggungjawab dari tiap bagian dalam komite BCP.
5. Menentukan pihak internal atau eksternal yang berkaitan dengan kelangsungan bisnis perusahaan.
6. Menentukan sumber daya baik manusia maupun perangkat untuk dapat memastikan bahwa proses berjalan dengan lancar dan sesuai dengan perencanan.
7. Membuat alur komunikasi saat terjadi gangguan dalam perusahaan beserta dengan kontak dari pihak yang akan dihubungi

3.2.4.2 Melakukan Analisis Risiko

Tahap analisis risiko merupakan tahap untuk melakukan identifikasi risiko beserta dampaknya pada organisasi serta penilaian risiko dan dampak risiko yang mengancam kegiatan organisasi serta mempersiapkan rencana untuk risiko yang dampaknya kritis bagi perusahaan. Aktivitas analisis risiko pada metodologi BCP disintesis dari ISO 31000 yaitu pada tahapan menilai risiko. Berikut ini detil aktivitas dari tahap analisis risiko:

1. Melakukan pendataan risiko yang mungkin dapat diterima oleh perusahaan berdasarkan komponen TI yaitu hardware, software, data, jaringan, prosedur dan manusia.
2. Melakukan analisis dari setiap risiko untuk mengetahui kemungkinan penyebab terjadinya risiko.
3. Memberikan nilai pada setiap risiko yang telah diidentifikasi berdasarkan aspek tingkat kemungkinan terjadinya risiko, tingkat dampak yang ditimbulkan dari risiko, dan tingkat kemampuan perusahaan untuk mendeteksi terjadinya suatu risiko.

3.2.4.3 Melakukan Analisis Dampak Bisnis

Pada tahap analisis dampak bisnis didapatkan dari sintesis ISO 22317:2015 mengenai *Business Impact Analysis*. Tahap ini berfokus kepada identifikasi dan prioritisasi fungsi bisnis serta aset, penentuan jangka waktu toleransi gangguan, serta identifikasi dampak dari gangguan pada perusahaan. Berikut ini merupakan aktivitas yang dilakukan dalam tahap ini:

1. Melakukan pendataan proses bisnis perusahaan beserta layanan TI yang mendukung.
2. Melakukan prioritisasi dari layanan TI sesuai dengan tingkat kritisnya yaitu sangat kritis, penting atau minor.
3. Melakukan prioritisasi proses bisnis perusahaan sesuai dengan tingkat kritisnya yaitu sangat kritis, penting atau minor.
4. Melakukan analisis dampak dari adanya gangguan, dengan melakukan analisis berdasarkan tiga aspek yaitu finansial, reputasi dan target teknis.
5. Menentukan waktu pemulihan pada tiap layanan TI, dimana terdapat tiga waktu yang ditentukan yaitu *Maximum Tolerable Downtime* (MTD), *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO).

3.2.4.4 Membuat Strategi Keberlangsungan Bisnis

Berdasarkan hasil dari analisis risiko dan dampak bisnis kemudian dibuat strategi keberlangsungan bisnis. Tahap pembuatan strategi keberlangsungan bisnis pada metodologi

BCP ini disintesis dari ISO 22317:2015 mengenai Business Impact Analysis. Penyusunan strategi keberlangsungan bisnis berfokus kepada penentuan tanggungjawab atas dampak dari gangguan yang menginterupsi proses bisnis dan pengembangan prosedur pengelolaan kerusakan atau gangguan. Berikut ini aktivitas yang dilakukan dalam membuat strategi keberlangsungan bisnis:

1. Menentukan strategi preventif atau pencegahan untuk mengurangi risiko terjadinya gangguan dan mengurangi dampak yang terjadi.
2. Menentukan strategi mengenai tindakan atau aksi yang harus dilakukan oleh tim iga DRP agar dapat mengatasi gangguan dan melakukan pemulihan.
3. Menentukan strategi dalam mengatasi gangguan dan mengembalikan proses bisnis agar dapat kembali berjalan dalam kondisi normal, strategi ini dilakukan oleh seluruh pihak yang terkait dalam BCP.
4. Melakukan koreksi terhadap strategi yang telah dibuat, apabila terdapat ketidaksesuaian atau kurang efektif.

3.2.4.5 Membuat Rencana Pemulihan Bencana

Pada tahap pembuatan rencana pemulihan bencana fokusnya adalah kepada penanganan insiden, prosedur saat bencana serta pihak yang bersangkutan dengan pemulihan dari bencana. Tahap pembuatan rencana pemulihan bencana disintesis dari ISO 24762:2012 mengenai *information and communications technology disaster recovery services*. Adapun berikut ini aktivitas yang harus dilakukan dalam membuat rencana pemulihan bencana:

1. Melakukan pendataan asset TI yang dimiliki oleh perusahaan.
2. Melakukan pendataan vendor jasa atau produk yang dibutuhkan dan digunakan oleh perusahaan beserta dengan tanggungjawabnya.
3. Menentukan lokasi server atau asset TI yang aman terhadap bencana

4. Membuat bentuk kontrol dari bencana atau gangguan yang didasarkan pada kategori kontrol yaitu pencegahan sumber masalah (*preventive control*), pendeteksi sumber masalah saat bencana terjadi (*detective control*), dan pengurangan dampak (*corrective control*).
5. Menentukan bilamana akan dilakukan aktivasi pemulihan mulai dari deklarasi status sampai kepada de-aktivasi atau status dimana dapat beroperasi kembali.
6. Membuat skenario pengujian dan melakukan simulasi pengujian.
7. Melakukan evaluasi hasil pengujian dan merivisi bentuk kontrol dari rencana pemulihan bencana.

3.2.4.6 Membuat Pelatihan Karyawan

Tahap pelatihan karyawan terhadap BCP yang dibuat, disintesis berdasarkan COBIT 5: *Domain Manage Continuity* yaitu conduct continuity plan training (pelatihan rencana keberlangsungan). Pada tahap inipelatihan karyawan mencakup pada proses pelatihan yang terdiri dari penyampaian pelatihan, pelaksanaan pelatihan yang berisi latihan dan ujian, dan pemantauan kompetensi berdasarkan hasil latihan dan ujian. Berikut ini aktivitas dalam tahap membuat pelatihan karyawan:

1. Menentukan jenis pelatihan yang sesuai dengan kebutuhan perusahaan.
2. Menentukan mekanisme penyampaian pelatihan.
3. Merancang dan memenuhi sumber daya yang diperlukan dalam melaksanakan pelatihan.
4. Melaksanakan pelatihan sesuai dengan mekanisme yang telah ditentukan.

3.2.4.7 Pengujian BCP

Tahap pengujian BCP dilakukan setelah dokumen BCP berhasil dibuat.. Tahap pengujian BCP disintesis dari COBIT 5: Domain Manage Continuity praktek manajemen kunci exercise,test and review the BCP. Berikut ini aktivitas dalam melakukan pengujian BCP:

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

3.2.4.8 Peninjauan Keberlangsungan Bisnis

Pada tahap ini, aktivitasnya didapatkan dari sintesis pada praktik manajemen kunci review, maintain, and improve the continuity plan pada COBIT 5: Domain Manage Continuity. Berikut ini aktivitas dalam menentukan kebutuhan pengelolaan keberlangsunan bisnis:

1. Menentukan periode waktu peninjauan keberlangsungan bisnis.
2. Melakukan peninjauan keberlangsungan bisnis secara berkala.
3. Melakukan analisis ulang terhadap adanya dampak, risiko, dan strategi baru terkait dengan rencana keberlangsungan bisnis yang telah diterapkan.
4. Melakukan pertimbangan terhadap perubahan dari rencana keberlangsungan bisnis yang telah ditetapkan.

3.2.5 Evaluasi Implementasi Metodologi BCP

Pada tahap ini dilakukan evaluasi terhadap implementasi metodologi *Business Continuity Planning* yang digunakan dalam pembuatan dokumen BCP pada divisi TI Bank Pembangunan Daerah Jawa Timur. Evaluasi dilakukan guna mengetahui apakah setiap tahap yang ada pada metodologi BCP dapat diimplementasi pada pembuatan dokumen BCP pada divisi TI Bank Pembangunan Daerah Jawa Timur.

3.2.6 Pembuatan Kesimpulan dan Saran

Berdasarkan implementasi metodologi BCP untuk membuat dokumen perencanaan keberlangsungan bisnis, maka didapatkan temuan-temuan selama pelaksanaan. Kemudian dari temuan-temuan tersebut dapat ditarik kesimpulan dan kemudian pemberian saran terhadap temuan-temuan tersebut.

BAB IV
PERANCANGAN

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

4.1 Perancangan Studi Kasus

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

4.1.1 Tujuan Studi Kasus

Pada penelitian ini dilakukan pembuatan *business continuity plan* (BCP) sebagai salah satu upaya untuk mitigasi risiko. Penelitian ini membutuhkan studi kasus yang digunakan sebagai objek untuk menggali lebih dalam terkait keadaan dan kebutuhan terkait BCP itu sendiri. Menurut Yin, studi kasus adalah sebuah cara unik untuk mengamati suatu fenomena alam yang ada dalam satu set data[33].Yin mengemukakan bahwa ada tiga jenis studi kasus, antara lain adalah, eksploratoris (menggali) yaitu melakukan eksplorasi terhadap fenomena apapun dalam data yang berfungsi sebagai tempat tujuan untuk meneliti, deskriptif yaitu digunakan untuk mengambarkan fenomena alamiah yang terjadi pada data dalam bentuk narasi, dan eksplanatoris (memperjelas) yaitu menjelaskan fenomena dalam data mulai dari hal yang dasar hingga dalam dan menjelaskan hubungan klausal dalam konteks kehidupan nyata.

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

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

1. Bagaimana hasil dokumen perencanaan keberlangsungan bisnis pada Bank Pembangunan Daerah di Jawa Timur?
2. Apakah semua tahap pada metodologi *Business Continuity Planning* dapat dilakukan pada pembuatan dokumen BCP Bank Pembangunan Daerah Jawa Timur?

4.2 Perancangan Pengumpulan Data dan Informasi

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

Proses wawancara akan dilakukan pada Divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur. Diharapkan setelah melakukan wawancara akan didapatkan informasi terkait risiko TI yang dihadapi oleh perusahaan, proses bisnis terkait TI, serta informasi lain terkait analisis dampak bisnis.

Tabel 4.2-1 Pengumpulan Data dan Informasi

Nama Proses	Pengumpulan Data dan Informasi
Teknik	*Interview*/Wawancara Teknik wawancara akan dilakukan dengan metode tanya jawab langsung dengan narasumber. Wawancara akan dilakukan secara terstruktur, dimana peneliti telah menyiapkan pertanyaan pertanyaan yang dibutuhkan terlebih dahulu.
Objek	Aset TI, Proses Bisnis terkait TI, dan Risiko TI
Kebutuhan Proses	Laptop Interview Protocol Handphone/ perekam Alat Tulis

Nama Proses	Pengumpulan Data dan Informasi
Tahap Pelaksanaan	Tahapan dalam melakukan wawancara adalah sebagai berikut: 1. Menetapkan tujuan dan jumlah wawancara 2. Menentukan narasumber *3.* Membuat *interview protocol* 4. Memulai proses wawancara 5. Mendokumentasikan hasil wawancara

4.2.1 Tujuan dan Jumlah Wawancara

Sebelum melakukan wawancara, maka terlebih dahulu ditentukan tujuan wawancara. Tujuan ditentukan agar proses wawancara dan pengambilan informasi sesuai dengan tujuan penelitian dan peneliti bisa mendapatkan data dan informasi yang dibutuhkan.

Tabel 4.2-2 Tujuan Wawancara

Wawancara ke-	Narasumber	Tujuan Wawancara
1	Adimas I.	Wawancara ini bertujuan untuk mengetahui aset teknologi informasi yang dimiliki serta kerentanan dan ancaman dan pengamanan yang telah dilakukan di perusahaan.
2	M. Arief. R	Wawancara ini dilakukan dengan tujuan untuk mengetahui kondisi umum yang ada pada divisi TI Bank Pembangunan Daerah Jawa Timur seperti sub fungsional, tugas dan tanggung jawab, proses bisnis yang ada pada tiap sub fungsional serta layanan TI yang digunakan pada setiap proses bisnis.
3	M. Arief. R	Wawancara ini dilakukan dengan tujuan untuk mengetahui informasi terkait risiko dan analisis dampak bisnis.

4.2.2 Profil Narasumber Wawancara

Sebelum melakukan wawancara, peneliti terlebih dahulu menentukan narasumber. Narasumber yang dipilih sesuai tujuan wawancara dan berada dalam kapasitas objek wawancara. Hal ini bertujuan agar informasi yang didapatkan lebih valid serta relevan dengan cakupan wawancara. Berikut ini merupakan profil dari narasumber yang akan diwawancarai dalam penelitian ini:

Tabel 4.2-3 Profil Narasumber Wawancara

Nama	Jabatan
Adimas I.	Grup IT Security Analyst
M. Arief. R	Grup IT Governance & Risk Management Junior Analyst

4.2.3 Daftar Pertanyaan Wawancara

Daftar pertanyaan wawancara disusun untuk memudahkan dalam pengambilan data yang terkait dengan penelitian. Berikut ini adalah daftar pertanyaan wawancara.

Tabel 4.2-4 Daftar Pertanyaan Wawancara

Tujuan Pertanyaan	Detail Ringkas Pertanyaan
Untuk mengetahui kondisi umum pada divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur.	• Kondisi umum divisi Teknologi Informasi pada Bank Pembangunan Daerah Jawa Timur. • Pembagian sub fungsi dari divisi Teknologi Informasi pada Bank Pembangunan Daerah Jawa Timur • Tupoksi dari setiap fungsi yang ada pada divisi Teknologi Informasi.
Untuk menggali informasi terkait dengan aset TI, Sistem Informasi dan proses bisnis yang terkait TI pada divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur	• Proses Bisnis terkait Teknologi Informasi • Aset Teknologi Informasi • Fungsional bisnis pengguna layanan Teknologi Informasi. • Komponen pendukung layanan TI
Untuk menggali informasi terkait identifikasi ancaman,	• Ancaman pada aset TI • Kerentanan aset Teknologi Informasi

Tujuan Pertanyaan	Detail Ringkas Pertanyaan
kerentanan, serta risiko aset teknologi informasi	
Untuk menggali informasi terkait analisa dampak bisnis	• Dampak gangguan TI terhadap finansial, reputasi dan operasional dari divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur.
Untuk menggali informasi terkait praktik keamanan yang telah diterapkan serta kelemahan perusahaan.	• Kontrol keamanan yang diterapkan dalam rangka mengantisipasi terjadinya risiko.

4.3 Perancangan Evaluasi Implementasi Metodologi

Perangkat evaluasi dibuat dalam penelitian untuk dapat memudahkan peneliti dalam mengetahui apakah semua tahapan pada metodologi Business Continuity Planning dapat dilakukan dalam pembuatan dokumen BCP. Perangkat evaluasi yang digunakan adalah berupa *checklist* implementasi. Checklist implementasi berisi setiap aktivitas yang ada pada metodologi *Business Continuity Planning*. Berikut ini tahap yang ada pada setiap fase metodologi Business Continuity Planning.

Gambar 4.3-1 Fase Metodologi *Business Continuity Planning*

Pada checklist evaluasi digunakan tiga skala yaitu 1 hingga 3 untuk mengevaluasi aktivitas dalam implementasi metodologi. Hal ini digunakan agar dapat diketahui bagaimana aktivitas pada metodologi jika diterapkan dalam pembuatan dokumen BCP divisi TI Bank Pembangunan Daerah Jawa Timur. Berikut ini penjelasan skala implementasi metodologi BCP.

Tabel 4.3-1 Skala Implementasi Metodologi BCP

Skala	Keterangan
1	Tidak dapat diimplementasi.
2	Dapat diimplemetasi perubahan.
3	Dapat diimplementasi seluruhnya

Setiap aktivitas yang ada pada tahapan metodologi dimasukkan dalam *checklist* evaluasi. Kemudian skala yang digunakan serta justifikasi dimasukkan dalam *checklist* evaluasi. Checklist diisi dengan mencentang salah satu skala pada tiap aktivitas sesuai dengan implementasinya, kemudian diisi justifikasi dari setiap penilaian yang diberikan. Berikut ini merupakan *checklist* evaluasi implementasi metodologi *Business Continuity Planning*:

Tabel 4.3-2 *Checklist* Evaluasi Implementasi Metodologi BCP

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

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
		Pembuatan Alur Komunikasi				
Implementasi	Analisis Risiko	Pendataan Kemungkinan Risiko				
		Analisis Risiko				
		Penilaian Risiko				
	Analisis Dampak Bisnis	Pendataan Proses Bisnis dan TI				
		Prioritisasi Layanan TI				
		Prioritisasi Proses Bisnis				
		Analisis Dampak Gangguan				
		Penentuan Waktu Pemulihan				
	Strategi keberlangsungan Bisnis	Penentuan Strategi Preventif				
		Penentuan Strategi Saat Gangguan				
		Penentuan Strategi Pemulihan				
		Koreksi Terhadap Strategi				
	Rencana Pemulihan Bencana	Pendataan Aset Teknologi informasi				
		Pendataan Vendor				

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
		Penentuan Lokasi Server dan Aset TI				
		Pembuatan Kontrol				
		Permintaan Aktivasi dan Deaktivasi				
		Skenario Pengujian				
		Evaluasi Bentuk Kontrol				
	Pelatihan Karyawan	Penentuan Jenis Pelatihan				
		Mekanisme Penyampaian Pelatihan				
		Rencana Kebutuhan Pelatihan				
		Pelaksanaan pelatihan				
Pemantauan dan Review	Pengujian BCP	Rencana Mekanisme Pengujian				
		Pengujian				
		Pencatatan Temuan				
		Dokumentasi Hasil Pengujian				
Pemeliharaan dan Peningkatan	Peninjauan Keberlangsungan bisnis	Penentuan Periode Waktu Peninjauan				
		Peninjauan Secara Berkala				
		Pengkajian Ulang				

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
		Terhadap rencana				
		Pertimbangan Terhadap Perubahan				

4.4 Pengolahan Data dan Informasi

Pengolahan data dan informasi adalah sebuah proses yang dilakukan setelah proses pengambilan data selesai. Penelitian ini termasuk penelitian kualitatif, dimana pengumpulan data dilakukan dengan wawancara, observasi, dan mempelajari dokumen perusahaan. Data yang telah terkumpul akan diterjemahkan dan dianalisis oleh penulis. Analisis yang akan dilakukan pada penelitian ini mencakup beberapa hal, sebagai berikut:

4.4.1 Analisis Risiko

Pada tahap analisis risiko terdapat tiga aktivitas yang perlu untuk dilakukan yaitu melakukan pendataan kemungkinan risiko, yaitu mendata kemungkinan risiko, melakukan analisis risiko dan melakukan penilaian risiko. Berikut ini penjelasan yang dilakukan dalam setiap tahap.

1. Identifikasi Risiko
   Pada tahap ini dilakukan pendataan terhadap risiko yang mungkin terjadi pada divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur. Identifikasi risiko dilakukan dengan pendekatan OCTAVE. Aktivitas pertama yang perlu dilakukan untuk melakukan identifikasi risiko adalah membuat daftar aset TI kritis yang ada pada divisi TI Bank Pembangunan Daerah Jawa Timur. Berikut ini adalah contoh tabel yang harus diisi.

Tabel 4.4-1 Contoh Tabel Aset Kritis

Jenis Aset IT	ID Aset IT	Nama Aset IT	Deskripsi Fungsi Aset IT	Kategori Aset IT

Tahap berikutnya adalah membuat kebutuhan keamanan aset kritis berdasarkan CIA Triad. Berikut ini adalah rancangan tabel kebutuhan keamanan aset kritis.

Tabel 4.4-2 Contoh Tabel Kebutuhan Keamanan Aset Kritis

Nama Aset TI	Kebutuhan Keamanan berdasar CIA Triad	Penjelasan

Kemudian dibuat daftar ancaman untuk setiap aset kritis beserta dengan penyebabnya. Ancaman dibuat sesuai dengan kategori jenis aset kritis. Berikut ini contoh tabel jenis ancaman aset kritis.

Tabel 4.4-3 Contoh Tabel Ancaman Aset Kritis

Kategori Aset Kritis	Ancaman	Penyebab

Selanjutnya dibuat praktik keamanan yang telah dilakukan oleh organisasi pada aset kritis perusahaan. Berikut ini adalah contoh tabel praktik keamanan aset kritis.

Tabel 4.4-4 Contoh Tabel Praktik Keamanan

Jenis Aset TI	Nama Aset TI	Praktik Keamanan

Kemudian dibuat daftar kelemahan dari organisasi sesuai dengan kategori aset. Berikut ini adalah contoh tabel kelemahan organisasi.

Tabel 4.4-5 Contoh Tabel Kelemahan Organisasi

Kategori Aset Kritis	Kelemahan	Deskripsi

Selanjutnya adalah melakukan identifikasi terhadap ancaman pada komponen aset kritis sehingga dapat diketahui kerentanan dari aset kritis. Berikut ini adalah contoh tabel ancaman komponen aset kritis dan daftar kerentanan aset kritis.

Tabel 4.4-6 Contoh Tabel Ancaman Komponen Aset

Nama Aset Kritis	Komponen Utama Aset Kritis	Ancaman

Tabel 4.4-7 Contoh Tabel Kerentanan Aset Kritis

Nama Aset Kritis	Kerentanan Aset Kritis

Sehingga dari pendekatan yang dilakukan dengan metode OCTAVE, dibuat daftar risiko yang mungkin terjadi sesuai dengan ancaman yang dapat menimpa aset kritis. Berikut ini adalah contoh tabel daftar risiko TI.

Tabel 4.4-8 Contoh Tabel Daftar Risiko TI

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab

2. Analisis Risiko

   Pada tahap analisis risiko dilakukan identifikasi pada setiap kemungkinan risiko. Identifikasi dilakukan dengan menggunakan FMEA. Identifikasi dilakukan pada tiga aspek yaitu pada *severity*, *occurrence* dan *detection*. Setiap kemunginan risiko diberikan masing-masing nilai *severity*,

occurrence dan *detection* yang sesuai dengan keadaan organisasi. Berikut ini adalah kriteria penilaian pada FMEA:

1. *Severity* (tingkat keparahan) /*Impact*
   Tingkat keparahan atau severity merupakan pengukuran dalam memperkirakan secara numerik dari seberapa parak akibat dari risiko yang terjadi pada para pekerja/pihak ketiga/pelanggan. Pengukuran nilai dampak akan dilihat seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek aspek penting dalam organisasi. Terdapat tiga aspek yang akan dijabarkan yaitu aspek jadwal, aspek biaya dan aspek teknis. Berikut merupakan penjelasan dari kriteria nilai dampak [21].

Tabel 4.4-9 Kriteria Penilaian Severity

Dampak	Dampak dari Efek	Ranking
Akibat Berbahaya	Melukai pelanggan atau karyawan	10
Akibat Serius	Aktivitas yang ilegal	9
Akibat Ekstrim	Mengubah produk atau jasa menjadi tidak layak untuk 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 diatasi tanpa kehilangan sesuatu	3
Akibat Sangat Ringan	Tanpa disadari terjadi gangguan kecil pada kinerja	2
Tidak Ada Akibat	Tanpa disadari dan tidak mempengaruhi kinerja	1

2. *Occurance* (Nilai Kemungkinan) Likelihood

Nilai kemungkinan atau *occurence* adalah pengukuran terhadap tingkat frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat mengakibatkan kegagalan. Berikut merupakan pejelasan dari kriteria kemungkinan [21].

Tabel 4.4-10 Kriteria Penilaian Occurance

Kemungkinan Kegagalan	Kemungkinan	Ranking
Very High: Kegagalan hampir/ tidak dapat dihindari	Lebih dari satu 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 sebulan	7
Moderately high: Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan	6
Moderate: Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan	5
Moderate Low: Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relatif kecil	Satu kali dalam 1-3 tahun	3
Very Low: Kegagalan terjadi relatif kecil	Satu kali dalam 3-6 tahun	2
Remote: Kegagalan tidak pernah terjadi	Satu kali dalam 6-50 tahun	1

3. *Detection* (deteksi) / Cause
   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 [21].

Tabel 4.4-11 Kriteria Penilaian Detection

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

3. Penilaian Risiko

Pada tahap penilaian risiko dilakukan perhitungan nilai RPN untuk mengetahui tingkatan risiko. Nilai RPN didapatkan dari hasil kalkulasi *severity*, *occurence*, dan *detection*. Berikut ini adalah rumus dari RPN.

RPN= Severity * Occurence * Detection

Skala Nilai RPN yang didapat dari perhitungan akan menghasilkan level resiko tertentu. Berikut merupakan skala penentuan level risiko berdasarkan nilai RPN.

Tabel 4.4-12 Skala Nilai RPN[19]

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

4.4.2 Analisis Dampak Bisnis

Tahap yang dilakukan setelah analisis risiko dilakukan adalah melakukan analisis dampak bisnis. Analisis dampak bisnis dilakukan untuk menganalisis dampak yang timbul kepada bisnis akibat gangguan. Analisis Dampak Bisnis dijalankan dengan menggunakan pendekatan Metodologi *Business Continuity Planning*. Langkah-langkah dalam melakukan analisis dampak bisnis dengan metodologi *Business Continuity Planning* didapatkan dari sintesis ISO 22317:2015 mengenai *Business Impact Analysis.*

Setelah data mengenai proses bisnis serta layanan TI dikumpulkan, selanjutnya dilakukan prioritisasi terhadap layanan TI yang sesuai dengan tingkatan kritisnya yaitu sangat kritis, penting dan minor. Selanjutnya, dilakukan prioritisasi terhadap proses bisnis perusahaan yang sesuai dengan tingat kritisnya yaitu sangat kritis, penting dan minor. Setelah membuat prioritisasi proses bisnis, dilakukan analisis dari dampak gangguan terhadap tiga aspek pada bisnis yaitu aspek finansial, reputasi dan target teknis. Kemudian ditentukan waktu pemulihan. Menentukan waktu pemulihan pada tiap layanan TI, dimana terdapat tiga waktu yang ditentukan yaitu

Maximum Tolerable Downtime (MTD), *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO).

4.4.3 Strategi Keberlangsungan Bisnis

Setelah dilakukan analisis risiko dan dampak bisnis dari divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur, ditentukan strategi Perencanaan Keberlangsungan Bisnis. Penyusunan strategi keberlangsungan bisnis dilakukan berdasarkan metodologi *Business Continuity Planning* yang disintesis dari ISO 22317:2015 mengenai *Business Impact Analysis.* Strategi keberlangsungan bisnsis dikategorikan menjadi empat yaitu strategi preventif, strategi DRP, strategi saat gangguan dan strategi korektif. Berikut ini merupakan penjelasan dari masing-masing strategi[34]:

- **Strategi Preventif**

  Strategi Preventif adalah tindakan atau aksi organisasi yang dilakukan dalam rangka mengurangi risiko terjadinya gangguan serta mengurangi dampak yang akan ditimbulkan oleh risiko tersebut. Strategi preventif dibuat agar organisasi menjadi lebih siap dalam menghadapi gangguan yang akan terjadi. Strategi preventif juga diharapkan dapat membantu organisasi dalam menghadapi gangguan yang terjadi sehingga organisasi dapat menyelesaikan permasalahan akibat gangguan dalam batas waktu yang telah ditentukan.
- **Strategi Saat Gangguan**

  Strategi saat gangguan adalah aksi organisasi dalam mengatasi gangguan dan kemudian mengembalikan proses bisnis ke keadaan yang semula. Perbedaan strategi saat gangguan dengan strategi DRP adalah pada strategi saat gangguan tidak terbatas hanya pada tim DRP, tetapi juga pada keseluruhan komite BCP terkait. Fokus utama strategi adalah mengembalikan kondisi organisasi pada keadaan normal.
- **Strategi Korektif**

Strategi Korektif merupakan tindakan yang dilakukan organisasi untuk memperbaiki kinerja perencanaan BCP. Strategi korektif dilaksanakan saat organisasi menilai ada ketidaksesuaian pada perencanaan BCP yang disusun. Strategi korektif diharapkan dapat membantu organisasi untuk meningkatkan performa dari strategi BCP.

Untuk membuat strategi keberlangsungan bisnis tahap yang dilakukan adalah yang pertama menentukan strategi preventif atau pencegahan untuk mengurangi risiko terjadinya gangguan dan mengurangi dampak yang terjadi. Selanjutnya adalah menentukan strategi yang harus dilakukan oleh tim DRP agar dapat mengatasi gangguan dan melakukan pemulihan. Setelah itu menentukan strategi dalam mengatasi gangguan dan mengembalikan proses bisnis agar dapat kembali berjalan dalam kondisi normal, strategi ini dilakukan oleh seluruh pihak yang terkait dalam BCP. Kemudian, dilakukan koreksi terhadap strategi yang telah dibuat, apabila terdapat ketidaksesuaian atau kurang efektif.

4.5 Rencana Validasi BCP

Tahap validasi merupakan tahap dimana peneliti memastikan bahwa dokumen BCP yang telah dibuat telah sesuai dengan kebutuhan organisasi. Tahap ini dilakukan untuk memastikan bahwa dokumen BCP yang telah dibuat telah sesuai dan dapat diterima oleh perusahaan, sehingga tahap validasi ini penting dalam penelitian ini. Berikut ini merupakan rencana validasi yang akan diajukan oleh peneliti kepada divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur:

Tabel 4.5-1 Rencana Validasi

No	Nama Validasi	Keterangan
1.	Validasi kesesuaian analisis risiko	Validasi ini bertujuan untuk memaastikan bahwa analisis risiko yang telah dibuat sesuai dengan kebuthan organisasi dari hasil penggalian data yang dilakukan pada divisi teknologi

		informasi Bank Pembangunan Daerah Jawa Timur.
2.	Validasi kesesuaian dampak bisnis	Validasi kesesuaian dampak bisnis bertujuan untuk memastikan kesesuaian analisis dampak bisnis dengan kebutuhan organisasi berdasarkan penggalian data yang dilakukan pada divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur.
3.	Validasi kesesuaian dokumen *Business Continuity Plan*	Validasi kesesuaian dokumen BCP dilakukan untuk memastikan bahwa dokumen BCP yang dibuat telah sesuai dengan kebutuhan perusahaan berdasarkan penelitian yang telah dilakukan.

BAB V
IMPLEMENTASI

Bab ini berisi penjelasan mengenai hasil dari perancangan dan proses pelaksanaan dari penelitian. Selain itu, dijelaskan mengenai hasil pengumpulan data dan informasi.

5.1 Hasil Pengumpulan Data dan Informasi

Proses pengumpulan data dan informasi dilakukan dengan menggunakan metode wawancara dan analisis dokumen.

5.1.1 Hasil Wawancara

Pengumpulan data menggunakan metode wawancara dilakukan kepada pihak terkait pada divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur. Berikut ini merupakan keterangan pelaksanaan tahap pengumpulan data dengan wawancara.

Tabel 5.1-1 Hasil Wawancara

1.	Narasumber	Adimas I.
	Jabatan	Grup IT Security Junior Analyst
	Tanggal	07-05-2018
	Lokasi	Kantor Bank Pembangunan Daerah Jawa Timur
	Topik	Analisis Risiko
	Hasil	Lampiran A
2.	Narasumber	M.Arief R.
	Jabatan	Grup IT Governance & Risk Management Analyst
	Tanggal	09-05-2018
	Lokasi	Kantor Bank Pembangunan Daerah Jawa Timur
	Topik	Kondisi Umum Analisis Risiko Analisis Dampak Bisnis
	Hasil	Lampiran B

5.2 Hasil Validasi BCP

Tahap validasi BCP merupakan tahapan untuk memastikan bahwa analisis yang dilakukan telah benar dan sesuai dengan kondisi perusahaan. Validasi dilakukan juga sebagai konfimasi bahwa dokumen yang dikerjakan oleh peneliti sudah sesuai dengan kebutuhan divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur. Proses validasi dilakukan dengan mengajukan surat konfirmasi kepada perwakilan divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur. Validasi dilakukan pada bagian analisis risiko, analisis dampak bisnis, dan dokumen BCP.

Validasi analisis risiko dilakukan setelah setiap potensi risiko yang ada dinilai dan dibuat prioritisasinya sesuai dengan risiko tertinggi. Berdasar hasil analisis risiko didapatkan 4 risiko tertinggi dengan tingkat *low*. Setelah dilakukan validasi didapatkan bahwa analisis risiko yang dilakukan telah sesuai dengan kondisi perusahaan.

Validasi analisis dampak bisnis dilakukan setelah proses bisnis dan layanan diberi prioritisasi serta ditentukan waktu pemulihan dan dilakukan analisa dampak bisnis. Dari hasil analisis dampak bisnis yang telah dilakukan, didapatkan prioritasi untuk proses bisnis serta layanan TI dari organisasi, analisis dampak gangguan serta strategi BCP yang didapatkan dari proses pengolahan data dampak bisnis yang didapatkan dari wawancara, setelah dilakukan validasi kepada pihak organisasi ternyata hasil dari analisis dampak bisnis memiliki kesesuaian dengan kondisi sebenarnya pada organisasi, hal ini membuktikan bahwa proses validasi telah memastikan bahwa hasil analisa yang dilakukan sudah benar dan sesuai dengan keadaan perusahaan.

Validasi dokumen BCP dilakukan setelah dokumen BCP dibuat. Mulai dari kebutuhan perencanaan keberlangsungan bisnis hingga peninjauan keberlangsungan bisnis. Setelah dilakukan validasi kepada organisasi, dokumen BCP yang

dibuat telah sesuai dengan kondisi perusahaan. Untuk hasil validasi dari analisis risiko dapat dilihat pada lampiran D, hasil validasi analisis dampak bisnis dapat dilihat pada lampiran E dan hasil validasi terdapat pada lampiran F.

5.3 Hambatan Pengumpulan Data

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

- Proses pengumpulan data serta validasi membutuhkan waktu yang cukup lama karena dilakukan secara bertahap.
- Analisis dampak bisnis dan analisis risiko membutuhkan waktu yang cukup lama karena terdapat koreksi yang perlu dilakukan dari feedback perusahaan.

Meskipun terdapat hambatan dan rintangan, penelitian ini tetap berjalan dengan lancar berkat bantuan dari divisi TI Bank Pembangunan Daerah Jawa Timut. Pihak divisi TI sangat bersedia membantu serta terbuka untuk membantu penelitian dengan meluangkan waktu serta memberikan respon yang cepat dan baik saat proses pengambilan data dan validasi.

(Halaman ini sengaja dikosongkan)

BAB VI
HASIL DAN PEMBAHASAN

Bab ini berisi penjelasan dari proses pembuatan dokumen *Business Continuity Plan* dengan menggunakan metodologi *Business Continuity Planning* serta evaluasi dari implementasi metodologi.

6.1 Hasil Dokumen Business Continuity Plan

Pada bagian ini dijelaskan mengenai hasil dokumen BCP pada divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur yang dibuat dengan menggunakan metodologi *Business Continuity Planning*.

6.1.1 Kebutuhan pengelolaan Keberlangsungan Bisnis

Pada fase ini dilakukan penentuan terhadap kebutuhan organisasi akan dokumen BCP. Penentuan kebutuhan pengelolaan Keberlangsungan Bisnis dilakukan dengan menentukan tujuan keberlangsungan bisnis, ruang lingkup, peran dan tanggung jawab komite BCP, pihak terkait

6.1.1.1 Tujuan Keberlangsungan Bisnis

Pada bagian ini dijelaskan mengenai tujuan dari perencanaan keberlangsungan bisnis yang dibuat pada organisasi. Tujuan akan dijadikan sebagai acuan dalam penyusunan dokumen BCP. Sehingga dokumen BCP yang dibuat diharapkan dapat menunjang proses bisnis dan tujuan organisasi. Tujuan keberlangsungan bisnis ditentukan berdasarkan kebutuhan rencana keberlangsungan bisnis perusahaan. Berikut ini merupakan kebutuhan rencana keberlangsungan bisnis dari divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur.

1. Rencana keberlangsungan bisnis dapat menjaga proses bisnis tetap berjalan saat ada gangguan.
2. Rencana keberlangsungan bisnis mempertimbangkan risiko dan dampak bisnis bagi proses bisnis perusahaan.

3. Rencana keberlangsungan bisnis menyesuaikan dengan sumber daya manusia dan teknologi informasi pada divisi teknologi informasi
4. Rencana keberlangsungan bisnis dapat diperbaharui saat dibutuhkan perbaikan.
5. Rencana keberlangsungan bisnis disesuaikan dengan operasional proses bisnis dari perusahaan.
6. Rencana keberlangsungan bisnis yang dibuat berlaku dan dapat digunakan hingga 5 tahun.

Sehingga dari kebutuhan perusahaan terhadap BCP didapatkan tujuan Rencana Keberlangsungan divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur. Berikut ini merupakan tujuan Rencana Keberlangsungan Bisnis pada divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur.

1. Memastikan proses bisnis kritis yang ada pada divisi teknologi infromasi tetap berlangsung meskipun terjadi gangguan maupun bencana.
2. Mengetahui risiko yang dapat terjadi serta bagaimana tingkatan dari risiko.
3. Mengurangi dampak dari risiko yang terjadi akibat gangguan atau bencana yang menimpa perusahaan.
4. Mendokumentasikan strategi dalam mempertahankan keberlangsungan bisnis, proses bisnis kritis, layanan Teknologi Informasi yang bersifat kritis serta pemulihan dari gangguan pada bisnis.

6.1.1.2 Ruang Lingkup

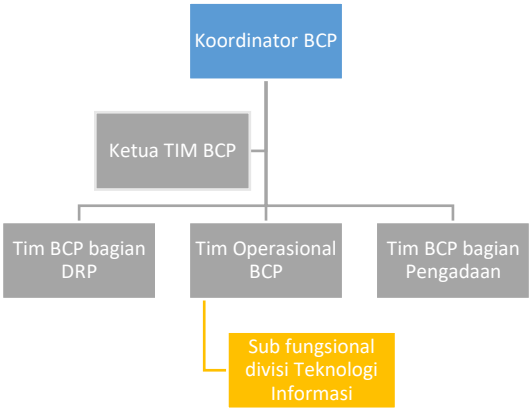
Pada bagian ini dijelaskan mengenai lingkup dari dokumen BCP yang akan dibuat. Pada pembuatan dokumen BCP divisi teknologi infomasi Bank Pembangunan Daerah Jawa Timur mencakup kepada beberapa sub fungsional divisi teknologi informasi. Berikut ini merupakan sub fungsional yang masuk dalam ruang lingkup pengerjaan dokumen:

Tabel 6.1-1 Ruang Lingkup BCP

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi
Grup IT Infrastructure &Network Operation	Monitoring Availability Jaringan
Grup IT Management Information System	Permintaan Data Restore & Recovery
Grup IT Support & Helpdesk	Penanganan Insiden Penambahan User Penghapusan User Perubahan User
Grup IT Security	Penanganan Insiden Pengamanan Informasi Monitoring Hak Akses Logis
Grup IT Data Center	Akhir periode

6.1.1.3 Peran dan Tanggung Jawab Komite BCP

Pada bagian ini dijelaskan mengenai struktur dan peran serta tanggung jawab dari komite BCP. Komite BCP dibentuk untuk dapat memastikan bahwa SDM yang terlibat telah menjalankan perencanaan keberlangsungan bisnis dengan baik. Struktur komite BCP disesuaikan dengan struktur organisasi dan sumber daya yang ada pada divisi TI Bank Pembangunan Daerah Jawa Timur. Berdasarkan struktur komite BCP yang sesuai dengan divisi TI Bank Pembangunan Daerah Jawa Timur, dibuat peran dan tanggung jawab dari setiap anggota komite pada perencanaan keberlangsungan bisnis. Berikut ini adalah struktur serta peran dan tanggung jawab dari setiap komite BCP.



Gambar 6.1-1 Struktur Komite BCP

1. Koordinator BCP
   - Bertanggung jawab untuk meninjau kembali BCP
   - Mengawasi penerapan BCP
   - Mengawasi proses BCP
2. Ketua Tim BCP
   - Mengembangkan BCP
   - Melakukan pengawasan terhadap anggota tim pada setiap bagian
   - Melakukan pelatihan dan pengujian yang sesuai dengan BCP
   - Memberikan arahan kepada anggota tim BCP
   - Mengawasi kesesuaian pelaksanaan BCP
3. Tim BCP bagian DRP
   - Melakukan pemulihan aset TI
   - Melakukan backup dan restore
4. Tim Operasional BCP
   - Melaksanakan operasional dari BCP
5. TIM BCP bagian Pengadaan
   - Menghubungi vendor penyedia layanan Teknologi Informasi pada perusahaan

- Menyediakan perangkat yang diperlukan untuk pemulihan
- Mendata aset dan infrastruktur teknologi informasi yang mengalami kerusakan

6. Sub fungsional divisi Teknologi Informasi
   - Menghubungi Tim BCP saat terjadi gangguan
   - Melaksanakan arahan terkait BCP

6.1.1.4 Pihak Terkait

Pada bagian ini ditentukan pihak-pihak yang terkait dengan keberlangsungan bisnis perusahaan. Hal ini dilakukan untuk dapat mengetahui siapa saja yang berhubungan dengan keberlangsungan bisnis perusahaan. Pihak yang terkait dibedakan menjadi dua yaitu pihak eksternal dan pihak internal. Pihak eksternal merupakan pihak di luar perusahaan yang berhubungan dengan keberlangsungan bisnis perusahaan. Sedangkan pihak internal merupakan pihak dalam perusahaan yang berhubungan dengan keberlangsungan bisnis perusahaan. Berikut ini merupakan pihak yang terkait dengan keberlangsungan bisnis perusahaan.

Tabel 6.1-2 Pihak Terkait BCP

Pihak Eksternal	Vendor
	Rekan Bisnis
	Customer
	Kantor Cabang
Pihak Internal	Pegawai Divisi TI
	Pegawai Divisi non TI
	Dewan Komisaris

6.1.1.5 Sumber daya yang Dibutuhkan

Dalam mempertahankan keberlangsungan bisnis, diperlukan dukungan sumber daya untuk memastikan bahwa keberlangsungan bisnis berjalan lancar sesuai dengan perencanaan. Oleh karena itu, pada bagian ini dilakukan didentifikasi sumber daya dan ketersediaan infrastruktur. Identifikasi sumber daya yang sekiranya dibutuhkan dalam melaksanakan rencana keberlangsungan bisnis. Tahap ini

dilakukan dengan menganalisis kebutuhan sumber daya yang dibutuhkan selama proses pelaksanaan keberlangsungan bisnis dengan menyesuaikan sumber daya yang dimiliki oleh perusahaan. Berikut ini sumber daya yang dibutuhkan dalam perencanaan keberlangsungan bisnis.

Tabel 6.1-3 Daftar Sumber Daya

Jenis Sumber Daya	Nama Sumber Daya
Hardware	Server Cadangan
	Genset
	UPS
	Alat Komunikasi
	Disaster Recovery Center
People	Staff Operasional
	Tim BCP
Dokumen	Daftar Aset TI
	Laporan Kondisi Perangkat dan Layanan TI
	Daftar Vendor
	Daftar Kontak Darurat
	Prosedur Terkait BCP

6.1.1.6 Alur Komunikasi

Pada perencanaan keberlangsungan bisnis, ditetapkan alur komunikasi untuk menjamin kelancaran proses BCP yang telah direncanakan. Alur komunikasi merupakan proses komunikasi yang dilakukan untuk menginformasikan gangguan yang terjadi. Terdapat dua alur komunikasi yang akan dibuat, yaitu alur komunikasi ketika terjadi gangguan kecil atau sedang dan alur komunikasi ketika terjadi bencana atau gangguan besar.

Alur komunikasi gangguan ringan/sedang disesuaikan dengan alur yang telah ada pada perusahaan. Hal ini dilakukan karena telah terdapat prosedur pelaporan gangguan ringan/sedang pada perusahaan. Berikut ini alur komunikasi jika terjadi gangguan ringan/ sedang:

1. Sub fungsional bisnis yang mengalami gangguan ringan/sedang menghubungi layanan helpdesk yang tersedia.

2. Baguan sub fungsional yang mengalami gangguan menceritakan gangguan dan kendala yang dialami.
3. Bagian helpdesk menganalisis permasalahan yang terjadi dan menangani permasalahan.
4. Bagian helpdesk menjalankan prosedur sesuai dengan jenis permasalahan yang terjadi.

Alur komunikasi gangguan besar/ bencana dibuat dengan melakukan analisis terhadap kondisi perusahaan dan menyesuaikan dengan komite BCP yang telah dibuat. Berikut ini alur komunikasi saat terjadi gangguan besar/ bencana:

1. Ketika terjadi gangguan pada beberapa sub fungsional dan proses bisnis, perwakilan dari setiap sub fungsional bisnis yang mengalami gangguan menghubungi komite BCP.
2. Selanjutnya, komite BCP melakukan tugas dan tanggung jawabnya masing-masing. Kemudian mengarahkan perwakilan setiap sub-fuungsionaluntuk melakukan evakuasi serta tetap berkomunikasi dengan sub fungsional lain dan tim BCP untuk mengetahui kondisi.
3. Tim bagian DRP melakukan perlindungan dan pengamanan kepada aset TI.
4. Bagian opeasional BCP menghubungi pihak-pihak yang dibutuhkan seperti pemadam kebakaran, vendor atau petugas medis jika dibutuhkan.
5. Selanjutnya tim pengadaan BCP melakukan pendataan infrastruktur dan aset TI yang mengalami kerusakan serta menghitung biaya dan memperkirakan waktu pemulihan.
6. Jika proses bisnis masih terhenti, maka proses bisnis dijalankan secara manual jika bisa. Proses manual diputuskan oleh koordinator BCP.
7. Tim bagian DRP melakukan pemulihan terhadap perangkat dan infrastruktur sehingga kembali kepada kondisi normal.

8. Jika perangkat dan infrastruktur berhasil dipulihkan maka tim BCP mengembalikan proses bisnis kepada kondisi awal.

Untuk memperlancar alur komunikasi yang dilakukan,digunakan beberapa alat komunikasi darurat. Berikut ini daftar alat komunikasi darurat yang disediakan oleh tim BCP untuk digunakan dalam pengkomunikasian bencana:

1. Telepon
2. Telepon Genggam
3. Email

6.1.2 Analisis Risiko

Pada tahap analisis risiko terdapat beberapa aktivitas yang dilakukan yaitu mendata kemungkinan risiko, melakukan analisis risiko dan melakukan penilaian terhadap risiko. Untuk pendataan kemungkinan risiko dan analisis risiko digunakan pendekatan dengan metode OCTAVE dan untuk menilai risiko digunakan metode FMEA.

6.1.2.1 Melakukan Analisis Risiko

Analisis risiko pada divisi teknologi akan berbasis pada aset teknologi informasi. Analisis risiko dilakukan dengan pendekatan metode OCTAVE. Berdasarkan metode OCTAVE, dalam analisis risiko terdapat beberapa tahap yang harus dilakukan. Pertama-tama adalah dengan membuat profil terkait dengan aset teknologi informasi. Pada tahap pembuatan profil terkait aset teknologi informasi pertama-tama dibuat daftar aset kritis yang dimiliki oleh divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur. Daftar aset teknologi informasi didapatkan dari hasil wawancara dengan pihak divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur. Tingkat kritis aset TI telah ditentukan oleh perusahaan. Berikut ini hasil dari daftar aset teknologi informasi yang telah dibuat.

Tabel 6.1-4 Daftar Aset TI

Jenis Aset IT	ID Aset IT	Nama Aset IT	Deskripsi Fungsi Aset IT	Kategori Aset IT
Hardware	A01	UPS	Sebagai tenaga cadangan saat listrik mati	Kritis
	A02	AS400 (Banking Server)	Server perbankan yang menyimpan data-data transaksi	Kritis
	A03	AC Kering	Mendinginkan ruangan server	Kritis
	A04	Server	Menyediakan data dan aplikasi yang dibutuhkan oleh user.	Kritis
	A05	Notebook	Untuk membantu karyawan dalam melakukan pekerjaan	Minor
	A06	Firewall	Perangkat yang mengontrol dan membatasi akses masuk dari luar ke jaringan.	Penting
	A07	Genset	Tenaga pengganti saat listrik mati agar server tetap menyala	Kritis
Software	A08	Docnum (Document Management)	Software untuk mengelola dokumen	Penting
	A09	Security Application AS400	Aplikasi untuk menyimpan data terkait aktivitas dari AS400	Kritis
	A10	Aplikasi status cabang	Aplikasi untuk tracking status dari kantor cabang.	Kritis
	A11	Estim	Sistem informasi Corebanking	Kritis

Jenis Aset IT	ID Aset IT	Nama Aset IT	Deskripsi Fungsi Aset IT	Kategori Aset IT
	A12	Network Monitoring System	Aplikasi yang digunakan untuk	Kritis
	A13	Software Helpdesk	Aplikasi untuk melaporkan adanya gangguan.	Penting
	A14	Compleo	Mengenerate laporan dari core banking.	Kritis
	A15	Vulnerability Assessment System	Aplikasi untuk mendeteksi kerentanan pada sistem.	Penting
Data	A16	Database	Database berisi data user, transaksi, nasabah dan data cabang.	Kritis
Network	A17	Kabel Fiber Optik	Kabel yang mengalirkan internet.	Kritis
	A18	Switch	Membagi jaringan	Kritis
	A19	Main Router	pembagi atau penyalur IP address secara stastis atau memakai DHCP kepada seluruh perangkat komputer atau laptop yang terhubung pada perangkat router	Kritis
People	A20	Staff departemen Teknologi Informasi	Karyawan yang bekerja pada departemen Teknologi Informasi	Kritis
	A21	Staff Non Departemen TI	Karyawan yang bekerja pada	Kritis

Jenis Aset IT	ID Aset IT	Nama Aset IT	Deskripsi Fungsi Aset IT	Kategori Aset IT
			departemen selain Teknologi Informasi	

Tabel 6.1-5 Daftar Aset Kritis

Jenis Aset IT	ID Aset IT	Nama Aset IT
Hardware	A01	UPS
	A02	AS400 (Banking Server)
	A03	AC Kering
	A04	Server
	A07	Genset
Software	A09	Security Application AS400
	A10	Aplikasi status cabang
	A11	Estim
	A12	Network Monitoring System
	A14	Compleo
Data	A16	Database
Network	A17	Kabel Fiber Optik
	A18	Switch
	A19	Main Router
People	A20	Staff departemen Teknologi Informasi
	A21	Staff Non Departemen TI

Setelah membuat daftar aset kritis, selanjutnya adalah membuat daftar kebutuhan keamanan aset kritis berdasarkan aspek CIA Triad. Hal ini dilakukan agar dapat diketahui bagaimana kebutuhan keamanan untuk setiap aset kritis sehingga dapat diketahui apa saja yang perlu dilakukan oleh organisasi. Berikut ini merupakan kebutuhan keamanan aset kritis.

Tabel 6.1-6 Daftar Kebutuhan Keamanan

Nama Aset TI	Kebutuhan Keamanan berdasar CIA Triad	Penjelasan
UPS	Availability (Ketersediaan)	UPS harus tersedia pada saat diperlukan.
AS400 (Banking Server)	Confidentiality (kerahasiaan)	Pihak yang tidak memiliki wewenang tidak boleh mengakses server.

Nama Aset TI	Kebutuhan Keamanan berdasar CIA Triad	Penjelasan
	Integrity (Integritas)	Diperlukan autentikasi untuk dapat mengakses server
	Availability (Ketersediaan)	Server dapat diakses selama 24 jam
AC Kering	Availability (Ketersediaan)	AC harus menyala 24 jam
Server	Confidentiality (kerahasiaan)	Pihak yang tidak memiliki wewenang tidak boleh mengakses server.
	Integrity (Integritas)	Diperlukan autentikasi untuk dapat mengakses server
	Availability (Ketersediaan)	Server dapat diakses selama 24 jam
Genset	Availability (Ketersediaan)	Genset harus bisa digunakan saat listrik padam
Security Application AS400	Confidentiality (kerahasiaan)	Dilengkapi autentikasi sebelum mengakses software.
	Integrity (Integritas)	Terdapat validasi sebelum melakukan input dan modifikasi.
	Availability (Ketersediaan)	Software selalu dapat diakses saat dibutuhkan.
Aplikasi status cabang	Confidentiality (kerahasiaan)	Dilengkapi autentikasi sebelum mengakses software.
	Integrity (Integritas)	Aplikasi harus menampilkan data terkini.
	Availability (Ketersediaan)	Software selalu dapat diakses saat dibutuhkan.
Estim	Confidentiality (kerahasiaan)	Untuk dapat mengakses aplikasi, diharuskan memasukkan password.
	Integrity (Integritas)	Terdapat hak akses yang berbeda untuk setiap user.
	Availability (Ketersediaan)	Software Estim harus dapat diakses selama 24 jam.

Nama Aset TI	Kebutuhan Keamanan berdasar CIA Triad	Penjelasan
Network Monitoring System	Confidentiality (kerahasiaan)	Dilengkapi autentikasi sebelum mengakses software.
	Integrity (Integritas)	Aplikasi harus menampilkan data secara *realtime*.
	Availability (Ketersediaan)	Software selalu dapat diakses saat dibutuhkan.
Compleo	Confidentiality (kerahasiaan)	Dilengkapi autentikasi sebelum mengakses software.
	Integrity (Integritas)	Aplikasi menampilkan data yang benar.
	Availability (Ketersediaan)	Software selalu dapat diakses saat dibutuhkan.
Database	Confidentiality (kerahasiaan)	Data harus dienkripsi.
	Integrity (Integritas)	Terdapat hak akses yang berbeda untuk setiap user dan departemen
	Availability (Ketersediaan)	Data Nasabah harus bisa selalu diakses.
	Integrity (Integritas)	Terdapat hak akses yang berbeda untuk setiap user dan departemen
	Availability (Ketersediaan)	Data Cabang harus bisa selalu diakses.
Kabel Fiber Optik	Availability (Ketersediaan)	Jaringan harus terus menyala selama 24 jam.
Switch	Availability (Ketersediaan)	Switch harus terus menyala.
Main Router	Confidentiality (kerahasiaan)	Router harus diletakkan pada tempat yang tersembunyi dan diberi pelindung agar tidak mudah diotak-atik.
	Integrity (Integritas)	Hanya pegawai dengan hak akses yang bisa mengkonfigurasi router.
	Availability (Ketersediaan)	Router harus terus menyala
	Confidentiality (kerahasiaan)	Data pribadi pegawai dan yang berkaitan dengan

Nama Aset TI	Kebutuhan Keamanan berdasar CIA Triad	Penjelasan
Staff departemen Teknologi Informasi		perusahaan ada yang harus dirahasiakan guna mengantisipasi kebocoran data yang bisa terjadi
	Integrity (Integritas)	Terdapat SOP pegawai.
	Availability (Ketersediaan)	Terdapat kontrak kerja pegawai.
Staff Non Departemen TI	Confidentiality (kerahasiaan)	Data pribadi pegawai dan yang berkaitan dengan perusahaan ada yang harus dirahasiakan guna mengantisipasi kebocoran data yang bisa terjadi
	Integrity (Integritas)	Terdapat SOP pegawai.
	Availability (Ketersediaan)	Terdapat kontrak kerja pegawai.

Setelah mendefinisikan kebutuhan keamanan dari aset, dibuat ancaman yang dapat menimpa aset. Ancaman yang dapat menimpa aset dikelompokkan berdasarkan kategori dari aset kritis. Analisis terhadap ancaman dikategorikan sesuai dengan jenis dari aset teknologi informasi. Berikut ini merupakan daftar ancaman yang dapat menimpa aset Teknologi Informasi.

Tabel 6.1-7 Daftar Ancaman Aset TI

Kategori Aset Kritis	Ancaman	Penyebab
Hardware	*Hardware Failure*	Pemeliharaan yang tidak teratur
		Usia perangkat yang sudah melebihi batas.
		Kondisi lingkungan perangkat tidak sesuai (suhu ruang dan kelembapan)
	Gempa Bumi	Ketidakstabilan alam
	Power Failure	Pemadaman listrik
		Kabel daya terputus

Kategori Aset Kritis	Ancaman	Penyebab
		Arus pendek listrik
	Kebakaran	Api / Ledakan
		Arus pendek listrik
	Sabotase	Kurang pengawasan
		Tidak ada penanggungjawab
	Banjir	Ketidakstabilan alam
		Kebocoran saluran air
	Cyber Crime	Virus dan Malware
		Social Engineering
		Hacker
Software	*Cyber Crime*	Virus dan Malware
		Hacker
		Social Engineering
	Software Failure	*Software Bug*
		Software incompatible
		Overload Request
		Out of date software version
Data	*Data Corruption*	Terjadi kesalahan saat pemrosesan data
		Virus atau malware
		Kerusakan pada lokasi penyimpanan
	Pencurian Data dan Informasi	Unauthorized user
		Hacker
	Data Loss	Kerusakan server penyimpanan data
		Virus dan malware
		Hacker
		Kapasitas penyimpanan penuh
		Terhapus secara tidak sengaja
Network	*Network Failure*	Terputusnya jaringan dari service provider
		Kabel terputus
	Kerusakan	Pemeliharaan yang tidak teratur
		Usia perangkat melebihi batas
	Power Failure	Pemadaman listrik
		Kabel daya terputus

Kategori Aset Kritis	Ancaman	Penyebab
		Arus pendek listrik
People	*Social Engineering*	Kurangnya pengetahuan karyawan
	Kecelakaan	Terjadi bencana alam
		Terjadi kecelakaan kerja

Selanjutnya adalah membuat praktik keamanan yang telah dilakukan organisasi. Hal ini dilakukan untuk mengetahui bagaimana pengamanan yang telah dilakukan organisasi untuk menghadapi ancaman. Dengan mengetahui praktik keamanan yang telah diterapkan organisasi nantinya akan membantu dalam penilaian deteksi dari risiko. Praktik kemanan didapatkan dari hasil observasi terhadap ruang data center dan kondisi perusahaan. Berikut ini adalah praktik keamanan yang telah dilakukan oleh divisi teknologi informasi dari Bank Pembangunan Daerah Jawa Timur.

Tabel 6.1-8 Praktik Keamanan Organisasi

Jenis Aset IT	Nama Aset IT	Praktik Kemanan
Hardware	UPS	Menggunakan door access pada ruang penyimpanan UPS (ruang data center) Membatasi orang yang masuk ke ruang data center Dilakukan pengecekan dan pemeliharaan secara rutin
	AS400 (Banking Server)	Menggunakan door access pada ruang server Mengaktifkan firewall dan memasang firewall hardware Memasang CCTV Memasang sensor suhu dan kelembapan Memasang sensor kebakaran Menggunakan genset sebagai sumber tenaga cadangan Membatasi orang yang masuk ke ruang server Dilakukan backup secara rutin Dilakukan pemeliharaan secara rutin

Jenis Aset IT	Nama Aset IT	Praktik Kemanan
	AC Kering	Menggunakan door access pada ruang penyimpanan UPS (ruang data center) Membatasi orang yang masuk ke ruang data center Dilakukan pengecekan dan pemeliharaan secara rutin
	Server	Menggunakan door access pada ruang server Mengaktifkan firewall dan memasang firewall hardware Memasang CCTV Memasang sensor suhu dan kelembapan Memasang sensor kebakaran Menggunakan genset sebagai sumber tenaga cadangan Membatasi orang yang masuk ke ruang server Dilakukan backup secara rutin Dilakukan pemeliharaan secara rutin
	Genset	Menyediakan ventilasi pada ruang genset Dilakukan pemeliharaan dan pengecekan secara rutin
Software	Security Application AS400	Hanya user tertentu yang dapat mengakses Untuk masuk ke aplikasi harus memiliki username dan password.
	Aplikasi status cabang	Hanya user tertentu yang dapat mengakses
	Estim	Hanya user yang terdaftar yang dapat mengakses Untuk masuk ke aplikasi harus memiliki username dan password.
	Network Monitoring System	Hanya user tertentu yang dapat mengakses
	Compleo	Hanya user tertentu yang dapat mengakses Untuk masuk ke aplikasi harus memiliki username dan password.

Jenis Aset IT	Nama Aset IT	Praktik Kemanan
Data	Database	Database dibackup secara berkala Membuat mirror database
Network	Kabel Fiber Optik	Meletakkan kabel ditempat tersembunyi Melakukan pengecekan dan pemeliharaan rutin terhadap kabel
	Switch	Meletakkan switch pada lokasi tersembunyi Melakukan pengecekan dan pemeliharaan rutin terhadap switch
	Main Router	Meletakkan router pada lokasi tersembunyi Melakukan pengecekan dan pemeliharaan rutin terhadap router
People	Staff departemen Teknologi Informasi	Prosedur dan panduan pegawai.
	Staff Non Departemen TI	Prosedur dan panduan pegawai.

Kemudian dilakukan pembuatan kelemahan yang dimiliki oleh organisasi. Kelemahan organisasi akan menjadi masukan dalam melakukan analisa terhadap risiko. Berikut ini daftar dari kelemahan yang dimiliki oleh organisasi.

Tabel 6.1-9 Daftar Kelemahan Organisasi

Kategori	Kelemahan	Deskripsi
Software	Tidak terdapat alert pada log aktivitas yang mencurigakan dari user.	Log aktivitas user di review satu per satu, belum terdapat alert yang mendeteksi aktivitas yang mencurigakan.

Selanjutnya adalah melakukan identifikasi terhadap komponen utama dari aset dan kerentanannya. Hasil dari identifikasi adalah berupa daftar komponen utama dari aset dan kelemahannya. Berikut ini adalah daftar komponen utama aset teknologi informasi.

Tabel 6.1-10 Komponen Utama Aset TI

Nama Aset Kritis	Komponen Utama Aset Kritis	Ancaman pada Aset Utama berdasarkan Komponen
AS400 (Banking Server)	Sistem Operasi	Sistem Operasi terkena virus
		Sistem Operasi diretas
	Firewall	Firewall diretas
	Antivirus	Antivirus *Out of Date*
Server	Sistem Operasi	Sistem Operasi terkena virus
		Sistem Operasi diretas
	Firewall	Firewall diretas
	Antivirus	Antivirus *Out of Date*
Database	Hardisk Server	Hardisk rusak
		Kapasitas hardisk terbatas
Jaringan WAN	Kabel	Kabel terputus
	Router	Listrik mati Kerusakan Kesalahan konfigurasi
Pegawai	Pengetahuan	Human error Penyalahgunaan wewenang

Setelah komponen utama dari aset TI diketahui, selanjutnya diidentifikasi kerentanan dari aset TI. Dari hasil kerentanan akan dapat digunakan untuk melakukan analisis lebih dalam terkait risiko yang dapat menimpa aset berdaasar komponennya. Berikut ini merupakan daftar kerentanan dari komponen utama aset teknologi informasi.

Tabel 6.1-11 Daftar Kerentanan Aset Kritis

Nama aset kritis	Kerentanan aset kritis
AS400 (Banking Server)	Sistem Operasi dapat terkena virus
	Sistem operasi dapat diretas oleh hacker
	Antivirus harus selalu di update
Server	Sistem Operasi dapat terkena virus
	Sistem operasi dapat diretas oleh hacker
	Antivirus harus selalu di update

Nama aset kritis	Kerentanan aset kritis
Database	Keterbatasan kapasitas hardisk
Jaringan WAN	Peletakan kabel harus rapi agar kabel tidak terputus
Pegawai	Pegawai dapat menyalahgunakan wewenang
	Pegawai dapat lalai dalam melaksanakan tugas sehingga menimbulkan kesalahan

Sehingga dari rangkaian tahap analisis risiko dengan pendekatan OCTAVE yang telah dilakukan didapatkan risiko yang mungkin terjadi pada aset Teknologi Informasi. Berikut ini risiko pada aset kritis divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur.

Tabel 6.1-12 Daftar Risiko TI

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab
UPS	*Hardware Failure*	H01	UPS rusak	Pemeliharaan yang tidak teratur
		H02		Kondisi perangkat yang tidak layak
		H03		Usia perangkat yang sudah melebihi batas.
	Kebakaran	H04	UPS terbakar	Api / Ledakan
		H05		Arus pendek listrik
AS400 (Banking Server)	*Hardware Failure*	H06	Server rusak	Pemeliharaan yang tidak teratur
		H07		Usia server lebih dari 5 tahun .
		H08		Kondisi lingkungan perangkat tidak sesuai (suhu ruang dan kelembapan)
	Gempa Bumi	H09	Server rusak	Ketidakstabilan alam
	Power Failure	H10	Server Mati	Pemadaman listrik

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab
		H11		Kabel daya terputus
		H12		Arus pendek listrik
	Kebakaran	H13	Server Terbakar	Api / Ledakan
		H14		Arus pendek listrik
	Sabotase	H15	Penyalahgunaan Server	Kurang pengawasan
		H16		Tidak ada penanggungjawab
	Banjir	H17	Server Rusak	Kebocoran saluran air
	Cyber Crime	H18	Server Diretas	Virus dan Malware
		H19		Hacker
AC Kering	*Power Failure*	H20	AC Mati	Pemadaman listrik
		H21		Kabel daya terputus
		H22		Arus pendek listrik
	Hardware Failure	H23	AC Rusak	Pemeliharaan yang tidak teratur
		H24		Usia perangkat yang sudah melebihi batas.
	Banjir	H25	AC Rusak	Kebocoran saluran air pembuangan
Server	*Hardware Failure*	H26	Server Rusak	Pemeliharaan yang tidak teratur
		H27		Usia perangkat yang sudah melebihi batas.
		H28		Kondisi lingkungan perangkat tidak sesuai (suhu ruang dan kelembapan)
	Gempa Bumi	H29	Server Rusak	Ketidakstabilan alam

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab
	Power Failure	H30	Server Mati	Pemadaman listrik
		H31		Kabel daya terputus
		H32		Arus pendek listrik
	Kebakaran	H33	Server Terbakar	Api / Ledakan
		H34		Arus pendek listrik
	Sabotase	H35	Penyalahgunaan Server	Kurang pengawasan
		H36		Tidak ada penanggungjawab
	Banjir	H37		Kebocoran saluran air
	Cyber Crime	H38	Server Diretas	Virus dan Malware
		H39		Hacker
Genset	*Hardware Failure*	H40	Genset Rusak	Pemeliharaan yang tidak teratur
		H41		Usia perangkat yang sudah melebihi batas.
		H42		Pengisian bahan bakar yang tidak sesuai
Security Application AS400	*Cyber Crime*	S01	Software diretas	Virus dan Malware
		S02		*Hacker*
				Social Engineering
	Software Failure	S03	Software tidak dapat diakses	*Software Bug*
		S04		*Operating System incompatible*
		S05		*Overload Request*
		S06		*Out of date software version*
Aplikasi status cabang	*Cyber Crime*	S07	Software Diretas	Virus dan Malware
		S08		*Hacker*
		S09		*Social Engineering*

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab
	Software Failure	S10	Software tidak dapat diakses	*Software Bug*
		S11		*Software incompatible*
		S12		*Overload Request*
		S13		*Out of date software version*
Estim	*Cyber Crime*	S14	Software Diretas	Virus dan Malware
		S15		*Hacker*
		S16		*Social Engineering*
	Software Failure	S17	Software tidak dapat diakses	*Software Bug*
		S18		*Software incompatible*
		S19		*Overload Request*
		S20		*Out of date software version*
Network Monitoring System	*Cyber Crime*	S21	Software Diretas	Virus dan Malware
		S22		*Hacker*
		S23		*Social Engineering*
	Software Failure	S24	Software tidak dapat diakses	*Software Bug*
		S25		*Software incompatible*
		S26		*Overload Request*
		S27		*Out of date software version*
Compleo	*Cyber Crime*	S21	Software Diretas	Virus dan Malware
		S22		*Hacker*
		S23		*Social Engineering*
	Software Failure	S24	Software tidak dapat diakses	*Software Bug*
		S25		*Software incompatible*
		S26		*Overload Request*
		S27		*Out of date software version*
Database	*Data Corruption*	D01	Data Rusak	Terjadi kesalahan saat pemrosesan data

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab
		D02		Virus atau malware
		D03		Kerusakan pada lokasi penyimpanan
	Pencurian Data dan Informasi	D04	Data Dicuri	Unauthorized user
		D05		Hacker
	Data Loss	D06	Data hilang	Kerusakan server penyimpanan data
		D07		Virus dan malware
		D08		Hacker
		D09		Kapasitas penyimpanan penuh
		D10		Terhapus secara tidak sengaja
Kabel Fiber Optik	*Network Failure*	N01	Jaringan Terputus	Terputusnya jaringan dari service provider
		N02		Kabel terputus
Switch	Kerusakan	N03	Switch Rusak	Terputusnya jaringan dari service provider
		N04		Kabel terputus
	Power Failure	N05	Switch Mati	Pemadaman listrik
		N06		Kabel terputus
		N07		Konslet listrik
Main Router	Kerusakan	N08	Router Rusak	Pemeliharaan yang tidak teratur
		N09		Kondisi perangkat yang tidak layak
	Power Failure	N10	Router Mati	Pemadaman listrik
		N11		Kabel terputus
		N12		Konslet listrik
Staff departeme n	*Social Engineering*	P01	Penyalahg unaan akses oleh	Kurangnya pengetahuan karyawan

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab
Teknologi Informasi			orang asing	
	Kecelakaan	P02	Staff Terluka	Terjadi bencanan alam
		P03		Terjadi kecelakaan kerja
Staff Non Departemen TI	*Social Engineering*	P04	Penyalahgunaan akses oleh orang asing	Kurangnya pengetahuan karyawan
	Kecelakaan	P05	Staff Terluka	Terjadi bencana alam
		P06		Terjadi kecelakaan kerja

6.1.2.2 Penilaian Risiko

Pada tahap penilaian risiko diberikan nilai pada setiap risiko yang ada. Penilaian dilakukan dengan menggunakan metode FMEA. Pada metode FMEA terdapat tiga aspek dalam penilaian risiko sebelum didapatkan RPN atau nilai akhir risiko. Nilai RPN digunakan untuk melakukan prioritisasi terhadap risiko. Tiga aspek yang terdapat pada penilaian metode FMEA adalah *Severity*, *Occurence* dan *Detection*. Nilai dari ketiga aspek tersebut didapatkan sesuai dengan keadaan yang ada pada organisasi yang telah didefinisikan pada proses analisis risiko. Justifikasi penilaian risiko dapat dilihat pada Lampiran C. Berikut ini adalah hasil analisis risiko pada divisi teknologi informasi.

Tabel 6.1-13 Penilaian Risiko

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
UPS	*Hardware Failure*	H01	UPS rusak	Pemeliharaan yang tidak teratur	3	3	3	27	Low
		H02		Kondisi perangkat yang tidak layak	6	2	3	36	Low
		H03		Usia perangkat yang sudah melebihi batas.	2	2	2	8	Very Low
	Kebakaran	H04	UPS terbakar	Api / Ledakan	10	1	1	10	Very Low
		H05		Arus pendek listrik	10	1	5	50	Low
AS400 (Banking Server)	*Hardware Failure*	H06	Server rusak	Pemeliharaan yang tidak teratur	8	1	1	8	Very Low
		H07		Usia server lebih dari 5 tahun .	5	1	1	5	Very Low
		H08		Kondisi lingkungan perangkat tidak sesuai (suhu ruang dan kelembapan)	2	1	1	2	Very Low
	Gempa Bumi	H09	Server rusak	Ketidakstabilan alam	8	1	1	8	Very Low
	Power Failure	H10	Server Mati	Pemadaman listrik	8	1	1	8	Very Low

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
		H11		Kabel daya terputus	5	1	1	5	Very Low
		H12		Arus pendek listrik	10	1	1	10	Very Low
	Kebakaran	H13	Server Terbakar	Api / Ledakan	10	1	1	10	Very Low
		H14		Arus pendek listrik	10	1	1	10	Very Low
	Sabotase	H15	Penyalah gunaan Server	Kurang pengawasan	9	1	1	9	Very Low
		H16		Tidak ada penanggungjawab	9	1	1	9	Very Low
	Banjir	H17	Server Rusak	Kebocoran saluran air	8	1	1	8	Very Low
	Cyber Crime	H18	Server Diretas	Virus dan Malware	9	1	1	9	Very Low
		H19		Hacker	9	1	1	9	Very Low
AC Kering	*Power Failure*	H20	AC Mati	Pemadaman listrik	3	2	1	6	Very Low
		H21		Kabel daya terputus	3	1	4	12	Very Low

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
		H22		Arus pendek listrik	3	1	5	15	Very Low
	Hardware Failure	H23	AC Rusak	Pemeliharaan yang tidak teratur	3	1	2	6	Very Low
		H24		Usia perangkat yang sudah melebihi batas.	3	1	2	6	Very Low
	Banjir	H25	AC Rusak	Kebocoran saluran air pembuangan	5	2	3	30	Low
Server	*Hardware Failure*	H26	Server Rusak	Pemeliharaan yang tidak teratur	8	1	1	8	Very Low
		H27		Usia perangkat yang sudah melebihi batas.	5	1	1	5	Very Low
		H28		Kondisi lingkungan perangkat tidak sesuai (suhu ruang dan kelembapan)	2	1	1	2	Very Low
	Gempa Bumi	H29	Server Rusak	Ketidakstabilan alam	8	1	1	8	Very Low
	Power Failure	H30	Server Mati	Pemadaman listrik	8	1	1	8	Very Low
		H31		Kabel daya terputus	5	1	1	5	Very Low

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
		H32		Arus pendek listrik	10	1	1	10	Very Low
	Kebakaran	H33	Server Terbakar	Api / Ledakan	10	1	1	10	Very Low
		H34		Arus pendek listrik	10	1	1	10	Very Low
	Sabotase	H35	Penyalah gunaan Server	Kurang pengawasan	9	1	1	9	Very Low
		H36		Tidak ada penanggungjawab	9	1	1	9	Very Low
	Banjir	H37		Kebocoran saluran air	8	1	1	8	Very Low
	Cyber Crime	H38	Server Diretas	Virus dan Malware	9	1	1	9	Very Low
		H39		Hacker	9	1	1	9	Very Low
Genset	*Hardware Failure*	H40	Genset Rusak	Pemeliharaan yang tidak teratur	5	2	2	20	Very Low
		H41		Usia perangkat yang sudah melebihi batas.	3	1	2	6	Very Low
		H42		Pengisian bahan bakar yang tidak sesuai	2	1	1	2	Very Low

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
Security Application AS400	*Cyber Crime*	S01	Software diretas	Virus dan Malware	9	1	1	9	Very Low
		S02		*Hacker*	9	1	1	9	Very Low
				Social Engineering	9	1	1	9	Very Low
	Software Failure	S03	Software tidak dapat diakses	*Software Bug*	3	1	1	3	Very Low
		S04		*Operating System incompatible*	8	1	1	8	Very Low
		S05		*Overload Request*	5	1	1	5	Very Low
		S06		*Out of date software version*	8	1	1	8	Very Low
Aplikasi status cabang	*Cyber Crime*	S07	Software Diretas	Virus dan Malware	2	1	1	2	Very Low
		S08		*Hacker*	2	1	1	2	Very Low
		S09		*Social Engineering*	2	1	1	2	Very Low
	Software Failure	S10	Software tidak	*Software Bug*	2	1	1	2	Very Low

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
		S11	dapat diakses	*Software incompatible*	2	1	1	2	Very Low
		S12		*Overload Request*	2	1	1	2	Very Low
		S13		*Out of date software version*	2	1	1	2	Very Low
Estim	*Cyber Crime*	S14	Software Diretas	Virus dan Malware	9	1	1	9	Very Low
		S15		*Hacker*	9	1	1	9	Very Low
		S16		*Social Engineering*	9	1	1	9	Very Low
	Software Failure	S17	Software tidak dapat diakses	*Software Bug*	5	1	1	5	Very Low
		S18		*Software incompatible*	8	1	1	8	Very Low
		S19		*Overload Request*	7	2	1	14	Very Low
		S20		*Out of date software version*	8	1	1	8	Very Low
Database	*Data Corruption*	D01	Data Rusak	Terjadi kesalahan saat pemrosesan data	7	1	1	7	Very Low

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
		D02		Virus atau malware	7	1	1	7	Very Low
		D03		Kerusakan pada lokasi penyimpanan	8	1	1	8	Very Low
	Pencurian Data dan Informasi	D04	Data Dicuri	Unauthorized user	9	1	1	9	Very Low
		D05		Hacker	9	1	1	9	Very Low
	Data Loss	D06	Data hilang	Kerusakan server penyimpanan data	8	1	1	8	Very Low
		D07		Virus dan malware	9	1	1	9	Very Low
		D08		Hacker	9	1	1	9	Very Low
		D09		Kapasitas penyimpanan penuh	8	1	1	8	Very Low
		D10		Terhapus secara tidak sengaja	8	1	1	8	Very Low
Kabel Fiber Optik	*Network Failure*	N01	Jaringan Terputus	Terputusnya jaringan dari service provider	5	1	1	5	Very Low
		N02		Kabel terputus	5	1	1	5	Very Low

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
Switch	Kerusakan	N03	Switch Rusak	Terputusnya jaringan dari service provider	5	1	3	15	Very Low
		N04		Kabel terputus	5	1	3	15	Very Low
	Power Failure	N05	Switch Mati	Pemadaman listrik	3	2	1	6	Very Low
		N06		Kabel terputus	3	2	3	18	Very Low
		N07		Arus pendek listrik	3	1	3	9	Very Low
Main Router	Kerusakan	N08	Router Rusak	Pemeliharaan yang tidak teratur	5	1	1	5	Very Low
		N09		Kondisi perangkat yang tidak layak	8	1	1	8	Very Low
	Power Failure	N10	Router Mati	Pemadaman listrik	5	2	1	10	Very Low
		N11		Kabel terputus	5	1	3	15	Very Low
		N12		Arus Pendek listrik	5	1	3	15	Very Low
Staff departeme	*Social Engineering*	P01	Penyalah gunaan	Kurangnya pengetahuan karyawan	9	1	1	9	Very Low

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	OCC	DET	RPN	Tingkat Risiko
n Teknologi Informasi			akses oleh orang asing						
	Kecelakaan	P02	Staff Terluka	Terjadi bencanan alam	10	1	1	10	Very Low
		P03		Terjadi kecelakaan kerja	10	1	1	10	Very Low
Staff Non Departemen TI	*Social Engineering*	P04	Penyalahgunaan akses oleh orang asing	Kurangnya pengetahuan karyawan	9	1	1	9	Very Low
	Kecelakaan	P05	Staff Terluka	Terjadi bencana alam	10	1	1	10	Very Low
		P06		Terjadi kecelakaan kerja	10	1	1	10	Very Low

Sehingga dari hasil penilaian risiko didapatkan risiko dengan nilai tertinggi yaitu pada tingkat Low. Risiko dengan tingkat tertinggi akan dijadikan input kepada pembuatan strategi keberlangsungan bisnis. Terdapat empat risiko dengan tingkat low, yaitu:

1. UPS rusak yang disebabkan oleh pemeliharaan yang tidak teratur.
2. UPS rusak yang disebabkan oleh kondisi perangkat yang tidak layak.
3. UPS terbakar yang disebabkan arus pendek listrik.
4. AC rusak yang disebabkan kebocoran saluran air pembuangan.

6.1.3 Analisis Dampak Bisnis

Tahap analisis dampak bisnis dilakukan untuk mengetahui bagaimana dampak dari gangguan terhadap proses bisnis. Dengan mengetahui dampak bisnis yang ditimbulkan, perusahaan akan lebih mudah dalam menentukan strategi yang perlu diambil jika terjadi gangguan. Tahap analisis dampak bisnis dilakukan dengan berdiskusi dan melakukan wawancara dengan pihak divisi TI.

6.1.3.1 Proses Bisnis dan Layanan TI

Tahap analisis dampak bisnis diawali dengan mendaftar proses bisnis terkait TI serta layanan TI yang digunakan. Hal ini dilakukan agar dapat diketahui proses bisnis apa saja yang dimiliki oleh setiap sub fungsional divisi TI. Daftar proses bisnis serta layanan TI yang digunakan didapatkan dari proses wawancara.Berikut ini daftar proses bisnis dan layanan TI yang ada pada divisi Teknologi Informasi.

Tabel 6.1-14 Daftar Proses Bisnis dan Layanan TI

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Sistem dan Layanan TI
Grup IT Infrastructure &Network Operation	Monitoring Availability Jaringan	Network Monitoring System
	Konfigurasi dan Hardening Aplikasi dan Perangkat TI	DOCNUM
Grup IT Management Information System	Permintaan Data	Compleo
	Monitoring Kapasitas	DOCNUM
	Restore & Recovery	Estim
Grup IT Support & Helpdesk	Penanganan Insiden	Aplikasi helpdesk
	Penambahan User	Security Application AS400
	Perubahan User	Security Application AS400
	Penghapusan User	Security Application AS400
Grup IT Security	Penanganan Insiden Pengamanan Informasi	Vulnerability Assessment System

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Sistem dan Layanan TI
	Monitoring Hak Akses Logis	Estim
	Review Log Hak Akses Logis	Security Application AS400
Grup IT Data Center	Akhir periode	Aplikasi Status Cabang

6.1.3.2 Prioritisasi Layanan TI

Pada tahap ini dilakukan prioritisasi terhadap layanan TI. Prioritisasi ditentukan oleh perusahaan berdasarkan dengan keguanaan aplikasi tersebut. Hal ini dilakukan agar dapat diketahui Layanan TI mana yang bersifat kritis pada perusahaan. Pada bagian ini, prioritisasi layanan TI didapatkan dari hasil wawancara dengan pihak divisi TI. Hal ini dikarenakan perusahaan telah membuat daftar layanan TI beserta tingkat kritisnya. Berikut ini layanan TI beserta tingkat kritisnya.

Tabel 6.1-15 Prioritisasi Layanan TI

Layanan TI	Tingkat Kritis
Docnum (Document Management)	Penting
Security Application AS400	Kritis
Aplikasi status cabang	Kritis
Estim	Kritis
Network Monitoring System	Kritis
Aplikasi Helpdesk	Penting
Compleo	Kritis
Vulnerability Assessment System	Penting

6.1.3.3 Prioritisasi Proses Bisnis

Pada tahap ini dilakukan prioritisasi terhadap proses bisnis yang terkait dengan layanan TI organisasi. Untuk membuat prioritisasi proses bisnis, dilakukan pemetaan terhadap tingkat tingkat kritis layanan TI yang digunakan dengan tingkat kritis proses bisnis. Berikut ini prioritisasi proses bisnis dari tiap sub fungsional yang ada pada divisi TI.

Tabel 6.1-16 Prioritisasi Proses Bisnis

Fungsional Bisnis	Proses Bisnis terkait Layanan Teknologi Informasi	Aktivitas terkait Layanan TI	Tingkat Kritis
Grup IT Infrastructure &Network Operation	Monitoring Availability Jaringan	Melakukan Monitoring Availability Jaringan TI	Kritis
		Mendokumentasikan Laporan Monitoring Availability Jaringan TI	
	Konfigurasi dan Hardening Aplikasi dan Perangkat TI	Mendokumentasikan Seluruh Dokumen Implementasi Konfigurasi	Penting
Grup IT Management Information System	Permintaan Data	Melakukan Identifikasi dan Penarikan Data	Kritis
	Monitoring Kapasitas	Mendokumentasikan Laporan Monitoring Kapasitas Hardware	Penting
	Restore & Recovery	Melakukan Restore	Kritis
Grup IT Support & Helpdesk	Penanganan Insiden	Menerima dan Mencatat Laporan Kejadian	Penting
	Inventarisasi	Mendokumentasikan Daftar Inventarisasi Aset TI	Penting
	Penambahan User	Menambahkan User ID Baru	Kritis
	Perubahan User	Melakukan Perubahan User	Kritis
	Penghapusan User	Melakukan Penghapusan User ID	Kritis
Grup IT Security	Penanganan Insiden Pengamanan Informasi	Melakukan Analisis Insiden untuk Pencegahan.	Penting
	Monitoring Hak Akses Logis	Melakukan Review Periodik dan Analisis atas Pemakaian Hak Akses Logis	Kritis

Fungsional Bisnis	Proses Bisnis terkait Layanan Teknologi Informasi	Aktivitas terkait Layanan TI	Tingkat Kritis
		Menyusun dan Mendokumentasikan Laporan Monitoring Pengamanan Informasi	
	Review Log Hak Akses Logis	Melakukan Review Logbook	Kritis
		Menyusun dan Mendokumentasikan Laporan Review Logbook	
Grup IT Data Center	Akhir periode	Melakukan Monitoring Status Closing Kantor Cabang/KCP	Kritis

6.1.3.4 Penentuan Waktu Pemulihan

Pada bagian ini, dilakukan penentuan terhadap waktu pemulihan terhadap proses bisnis dan layanan TI. Waktu pemulihan ditentukan berdasarkan dengan tingkat kritis dari proses bisnis. Perusahaan memiliki requirement yaitu proses bisnis dan layanan TI kritis tidak boleh down lebih dari 2 jam serta pemulihan tidak lebih dari 2 jam. Sedangkan pada proses bisnis dan layanan TI dengan tingkat penting, waktu maksimal *down time* adalah 24 jam dan waktu pemulihan hingga 7 hari.
Berikut ini waktu pemulihan proses bisnis dan layanan TI dari divisi TI. Waktu pemulihan dibutuhkan oleh perusahaan agar pada saat menjalankan strategi pemulihan dapat diketahui layanan TI mana yang perlu di prioritaskan untuk ditangani.
Untuk setiap proses bisnis ditentukan waktu pemulihannya dari gangguan. Waktu pemulihan dibagi menjadi tiga yaitu:

- *Maximum Tolerable Downtime* (MTD)

MTD adalah waktu maksimal yang dapat ditoleransi perusahaan terhadap kegagalan pada proses bisnis, layanan

serta aset TI atau waktu maksimal untuk menyediakan layanan *continuity system* hingga sistem kembali tersedia.

- *Recovery Time Objective* (RTO)

RTO merupakan waktu lumpuh maksimal bagi sumber daya sistem dan layanan TI atau waktu pengembalian proses bisnis, layanan dan aset setelah gangguan atau bencana terjadi.

- *Recovery Point Objective* (RPO)

RPO merupakan jumlah waktu yang diperlukan setelah terjadinya gangguan, untuk memulihkan data serta layanan backup daata setelah gangguan terjadi.

Berikut ini merupakan hasil waktu pemulihan proses bisnis dan layanan TI.

Tabel 6.1-17 Waktu Pemulihan Proses Bisnis dan Layanan TI

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Sistem dan Layanan TI	MTD	RTO	RPO
Grup IT Infrastructure &Network Operation	Monitoring Availability Jaringan	Network Monitoring System	<2 Jam	<2 Jam	< 2 Jam
	Konfigurasi dan Hardening Aplikasi dan Perangkat TI	DOCNUM	4 – 24 Jam	4 – 24 Jam	7 hari
Grup IT Management Information System	Permintaan Data	Compleo	<2 Jam	<2 Jam	< 2 Jam
	Monitoring Kapasitas	DOCNUM	4 – 24 Jam	4 – 24 Jam	7 hari
	Restore & Recovery	Estim	<2 Jam	<2 Jam	< 2 Jam
		Compleo	<2 Jam	<2 Jam	< 2 Jam
Grup IT Support & Helpdesk	Penanganan Insiden	Aplikasi helpdesk	4 – 24 Jam	4 – 24 Jam	7 hari

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Sistem dan Layanan TI	MTD	RTO	RPO
	Penambahan User	Security Application AS400	<2 Jam	<2 Jam	< 2 Jam
	Perubahan User	Security Application AS400	<2 Jam	<2 Jam	< 2 Jam
	Penghapusan User	Security Application AS400	<2 Jam	<2 Jam	< 2 Jam
Grup IT Security	Penanganan Insiden Pengamanan Informasi	Vulnerability Assessment System	4 – 24 Jam	4 – 24 Jam	7 hari
	Monitoring Hak Akses Logis	Estim	<2 Jam	<2 Jam	< 2 Jam
	Review Log Hak Akses Logis	Estim	<2 Jam	<2 Jam	< 2 Jam
		Security Application AS400	<2 Jam	<2 Jam	< 2 Jam
Grup IT Data Center	Akhir periode	Aplikasi Status Cabang	<2 Jam	<2 Jam	< 2 Jam

6.1.3.5 Analisis Dampak Gangguan

Pada analisis dampak gangguan dilakukan penilaian dampak terjadinya gangguan terhadap proses bisnis. Analisis dampak gangguan akan dikategorikan menjadi tiga, yaitu kerusakan ringan, sedang dan tinggi. Kerusakan ringan terjadi ketika waktu gangguan kurang dari MTD yang telah ditentukan perusahaan, sedangkan kerusakan sedang terjadi ketika waktu gangguan sama dengan MTD, dan kerusakan tinggi terjadi ketika waktu gangguan melebihi MTD yang ditentukan oleh perusahaan. Penentuan dampak gangguan dilakukan dengan diskusi dengan pihak divisi TI pada Bank Pembangunan Daerah Jawa Timur. Analisis dampak gangguan dilakukan untuk mengetahui apa saja dampak yang diakibatkan ketika terjadi gangguan. Analisis dampak ditinjau menjadi tiga aspek yaitu aspek finansial, reputasi dan operasional. Pada aspek finansial dianalisis berapa biaya tambahan yang harus dikeluarkan oleh perusahaan yang diakibatkan oleh kerusakan . Dilakukan estimasi kerugian finansial dengan membuat 5 jenis skala kerugian finansial Berikut ini jenis dampak pada aspek finansial serta hasil dari analisis dampak gangguan pada aspek finansial.

Tabel 6.1-18 Jenis dampak Gangguan pada aspek Finansial

Skala	Deskripsi
1	Kerugian finansial 0 - 5 juta
2	Kerugian finansial 5 - 15 juta
3	Kerugian finansial 15 – 30 juta
4	Kerugian finansial 30 – 50 juta
5	Kerugian finansial diatas 50 juta

Dampak pada aspek reputasi adalah ketika kerusakan yang terjadi mempengaruhi reputasi dari perusahaan. Reputasi perusahaan dapat dilihat dari kepercayaan pelanggan terhadap perusahaan. Dampak dari kerusakan pada aspek reputasi dinyatakan dalam lima jenis dampak. Berikut ini penjelasan dari jenis-jenis dampak kerusakan terhadap aspek reputasi.

Tabel 6.1-19 Jenis Dampak Gangguan pada Aspek Reputasi

Jenis Dampak	Penjelasan
Tidak berdampak terhadap reputasi perusahaan	Kerusakan tidak mempengaruhi kepercayaan pelanggan
Berdampak kecil terhadap reputasi perusahaan	Kerusakan menyebabkan kepercayaan pelanggan sedikit menurun
Berdampak sedang terhadap reputasi perusahaan	Kerusakan menyebabkan kepercayaan pelanggan menjadi negatif
Berdampak besar terhadap reputasi perusahaan	Kerusakan menyebabkan perusahaan kehilangan kepercayaan pelanggan
Berdampak sangat besar terhadap reputasi perusahaan	Kerusakan menyebabkan perusahaan kehilangan kepercayaan pelanggan sulit untuk diperbaiki.

Dampak pada aspek operasional adalah ketika kerusakan yang terjadi mempengaruhi operasional dari perusahaan dan menyebabkan ketidakpuasan terhadap pelanggan. Dampak dari kerusakan pada aspek operasional dinyatakan dalam lima jenis dampak. Berikut ini penjelasan dari jenis-jenis dampak kerusakan terhadap aspek operasional.

Tabel 6.1-20 Jenis Dampak Gangguan pada Aspek Operasional

Jenis Dampak	Penjelasan
Tidak berdampak terhadap operasional perusahaan	Kerusakan tidak menyebabkan komplain dan tidak menyebabkan penurunan kepuasan pelanggan.
Berdampak kecil terhadap operasional perusahaan	Kerusakan menyebabkan sedikit

	komplain dan tidak menyebabkan penurunan kepuasan pelanggan.
Berdampak sedang terhadap operasional perusahaan	Kerusakan menyebabkan sedikit komplain dan menyebabkan sedikit penurunan terhadap kepuasan pelanggan.
Berdampak besar terhadap operasional perusahaan	Kerusakan menyebabkan beberapa komplain dan menyebabkan banyak penurunan tingkat kepuasan pelanggan.
Berdampak sangat besar terhadap operasional perusahaan	Kerusakan menyebabkan banyak komplaindan terjadi ketidakpuasan pelanggan terhadap perusahaan.

Berikut ini adalah dampak gangguan pada aspek finansial, reputasi dan operasional.

Tabel 6.1-21 Dampak Gangguan

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Finansial			Reputasi			Operasional		
		Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi
Grup IT Infrastructure &Network Operation	Monitoring Availability Jaringan	Kerugian Finansial 0 – 5 juta	Kerugian finansial 5 - 15 juta	Kerugian finansial 15 – 30 juta	Berdampak kecil terhadap reputasi perusahaan	Berdampak sedang terhadap reputasi perusahaan	Berdampak besar terhadap reputasi perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak besar terhadap operasional perusahaan
Grup IT Management Information System	Permintaan Data	Kerugian finansial 15 – 30 juta	Kerugian finansial 30 – 50 juta	Kerugian finansial diatas 50 juta	Berdampak sedang terhadap reputasi perusahaan	Berdampak besar terhadap reputasi perusahaan	Berdampak sangat besar terhadap reputasi perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak besar terhadap operasional perusahaan	Berdampak sangat besar terhadap operasional perusahaan

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Finansial			Reputasi			Operasional		
		Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi
	Monitoring Kapasitas	Kerugian finansial 15 – 30 juta	Kerugian finansial 30 – 50 juta	Kerugian finansial diatas 50 juta	Berdampak kecil terhadap reputasi perusahaan	Berdampak sedang terhadap reputasi perusahaan	Berdampak besar terhadap reputasi perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak besar terhadap operasional perusahaan
	Konfigurasi dan Hardening Aplikasi dan Perangkat TI	Ketugian Finansial 0 – 5 juta	Ketugian Finansial 0 – 5 juta	Ketugian Finansial 0 – 5 juta	Berdampak kecil terhadap reputasi perusahaan	Berdampak sedang terhadap reputasi perusahaan	Berdampak sangat besar terhadap reputasi perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak sangat besar terhadap operasional perusahaan
	Restore & Recovery	Kerugian finansia	Kerugian finansia	Kerugian finansia	Berdampak kecil terhadap	Berdampak sedang terhadap	Berdampak sedang terhadap	Berdampak kecil terhadap	Berdampak sedang terhadap	Berdampak sedang terhadap

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Finansial			Reputasi			Operasional		
		Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi
		l 15 – 30 juta	l 30 – 50 juta	l diatas 50 juta	reputasi perusahaan	reputasi perusahaan	reputasi perusahaan	operasional perusahaan	operasional perusahaan	operasional perusahaan
Grup IT Support & Helpdesk	Penanganan Insiden	Kerugian finansial 15 – 30 juta	Kerugian finansial 30 – 50 juta	Kerugian finansial diatas 50 juta	Berdampak sedang terhadap reputasi perusahaan	Berdampak besar terhadap reputasi perusahaan	Berdampak sangat besar terhadap reputasi perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak besar terhadap operasional perusahaan	Berdampak sangat besar terhadap operasional perusahaan
	Penambahan User	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Berdampak kecil terhadap reputasi perusahaan	Berdampak sedang terhadap reputasi perusahaan	Berdampak besar terhadap reputasi perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak besar terhadap operasional perusahaan

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Finansial			Reputasi			Operasional		
		Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi
	Perubahan User	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Berdampak kecil terhadap reputasi perusahaan	Berdampak sedang terhadap reputasi perusahaan	Berdampak besar terhadap reputasi perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak besar terhadap operasional perusahaan
	Penghapusan User	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Berdampak kecil terhadap reputasi perusahaan	Berdampak sedang terhadap reputasi perusahaan	Berdampak besar terhadap reputasi perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak besar terhadap operasional perusahaan
Grup IT Security	Penanganan Insiden Pengamanan Informasi	Kerugian finansial 15 – 30 juta	Kerugian finansial 30 – 50 juta	Kerugian finansial diatas 50 juta	Berdampak sedang terhadap reputasi	Berdampak besar terhadap reputasi	Berdampak sangat besar terhadap	Berdampak sedang terhadap operasio	Berdampak besar terhadap operasio	Berdampak sangat besar terhadap

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Finansial			Reputasi			Operasional		
		Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi
					perusahaan	perusahaan	reputasi perusahaan	nal perusahaan	nal perusahaan	operasional perusahaan
	Monitoring Hak Akses Logis	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Berdampak kecil terhadap reputasi perusahaan	Berdampak kecil terhadap reputasi perusahaan	Berdampak sedang terhadap reputasi perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak sedang terhadap operasional perusahaan
	Review Log Hak Akses Logis	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Berdampak kecil terhadap reputasi perusahaan	Berdampak kecil terhadap reputasi perusahaan	Berdampak sedang terhadap reputasi perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak kecil terhadap operasional perusahaan	Berdampak sedang terhadap operasional perusahaan

Fungsional Bisnis	Proses Bisnis terkait Teknologi Informasi	Finansial			Reputasi			Operasional		
		Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi	Kerusakan Ringan	Kerusakan Sedang	Kerusakan Tinggi
Grup IT Data Center	Akhir periode	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Kerugian Finansial 0 – 5 juta	Berdampak sedang terhadap reputasi perusahaan	Berdampak besar terhadap reputasi perusahaan	Berdampak sangat besar terhadap reputasi perusahaan	Berdampak sedang terhadap operasional perusahaan	Berdampak besar terhadap operasional perusahaan	Berdampak sangat besar terhadap operasional perusahaan

6.1.4 Strategi Keberlangsungan Bisnis

Pada bagian ini, strategi keberlangsungan bisnis dibuat berdasarkan hasil analisis risiko dan analisis dampak bisnis yang telah dilakukan sebelumnya. Strategi keberlangsungan bisnis atau strategi BCP merupakan langkah-langkah yang dilakukan agar proses bisnis perusahaan tetap berjalan di tengah gangguan yang terjadi. Strategi keberlangsungan bisnis pada divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur terbagi menjadi strategi aksi manajemen serta strategi yang bersifat lebih teknis yaitu strategi menanggulangi risiko. Pada setiap strategi dibuat strategi preventif, strategi saat gangguan, strategi pemulihan serta strategi korektif.

6.1.4.1 Strategi Aksi Manajemen

Strategi aksi manajemen merupakan respon dari manajemen terhadap gangguan pada proses bisnis. Strategi dibuat untuk mempertahankan proses bisnis dengan kategori kritis dan penting pada perusahaan. Strategi kebelangsungan proses bisnis mencakup kepada strategi preventif, saat gangguan, pemulihan dan korektif.

1. Strategi Preventif

Strategi preventif merupakan tindakan yang dilakukan dalam rangka mencegah kemungkinan terjadinya gangguan pada proses bisnis. Berikut ini merupakan strategi preventif untuk menjaga keberlangsungan proses bisnis.

Tabel 6.1-22 Strategi preventif

Strategi	Keterangan	Bentuk Kontrol
Melakukan pemeliharaan dan update rutin terhadap layanan TI yang digunakan	Layanan TI yang digunakan dalam proses bisnis yang kritis dan penting di update secara rutin serta dilakukan pemeliharaan terhadap perangkat hardware yang	Kebijakan Pemeliharaan

Strategi	Keterangan	Bentuk Kontrol
	digunakan dalam proses bisnis.	
Menyediakan server backup	Server backup disediakan sebagai cadangan jika server utama mengalami gangguan sehingga layanan TI yang digunakan dalam proses bisnis perusahaan.	Kebijakan Penyediaan Sistem Cadangan
Melakukan backup sistem secara rutin	Backup terhadap data dan sistem layanan TI yang digunakan dalam proses bisnis dilakukan agar jika terdapat gangguan yang menyebabkan data hilang, data-data penting dapat di restore kembali untuk digunakan.	Kebijakan Backup dan Recovery
Menyediakan DRC	Disaster Recovery Center dibuat agar saat terjadi bencana besar dan merusak server utama maupun perangkat pendukungnya, proses bisnis tetap dapat berjalan.	Kebijakan Penggunaan DRC
Melakukan monitoring dan analisis terhadap aktivitas user dan sistem	Monitoring dan analisis terhadap aktivitas user dan sistem dilakukan untuk memastikan keamanan dan mengantisipasi terjadinya gangguan pada sistem yang dapat berdampak pada terganggunya proses bisnis.	Kebijakan Monitoring dan Evaluasi User
Menyediakan helpdesk	Helpdesk disediakan agar dapat membantu menangani permasalahan yang terjadi pada saat ada gangguan.	Kebijakan Penyediaan Heldesk

2. Strategi saat gangguan

Strategi saat gangguan merupakan langkah-langkah atau aksi yang dilakukan ketika gangguan terjadi. Aksi ini dilakukan untuk dapat mengatasi gangguan dan mengembalikan proses

bisnis agar dapat berjalan kembali ke keadaan normal. Berikut ini merupakan strategi saat gangguan.

Tabel 6.1-23 Strategi Saat Gangguan

Strategi	Keterangan	Bentuk Kontrol
Melaporkan gangguan kepada helpdesk yang disediakan	Melaporkan gangguan kepada helpdesk jika terjadi gangguan dilakukan agar gangguan dapat segera ditangani.	Kebijakan Pelaporan Gangguan
Mengkomunikasikan kepada pihak terkait	Gangguan yang terjadi dikomunikasikan kepada pihak internal dan eksternal yang terkait.	Kebijakan Komunikasi Gangguan
Melakukan evakuasi karyawan jika dibutuhkan	Jika gangguan yang terjadi dapat mengancam keselamatan karyawan maka dilakukan evakuasi terhadap karyawan.	Kebijakan Evakuasi Bencana
Melakukan dokumentasi secara manual pada saat gangguan	Dokumentasi secara manual pada saat gangguan agar saat gangguan terjadi, data yang belum tersimpan dalam sistem dapat tersimpan manual untuk kemudian diinput saat sistem sudah kembali normal.	Kebijakan Penanganan Gangguan
Mengaktifkan DRC	DRC diaktifkan pada saat server serta perangkat utama lain tidak berfungsi akibat bencana maupun gangguan lain. DRC diaktifkan agar proses bisnis dapat berjalan seperti sedia kala.	Kebijakan Penggunaan DRC

3. Strategi Pemulihan

Strategi pemulihan merupakan tindakan atau aksi yang dilakukan oleh tim DRP untuk dapat mengatasi gangguan maupun bencana yang sedang terjadi. Berikut ini merupakan

strategi pemulihan untuk mempertahankan keberlangsungan bisnis.

Tabel 6.1-24 Strategi Pemulihan

Strategi	Keterangan	Bentuk Kontrol
Mengecek kerusakan perangkat serta data yang terjadi	Jika gangguan yang terjadi menyebabkan kerusakan pada perangkat serta infrastruktur maka dilakukan pengecekan kerusakan terhadap perangkat dan infrastruktur.	Kebijakan Pemulihan
Mengkomunikasikan kepada pihak maupun vendor terkait	Jika terdapat gangguan pada proses bisnis yang terkait dengan pihak maupun vendor tertentu, maka hal tersebut segera dikomunikasikan agar permasalahan dapat segera diselesaikan dan proses bisnis dapat kembali berjalan.	Kebijakan Komunikasi Gangguan
Melakukan pemulihan tehadap infrastruktur dan sistem yang mengalami kerusakan	Jika terjadi kerusakan pada infrastruktur dan sistem, maka dilakukan pemulihan agar dapat segera berfungsi secara normal.	Kebijakan Pemulihan
Melakukan restore data jika dibutuhkan	Jika terjadi kehilangan data maka dilakukan restore terhadap data yang telah di backup	Kebijakan Backup dan Restore
Melakukan dokumentasi terhadap gangguan	Dilakukan dokumentasi gangguan terhadap proses bisnis serta penanganannya untuk menjadi arsip perusahaan dan dapat dijadikan sebagai bahan evaluasi strategi.	Kebijakan Penanganan Gangguan

4. Strategi Korektif

Strategi korektif adalah aksi atau tindakan manajemen untuk dapat melakukan perbaikan terhadap kinerja perencanaan BCP secara terus menerus. Strategi korektif dilakukan ketika

organisasi menemui ketidaksesuaian atau ketidakefektifan dari perencanaan BCP yang telah dibuat. Berikut ini merupakan strategi korektif untuk mempertahankan keberlangsungan proses bisnis divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur.

Tabel 6.1-25 Strategi Korektif

Strategi	Keterangan	Bentuk Kontrol
Melakukan evaluasi terhadap penanganan gangguan yang telah terjadi	Perbaikan atau koreksi terhadap strategi dilakukan dengan mengevaluasi penanganan terhadap gangguan. Sehingga dari hasil evaluasi akan ditentukan tindakan korektif atau perbaikan yang sesuai.	Kebijakan Evaluasi Strategi

6.1.4.2 Strategi menanggulangi risiko

Strategi menanggulangi risiko merupakan aksi atau tindakan manajemen untuk dapat meminimalisir terjadinya risiko yang dapat menyebabkan gangguan pada proses bisnis beserta dengan bentuk kontrolnya. Strategi menanggulangi risiko dibuat berdasarkan hasil analisis risiko yang telah dilakukan sebelumnya. Risiko yang digunakan hanyalah risiko yang memiliki nilai RPN tertinggi. Pada divisi teknologi informasi, risiko yang tertinggi ada 4 dan berada pada tingkat Low. Risiko yang digunakan untuk membuat strategi adalah risiko UPS rusak akibat pemeliharaan tidak teratur, UPS rusak akibat kondisi perangkat yang tidak layak, UPS terbakar akibat arus pendek listrik dan AC rusak akibat kebocoran saluran pembuangan air. Dalam menanggulaingi risiko digunakan empat jenis strategi, yaitu strategi preventif, stratehi saat gangguan, strategi pemulihan dan strategi korektif. Berikut ini merupakan strategi menganggulangi risiko.

Tabel 6.1-26 Strategi menanggulangi risiko 1

Risiko : UPS Rusak Penyebab : Pemeliharaan yang tidak teratur			
Jenis Strategi	Tindakan	Keterangan	Bentuk Kontrol
Preventif	Memonitoring pelaksanaan pemeliharaan	Pemeliharaan yang dilakukan dimonitor untuk menghindari pemeliharaan yang tidak teratur. Monitoring dilakukan dengan memeriksa dokumentasi kegiatan pemeliharaan.	Prosedur Pengawasan Pemeliharaan
	Melakukan dokumentasi kegiatan pemeliharaan	Kegiatan pemeliharaan didokumentasi agar mudah dalam melakukan kontrol terhadap keadaan perangkat serta keteraturan pemeliharaan.	Prosedur Pemeliharaan Aset Formulir Aktivitas Pemeliharaan
	Menyiapkan perangkat cadangan	Perangkat cadangan disediakan agar UPS tetap dapat digunakan saat dibutuhkan ketika UPS utama mengalami kerusakan.	Prosedur Pengelolaan Aset Formulir Daftar Aset
Saat Gangguan	Melaporkan kepada staff terkait	Jika terjadi kerusakan, maka dilaporkan kepada staff yang bertanggungjawab terhadap perangkat agar segera ditangani.	Prosedur Pelaporan Gangguan
	Menggunakan UPS cadangan	Pada saat UPS rusak, UPS cadangan digunakan agar UPS tetap tersedia pada saat dibutuhkan.	Prosedur Penaganan Gangguan
	Mengidentifikasi kerusakan yang terjadi	Saat terjadi kerusakan pada UPS, dilakukan identifikasi terhadap kerusakan yang terjadi agar dapat diketahui perbaikan apa yang diperlukan untuk memulihkan UPS.	

Risiko : UPS Rusak Penyebab : Pemeliharaan yang tidak teratur			
Jenis Strategi	Tindakan	Keterangan	Bentuk Kontrol
Pemulihan	Melakukan perbaikan atau mengganti hardware	Dilakukan perbaikan terhadap UPS jika kerusakan masih tergolong ringan dan dilakukan penggantian jika kerusakan pada UPS parah.	Prosedur Perbaikan Hardware Prosedur Penggantian Hardware
	Mencatat solusi dalam mengatasi gangguan	Solusi penanganan terhadap gangguan dicatat untuk menjadi dokumentasi penanganan gangguan.	Prosedur Penanganan Gangguan Formulir Penanganan Gangguan
Korektif	Mendokumentasikan Gangguan yang terjadi	Gangguan yang terjadi didokumentasikan agar jika suatu saat terjadi gangguan yang sama dapat dilihat penyebab maupun penanganan yang perlu dilakukan secara cepat.	Prosedur Penanganan Gangguan Formulir Histori Gangguan
	Melakukan evaluasi terhadap dokumen gangguan	Strategi evaluasi ini akan dilakukan dengan melihat hasil dokumentasi dari insiden yang terjadi dan penanganan yang dilakukan. Kemudian nantinya ditentukan aksi tindakan korektif dan perbaikan yang sesuai.	Prosedur Evaluasi Strategi Formulir Evaluasi Strategi

Tabel 6.1-27 Strategi Menanggulangi Risiko 2

Risiko : UPS Rusak Penyebab : Kondisi perangkat yang tidak layak			
Jenis Strategi	Tindakan	Keterangan	Bentuk Kontrol
Preventif	Melakukan monitoring terhadap kapasitas hardware	Kapasitas hardware dimonitor untuk mengontrol kelayakan dari hardware. Monitor dilakukan dengan cara melakukan pencatatan terhadap lama pemakaian serta keadaan hardware secara berkala.	Prosedur Monitoring Kapasitas
	Melakukan pemeliharaan dan perbaikan secara rutin	Dilakukan pemeliharaan dan perbaikan secara rutin terhadap perangkat untuk memelihara kondisi perangkat.	Prosedur Pemeliharaan Aset Formulir Akrivitas Pemeliharaan
	Menyiapkan perangkat cadangan	Perangkat cadangan disediakan agar UPS tetap dapat digunakan saat dibutuhkan ketika UPS utama mengalami kerusakan.	Prosedur Pengelolaan Aset Formulir Daftar Aset
Saat Gangguan	Melaporkan kepada staff terkait	Jika terjadi kerusakan, maka dilaporkan kepada staff yang bertanggungjawab terhadap perangkat agar segera ditangani.	Prosedur Pelaporan Gangguan
	Menggunakan UPS cadangan	Pada saat UPS rusak, UPS cadangan digunakan agar UPS tetap tersedia pada saat dibutuhkan.	Prosedur Penaganan Gangguan
	Mengidentifikasi kerusakan yang terjadi	Saat terjadi kerusakan pada UPS, dilakukan identifikasi terhadap kerusakan yang terjadi agar dapat diketahui	

Risiko : UPS Rusak Penyebab : Kondisi perangkat yang tidak layak			
Jenis Strategi	Tindakan	Keterangan	Bentuk Kontrol
		perbaikan apa yang diperlukan untuk memulihkan UPS.	
Pemulihan	Melakukan perbaikan atau mengganti hardware	Dilakukan perbaikan terhadap UPS jika kerusakan masih tergolong ringan dan dilakukan penggantian jika kerusakan pada UPS parah.	Prosedur Perbaikan Hardware Prosedur Penggantian Hardware
	Mencatat solusi dalam mengatasi gangguan	Solusi penanganan terhadap gangguan dicatat untuk menjadi dokumentasi penanganan gangguan.	Prosedur Penanganan Gangguan Formulir Penanganan Gangguan
Korektif	Mendokumentasikan Gangguan yang terjadi	Gangguan yang terjadi didokumentasikan agar jika suatu saat terjadi gangguan yang sama dapat dilihat penyebab maupun penanganan yang perlu dilakukan secara cepat.	Prosedur Penanganan Gangguan Formulir Histori Gangguan
	Melakukan evaluasi terhadap dokumen gangguan	Strategi evaluasi ini akan dilakukan dengan melihat hasil dokumentasi dari insiden yang terjadi dan penanganan yang dilakukan. Kemudian nantinya ditentukan aksi tindakan korektif dan perbaikan yang sesuai.	Prosedur Evaluasi Strategi Formulir Evaluasi Strategi

Tabel 6.1-28 Strategi Menanggulangi Risiko 3

Risiko : UPS Terbakar Penyebab : Arus pendek listrik			
Jenis Strategi	Tindakan	Keterangan	Bentuk Kontrol
Preventif	Memonitoring daya listrik secara rutin	Daya listrik harus dimonitor secara rutin untuk memastikan bahwa daya litstrik tidak melebihi karena kelebihan daya akan menimbulkan terjadinya arus pendek listrik.	Prosedur Monitoring Daya Listrik
	Memasang sekring pada aliran listrik	Sekring perlu dipasang pada aliran listrik untuk mencegah terjadinya arus pendek listrik.	Prosedur Pemasangan Perangkat
	Melakukan pemeliharaan dan pengecekan rutin terhadap kondisi perangkat dan kabel	Pengecekan rutin terhadap kondisi perangkat dan kabel diperlukan untuk mengetahui apakah kondisi perangkat dan kabel telah baik dan tidak berpotensi untuk menimbulkan terjadinya arus pendek listrik.	Prosedur Pemeliharaan Infrastruktur
	Menyediakan tabung pemadam kebakaran	Tabung pemadam disediakan sebagai pertolongan pertama saat terjadi kebakaran sehingga api tidak membesar.	Prosedur Pemasangan Perangkat
Saat Gangguan	Memadamkan api	Ketika terjadi kebakaran, api harus segera dipadamkan dengan tabung pemadam kebakaran. Jika api membesar dan tidak dapat dipadamkan, maka harus segera menghubungi pemadam kebakaran.	Prosedur Kebakaran

Risiko : UPS Terbakar Penyebab : Arus pendek listrik			
Jenis Strategi	Tindakan	Keterangan	Bentuk Kontrol
	Mengevakuasi karyawan di sekitar lokasi	Karyawan yang ada di sekitar lokasi kebakaran harus segera dievakuasi jika kebakaran yang terjadi membesar.	Prosedur Evakuasi
	Mengidentifikasi kerusakan yang terjadi	Kerusakan yang terjadi akibat kebakaran diidentifikasi agar dapat diketahui perbaikan apa yang diperlukan untuk memulihkan UPS.	Prosedur Penaganan Gangguan
Pemulihan	Melakukan perbaikan atau mengganti hardware	Dilakukan perbaikan terhadap UPS jika kerusakan masih tergolong ringan dan dilakukan penggantian jika kerusakan pada UPS parah.	Prosedur Perbaikan Hardware Prosedur Penggantian Hardware
	Mencatat solusi dalam mengatasi gangguan	Solusi penanganan terhadap gangguan dicatat untuk menjadi dokumentasi penanganan gangguan.	Prosedur Penanganan Gangguan Formulir Penanganan Gangguan
Korektif	Mendokumentasikan Gangguan yang terjadi	Gangguan yang terjadi didokumentasikan agar jika suatu saat terjadi gangguan yang sama dapat dilihat penyebab maupun penanganan yang perlu dilakukan secara cepat.	Prosedur Penanganan Gangguan Formulir Histori Gangguan
	Melakukan evaluasi terhadap dokumen gangguan	Strategi evaluasi ini akan dilakukan dengan melihat hasil dokumentasi dari insiden yang terjadi dan penanganan yang dilakukan. Kemudian nantinya ditentukan aksi tindakan korektif dan perbaikan yang sesuai.	Prosedur Evaluasi Strategi Formulir Evaluasi Strategi

Tabel 6.1-29 Strategi Menanggulangi Risiko 4

Risiko : AC Rusak Penyebab : Kebocoran saluran air pembuangan			
Jenis Strategi	Tindakan	Keterangan	Bentuk Kontrol
Preventif	Melakukan pemeriksaan rutin terhadap pipa pembuangan	Pemeriksaan terhadap pipa pembuangan dilakukan untuk memastikan tidak ada pipa yang mengalami kebocoran.	Prosedur Pemeliharaan Infrastruktur
	Melakukan pemeliharaan dan perbaikan secara rutin	Dilakukan pemeliharaan dan perbaikan secara rutin terhadap perangkat untuk memelihara kondisi perangkat.	Prosedur Pemeliharaan Hardware
	Menyiapkan perangkat cadangan	Perangkat cadangan disediakan agar AC tetap dapat digunakan saat dibutuhkan ketika AC utama mengalami kerusakan.	Formulir Daftar Aset
Saat Gangguan	Mematikan aliran listrik di sekitar lokasi kebocoran	Aliran listrik disekitar area kebocoran harus dilakukan untuk menghindari terjadinya arus pendek listrik yang dapat menyebabkan kerusakan AC dan perangkat lainnya.	Prosedur Penaganan Gangguan
	Melaporkan kepada staff terkait	Jika terjadi kerusakan, maka dilaporkan kepada staff yang bertanggungjawab terhadap perangkat agar segera ditangani.	

Risiko : AC Rusak Penyebab : Kebocoran saluran air pembuangan			
Jenis Strategi	Tindakan	Keterangan	Bentuk Kontrol
	Menggunakan AC cadangan	Pada saat AC rusak, AC cadangan digunakan agar AC tetap tersedia.	
	Mengidentifikasi kerusakan yang terjadi	Saat terjadi kerusakan pada AC, dilakukan identifikasi terhadap kerusakan yang terjadi agar dapat diketahui perbaikan apa yang diperlukan untuk memulihkan AC.	
Pemulihan	Melakukan perbaikan atau mengganti hardware	Dilakukan perbaikan terhadap AC jika kerusakan masih tergolong ringan dan dilakukan penggantian jika kerusakan pada AC parah.	Prosedur Perbaikan Hardware Prosedur Penggantian Hardware
	Mencatat solusi dalam mengatasi gangguan	Solusi penanganan terhadap gangguan dicatat untuk menjadi dokumentasi penanganan gangguan.	Prosedur Penanganan Gangguan Formulir Penanganan Gangguan
Korektif	Mendokumentasikan Gangguan yang terjadi	Gangguan yang terjadi didokumentasikan agar jika suatu saat terjadi gangguan yang sama dapat dilihat penyebab maupun penanganan yang perlu dilakukan secara cepat.	Prosedur Penanganan Gangguan Formulir Histori Gangguan
	Melakukan evaluasi terhadap dokumen gangguan	Strategi evaluasi ini akan dilakukan dengan melihat hasil dokumentasi dari insiden yang terjadi dan penanganan yang dilakukan. Kemudian nantinya ditentukan aksi tindakan korektif dan perbaikan yang sesuai.	Prosedur Evaluasi Strategi Formulir Evaluasi Strategi

6.1.5 Rencana Pemulihan Bencana

Tahap pembuatan rencana pemulihan bencana berfokus pada hal-hal yang berkaitan dengan pemulihan insiden seperti penanganan insiden, pembuatan kontrol, serta pihak-pihak yang akan berkaitan dengan gangguan. Bagian ini akan melengkapi strategi pemulihan yang telah dibuat sebelumnya.

6.1.5.1 Pendataan Aset Teknologi Informasi

Pada tahap ini dilakukan pendataan terhadap aset TI yang dimiliki oleh perusahaan. Hal ini dilakukan agar perusahaan mengetahui aset apa saja yang dimiliki dan perlu untuk diamankan. Aset teknologi informasi didapatkan dengan melakukan wawancara. Berikut ini daftar aset TI yang dimiliki oleh divisi TI Bank Pembangunan Daerah Jawa Timur.

Tabel 6.1-30 Daftar Aset TI

Jenis Aset IT	Nama Aset IT
Hardware	UPS
	AS400 (Banking Server)
	AC Kering
	Server
	Notebook
	Firewall
	Genset
Software	Docnum (Document Management)
	Security Application AS400
	Aplikasi status cabang
	Estim
	Network Monitoring System
	Software Helpdesk
	Compleo
	Vulnerability Assessment System
Data	Data Transaksi
	Data Nasabah
	Data User
	Data Cabang
Network	Kabel Fiber Optik
	Switch
	Main Router

Jenis Aset IT	Nama Aset IT
People	Staff departemen Teknologi Informasi
	Staff Non Departemen TI

6.1.5.2 Pendataan Vendor

Pada tahap ini dilakukan pendataan terhadap vendor yang digunakan oleh perusahaan beserta nomor telepon yang dapat dihubungi. Daftar vendor dibutuhkan karena beberapa layanan disediakan oleh vendor, sehingga untuk melakukan pemulihan perlu untuk menghubungi vendor terkait. Vendor memiliki peran dan tanggung jawabnya terhadap pemulihan bencana. Daftar peran dan tanggung jawab vendor dibuat sesuai dengan kondisi vendor pada perusahaan. Berikut ini adalah peran dan tanggung jawab vendor:

1. Menyediakan layanan dan produk yang diperlukan oleh divisi TI Bank Pembangunan Daerah Jawa Timur.
2. Memastikan bahwa layanan yang disediakan telah memenuhi SLA yang disepakati.
3. Bersikap responsif terhadap keluhan yang diberikan oleh divisi TI.
4. Melakukan perbaikan terhadap produk dan layanan yang mengalami permasalahan.
5. Melakukan pemulihan pada produk atau layanan yang diberikan jika terjadi bencana.

Daftar vendor yang dimiliki perusahaan perlu untuk dibuat agar diketahui aset apa saja yang dikelola oleh vendor sehingga saat terjadi bencana, tim BCP dapat segera menghubungi vendor untuk dilakukan pemulihan. Berikut ini merupakan daftar vendor dari divisi TI.

Tabel 6.1-31 Daftar Vendor

Nama Vendor	Layanan	Contact
Multipolar	Server	021 5460011
Mitra Infosarana	Server	021 7943658
Trinet Prima Solusi	Server	021 34831212
PT.Intragama	Server	08158091112
Telkom	Jaringan Internet	-

6.1.5.3 Penentual Lokasi Server dan Aset TI

Pada tahap ini dilakukan penentuan lokasi aset TI. Hal ini dilakukan untuk mengamankan aset dari bencana. Pada aset TI cadangan ditentukan lokasi yang aman dari bencana. Berikut ini lokasi server dan aset TI divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur.

Tabel 6.1-32 Lokasi Server dan Aset TI

Aset TI	Lokasi
Banking Server	Kantor Pusat Bank Pembangunan Daerah Jawa Timur
Server	Kantor Pusat Bank Pembangunan Daerah Jawa Timur
UPS	Kantor Pusat Bank Pembangunan Daerah Jawa Timur
AC Kering	Kantor Pusat Bank Pembangunan Daerah Jawa Timur
Banking Server Backup	Disaster Recovery Center Citraland
Server Backup	Disaster Recovery Center Citraland
UPS Backup	Kantor Pusat Bank Pembangunan Daerah Jawa Timur
AC Kering Backup	Kantor Pusat Bank Pembangunan Daerah Jawa Timur

6.1.5.4 Permintaan Aktivasi dan Deaktivasi

Pada tahap permintaan aktivasi dan deaktivasi, dilakukan penenuan kondisi dan tindakan untuk memulai dan mengakhiri perencanaan pemulihan bencana. Apabila gangguan yang terjadi hanya pada satu sub fungsional dan tidak pada sub fungsional lain, serta gangguan tersebut mengganggu proses bisnis kritis dan proses bisnis penting, maka gangguan dapat diatasi dengan melaporkan kepada helpdesk operasional. Untuk kemudian gangguan tersebut dapat ditangani oleh bagian operasional.

Saat gangguan besar terjadi, strategi keberlangsungan bisnis diaktifkan. Strategi yang dilakukan mencakup strategi saat gangguan hingga strategi pemulihan agar proses bisnis dapat

tetap berjalan. Gangguan akan dikatakan sebagai bencana atau gangguan dengan skala besar jika sebagai berikut:

1. Gangguan disebabkan oleh kebakaran besar atau bencana.
2. Gangguan pada proes bisnis kritis dan waktu pemulihannya melebihi dari yang telah ditentukan.
3. Gangguan menyebabkan proses bisnis pada beberapa fungsional bisnis tidak berjalan.

Deaktivasi dilakukan ketika gangguan berhasil ditangani serta upaya pemulihan terhadap gangguan atau bencana telah berjalan. Untuk kemudian koordinator BCP mengumumkan bahwa dilakukan deaktivasi.

6.1.6 Pelatihan Karyawan

Pada tahap ini dilakukan pembuatan modul untuk pelatihan pada karyawan terkait dengan penanganan gangguan. Pelatihan karyawan dilakukan untuk memberi edukasi kepada karyawan jika gangguan terjadi sehingga karyawan dapat mengetahui langkah apa saja yang harus dilakukan ketika gangguan terjadi. Materi yang diberikan kepada karyawan disesuaikan dengan perencanaan keberlangsungan bisnis yang telah dibuat. Berikut ini merupakan gambaran modul pelatihan karyawan yang telah dibuat.

Tabel 6.1-33 Modul Pelatihan BCP 1

Modul Pelatihan BCP Divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur	
Nama Pelatihan	Pembekalan terkait gangguan pada proses bisnis
Jenis Pelatihan	Pemberian materi
Deskripsi	Pelatihan ini dilakukan untuk mengedukasi karyawan divisi teknologi informasi terkait dengan penyebab gangguan, dampak gangguan terhadap proses bisnis serta cara untuk penanganan gangguan.
Sasaran Pelatihan	Perwakilan karyawan dari setiap sub fungsional
Materi Umum	Pada pelatihan akan diberikan materi kepada karyawan mengenai:

Modul Pelatihan BCP Divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur	
	1. Pengetahuan mengenai jenis-jenis gangguan yang dapat menimpa komponen teknologi informasi. 2. Pengetahuan terkait dampak bisnis akibat gangguan yang terjadi pada proses bisnis. 3. Pengetahuan terkait tindakan yang harus dilakukan saat gangguan terjadi. 4. Alur komunikasi saat terjadi gangguan. 5. Prosedur yang dilakukan saat gangguan terjadi. 6. Pihak-pihak yang perlu dihubungi ketika terjadi gangguan.

Tabel 6.1-34 Modul Pelatihan BCP 2

Modul Pelatihan BCP Divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur	
Nama Pelatihan	Pembekalan penanganan gangguan
Jenis Pelatihan	Pemberian materi
Deskripsi	Pelatihan ini dilakukan untuk mengedukasi karyawan divisi teknologi informasi bagian helpdesk dan operasional terkait penanganan gangguan.
Sasaran Pelatihan	Karyawan bagian helpdesk dan operasional
Materi Umum	Pada pelatihan akan diberikan materi kepada karyawan mengenai: 1. Pengetahuan terkait risiko yang dapat mengancam infrastruktur dan aset TI. 2. Pengetahuan terkait cara menangani insiden dan gangguan kecil. 3. Pengetahuan cara melakukan backup dan restore.

6.1.7 Pengujian BCP

Pada tahap ini dilakukan pengujian terhadap dokumen keberlangsungan divisi teknologi informasi pada Bank Pembangunan Daerah Jawa Timur. Pengujian BCP dilakukan untuk melakukan konfirmasi terhadap kesesuaian rencana keberlangsungan bisnis yang dibuat berdasarkan metodologi *Business Continuity Planning*. Pada tahap pengujian BCP dibuat skenario pengujian. Jenis pengujian yang dilakukan adalah dengan *Supervised Walkthrough*, yaitu pengujian yang

dilakukan dengan membuat skenario untuk menguji rencana keberlangsungan bisnis serta *Non-business Interruption testing*, yaitu akan dilakukan simulasi terjadinya bencana dengan menggunakan prosedur yang telah dibuat.

Pada jenis pengujian *Non-business Interruption testing* dilakukan simulasi gangguan terhadap salah satu kemungkinan risiko yang dimiliki oleh divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur. Risiko yang dipilih adalah kerusakan pada UPS dan AC. Berikut ini skenario pengujian dengan *Non-business Interruption testing*.

Tabel 6.1-35 Skenario Pengujian BCP 1

SKENARIO PENGUJIAN BCP	
Jenis Pengujian	*Non-business Interruption testing*
Pelaku	Karyawan divisi teknologi informasi
Peran	Menonaktifkan UPS dan AC untuk sementara
Skenario Simulasi	UPS atau AC mengalami kerusakan sehingga tidak dapat digunakan saat dibutuhkan. Untuk mengatasi gangguan ini terdapat beberapa bentuk kontrol berupa prosedur. Maka prosedur-prosedur tersebut akan diuji keefektifannya. Berikut ini prosedur yang akan diuji: • Prosedur pelaporan gangguan • Prosedur penanganan gangguan

Pengujian yang selanjutnya adalah dengan metode *Supervised Walkthrough*, dimana pengujian dilakukan dengan mendiskusikan aksi serta keputusan yang akan dilakukan ketika terjadi gangguan atau bencana. Skenario pengujian dibuat berdasarkan salah satu kemungkinan risiko divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur yaitu UPS dan AC rusak. Berikut ini skenario pengujian dengan metode *Supervised Walkthrough*.

Tabel 6.1-36 Skenario Pengujian BCP 2

SKENARIO PENGUJIAN BCP	
Jenis Pengujian	*Supervised Walkthrough*

SKENARIO PENGUJIAN BCP	
Pelaku	Karyawan divisi teknologi informasi
Peran	Mendiskusikan dan mendokumentasikan hal yang terjadi selama pengujian dilakukan, penanganan yang dilakukan serta keputusan yang diambil.
Skenario Pengujian	• Mengkondisikan UPS dan AC dalam keadaan tidak berfungsi untuk sementara. • Karyawan yang terlibat dalam pengujian mendiskusikan dan mendokumentasikan hal yang terjadi selama pengujian dilakukan, penanganan yang dilakukan serta keputusan yang diambil. • Dari hasil pengujian dicatat juga terkait waktu penyelesaian dan dampak dari gangguan yang di ujikan.

6.1.8 Peninjauan Keberlangsungan Bisnis

Pada tahap peninjauan keberlangsungan bisnis, dokumen BCP yang telah dibuat ditinjau untuk dilihat keefektifannya dan kesesuaiannya dengan kondisi perusahaan. Hasil dari peninjauan yang dilakukan berupa *feedback* untuk melakukan perbaikan kepada dokumen BCP yang dibuat sehingga dapat meningkatkan kinerja keberlangsungan bisnis.

Langkah pertama dalam meninjau keberlangsungan bisnis adalah dengan menentukan waktu peninjauan keberlangsungan bisnis. Pada pembuatan dokumen BCP divisi teknologi informasi Bank Pembangunan Daerah Jawa Timur peninjauan keberlangsungan bisnis akan dilakukan setiap tahun. Kemudian dilakukan pembuatan formulir yang digunakan untuk melakukan peninjauan. Formulir yang dibuat adalah formulir pengecekan internal BCP dan formulir peninjauan manajemen. Berikut ini merupakan formulir pengecekan internal

Formulir pengecekan internal BCP merupakan masukan terhadap peninjauan yang akan dilakukan oleh manajemen terhadap BCP perusahaan. Formulir digunakan untuk mengecek BCP yang diterapkan pada perusahaan. Pengecekan mencakup pada hal umum terkait status terpenuhinya BCP hingga peninjauan BCP. Berikut ini formulir peninjauan Internal BCP.

Tabel 6.1-37 Formulir Pengecekan Internal BCP

Pertanyaan	Status			Keterangan
	Ya	Dalam Progress	Tidak	
Pengelolaan umum BCP				
Apakah tujuan BCP telah ditentukan dan disepakati oleh organisasi?				
Apakah peran dan tanggung jawab terhadap BCP telah terdefinisi pada level manajemen?				
Apakah terdapat pihak eksekutif yang bertanggung jawab terhadap BCP?				
Apakah BCP telah didokumentasi dengan baik oleh perusahaan?				
Apakah proses pada BCP telah sesuai dengan peraturan OJK?				
Apakah BCP telah sesuai dengan proses pada perusahaan?				
Apakah dokumen BCP telah mudah dipahami?				
Keselarasan BCP dengan perusahaan				
Apakah aset TI kritis yang mendukung				

Pertanyaan	Status			Keterangan
	Ya	Dalam Progress	Tidak	
proses bisnis telah didefinisikan oleh perusahaan?				
Apakah proses bisnis yang tergantung dengan TI telah diidentifikasi oleh perusahaan?				
Apakah risiko yang dapat terjadi dan mengancam proses bisnis diidentifikasi oleh perusahaan?				
Apakah prioritisasi layanan dan proses bisnis yang tergantung dengan TI telah dilakukan oleh perusahaan?				
Apakah waktu toleransi pemulihan terhadap gangguan telah ditentukan dan disepakati oleh manajemen senior?				
Apakah dampak bisnis dari gangguan terhadap proses bisnis telah dibuat?				
Pengelolaan Strategi BCP				
Apakah strategi pencegahan/ preventif terhadap gangguan telah didokumentasi -kan oleh perusahan?				
Apakah strategi saat gangguan terjadi telah didokumentasi oleh perusahaan?				
Apakah strategi pemulihan bencana				

Pertanyaan	Status			Keterangan
	Ya	Dalam Progress	Tidak	
telah didokumentasi oleh perusahaan?				
Apakah strategi korektif telah didokumentasi oleh perusahaan?				
Apakah strategi terkait dengan gangguan telah disepakati oleh manajemen senior?				
Apakah terdapat prosedur yang mendukung strategi BCP?				
Apakah strategi BCP telah dikomunikasikan kepada keseluruhan perusahaan?				
Apakah prosedur terkait BCP telah disosialisasikan kepada pegawai?				
Apakah BCP telah mencakup pada perencanaan komunikasi antar sub fungsional?				
Pelatihan dan pengujian BCP				
Apakah terdapat pelatihan karyawan terkait dengan BCP?				
Apakah pelatihan karyawan terkait BCP telah dilakukan?				
Apakah pengujian BCP dilakukan secara keseluruhan?				
Apakah semua aspek pada perencanaan pengujian telah				

Pertanyaan	Status			Keterangan
	Ya	Dalam Progress	Tidak	
dilakukan dalam waktu satu tahun terakhir?				
Apakah pengujian dilakukan oleh karyawan yang terkait dengan perencanaan?				
Apakah hasil pengujian telah didokumentasi?				
Pemeliharaan dan peninjauan BCP				
Apakah terdapat proses peninjauan pada BCP perusahaan?				
Apakah terdapat proses untuk menilai tingkat efektifitas BCP?				
Apakah dilakukan tindakan perbaikan terhadap BCP?				
Apakah terdapat dokumentasi terhadap peninjauan dan perbaikan BCP?				

Formulir peninjauan manajemen merupakan dokumen yang berisi hasil keputusan dari peninjauan yang dilakukan. Formulir berisi rangkuman keputusan dari setiap peserta rapat. Berikut ini merupakan formulir peninjauan manajemen.

Tabel 6.1-38 Formulir Peninjauan Manajemen

Masukan	Tanggal dan waktu Rapat:	
	Pemimpin Rapat:	
	Peserta Rapat:	

	Sumber daya yang dibutuhkan:	○ Laporan hasil tinjauan il pengecekan engujian BCP		
Analisis	Topik Diskusi	Keputusan/ Tindakan	Batas Waktu	Penanggung jawab
	Statu tindakan tinjauan manajemen sebelumnya			
	Perubahan internal dan eksternal terkait BCP			
	Hasil audit BCP			
	Korektif terhadap BCP			
	Kebutuhan perubahan terhadap BCP			

6.2 Hasil Evaluasi Implementasi Metodologi Business Continuity Planning

Tahap evaluasi implementasi metodologi BCP merupakan tahap dimana dilakukan penilaian apakah semua tahapan pada metodologi dapat digunakan dalam pembuatan dokumen BCP pada divisi TI Bank Pembangunan Daerah Jawa Timur. Tahap ini dilakukan setelah dokumen BCP dibuat dengan menggunakan metodologi *Business Continuity Planning*. Evaluasi dilakukan dengan mengisi *checklist* evaluasi implementasi metodologi. Berikut ini adalah aktivitas dan tahapan yang ada pada metodologi *Business Continuity Planning* yang diimplementasi

Gambar 6.2-1 Fase 1 Perencanaan

.

Gambar 6.2-2 Fase 2 Implementasi

Gambar 6.2-3 Fase 3 Pemantauan dan Review

Gambar 6.2-4 Fase 4 Pemeliharaan dan Peningkatan

Dalam evaluasi digunakan *checklist* dengan setiap aktivitas dalam metodologi dinilai dengan skala dalam rentang 1 hingga 3. Berikut ini penjelasan untuk setiap skala pada *checklist*.

Tabel 6.2-1 Skala Implementasi Metodologi

Skala	Keterangan
1	Tidak dapat diimplementasi.
2	Dapat diimplemetasi perubahan.
3	Dapat diimplementasi seluruhnya

Skala 1 dicentang jika aktivitas pada metodologi tidak dilakukan pada pembuatan dokumen BCP akibat tidak cocok atau tidak relevan dengan kebutuhan perusahaan. Skala 2 dicentang jika aktivitas pada metodologi dapat diimplementasi/ dilakukan pada pembuatan dokumen BCP tetapi terdapat perubahan yang dilakukan terhadap aktivitas yang diimplementasi. Perubahan yang dilakukan tersebut disesuaikan dengan kondisi perusahaan. Skala 3 dicentang ketika aktivitas pada metodologi dapat dilakukan seluruhnya pada pembuatan dokumen BCP. Checklist evaluasi berisi fase, tahap dan aktivitas yang ada pada metodologi. Setiap aktivitas dinilai penerapannya dengan mencentang pada salah satu skala.

Kemudian diberikan justifikasi untuk setiap penilaian. Berikut ini hasil evaluasi implementasi metodologi BCP beserta justifikasinya

Tabel 6.2-2 Hasil Evaluasi Metodologi BCP

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
Perencanaan	Penentuan Kebutuhan Pengelolaan Keberlangsungan Bisnis	Penentuan Tujuan			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP karena perusahaan perlu untuk menentukan tujuan dari pembuatan dokumen BCP.
		Penentuan Ruang Lingkup			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP karena perusahaan perlu untuk menentukan ruang lingkup agar cakupan dokumen BCP menjadi jelas.
		Pembentukan Komite			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP karena perusahaan perlu untuk menunjuk pihak yang memastikan BCP pada perusahaan berjalan.
		Penentuan Tanggung Jawab			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP agar setiap komite BCP dapat menjalankan tugasnya dengan efektif.
		Penentuan Pihak Terkait			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP karena perusahaan perlu untuk mengetahui siapa saja pihak yang terkait dengan perencanaan keberlangsungan bisnis perusahaan.
		Penentuan Sumberdaya			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP karena perusahaan perlu untuk menentukan sumber daya yang dibutuhkan dalam menjalankan perencaan keberlangsungan bisnis.

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
		Pembuatan Alur Komunikasi			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP karena perusahaan perlu untuk mendefinisikan alur komunikasi jika terjadi bencana untuk memudahkan penanganan saat bencana terjadi.
Implementasi	Analisis Risiko	Pendataan Kemungkinan Risiko			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP karena perusahaan perlu untuk mendata risiko apa saja yang dapat terjadi pada aset TI perusahaan.
		Analisis Risiko			✓	Aktivitas dapat dilakukan dalam pembuatan dokumen BCP karena perusahaan perlu untuk menganalisis kemunginan risiko yang telah dibuat.
		Penilaian Risiko			✓	Aktivitas penilaian risiko dapat diimplementasi dalam pembuatan dokumen BCP karena dibutuhkan penilaian risiko untuk mengetahui risiko yang paling mengancam perusahaan.
	Analisis Dampak Bisnis	Pendataan Proses Bisnis dan TI			✓	Aktivitas dapat diimplementasi pada pembuatan dokumen BCP karena perusahaan perlu untuk mendata proses bisnis dan layanan TI sebelum melakukan analisis dampak bisnis.
		Prioritisasi Layanan TI			✓	Aktivitas membuat prioritisasi layanan TI dapat diimplementasi dalam pembuatan dokumen BCP karena layanan TI yang digunakan perlu dibuat prioritisasi untuk mengetahui layanan yang bersifat kritis bagi departemen TI.

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
		Prioritisasi Proses Bisnis			✓	Aktivitas membuat prioritisasi proses bisnis dapat diimplementasi dalam pembuatan dokumen BCP karena dari tingkat kritis proses bisnis akan ditentukan waktu pemulihan dari proses bisnis dan layanan TI.
		Analisis Dampak Gangguan		✓		Aktivitas analisis dampak gangguan dapat diimplementasi dalam pembuatan dokumen BCP dengan perubahan. Perubahan yang dilakukan adalah dengan melakukan penentuan waktu pemulihan terlebih dahulu setelah itu mencari dampak bisnis dari gangguan. Perubahan terjadi akibat keadaan pada obyek penelitian.
		Penentuan Waktu Pemulihan		✓		Aktivitas penentuan waktu pemulihan dapat diimplementasi dalam pembuatan dokumen BCP namun dengan perubahan. Perubahan yang dilakukan adalah dengan menentukan terlabih dahulu waktu pemulihan lalu mencari dampak gangguan. Waktu pemulihan ditentukan berdasarkan tingkat kritis layanan TI dan proses bisnis. Perubahan terjadi akibat objek penelitian yang telah menentukan waktu pemulihan terlebih dahulu namun belum menentukan dampak gangguan pada proses bisnis.
		Penentuan Strategi Preventif		✓		Pada tahap pembuatan strategi keberlangsungan bisnis, setiap aktivitas mulai dari pembuatan

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
	Strategi keberlangsungan Bisnis	Penentuan Strategi Saat Gangguan		✓		strategi preventif hingga pembuatan strategi korektif dapat diimplementasi dalam pembuatan dokumen BCP dengan perubahan. Perubahan yang dilakukan adalah pada struktur strategi yang dibuat. Pada dokumen BCP divisi TI, strategi yang dibuat adalah strategi mempertahankan keberlangsungan bisnis dan strategi menanggulangi risiko.
		Penentuan Strategi Pemulihan		✓		
		Koreksi Terhadap Strategi		✓		
	Rencana Pemulihan Bencana	Pendataan Aset Teknologi informasi			✓	Aktivitas pendataan aset TI dapat diimplementasi pada pembuatan dokumen BCP karena untuk melakukan pemulihan, perusahaan perlu memiliki daftar aset TI yang dimiliki.
		Pendataan Vendor			✓	Aktivitas pendataan vendor dapat diimplementasi pada pembuatan dokumen BCP karena untuk melakukan pemulihan dengan cepat, perusahaan perlu mengetahui vendor apa saja yang digunakan perusahaan serta layanan dan produk apa yang disediakan.
		Penentuan Lokasi Server dan Aset TI			✓	Aktivitas penentuan lokasi server dan aset TI dapat diimplementasi pada pembuatan dokumen BCP karena perusahaan perlu untuk meletakkan aset dan server pada lokasi yang aman.
		Pembuatan Kontrol			✓	Aktivitas pembuatan kontrol dapat diimplementasi pada pembuatan dokumen BCP karena untuk menjalankan strategi keberlangsungan bisnis

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
						dibutuhkan prosedur atau bentuk kontrol yang mendukung.
		Permintaan Aktivasi dan Deaktivasi			✓	Aktivitas permintan aktivasi dan deaktivasi dapat diimplementasi pada pembuatan dokumen BCP karena perusahaan perlu mendefinisikan kondisi dimana strategi BCP perlu diaktifkan dan dihentikan.
		Skenario Pengujian		✓		Aktivitas pembuatan skenario pengujian dapat diimplementasi dalam pembuatan dokumen BCP dengan perubahan, yaitu dengan menggabungkan pembuatan skenario dengan tahap pengujian BCP.
		Evaluasi Bentuk Kontrol	✓			Aktivitas evaluasi bentuk kontrol tidak dapat diimplementasi pada pembuatan dokumen BCP karena tahap ini dapat dilakukan setelah dilakukan pengujian. Sedangkan dalam pembuatan dokumen BCP, pengujian hanya sebatas pembuatan skenario. Aktivitas tidak dapat diimplementasi karena keadaan pada obyek penelitian yang belum melakukan pengujian.
	Pelatihan Karyawan	Penentuan Jenis Pelatihan			✓	Aktivitas penentuan jenis pelatihan, mekanisme penyampaian pelatihan dan rencana kebutuhan pelatihan dapat diimplementasi pada pembuatan dokumen BCP dalam bentuk modul pelatihan. Hal ini dapat dilakukan karena perusahaan harus
		Mekanisme Penyampaian Pelatihan			✓	

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
		Rencana Kebutuhan Pelatihan			✓	menentukan bagaimana bentuk penyampaian pelatihan serta mekanisme pelatihan terkait gangguan.
		Pelaksanaan pelatihan	✓			Aktivitas pelaksanaan pelatihan tidak dapat diimplementasi dikarenakan keterbatasan objek sehingga pelatihan terbatas pada pembuatan modul pelatihan karyawan.
Pemantauan dan Review	Pengujian BCP	Rencana Mekanisme Pengujian			✓	Aktivitas rencana mekanisme pengujian dapat diimplementasi pada pembuatan dokumen BCP karena perusahaan perlu untuk membuat skenario pengujian BCP.
		Pengujian	✓			Aktivitas pengujian, pencatatan temuan serta dokumentasi hasil pengujian tidak diimplementasikan karena keterbatasan dari objek penelitian. Objek penelitian memutuskan untuk tidak melakukan pengujian untuk saat ini. Aktivitas ini tidak dapat dilakukan karena keadaan pada obyek penelitian.
		Pencatatan Temuan	✓			
		Dokumentasi Hasil Pengujian	✓			
Pemeliharaan dan Peningkatan	Peninjauan Keberlangsungan bisnis	Penentuan Periode Waktu Peninjauan			✓	Aktivitas penentuan periode waktu peninjauan dapat diimplementasikan dalam pembuatan dokumen BCP karena dokumen BCP perlu ditinjau secara rutin oleh perusahaan sehingga perusahaan perlu untuk menentukan waktu peninjauan.
		Peninjauan Secara Berkala	✓			Aktivitas peninjauan secara berkala, pengkajian ulang terhadap rencana serta pertimbangan

Fase	Tahap	Aktivitas	1	2	3	Justifikasi
		Pengkajian Ulang Terhadap rencana	✓			terhadap perubahan tidak dapat diimplementasikan karena dokumen BCP dapat ditinjau setelah dijalankan selama beberapa waktu setelah perencanaan keberlangsungan bisnis dijalankan.
		Pertimbangan Terhadap Perubahan	✓			

Sehingga dari hasil evaluasi yang telah dilakukan, didapatkan aktivitas pada metodologi yang dapat diimplementasi tanpa perubahan, dapat diimplementasi dengan perubahan dan tidak dapat diimplementasi. Berikut ini aktivitas yang dapat diimplementasi dengan sepenuhnya:

- Penentuan Tujuan
- Penentuan Ruang Lingkup
- Pembentukan Komite
- Penenuan Tanggung Jawab
- Penentuan Pihak Terkait
- Penentuan Sumber Daya
- Pembuatan Alur Komunikasi
- Pendataan kemungkinan Risiko
- Analisis Risiko
- Penilaian Risiko
- Pendataan Proses Bisnis dan Layanan TI
- Prioritisasi Proses Bisnis
- Prioritisasi Layanan TI
- Pendataan Aset TI
- Pendataan Vendor
- Penentuan Lokasi Server dan Aset TI
- Pembuatan Kontrol
- Permintaan Aktivasi dan Deaktivasi
- Penentuan Jenis Pelatihan
- Mekanisme Penyampaian Pelatihan
- Rencana Mekanisme Pengujian
- Penentuan Periode Waktu Peninjauan

Terdapat beberapa aktivitas yang dapat diimplementasi dengan perubahan. Perubahan dilakukan karena menyesuaikan dengan keadaan objek penelitian. Berikut ini aktivitas yang dapat diimplementasi dengan beberapa perubahan:

- Analisis Dampak Gangguan
- Penentuan Waktu Pemulihan
- Penentuan Strategi Prevetif
- Penentuan Strategi Saat Gangguan

- Koreksi Terhadap Strategi
- Skenario Pengujian

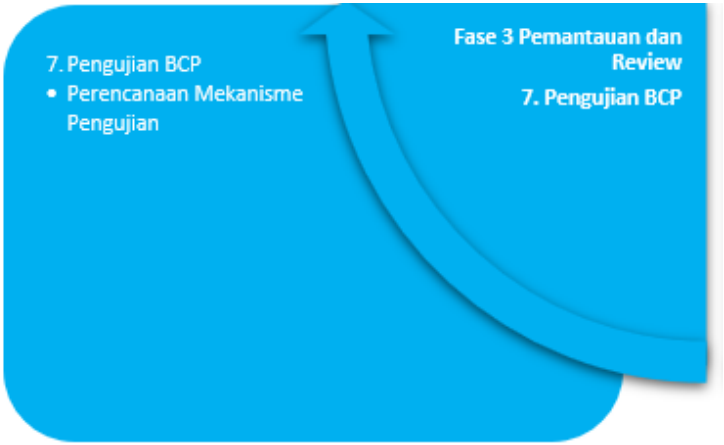
Ada beberapa aktivitas pada metodologi yang tidak dapat diimplementasi dikarenakan perusahaan memutuskan untuk tidak melakukannya untuk saat ini serta ada aktivitas yang tidak bisa dilakukan ketika BCP belum diterapkan selama beberapa waktu. Berikut ini aktivitas yang tidak dapat diimplementasi:

- Evaluasi Bentuk kontrol
- Pelaksanaan Pelatihan
- Pengujian
- Pencatatan Temuan
- Peninjauan Secara Berkala
- Pengkajian Ulang Terhadap Rencana
- Pertimbangan Terhadap Perubahan

Kemudian berdasarkan hasil evaluasi tersebut dapat digambarkan alur metodologi setelah implementasi dilakukan. Alur metodologi mencakup kepada aktivitas yang dapat diimplementasi tanpa perubahan dan aktivitas yang dapat diimplementasi dengan perubahan. Pada aktivitas yang dapat diimplementasi dengan perubahan dapat dibedakan dengan pemberian tanda kotak pada alur metodologi. Berikut ini bagan metodologi *Business Continuity Planning* hasil implementasi pada Divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur.

Gambar 6.2-5Hasil Fase 1 Metodologi BCP

Gambar 6.2-6 Hasil Fase 2 Metodologi BCP



Gambar 6.2-7 Hasil Fase 3 Metodologi BCP

Gambar 6.2-8 Hasil Fase 4 Metodologi BCP

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini akan dirangkum hasil akhir dari pembuatan tugas akhir menjadi kesimpulan dan dilengkapi dengan saran untuk penelitian selanjutnya.

7.1 Kesimpulan

Berdasarkan hasil penelitian dapat diambil beberapa kesimpulan sebagai berikut:

1. Penelitian ini telah menghasilkan dokumen perencanaan keberlangsungan bisnis divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur. Dokumen BCP dibuat dengan mengimplementasikan metodologi *Business Continuity Planning*. Adapun dokumen *Business Continuity Plan* berisi strategi yang dapat menjaga keberlangsungan bisnis. Terdapat dua jenis strategi yaitu strategi manajemen serta strategi menanggulangi risiko.
2. Berdasarkan evaluasi yang telah dilakukan terhadap implementasi metodologi *Business Continuity Planning* didapatkan bahwa sebagian besar aktivitas dapat diimplementasi pada pembuatan dokumen BCP divisi TI Bank Pembangunan Daerah Jawa Timur. Namun terdapat beberapa aktivitas yang tidak dapat diimplementasi dan dapat diimplementasi dengan beberapa perubahan. Perubahan tersebut dilakukan akibat menyesuaikan dengan keadaan perusahaan yang menjadi objek penelitian. Beberapa aktivitas tidak dapat diimplementasi karena ada aktivitas yang dapat dilakukan setelah beberapa saat setelah BCP diterapkan serta objek penelitian yang memutuskan untuk tidak melakukan untuk saat ini.

7.2 Saran

Berdasarkan pengerjaaan penelitian ini maka diberikan usulan terhadap perbaikan metodologi. Berikut ini adalah usulan perbaikan metodologi *Business Continuity Planning*:

1. Pada aktivitas analisis risiko dan penilaian risiko tidak diberikan arahan jelas mengenai cara melakukan analisis risiko sehingga diperlukan penggunaan pendekatan lain. Pada metodologi belum didefinisikan pendekatan yang harus digunakan. Sehingga usulan yang dapat diberikan adalah metodologi *Business Continuity Planning* perlu menjelaskan metode apa yang dapat digunakan dalam melakukan analisis risiko dan penilaian risiko.
2. Pada tahap analisis dampak bisnis terdapat perbedaan urutan dari metodologi dengan implementasi pembuatan dokumen BCP divisi TI Bank Pembangunan Daerah Jawa Timur. Sehingga usulan yang dapat diberikan adalah perlu dilakukan pengkajian ulang terhadap tahap analisis dampak bisnis yang ada pada metodologi *Business Continuity Planning* untuk diketahui urutan aktivitas yang lebih sesuai.
3. Diperlukan adanya lebih banyak studi kasus empiris terhadap metodologi *Business Continuity Planning* pada bidang lain agar dapat diketahui apakah metodologi bisa diimplementasikan pada perusahaan dengan bidang berbeda.
4. Berdasarkan implementasi metodologi Business Continuity Planning yang telah dilakukan didapatkan bahwa metodologi belum memberikan arahan yang cukup jelas dalam aktivitas-aktivitas perencanaan keberlangsungan bisnis. Sehingga perlu dilakukan pendetailan tahapan terhadap aktivitas yang ada sehingga memudahkan implementasi metodologi.

Adapun saran yang dapat disampaikan untuk penelitian selanjutnya adalah melanjutkan aktivitas yang tidak dapat

diimplementasi serta menemukan metode evaluasi yang lebih efektif dalam implementasi metodologi. Sehingga nantinya dapat diketahui apakah aktivitas-aktivitas pada metodologi *Business Continuity Planning* tersebut dapat diimplementasi pada dokumen perencanaan keberlangsungan bisnis.

(*Halaman ini sengaja dikosongkan)*

DAFTAR PUSTAKA

[1] S. Snedaker, *Business Continuity and Disaster Recovery Overview*. 2007.

[2] P. K. Preetish Ranjan, "Business Continuity Planning in Indian Perspective," *J. Adv. Comput. Res. An Int. J.*, 2012.

[3] Y. Muflihah, "Business Continuity Plan: Sebuah Usulan Metodologi, Empiris PT PLN (Persero) Distribusi Jawa Timur," 2017.

[4] A. A. Amanda, "Konsep Penyusunan Kerangka Kerja Business Continuity Plan Teknologi dan Sistem Informasi," 2014.

[5] U. R. Isnaini, "Formulasi Strategi Untuk Acuan Dokumen Perencanaan Keberlangsungan Bisnis (BCP) Berbasis Teknologi di PT. Pertamina Refinery Unit IV Cilacap," 2016.

[6] "ISO Guide 31000," p. 9, 2009.

[7] NIST, "Contingency Planning Guide for Information Technology Systems, NIST Special Publication."

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

[9] M. Spremic, "Emerging issues in IT Governance: implementing the corporate IT risks management model," pp. 219–228, 2008.

[10] S. Priti, *Practitioner's Guide to Business Impact Analysis*. 2017.

[11] B.-C. Bjork, "Information Technology in Construction : Domain Definition and Research Issues," *Int. J. Comput. Integr. Des. Constr. SETO, London*, vol. 1, pp. 1–16, 1999.

[12] J. O. G. Marakas, *Introduction to Information Systems 15th Edition*. 2010.

[13] H. Carr and C. A. Snyder, "The Management of Telecommunications," 1997.

[14] R. G. S. Ali Torabi, "An enhanced risk assessment framework for business continuity management systems," 2016.

[15] A. D. Christopher Alberts, “Introduce to the OCTAVE Approach,” *Pittsbg. Carnegie Mellon Softw. Eng. Inst.*, 2003.

[16] J. F. Richard A. Caralli, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” 2007.

[17] J. Kouns and M. Daniel, “Information Technology Risk Management in Enterprise Environments,” 2010.

[18] C. S. Carlson, *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis, First Edition*. John Wiley & Sons, Inc, 2012.

[19] Dyadem Engineering Corporation, “Guidelines for Failure Mode and Effects Analysis For Automotive, Aerospace and General Manufacturing Industries,” 2003.

[20] D. and W. Gygi, “No Title,” 2005.

[21] S. D, “Failure Mode and Effect Analysis FMEA from Theory to Execution Second Edition,” 2003.

[22] Technical Committee ISO/TC 223, “ISO 22301 Societal Security-Business Continuity Management Systems-Requirements,” 2012.

[23] M. Devargas, *Survival is Not Compulsory: An Introduction to Business Continuity Planning*. 1999.

[24] Federal Office for Information Security, *Business Continuity Management for SMEs using the Cloud*. 2013.

[25] H. U. K. Venclova, “Advantages and Disadvantages of Business Continuity Management,” *Advantages Disadvantages Bus. Contin. Manag.*, 2013.

[26] Griffith University, “Business Continuity Management Framework,” 2013.

[27] A. Hiles, *The Definitive Handbook of Business Continuity Management Second Edition*. 2007.

[28] SANS Institute, “Introduction to Business Continuity Planning,” 2002.

[29] S. Snedaker *et al.*, “P Lanning for C Olorado ’ S,”

Education, vol. 5, no. 1, pp. 99–131, 2012.

[30] ISACA, "COBIT 5 Enabling Processes," 2012.

[31] D. M, "Business Continuity Planning (BCP) Methodology-Essential For Every Business," *IEEE GCC Conf. Exhib.*, 2011.

[32] M. J. Virginia Cerullo, "Business Continuity Planning: A Comprehensive Approach. Information Systems Management," 2004.

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

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

(*Halaman ini sengaja dikosongkan)*

BIODATA PENULIS

Penulis adalah mahasiswa S1 Jurusan Sistem Informasi, Institut Teknologi Sepuluh Nopember Surabaya yang dilahirkan di Semarang, 17 Mei 1995. Penulis pernah menempuh pendidikan di SDK Aletheia Mataram, SMPK Aletheia Mataram, SMA Negeri 1 Mataram, dan melanjutkan ke ITS dengan mengambil jurusan Sistem Informasi dengan fokus bidang manajemen sistem informasi.

Selain aktif dalam bidang akademis penulis juga aktif dalam organisasi kemahasiswaan, baik di dalam maupun di luar kampus. Beberapa organisasi pernah menjadi ladang untuk menimba ilmu dan pengalaman bagi penulis, antara lain adalah HMSI sebagai kepala divisi Manajemen Bisnis departemen Kewirausahaan (2016/2017), serta staff Pengembangan Kompetensi Persekutuan Mahasiswa Kristen ITS (2016/2017) dan aktif dalam beberapa kegiatan kepanitiaan.

Penulis yang memiliki hobi membaca buku dan belajar bisnis ini juga pernah menjalani kerja praktek di PT. Pos Indonesia terkait bidang *Digital Marketing*. Penulis dapat dihubungi di rachelcarolinac@gmail.com

(Halaman ini sengaja dikosongkan)

LAMPIRAN A: HASIL WAWANCARA

Tujuan Interview	:	Wawancara dilakukan untuk mengetahui aset teknologi informasi serta komponennya dan juga pengamanan apa saja yang sudah diterapkan kepada aset teknologi informasi.
Tanggal	:	07-05-2018
Waktu	:	10.00-11.00
Lokasi	:	Kantor Bank Pembangunan Daerah Jawa Timur
Narasumber	:	Adimas I.
Jabatan	:	Grup IT Security Junior Analyst

Kategori Pertanyaan : Analisis Risiko	
No	Pertanyaan
1.	Apa saja aset Teknologi Informasi yang dimiliki oleh divisi Teknologi Informasi? **Jawaban:** Hardware pada ruang data center: • UPS • AS400 (Banking Server) • AC Kering • Apar (alat pemadam kebakaran) • Server • Genset Software: • Docnum (Document Management) • Security Application AS400 • Aplikasi Status Cabang • Compleo • Estim Network: • Switch • Main Router • Jaringan Internet Data: • Data Transaksi People: • Karyawan Bank Pembangunan Daerah Jawa Timur

2.	Apa saja aset Teknologi Informasi yang dimiliki oleh divisi Teknologi Informasi yang kritis? **Jawaban:** Hardware pada ruang data center: • UPS • AS400 (Banking Server) • AC Kering • Server • Genset Software: • Security Application AS400 • Aplikasi Status Cabang • Compleo • Estim Network: • Switch • Main Router • Jaringan Internet Data: • Data Transaksi People: • Karyawan Bank Pembangunan Daerah Jawa Timur
3.	Apa saja ancaman yang dapat terjadi kepada aset teknologi informasi? **Jawaban:** Pada aset teknologi informasi yang ada pada data center, ancaman yang dapat terjadi adalah hacker (server), orang yang tidak berkepentingan, kebakaran, pemadaman listrik serta human error.
4.	Apa saja kerentanan yang dimiliki oleh aset teknologi informasi? **Jawaban**: Pada server dan AS400 (Banking Server) kerentanannya adalah suhu yang harus berada pada 20 ° sampai 25 ° C dan kelembapan dalam ruangan 45% sampai 50% RH. Jika lebih atau kurang dari itu akan menimbulkan kerusakan pada server. Kemudian pada genset, kondisi ruangan harus memiliki ventilasi udara, jika ruangan dari genset tertutup maka genset akan menjadi panas dan mati.
5.	Pengamanan apa saja yang telah diterapkan pada aset teknologi informasi? **Jawaban:**

	Pengamanan pada data center: • Memasang akses kontrol pintu • Memasang cctv • Pencatatan aktivitas pada ruang data center • Memasang kunci ganda pada ruang server disimpan • Memasang alarm pada pintu ruang server • Memasang alat pemadam kebakaran Pengamanan pada server: • Memasang hardware firewall pada server • Mengaktifkan antivirus dan firewall server. Pengamanan pada aset TI • Melakukan pemeliharaan perangkat secara rutin • Melakukan monitoring kapasitas kepada aset TI. • Melakukan backup dan recovery secara rutin • Menyediakan perangkat hardware cadangan
6.	Apa saja ancaman yang dapat menimpa Aset TI perusahaan? • Ancaman yang dapat menimpa aset hardware: • Bencana alam • Kebakaran • Sabotase • Pemadaman Listrik • Kerusakan perangkat Ancaman yang dapat menimpa aset software: • Virus dan Malware • Hacker • Social Engineering • Bug Software Ancaman yang dapat menimpa aset jaringan: • Kerusakan Jaringan • Pemadaman Listrik Ancaman yang dapat menimpa aset data: • Data corrupt • Kehilangan data • Pencurian data

(Halaman ini sengaja dikosongkan)

LAMPIRAN B: HASIL WAWANCARA

Tujuan Interview	:	Mengetahui kondisi umum dan informasi terkait analisis dampak bisnis
Tanggal	:	09-05-2018
Waktu	:	10.00-11.30 , 14.00-15.00
Lokasi	:	Kantor Bank Pembangunan Daerah Jawa Timur
Narasumber	:	M. Arief R.
Jabatan	:	Grup IT Governance and Risk Management Analysis

Kategori Pertanyaan : Kondisi Umum	
No	Pertanyaan
1.	Apa saja sub fungsional yang ada pada divisi Teknologi Informasi yan melakukan proses terkait TI? **Jawaban:** • Grup IT Infrastructure & Network • Grup IT Management Information System • Grup IT Support & Helpdesk • Grup IT Security • Grup IT Data Center
2.	Apa saja peran dan tanggung jawab setiap sub fungsional? **Jawaban:** **Grup IT Infrastructure & Network:** • Melakukan Monitoring Kapasitas • Melakukan Konfigurasi dan Hardening Aplikasi dan Perangkat TI • Melakukan Disposal • Melakukan Pemasangan / Relokasi Jaringan • Melakukan Monitoring ketersediaan Jaringan **Grup IT Management Information System** • Melakukan monitoring kapasitas • Melakukan implementasi sistem aplikasi • Melakukan Post Implementation Review • Melayani Permintaan Data • Melakukan Konfigurasi dan Hardening Aplikasi dan Perangkat TI • Melakukan Restore dan Recovery **Grup IT Support & Helpdesk** • Melakukan Penanganan Insiden dan Masalah • Melakukan Inventarisasi

	• Melakukan Disposal • Melakukan Pemeliharaan Aset TI • Melakukan Penambahan User • Melakukan Penghapusan User • Melakukan Perubahan User **Grup IT Security** • Melakukan Penanganan Insiden Pengamanan Informasi • Melakukan Penanganan Insiden Pengamanan Informasi • Melakukan Penambahan User • Melakukan Penghapusan User • Melakukan Perubahan User • Melakukan Pengelolaan Akses ke Data Center • Melakukan Review Log Hak Akses Logis • Melakukan Penetapan Klasifikasi Dokumen • Melakukan Monitoring Hak Akses Logis • Melakukan Monitoring Hak Akses Fisik **Grup IT Data Center** • Melakukan Implementasi Sistem Aplikasi • Melakukan Post Implementation Review • Melakukan Manajemen Perubahan • Melakukan Patch Management • Melakukan Backup • Melakukan Akhir Periode • Menggunakan Power User • Mengelola Akses ke Database dan Infrastruktur • Mengelola Akses ke Data Center
3.	Apa saja proses bisnis terkait teknologi informasi yang ada pada divisi teknologi informasi? **Jawaban:** **Grup IT Infrastructure & Network:** • Monitoring ketersediaan Jaringan **Grup IT Management Information System** • Monitoring kapasitas • Permintaan Data • Konfigurasi dan Hardening Aplikasi dan Perangkat TI • Restore dan Recovery **Grup IT Support & Helpdesk** • Penanganan Insiden dan Masalah • Inventarisasi • Penambahan User • Penghapusan User • Perubahan User **Grup IT Security**

	• Penanganan Insiden Pengamanan Informasi • Review Log Hak Akses Logis • Monitoring Hak Akses Logis **Grup IT Data Center** • Akhir Periode
4.	Apa saja layanan yang digunakan di divisi TI? **Jawaban:** • Docnum • Security Application AS400 • Aplikasi Status Cabang • Estim • Network Monitoring System • Aplikasi Helpdesk • Compleo • Vulnerability Assessment System
Kategori Pertanyaan : Analisis Dampak Bisnis	
No	Pertanyaan
1.	Layanan TI mana sajakah yang bersifat kritis, penting dan minor? **Jawaban:** Layanan TI Kritis: • Security Application AS400 • Aplikasi Status Cabang • Estim • Network Monitoring System • Compleo Layanan TI Penting: • Docnum • Aplikasi Helpdesk • Vulnerability Asessment System Layanan TI Minor: -
2.	Proses bisnis mana sajakah yang bersifat kritis, penting dan minor? Jawaban: Proses Bisnis Kritis: • Monitoring Availability Jaringan • Permintaan Data • Restore dan Recovery • Penambahan User • Perubahan User • Penghapusan User • Monitoring Hak Akses Logis

	• Review Hak Akses Logis • Akhir Periode Proses Bisnis Penting: • Konfigurasi dan Hardening Aplikasi dan Perangkat TI • Monitoring Kapasitas • Penanganan Insiden • Inventarisasi • Penanganan Insiden Pengamanan Informasi Proses Bisnis Minor : -
3.	Bagaimana waktu pemulihan untuk setiap proses bisnis dan layanan? **Jawaban:** Pada proses bisnis kritis waktu maksimal kegagalan adalah kurang dari 2 jam sedangkan pada proses bisnis penting waktunya diantara 4 hingga 24 jam. Sedangkan waktu pemulihan yang diperlukan untuk proses bisnis dan layanan TI kritis adalah kurang dari 2 jam serta pada proses bisnis dan layanan TI penting adalah 7 hari.

LAMPIRAN C: ANALISIS RISIKO

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
UPS	*Hardware Failure*	H01	UPS rusak	Pemeliharaan yang tidak teratur	3	UPS yang rusak akibat pemeliharaan yang tidak teratur mengakibatkan UPS tidak dapat digunakan saat dibutuhkan.	3	Kegagalan akibat pemeliharaan yang tidak teratur memiliki peluang kecil untuk terjadi karena telah dilakukan pemeliharaan tderatur kepada perangkat.	3	Terdapat penjadwalan untuk memastikan pemeliharaan dilakukan secara teratur dan dilakukan pengecekan terhadap pelaksanaan	27
		H02		Kondisi perangkat yang tidak layak	6	UPS yang rusak akibat kondisi yang tidak layak akan menyebabkan kerusakan yang lebih parah.	2	Kegagalan akibat kondisi perangkat yang tidak layak relatif kecil karena dilakukan pengecekan	3	Terdapat pemeriksaan rutin terhadap perangkat yang dapat mendeteksi ketidak layakan yang	36

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
								rutin terhadap perangkat.		ada pada perangkat.	
		H03		Usia perangkat yang sudah melebihi batas.	2	UPS yang rusak akibat usia perangkat yang melebihi batas mengakibatkan UPS tidak dapat digunakan saat dibutuhkan.	2	Kegagalan akibat usia perangkat yang melebihi batas relatif kecil karena perangkat diganti secara berkala sesuai waktu pemakaian ideal.	2	Terdapat manajemen kapasitas perangkat perusahaan yang mengontrol usia perangkat dan dilakukan penggantian rutin perangkat jika usianya telah mencapai batas tertentu	8
	Kebakaran	H04	UPS terbakar	Api / Ledakan	10	UPS yang terbakar dapat mengancam karyawan serta perangkat lain yang berada di	1	Kegagalan belum pernah terjadi karena lokasi penyimpanan UPS telah jauh	1	Terdapat sensor pendeteksi suhu dan api. Jika suhu meningkat	10

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						sekitar ruang penyimpanan.		dari sumber api dan pemicu ledakan.		drastis akan ada notifikasi yang diterima oleh departemen TI.	
		H05		Arus pendek listrik	10	UPS yang terbakar akibat arus pendek listrik dapat mengancam karyawan serta perangkat lain yang berada di sekitar ruang penyimpanan .	1	Kegagalan belum pernah terjadi karena terdapat perangkat yang mencegah terjadinya arus pendek listrik.	5	Terdapat sekring untuk memutus listrik jika terjadi arus pendek listrik.	50
AS400 (Banking Server)	*Hardware Failure*	H06	Server rusak	Pemeliharaan yang tidak teratur	8	Server yang rusak akan menyebabkan terganggunya proses pada perusahaan.	1	Kegagalan belum pernah terjadi karena terlah jadwal pemeliharaan yang dilakukan secara rutin.	1	Terdapat vendor yang melakukan pemeliharaan serta ada penjadwalan untuk	8

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
										memastikan pemeliharaan dilakukan secara teratur dan dilakukan pengecekan terhadap pelaksanaan	
		H07		Usia server lebih dari 5 tahun .	5	Server yang rusak akibat usia yang melebihi batas akan menghambat proses bisnis perusahaan sehingga menurunkan kinerja.	1	Kegagalan belum pernah terjadi karena jika usia server telah lebih dari 5 tahun maka server akan diganti.	1	Server diganti secara rutin jika usia sudah mendekati batas maksimal pemakaian.	5
		H08		Kondisi lingkungan perangkat tidak sesuai	2	Server yang rusak akibat kondisi lingkungan	1	Kegagalan belum pernah terjadi karena kondisi	1	Terdapat sensor suhu dan kelembapan	2

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
				(suhu ruang dan kelembapan)		yang tidak sesuai akan menyebabkan gangguan kecil.		lingkungan sudah sesuai dengan kebutuhan serta suhu dan kelembapan terus di pantau.		dan terdapat notifikasi jika terjadi perubahan suhu dan kelembapan secara signifikan.	
	Gempa Bumi	H09	Server rusak	Ketidakstabilan alam	8	Gempa bumi akan menyebabkan server menjadi rusak dan banyak layanan yang tidak dapat diakses.	1	Kegagalan akibat gempa bumi belum pernah terjadi.	1	Jika terjadi bencana maka server otomatis akan dialihkan ke server cadangan dan dilakukan pengamanan terhadap server utama	8
	Power Failure	H10	Server Mati	Pemadaman listrik	8	Server yang mati akan mengakibatkan layanan	1	Kegagalan akibat pemadaman listrik belum	1	Terdapat ups yang otomatis menyala jika terjadi	8

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						teknologi informasi tidak dapat diakses.		pernah terjadi karena terdapat sumber tenaga cadangan saat listrik mati yaitu genset.		pemadaman listrik.	
		H11		Kabel daya terputus	5	Server yang mati akibat kabel daya yang terputus akan menyebabkan	1	Kegagalan belum pernah terjadi karena telah dilakukan pemeriksaan secara rutin terhadap komponen perangkat.	1	Dilakukan pemeriksaan rutin terhadap infrastruktur server sehingga kerusakan akan terdeteksi sebelum terjadi.	5
		H12		Arus pendek listrik	10	Arus pendek listrik akan mengancam atau melukai pegawai.	1	Kegagalan belum pernah terjadi karena terdapat perangkat yang mencegah	1	Terdapat sekring yang memutus aliran listrik jika terjadi	10

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
								terjadinya arus pendek listrik.		arus pendek listrik.	
	Kebakaran	H13	Server Terbakar	Api / Ledakan	10	Server yang terbakar dapat mengancam karyawan serta perangkat lain yang berada di sekitar ruang penyimpanan.	1	Kegagalan belum pernah terjadi karena lokasi penyimpanan UPS telah jauh dari sumber api dan pemicu ledakan.	1	Terdapat sensor api serta suhu dan akan ada notifikasi jika suhu berubah secara signifikan.	10
		H14		Arus pendek listrik	10	Server yang terbakar akibat arus pendek listrik dapat mengancam karyawan serta perangkat lain yang berada di sekitar ruang penyimpanan .	1	Kegagalan belum pernah terjadi karena terdapat perangkat yang mencegah terjadinya arus pendek listrik.	1	Terdapat sekting yang akan memutus listrik jika terjadi arus pendek listrik.	10
	Sabotase	H15	Penyalahgun	Kurang pengawasan	9	Penyalahgunaan server akibat	1	Kegagalan belum pernah	1	Pada ruang data center	9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
			aan Server			kurangnya pengawasan akan menyebabkan aktivitas ilegal.		terjadi karena untuk dapat masuk ke ruang server diperlukan memiliki kartu khusus dan harus ditemani oleh staff data center.		dipasang cctv serta door access yang mencegah orang yang tidak berkepentingan untuk masuk. Selain itu orang yang memasuki data center harus mengisi logbook sebagai dokumentasi aktivitas.	
		H16		Tidak ada penanggungjawab	9	Penyalahgunaan server akibat kurangnya pengawasan akan menyebabkan	1	Kegagalan belum pernah terjadi karena ada pertugas yang bertanggungjaw	1	Terdapat staff khusus yang bertanggungjawab terhadap ruang data center.	9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						akterivitas ilegal.		ab terhadap ruang data center.			
	Banjir	H17	Server Rusak	Kebocoran saluran air	8	Jika server rusak akibat kebocoran air maka layanan teknologi informasi tidak akan bisa diakses.	1	Kegagalan belum pernah terjadi.	1	Lokasi pipa pembuangan dijauhkan dari server serta dilakukan pemeriksaan secara rutin terhadap pipa pembuangan air.	8
	Cyber Crime	H18	Server Diretas	Virus dan Malware	9	Server yang terkena virus atau malware akan menimbulkan server diakses oleh orang asing.	1	Kegagalan belum pernah terjadi karena OS dari server tergolong aman.	1	Server core banking memiliki bahasa pemrograman yang unik dan cukup sulit sehingga akan sulit untuk diretas	9
		H19		Hacker	9	Server yang diretas oleh	1	Kegagalan belum pernah	1		9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						hacker akan menimbulkan server diakses oleh orang asing.		terjadi karena tingkat keamanan pada server yang tinggi.		maupun terinfeksi virus.	
AC Kering	*Power Failure*	H20	AC Mati	Pemadaman listrik	3	AC yang mati akibat pemadaman listrik akan menyebabkan suhu pada ruangan data center naik.	2	Kemungkinan kegagalan relatif kecil karena terdapat genset sebagai sumber tenaga cadangan.	1	Terdapat UPS yang otomatis menjadi sumber tenaga cadangan ketika terjadi pemadaman listrik.	6
		H21		Kabel daya terputus	3	AC yang mati akibat kabel daya terputus akan menyebabkan suhu pada ruangan data center naik.	1	Kegagalan belum pernah terjadi karena selalu dilakukan pemeriksaan terhadap komponen dari perangkat.	4	Dilakukan pemeriksaan rutin terhadap infrastruktur perangkat sehingga jika terdapat kabel yang bermasalah akan segera	12

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
										terdeteksi saat dilakukan pemeriksaan.	
		H22		Arus pendek listrik	3	AC yang mati akibat arus pendek listrik akan menyebabkan suhu pada ruangan data center naik.	1	Kegagalan belum pernah terjadi karena terdapat perangkat yang mencegah terjadinya arus pendek listrik.	5	Terdapat sekring yang memutus aliran listrik secara otomatis ketika terjadi arus pendek listrik.	15
	Hardware Failure	H23	AC Rusak	Pemeliharaan yang tidak teratur	3	AC yang rusak akan meningkatkan suhu pada ruang data center dan mengganggu kinerja dari server.	1	Kegagalan belum pernah terjadi karena telah dilakukan pemeliharaan secara teratur..	2	Terdapat penjadwalan pemeliharaan serta pemeriksaan terhadap pemeliharaan yang dilakukan.	6
		H24		Usia perangkat	3	AC yang rusak akibat usia yang	1	Kegagalan belum pernah	2	Terdapat monitoring	6

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
				yang sudah melebihi batas.		melebihi batas akan meningkatkan suhu pada ruang data center dan mengganggu kinerja dari server.		terjadi karena perangkat yang usianya melebihi batas segera diganti.		kapasitas perangkat, jika ada perangkat yang usianya melebihi batas akan segera diganti.	
	Banjir	H25	AC Rusak	Kebocoran saluran air pembuangan	5	Jika terjadi kebocoran maka air dapat merusak perangkat lain dan dapat	2	Kemungkinan kegagalan terjadi relatif kecil karena telah dilakukan pemeriksaan rutin terhadap kondisi saluran pembuangan air.	3	Telah dilakukan pemeriksaan rutin terhadap pipa pembuangan air sehingga kebocoran mudah terdeteksi.	30
Server	*Hardware Failure*	H26	Server Rusak	Pemeliharaan yang tidak teratur	8	Server yang rusak akan menyebabkan terganggunya	1	Kegagalan belum pernah terjadi karena terlah terdapat jadwal	1	Pemeliharaan terhadap server telah dihandle oleh vendor dan	8

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						proses pada perusahaan.		pemeliharaan yang dilakukan secara rutin.		dilakukan secara rutin.	
		H27		Usia perangkat yang sudah melebihi batas.	5	Server yang rusak akibat usia yang melebihi batas akan menghambat proses bisnis perusahaan sehingga menurunkan kinerja.	1	Kegagalan belum pernah terjadi karena jika usia server telah lebih dari 5 tahun maka server akan diganti.	1	Terdapat monitoring terhadap kapasitas aset TI perusahaan. Aset akan diganti jika mendekati batas usia maksimal penggunaan.	5
		H28		Kondisi lingkungan perangkat tidak sesuai (suhu ruang dan kelembapan)	2	Server yang rusak akibat kondisi lingkungan yang tidak sesuai akan menyebabkan gangguan kecil.	1	Kegagalan belum pernah terjadi karena kondisi lingkungan sudah sesuai dengan kebutuhan serta	1	Terdapat sensor untuk memantau suhu dan kelembapan ruangan. Jika suhu dan kelembapan	2

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
								suhu dan kelembapan terus di pantau.		berubah secara tiba-tiba, maka akan ada notifikasi pemberitahuan yang diterima oleh staff.	
	Gempa Bumi	H29	Server Rusak	Ketidakstabilan alam	8	Gempa bumi akan menyebabkan server menjadi rusak dan banyak layanan yang tidak dapat diakses.	1	Kegagalan akibat gempa bumi belum pernah terjadi.	1	Saat bencana terjadi maka server cadangan otomatis difungsikan.	8
	Power Failure	H30	Server Mati	Pemadaman listrik	8	Server yang mati akan mengakibatkan layanan teknologi	1	Kegagalan akibat pemadaman listrik belum pernah terjadi karena terdapat	1	UPS akan otomatis berfunngsi ketika terjadi pemadaman listrik.	8

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						informasi tidak dapat diakses.		sumber tenaga cadangan saat listrik mati yaitu genset.			
		H31		Kabel daya terputus	5	Server yang mati akibat kabel daya yang terputus akan menyebabkan	1	Kegagalan belum pernah terjadi karena telah dilakukan pemeriksaan secara rutin terhadap komponen perangkat.	1	Server telah dikelola secara rutin dan diperiksa secara rutin. Jika terdapat infrastruktur yang kondisinya tidak baik langsung diganti.	5
		H32		Arus pendek listrik	10	Arus pendek listrik akan mengancam atau melukai pegawai.	1	Kegagalan belum pernah terjadi karena terdapat perangkat yang mencegah	1	Terdapat sekring yang otomatis memutus arus listrik ketika terjadi arus pendek, selain	10

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
								terjadinya arus pendek listrik.		itu dilakukan uji daya secara rutin untuk memastikan daya listrik tidak tinggi atau rendah.	
	Kebakaran	H33	Server Terbakar	Api / Ledakan	10	Server yang terbakar dapat mengancam karyawan serta perangkat lain yang berada di sekitar ruang penyimpanan.	1	Kegagalan belum pernah terjadi karena lokasi penyimpanan telah jauh dari sumber api dan pemicu ledakan.	1	Terdapat sensor api dan suhu, jika suhu berubah tiba-tib akan ada notifikasi.	10
		H34		Arus pendek listrik	10	Server yang terbakar akibat arus pendek listrik dapat mengancam karyawan serta perangkat lain	1	Kegagalan belum pernah terjadi karena terdapat perangkat yang mencegah	1	Terdapat sekring yang memutus arus listrik secara otomatis ketika terjadi	10

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						yang berada di sekitar ruang penyimpanan .		terjadinya arus pendek listrik.		arus pendek listrik.	
	Sabotase	H35	Penyalahgunaan Server	Kurang pengawasan	9	Penyalahgunaan server akibat kurangnya pengawasan akan menyebabkan aktivitas ilegal.	1	Kegagalan belum pernah terjadi karena untuk dapat masuk ke ruang server diperlukan memiliki kartu khusus dan harus ditemani oleh staff data center.	1	Pada ruang data center dipasang door access sehingga orang yang tidak berwenang tidak dapat masuk, selain itu dipasang cctv dan dilakukan dokumentasi aktivitas pada ruang server dalam bentuk logbook.	9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
		H36		Tidak ada penanggungjawab	9	Penyalahgunaan server akibat kurangnya pengawasan akan menyebabkan akterivitas ilegal.	1	Kegagalan belum pernah terjadi karena ada pertugas yang bertanggungjawab terhadap ruang data center.	1	Terdapat admin atau staff yang bertanggungjawab terhadp ruang data center.	9
	Banjir	H37		Kebocoran saluran air	8	Jika server rusak akibat kebocoran air maka layanan teknologi informasi tidak akan bisa diakses.	1	Kegagalan belum pernah terjadi.	1	Dilakukan pemeriksaan rutin terhadap pipa pembuangan air sehingga kebocoran dapat dideteksi lebih awal.	8
	Cyber Crime	H38	Server Diretas	Virus dan Malware	9	Server yang terkena virus atau malware akan	1	Kegagalan belum pernah terjadi karena	1	Pemasangan firewall dan antivirus pada server.	9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						menimbulkan server diakses oleh orang asing.		OS dari server tergolong aman.			
		H39		Hacker	9	Server yang diretas oleh hacker akan menimbulkan server diakses oleh orang asing.	1	Kegagalan belum pernah terjadi karena tingkat keamanan pada server yang tinggi.	1	Terdapat aplikasi pendeteksi log aktivitas server, jika ada aktivitas mencurigakan maka akan ada notifikasi.	9
Genset	*Hardware Failure*	H40	Genset Rusak	Pemeliharaan yang tidak teratur	5	Genset yang rusak akibat pemeliharaan yang tidak teratur akan menyebabkan genset tidak dapat digunakan saat terjadi	2	Kemungkinan kegagalan terjadi relatif kecil karena telah dilakukan pemeliharaan secara teratur	2	Terdapat jadwal pemeliharaan genset serta pengawasan terhadap pelaksanaan pemeliharaan yang dilakukan.	20

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						pemadaman listrik.					
		H41		Usia perangkat yang sudah melebihi batas.	3	Genset yang rusak akibat usia yang melebihi batas menyebabkan genset tidak dapat digunakan saat dibutuhkan	1	Kegagalan belum pernah terjadi karena perangkat yang melebihi batas diganti.	2	Dilakukan montioring terhadap usia dan kondisi perangkat, jika usia sudah mencapai batas maksimal maka perangkat segera diganti.	6
		H42		Pengisian bahan bakar yang tidak sesuai	2	Pengisian bahan bakar yang tidak sesuai akan mengganggu kinerja genset dan merusak hingga menyebabkan	1	Kegagalan belum pernah terjadi karena pengisian bahan bakar genset selalu sesuai dengan yang dibutuhkan.	1	Terdapat prosedur untuk pengisian bahan bakar genset dan dokumentasi setiap	2

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						genset tidak dapat digunakan.				pengisian dilakukan.	
Security Application AS400	*Cyber Crime*	S01	Software diretas	Virus dan Malware	9	Modul pada security application yang mengelola user dan hal lain terkait server yang diretas akibat terkena virus malware akan diakses secara ilegal oleh orang asing.	1	Kegagalan belum pernah terjadi karena bahasa pemrograman aplikasi sangat aman.	1	Telah dipasang antivirus dan firewal pada setiap komputer.	9
		S02		*Hacker*	9	Modul pada security application yang mengelola user dan hal lain terkait server yang diretas	1	Kegagalan belum pernah terjadi karena sistem dari aplikasi sangat aman.	1	Terdapat aplikasi pendeteksi log user sehingga jika ada aktivitas yang mencuigakan	9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						akan diakses secara ilegal oleh orang hacker.				akan segera terdeteksi.	
				Social Engineering	9	Modul pada security application yang mengelola user dan hal lain terkait server yang diretas akibat social engineer akan diakses secara ilegal oleh orang asing.	1	Kegagalan belum pernah terjadi karena para karyawan telah waspada.	1	Telah dilakukan sosialisasi kepada seluruh karyawan terkait dengan social engineering.	9
	Software Failure	S03	Software tidak dapat diakses	*Software Bug*	3	Software yang tidak dapat diakses akibat software bug akan menyebabkan pengelolaan	1	Kegagalan belum pernah terjadi.	1	Dilakukan update aplikasi secara rutin.	3

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						user dan proses lain yang didukung oleh Security Application menjadi terganggu.					
		S04		*Operating System incompatible*	8	Software yang tidak dapat diakses akibat OS yang incompatible menyebabkan layanan terkait Security Application menjadi tidak tersedia.	1	Kegagalan belum pernah terjadi.	1	Dilakukan update OS secara rutin.	8
		S05		*Overload Request*	5	Software yang tidak dapat diakses akibat overload request menyebabkan	1	Kegagalan belum pernah terjadi.	1	Membatasi akses user yang tidak berkepentinga n. Serta	5

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						beberapa proses yang menjadi terganggu selama beberapa saat dan menurunkan kinerja.				melakukan block kepada user yang melakukan over request.	
		S06		*Out of date software version*	8	Software Security Application yang tidak dapat diakses akibat versi yang *out of date* akan menyebabkan layanan tidak dapat diakses hingga software diperbarui.	1	Kegagalan belum pernah terjadi.	1	Terdapat notifikasi pengingat update aplikasi.	8
Aplikasi status cabang	*Cyber Crime*	S07	Software Diretas	Virus dan Malware	2	Software status cabang yang diretas tidak terlalu	1	Kegagalan belum pernah terjadi karena bahasa	1	Telah dipasang antivirus dan firewal pada	2

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						berdampak besar karena aplikasi tidak menyimpan data yang confidential dan tidak terlalu berdampak pada kinerja perusahaan.		pemrograman aplikasi sangat aman.		setiap komputer.	
		S08		*Hacker*	2	Software status cabang yang diretas tidak terlalu berdampak besar karena aplikasi tidak menyimpan data yang confidential dan tidak terlalu berdampak pada	1	Kegagalan belum pernah terjadi karena sistem dari aplikasi sangat aman.	1	Terdapat aplikasi pendeteksi log user sehingga jika ada aktivitas yang mencuigakan akan segera terdeteksi.	2

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						kinerja perusahaan.					
		S09		*Social Engineering*	2	Software status cabang yang diretas tidak terlalu berdampak besar karena aplikasi tidak menyimpan data yang confidential dan tidak terlalu berdampak pada kinerja perusahaan.	1	Kegagalan belum pernah terjadi karena para karyawan telah waspada.	1	Telah dilakukan sosialisasi kepada seluruh karyawan terkait dengan social engineering.	2
	Software Failure	S10	Software tidak dapat diakses	*Software Bug*	2	Jika software tidak dapat diakses dampaknya sedikit mengganggu	1	Kegagalan belum pernah terjadi.	1	Dilakukan update aplikasi secara rutin.	2
		S11		*Software incompatible*	2		1	Kegagalan belum pernah terjadi.	1	Dilakukan update OS secara rutin.	2

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
		S12		*Overload Request*	2	kinerja perusahaan	1	Kegagalan belum pernah terjadi.	1	Membatasi akses user yang tidak berkepentinga n. Serta melakukan block kepada user yang melakukan over request.	2
		S13		*Out of date software version*	2		1	Kegagalan belum pernah terjadi.	1	Terdapat notifikasi pengingat update aplikasi.	2
Estim	*Cyber Crime*	S14	Softw are Direta s	Virus dan Malware	9	Risiko yang terjadi merupakan aktivitas yang ilegal dan berbahaya bagi perusahaan	1	Kegagalan belum pernah terjadi karena bahasa pemrograman aplikasi sangat aman.	1	Telah dipasang antivirus dan firewal pada setiap komputer.	9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
		S15		*Hacker*	9	karena estim merupakan sistem informasi perbankan yang sangat penting bagi perusahaan.	1	Kegagalan belum pernah terjadi karena sistem dari aplikasi sangat aman.	1	Terdapat aplikasi pendeteksi log user sehingga jika ada aktivitas yang mencuigakan akan segera terdeteksi.	9
		S16		*Social Engineering*	9		1	Kegagalan belum pernah terjadi karena para karyawan telah waspada.	1	Telah dilakukan sosialisasi kepada seluruh karyawan terkait dengan social engineering.	9
	Software Failure	S17	Softw are tidak dapat	*Software Bug*	5	Kegagalan aplikasi yang diakibatkan oleh bug pada software akan	1	Kegagalan belum pernah terjadi.	1	Dilakukan update aplikasi secara rutin.	5

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
			diakses			menyebabkan keluhan dan kinerja perusahaan akan menurun karena terganggunya proses bisnis.					
		S18		*Software incompatible*	8	Aplikasi yang tidak dapat diakses akibat software incompatible mengakibatkan layanan menjadi tidak layak untuk digunakan.	1	Kegagalan belum pernah terjadi.	1	Dilakukan update OS secara rutin.	8
		S19		*Overload Request*	7		2	Kemungkinan kegagalan untuk terjadi relatif kecil karena kapasitas server cukup besar	1	Membatasi akses user yang tidak berkepentingan. Serta melakukan	14

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
								untuk menerima *request* dari user.		block kepada user yang melakukan over request.	
		S20		*Out of date software version*	8	Aplikasi yang tidak dapat diakses akibat versi yang out of date mengakibatkan layanan menjadi tidak layak untuk digunakan.	1	Kegagalan belum pernah terjadi.	1	Terdapat notifikasi pengingat update aplikasi.	8
Database	*Data Corruption*	D01	Data Rusak	Terjadi kesalahan saat pemrosesan data	7	Ketika data menjadi rusak maka akan mengganggu proses yang ada pada bank dan menyebabkan pelanggan	1	Kegagalan belum pernah terjadi.	1	Terdapat backup data.	7

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						menjadi tidak puas.					
		D02		Virus atau malware	7	Ketika data menjadi rusak akibat virus atau malware maka akan mengganggu proses yang ada pada bank dan menyebabkan pelanggan menjadi tidak puas.	1	Kegagalan belum pernah terjadi.	1	Terdapat antivirus	7
		D03		Kerusakan pada lokasi penyimpanan	8	Data yang rusak akibat kerusakan hardisk menyebabkan perangkat tidak layak untuk digunakan.	1	Kegagalan belum pernah terjadi.	1	Melakukan mirroring serta backup secara rutin terhadap data.	8

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
	Pencurian Data dan Informasi	D04	Data Dicuri	Unauthorized user	9	Data yang dicuri akan menyebabkan data perusahaan menjadi tersebar dan diakses oleh orang asing.	1	Kegagalan belum pernah terjadi.	1	Melakuakan verifikasi user serta memonitor aktivitas user.	9
		D05		Hacker	9	Data yang dicuri akan menyebabkan data perusahaan menjadi tersebar dan diakses oleh hacker.	1	Kegagalan belum pernah terjadi.	1		9
	Data Loss	D06	Data hilang	Kerusakan server penyimpanan data	8	Data yang hilang akibat kerusakan server akan menyebabkan layanan pada perusahaan menjadi terhenti.	1	Kegagalan belum pernah terjadi.	1	Melakukan mirroring serta backup secara rutin terhadap data.	8

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
		D07		Virus dan malware	9	Data hilang yang diakibatkan oleh virus dan malware merupakan aktivitas ilegal dan berbahaya bagi perusahaan.	1	Kegagalan belum pernah terjadi.	1	Telah digunakan antivirus.	9
		D08		Hacker	9	Data hilang yang diakibatkan oleh hacker merupakan aktivitas ilegal dan berbahaya bagi perusahaan.	1	Kegagalan belum pernah terjadi.	1	Dilakukan monitoring terhadap aktivitas user serta melakukan block terhadap aktivitas yang mencurigakan.	9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
		D09		Kapasitas penyimpanan penuh	8	Data yang hilang akibat kapasitas penyimpanan yang penuh akan menyebabkan layanan menjadi tidak layak karena data yg diinput tidak dapat disimpan.	1	Kegagalan belum pernah terjadi karena selalu dilakukan backup sebelum kapasitas menjadi penuh.	1	Terdapat notifikasi kapasitas data saat ini dan ada alert jika kapasitas hampir penuh.	8
		D10		Terhapus secara tidak sengaja	8	Data yang hilang akibat terhapus secara tidak sengaja akan menyebabkan layanan menjadi tidak layak karena data yang	1	Kegagalan belum pernah terjadi.	1	Terdapat log aktivitas user.	8

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						dibutuhkan tidak ada.					
Kabel Fiber Optik	*Network Failure*	N01	Jaringan Terputus	Terputusnya jaringan dari service provider	5	Jaringan terputus akan menyebabkan beberapa layanna menjadi tidak dapat diakses sehingga terjadi penutunan kinerja bahkan menimbulkan keluhan dari pelanggan maupun internal perusahan.	1	Kegagalan belum pernah terjadi karena terdapat jaringan backup.	1	Menyediakan jaringan cadangan yang otomatis berfungsi jika jaringan utama terputus.	5
		N02		Kabel terputus	5	Kabel terputus akan menyebabkan kegagalan jaringan sehingga	1	Kegagalan belum pernah terjadi karena dilakukan pengecekan secara rutin	1	Dilakukan pemeliharaan secara rutin terhadap infrastruktur kabel untuk	5

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						beberapa layanna menjadi tidak dapat diakses sehingga terjadi penutunan kinerja bahkan menimbulkan keluhan dari pelanggan maupun internal perusahan.		terhadap kabel dan perangkat jaringan.		mendeteksi kemungkinan kerusakan.	
Switch	Kerusakan	N03	Switch Rusak	Pemeliharaan yang tidak teratur	5	Kerusakan pada switch akibat pemeliharaan yang tidak teratur akan menyebabkan jaringan mati dan beberapa layanna menjadi tidak dapat diakses	1	Kegagalan belum pernah terjadi.	3	Dilakukan pemeliharaan teratur terhadap perangkat jaringan.	15

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						sehingga terjadi penutunan kinerja bahkan menimbulkan keluhan dari pelanggan maupun internal perusahan.					
		N04		Usia perangkat yang sudah melebihi batas.	5	Kerusakan pada switch akibat usia perangkat yang melebihi batas akan menyebabkan jaringan mati dan beberapa layanna menjadi tidak dapat diakses sehingga terjadi penutunan kinerja bahkan menimbulkan	1	Kegagalan belum pernah terjadi karena perangkat yang usianya melebihi batas segera diganti.	3	Dilakukan monitoring terhadap kapasitas perangkat serta dilakukan penggantian terhadap perangkat yang usianya mencapai batas maksimal penggunaan.	15

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						keluhan dari pelanggan maupun internal perusahan.					
	Power Failure	N05	Switch Mati	Pemadaman listrik	3	Switch yang mati akan menyebabkan gangguan kecil pada jaringan	2	Kemungkinan kegagalan relatif kecil karena terdapat sumber tenaga cadangan yaitu genset.	1	terdapat UPS yang langsung menyala otomatis sebagai sumber tenaga cadangan ketika terjadi pemadaman listrik.	6
		N06		Kabel terputus	3		2	Kemungkinan kegagalan relatif kecil	3	Telah dilakukan pemeriksaan terhadap infrastruktur perangkat secara rutin untuk mendeteksi	18

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
										keadaan kabel.	
		N07		Arus pendek listrik	3		1	Kegagalan belum pernah terjadi karena terdapat perangkat yang mencegah arus pendek listrik.	3	Terdapat sekring yang otomatis menmutus arus listrik ketika terjadi arus pendek. Dilakukan pengukuran daya secara rutin untuk mendeteksi kemungkinan terjadi hhubungan arus pendek.	9
,Main Router	Kerusakan	N08	Router Rusak	Pemeliharaan yang tidak teratur	5	Router yang rusak akibat pemeliharaan yang tidak teratur akan	1	Kegagalan belum pernah terjadi karena telah dilakukan	1	Dilakukan penjadwalan pemeliharaan serta dilakukan	5

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						menyebabkan keluhan terkait jaringan yang bermasalah.		pemeliharaan secara teratur.		monitoring terhadap pemeliharaan.	
		N09		Kondisi perangkat yang tidak layak	8	Jika router rusak akibat kondisi yang tidak layak maka menyebabkan router menjadi tidak layak untuk digunakan.	1	Kerusakan pada switch akibat pemeliharaan yang tidak teratur akan menyebabkan jaringan mati dan beberapa layanna menjadi tidak dapat diakses sehingga terjadi penutunan kinerja bahkan menimbulkan keluhan dari pelanggan maupun internal perusahan.	1	Dilakukan monitoring terhadap kapasitas perangkat, jika keadaan perangkat tidak baik maka akan dilakukan penanganan.	8

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
	Power Failure	N10	Router Mati	Pemadaman listrik	5	Router yang mati akibat pemadaman listrik akan menyebabkan jaringan terganggu dan terjadi penurunan kinerja organisasi.	2	Kemungkinan kegagalan relatif kecil karena terdapat sumber tenaga cadangan yaitu genset.	1	terdapat UPS yang langsung menyala otomatis sebagai sumber tenaga cadangan ketika terjadi pemadaman listrik.	10
		N11		Kabel terputus	5	Router yang mati akibat kabel yang terputus akan menyebabkan jaringan terganggu dan terjadi penurunan kinerja organisasi.	1	Kegagalan belum pernah terjadi karena selalu dilakukan pengecekan rutin terhadap perangkat beserta komponennya.	3	Telah dilakukan pemeriksaan terhadap infrastruktur perangkat secara rutin untuk mendeteksi keadaan kabel.	15

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
		N12		Arus Pendek listrik	5	Router yang mati akibat arus pendek listrik akan menyebabkan jaringan terganggu dan terjadi penurunan kinerja organisasi.	1	Kegagalan belum pernah terjadi karena terdapat perangkat yang mencegah terjadinya arus pendek listrik.	3	Terdapat sekring yang otomatis menmutus arus listrik ketika terjadi arus pendek. Dilakukan pengukuran daya secara rutin untuk mendeteksi kemungkinan terjadi hhubungan arus pendek.	15
Staff departemen Teknologi Informasi	*Social Engineering*	P01	Penyalahgunaan akses oleh orang asing	Kurangnya pengetahuan karyawan	9	Orang yang melakukan social engineering dapat memperoleh akses kepada	1	Kegagalan belum pernah terjadi karena karyawan perusahaan telah diberi sosialisasi	1	Dilakukan sosialisasi terkait social engineering dan monitoring	9

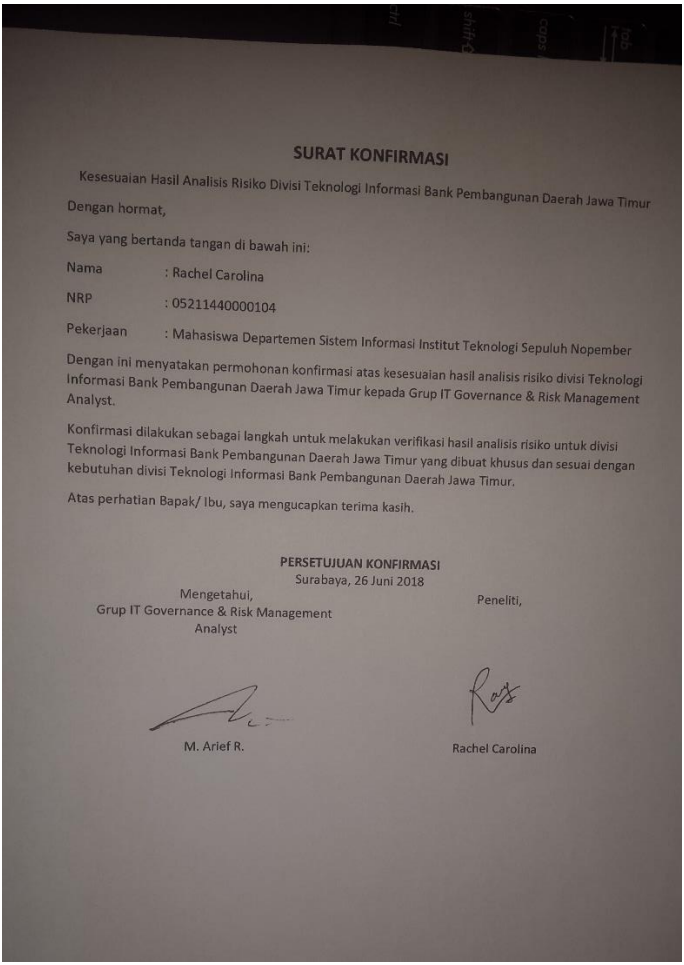
Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
						sistem perusahaan.		terkait keamanan informasi.		terhaadap aktivitas user.	
	Kecelakaan	P02	Staff Terluka	Terjadi bencanan alam	10	Bencana yang terjadi dapat melukai karyawan.	1	Kegagalan belum pernah terjadi.	1	Dilakukan evakuasi terhadap karyawan ketika terjadi bencana serta dilakukan	10
		P03		Terjadi kecelakaan kerja	10	Dampak dari kecelakaan yang terjadi adalah karyawan dapat terluka.	1	Kegagalan belum pernah terjadi.	1	Dilakukan pembuatan SOP keselamatan kerja serta dilakukan pengawasan terhadap pelaksanaan SOP.	10
Staff Non	*Social Engineering*	P04	Penyalahgunaan	Kurangnya pengetahuan karyawan	9	Orang yang melakukan social	1	Kegagalan belum pernah terjadi karena	1	Dilakukan sosialisasi terkait social	9

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
Departemen TI			akses oleh orang asing			engineering dapat memperoleh akses kepada sistem perusahaan.		karyawan perusahaan telah diberi sosialisasi terkait keamanan informasi.		engineering dan monitoring terhaadap aktivitas user.	
	Kecelakaan	P05	Staff Terluka	Terjadi bencana alam	10	Bencana yang terjadi dapat melukai karyawan.	1	Kegagalan belum pernah terjadi.	1	Dilakukan evakuasi terhadap karyawan ketika terjadi bencana serta dilakukan	10
		P06		Terjadi kecelakaan kerja	10	Dampak dari kecelakaan yang terjadi adalah karyawan dapat terluka.	1	Kegagalan belum pernah terjadi.	1	Dilakukan pembuatan SOP keselamatan kerja serta dilakukan pengawasan terhadap	10

Nama Aset TI	Ancaman	ID Risiko	Risiko	Penyebab	SEV	Justifikasi	OCC	Justifikasi	DET	Justifikasi	RPN
										pelaksanaan SOP.	

(Halaman ini sengaja dikosongkan)

LAMPIRAN D: VALIDASI ANALISIS RISIKO



SURAT KONFIRMASI

Kesesuaian Hasil Analisis Risiko Divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama : Rachel Carolina

NRP : 05211440000104

Pekerjaan : Mahasiswa Departemen Sistem Informasi Institut Teknologi Sepuluh Nopember

Dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis risiko divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur kepada Grup IT Governance & Risk Management Analyst.

Konfirmasi dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis risiko untuk divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur yang dibuat khusus dan sesuai dengan kebutuhan divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur.

Atas perhatian Bapak/ Ibu, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI

Surabaya, 26 Juni 2018

Mengetahui,
Grup IT Governance & Risk Management
Analyst

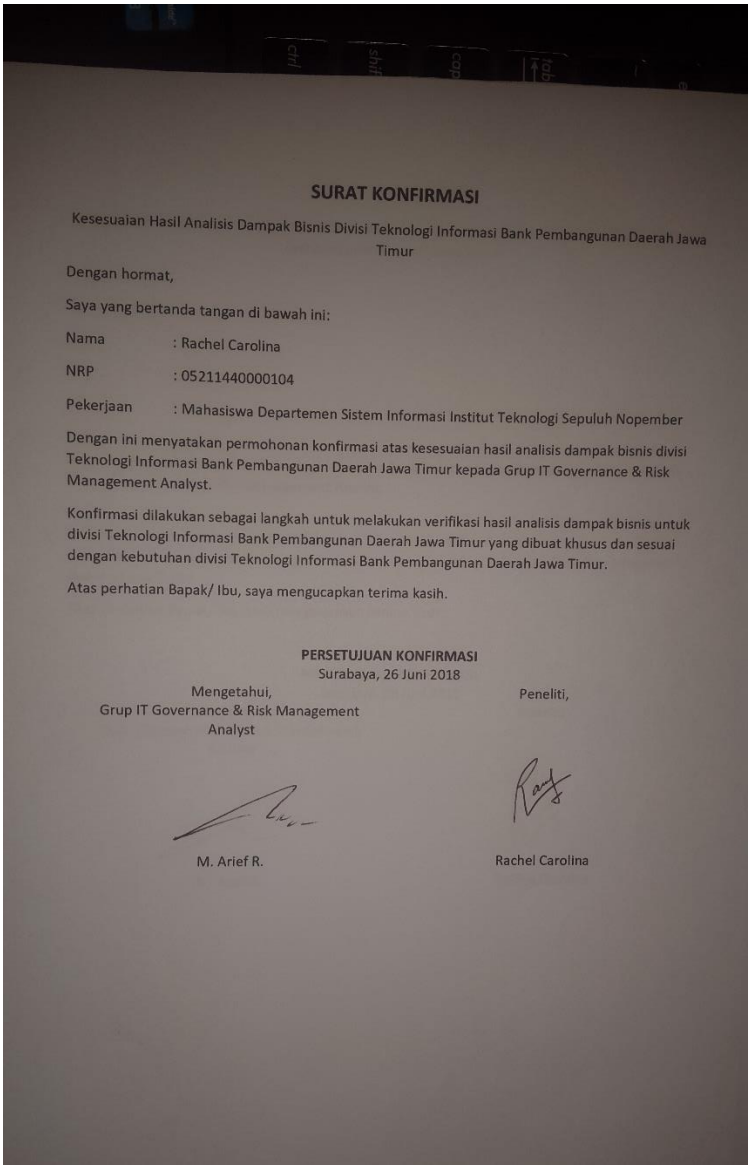
M. Arief R.

Peneliti,

Rachel Carolina

(Halaman ini sengaja dikosongkan)

LAMPIRAN E: VALIDASI ANALISIS DAMPAK BISNIS



SURAT KONFIRMASI

Kesesuaian Hasil Analisis Dampak Bisnis Divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama : Rachel Carolina

NRP : 05211440000104

Pekerjaan : Mahasiswa Departemen Sistem Informasi Institut Teknologi Sepuluh Nopember

Dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil analisis dampak bisnis divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur kepada Grup IT Governance & Risk Management Analyst.

Konfirmasi dilakukan sebagai langkah untuk melakukan verifikasi hasil analisis dampak bisnis untuk divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur yang dibuat khusus dan sesuai dengan kebutuhan divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur.

Atas perhatian Bapak/ Ibu, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI

Surabaya, 26 Juni 2018

Mengetahui,
Grup IT Governance & Risk Management Analyst

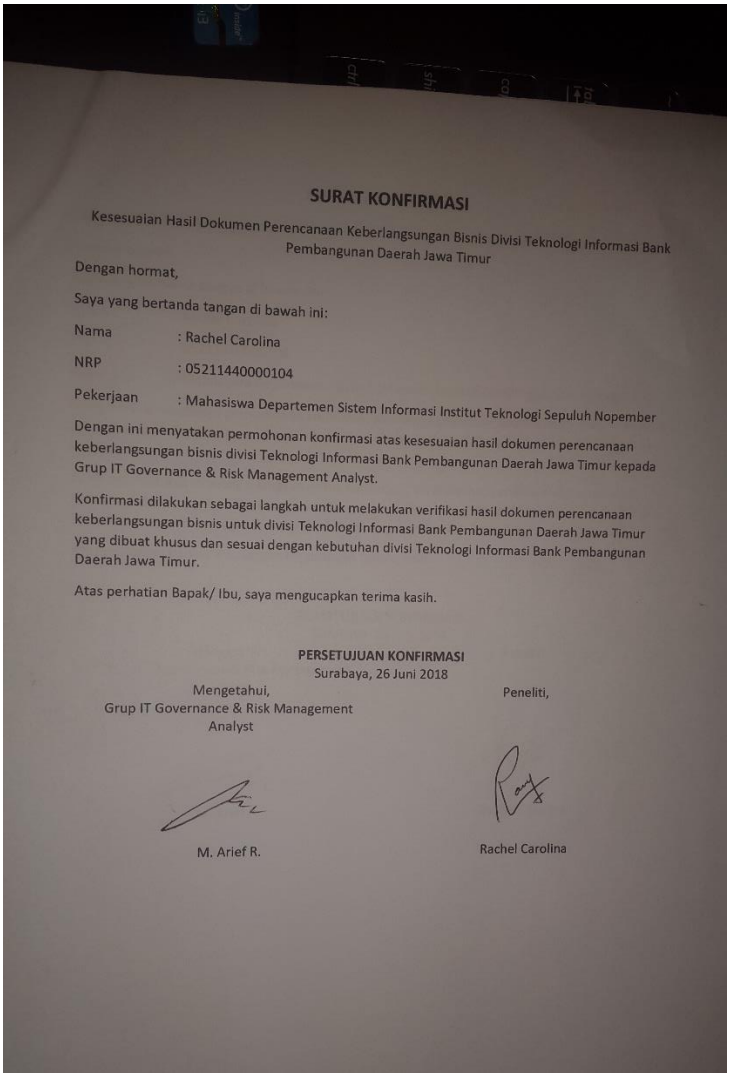
M. Arief R.

Peneliti,

Rachel Carolina

(Halaman ini sengaja dikosongkan)

LAMPIRAN F: VALIDASI DOKUMEN BCP



SURAT KONFIRMASI

Kesesuaian Hasil Dokumen Perencanaan Keberlangsungan Bisnis Divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

Nama : Rachel Carolina

NRP : 05211440000104

Pekerjaan : Mahasiswa Departemen Sistem Informasi Institut Teknologi Sepuluh Nopember

Dengan ini menyatakan permohonan konfirmasi atas kesesuaian hasil dokumen perencanaan keberlangsungan bisnis divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur kepada Grup IT Governance & Risk Management Analyst.

Konfirmasi dilakukan sebagai langkah untuk melakukan verifikasi hasil dokumen perencanaan keberlangsungan bisnis untuk divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur yang dibuat khusus dan sesuai dengan kebutuhan divisi Teknologi Informasi Bank Pembangunan Daerah Jawa Timur.

Atas perhatian Bapak/ Ibu, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI

Surabaya, 26 Juni 2018

Mengetahui,
Grup IT Governance & Risk Management Analyst

M. Arief R.

Peneliti,

Rachel Carolina