BUSINESS CONTINUITY PLAN PADA TEKNOLOGI DAN SISTEM INFORMASI BPR BANK SURYA YUDHA BANJARNEGARA

TUGAS AKHIR

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

Oleh:

ANINDITA ALISIA AMANDA
5210 100 162

Surabaya, Juli 2014

KETUA
JURUSAN SISTEM INFORMASI

Dr. Eng. Febriliyana Samopa S.Kom, M.Kom
NIP 19730219 199802 1 001

BUSINESS CONTINUITY PLAN PADA TEKNOLOGI DAN SISTEM INFORMASI BPR BANK SURYA YUDHA BANJARNEGARA

TUGAS AKHIR

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

Oleh :

ANINDITA ALISIA AMANDA
5210 100 162

Disetujui Tim Penguji : Tanggal Ujian : 17 Juni 2014
Periode Wisuda : September 2014

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

Tony Dwi Susanto, S.T., M.T., Ph.D. **(Penguji 1)**

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

BUSINESS CONTINUITY PLAN PADA TEKNOLOGI DAN SISTEM INFORMASI BPR BANK SURYA YUDHA BANJARNEGARA

Nama Mahasiswa : ANINDITA ALISIA AMANDA
NRP : 5210 100 162
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing : Dr. Apol Pribadi S., S.T, M.T

ABSTRAK

Penelitian ini bertujuan untuk memberikan suatu cara untuk menyusun sebuah kerangka Business Continuity Plan (BCP), yang sesuai dengan kebutuhan perusahaan terkait keberlanjutan bisnis. Business Continuity Plan merupakan solusi terbaik untuk mencegah kelumpuhan sistem dan teknologi informasi serta operasional bisnis perusahaan yang dapat mengoptimalkan kualitas layanan untuk nasabahnya. Penyusunan kerangka dilakukan dengan melakukan formulasi antara kebutuhan dan tujuan perusahaan terkait keberlanjutan bisnis dengan sintesis standar kerangka BCP yang digunakan sebagai acuan, dari ISO 22301:2012, Bank of Japan dan Dutch Financial Sector. Ketiga standar tersebut akan dianalisis dan proses sintesis untuk mendapatkan hasil yangs sesuai dengan kebutuhan perusahaan.

Penelitian dilakukan pada sebuah industri perbankan, BPR (Bank Perkreditan Rakyat) Bank Surya Yudha Banjarnegara. Di mana, teknologi informasi telah menjadi sesuatu hal yang penting bagi perusahaan perbankan untuk dapat meningkatkan kualitas layanan kepada para nasabahnya. Oleh karena itulah, BCP dinilai akan menjadi solusi yang membantu perusahaan ini untuk tetap konsisten dan optimal dalam menghindari dan mengatasi segala bentuk ancaman yang mungkin muncul.

Penelitian ini dilakukan dengan metode yang diawali dengan tahapan identifikasi permasalahan, pengumpulan data, penyusunan kerangka BCP perusahaan, pengolahan data,

analisis BCP, verifikasi dan validasi BCP serta dokumentasi BCP.

Penelitian ini diharapkan dapat menunjukkan bahwa implementasi BCP di sebuah perusahaan merupakan sesuatu hal yang unik, di mana setiap implementasi tersebut harus disesuaikan dengan kebutuhan perusahaan. Pendekatan yang digunakan dalam penelitian ini mengharuskan perusahaan untuk aktif melakukan peningkatan secara terus-menerus (continuous improvement) mengingat kebutuhan perusahaan yang dapat berubah-ubah sesuai dengan perkembangan teknologi informasi dan regulasi perbankan yang berlaku.

Kata kunci: Business Continuity Plan (BCP), ISO 22301:2012, Bank of Japan, Dutch Financial Sector, risiko, teknologi informasi.

BUSINESS CONTINUITY PLAN IN INFORMATION SYSTEMS AND TECHNOLOGY BPR BANK SURYA YUDHA BANJARNEGARA

Name : **ANINDITA ALISIA AMANDA**
NRP : **5210 100 162**
Department : **Information Systems FTIF -ITS**
Supervisor : **Dr. Apol Pribadi S., S.T, M.T**

Abstract

This research aims to provide method to develop framework of a Business Continuity Plan (BCP), which is accordance with the business continuity requirements of the company. Business Continuity Plan is the best solution to prevent paralysis of information systems and technology and business operations that can optimize service quality to the bank's customers. This research is related to formulation framework between business continuity requirements and the standard references that used in this research like; ISO 22301:2012, Bank of Japan and Dutch Financial Sector. Those standards will be analyzed and synthesized to obtain result that accordance with company's business continuity requirements.

Research carried out on a banking industry in a rural bank, BPR Bank Surya Yudha Banjarnegara. In this bank, information technology has become essential for company to be able to improve the quality of banking services to its customers. Hence, BCP becomes one of solutions that help company to avoids and overcomes threats consistently.

This research was conducted with the method that begins with problem identification stage, data collection, preparation of

BCP framework, data processing, analysis BCP, verification and validation of BCP and BCP documentation.

This research proves that BCP in a company is something unique, where each implementation Should be adjusted to the business continuity requirements of the company. The approach that used in this study requires companies to actively conduct continuous improvement. Because the business continuity requirements can change fluctuately, according to the development of information technology and banking regulations.

Keywords: Business Continuity Plan (BCP), ISO 22301:2012, Bank of Japan, Dutch Financial Sector, risk, information technology.

LAMPIRAN

Berikut ini adalah lampiran dokumen dari penelitian ini. Dokumen-dokumen ini dapat dijadikan sebagai bukti dari pengerjaan penelitian ini. Namun dalam lampiran di buku penelitian ini, tidak semua proses dapat ditampilkan di sini, mengingat tingkat kerahasiaan penelitian yang cukup tinggi terkait manajemen risiko teknologi informasi. Sehingga hasil selengkapnya dari penelitian ini disampaikan dalam dokumen produk BCP perusahaan.

KODE LAMPIRAN	LAMPIRAN
A	Lampiran Dokumen Verifikasi Kesesuaian Kebutuhan dan Keinginan Perusahaan terhadap Business Continuity Plan (BPR Bank Surya Yudha Banjarnegara
B	Lampiran Dokumen Verifikasi Kesesuaian Kerangka Kerja Business Continuity Plan (BCP) untuk BPR Bank Surya Yudha Banjarnegara
C	Lampiran Dokumen Verifikasi Kesesuaian Dokumen BCP BPR Bank Surya Yudha Banjarnegara
D	Lampiran Contoh Analisis Dampak Bisnis
E	Lampiran Contoh Manajemen Risiko
F	Lampiran Contoh Kebijakan Komite Pengarah Teknologi Informasi
G	Lampiran Contoh Prosedur Mekanisme Komite Pengarah Teknologi Informasi
H	Lampiran Contoh Formulir Audit Internal Mekanisme Komite Pengarah Teknologi Informasi

KODE LAMPIRAN	LAMPIRAN
I	Lampiran Contoh Formulir Audit Internal Perusahaan BCP
J	Lampiran Contoh Formulir Peninjauan Manajemen
K	Dokumentasi

BAB II
TINJAUAN PUSTAKA

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

2.1 Risiko

Paradigma yang terjadi pada sebagian besar perusahaan di Indonesia dalam hal mengambil keputusan adalah, pengambilan keputusan diambil karena besarnya keuntungan yang didapat, bukan karena besarnya risiko yang akan terjadi. Berdasarkan ISO 31000:2009, risiko (*risk*) adalah *effect of uncertainty on objectives*, atau dengan kata lain adalah sebuah efek yang ditimbulkan dari sebuah ketidakpastian dalam pencapaian tujuan-tujuan dalam suatu organisasi atau perusahaan. Efek tersebut merupakan penyimpangan dari sesuatu yang sudah diekspektasikan sebelumnya, yang dapat berupa hal positif maupun negatif. Tujuan-tujuan juga dapat didefinisikan dari beberapa aspek seperti keuangan, keamanan, dan aspek lainnya, serta dapat diimplementasikan pada level strategis, proyek, proses dan level lainnya.

Berdasarkan pengertian dari *Institute of Risk Management* (IRM), risiko adalah sebuah kombinasi dari kemungkinan terjadinya kejadian yang tidak pasti (*uncertain event*) beserta segala bentuk konsekuensinya. Konsekuensi dari kejadian tersebut dapat berupa hal yang positif dan negatif. Di mana, setiap kejadian yang positif akan menghasilkan kesempatan (*opportunity*) dan kejadian yang negatif akan menghasilkan ancaman (*threat*) bagi perusahaan atau organisasi yang bersangkutan.

PMBoK (*Project Management Body of Knowledge*) juga memaparkan definisi dari risiko. Risiko menurut PMBoK adalah sebuah kejadian yang tidak pasti atau sebuah kondisi yang apabila terjadi, akan menimbulkan efek setidaknya pada satu tujuan proyek. Tujuan proyek tersebut adalah ruang lingkup proyek

(*scope*), penjadwalan proyek (*schedule*), biaya proyek (*cost*) dan kualitas dari proyek yang dilakukan (*quality*).

Perlu adanya penjelasan mengenai perbedaan antara kosakata *risk* (risiko) dengan *uncertainty* (ketidakpastian). Di mana, setiap risiko adalah ketidakpastian, namun tidak semua ketidakpastian adalah risiko.

2.1.1 Risiko Teknologi Informasi / Sistem Informasi

Teknologi informasi adalah penggunaan komputer dan peralatan telekomunikasi untuk menyimpan (*store*), menerima (*retrieve*), mengirimkan (*transmit*) dan memanipulasi (*manipulate*) data. Sedangkan menurut SEI (2007), Sistem Informasi adalah kombinasi antara kegiatan teknologi informasi dengan aktivitas orang-orang yang mendukung manajemen operasional dan pengambilan keputusan.

Risiko teknologi informasi/sistem informasi (*IT/IS Risk)* adalah segala bentuk kejadian yang tidak pasti dalam aspek teknologi informasi maupun sistem informasi, yang dapat menghasilkan efek atau dampak bagi tujuan proyek, perusahaan atau organisasi.

2.2 Manajemen Risiko

Manajemen risiko adalah sebuah bidang ilmu yang membahas bagaimana sebuah perusahaan atau organisasi dapat menerapkan ukuran dalam melakukan pemetaan permasalahan dengan pendekatan manajemen secara komprehensif dan sistematis. Berdasarkan ISO 31000:2009, manajemen risiko adalah aktivitas yang terkoordinir untuk menjalankan dan mengawasi sebuah perusahaan atau organisasi dengan pendekatan risiko.

Institute of Risk Management (IRM) menjelaskan bahwa manajemen risiko adalah sebuah proses yang bertujuan untuk membantu organisasi atau perusahaan dalam memahami, mengevaluasi dan mengambil tindakan untuk risiko-risiko yang

muncul, dengan meningkatkan kemungkinan untuk berhasil dan mengurangi kemungkinan kegagalan.

H.M. Treasury menjelaskan bahwa manajemen risiko adalah sebuah proses yang meliputi identifikasi, penilaian dan menentukan risiko , pengambilan tindakan untuk melakukan mitigasi atau antisipasi serta pemantauan dan melakukan *review progress* dari setiap tahapan yang ada.

Business Continuity Institute menjelaskan bahwa manajemen risiko adalah sebuah budaya, proses dan struktur yang ditempatkan untuk mengelola kesempatan potensial secara efektif dan mencegah efek buruk yang dapat terjadi pada perusahaan atau organisasi.

Oleh karena itulah, dapat disimpulkan bahwa manajemen risiko adalah sebuah proses pengelolaan risiko pada sebuah perusahaan atau organisasi tertentu, yang memiliki tujuan untuk meminimalisasi risiko yang mungkin muncul.

2.2.1 Manajemen Risiko Teknologi Informasi/Sistem Informasi

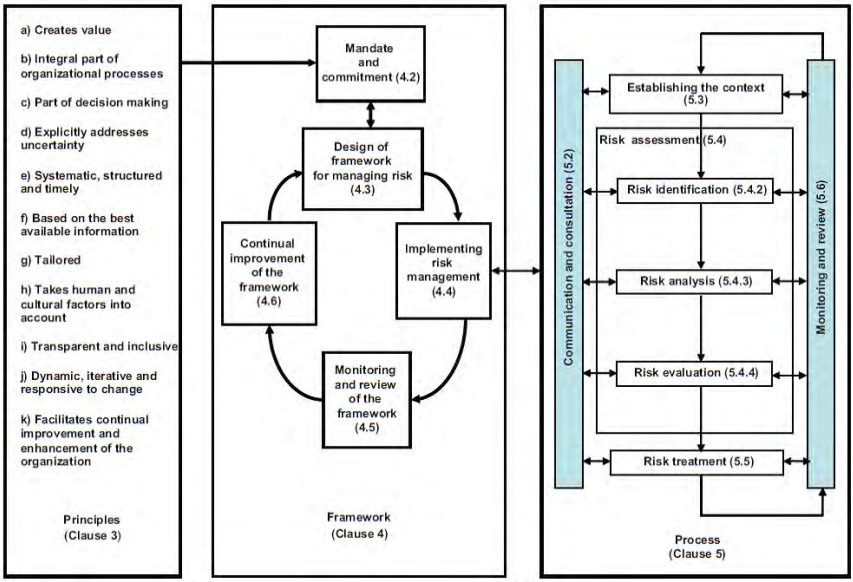
Teknologi dan Sistem Informasi hampir dapat dipastikan telah diimplementasikan pada setiap perusahaan untuk membantu proses bisnis operasional dan pengambilan keputusan perusahaan. Teknologi dan Sistem Informasi yang berkembang begitu pesat dapat mendatangkan kesempatan sekaligus ancaman bagi perusahaan itu sendiri. Hal ini dibuktikan dengan tingginya kebocoran informasi internal perusahaan dan serangan yang mengancam sistem keamanan komputer perusahaan. Berdasarkan hal-hal itulah perlu diimplementasi sebuah pengelolaan risiko dalam hal teknologi informasi.

Manajemen risiko teknologi informasi adalah pengelolaan risiko teknologi informasi /sistem informasi pada sebuah organisasi atau perusahaan tertentu yang memiliki tujuan untuk meminimalisasi risiko yang mungkin muncul dengan solusi yang berhubungan dengan aspek teknologi informasi/sistem informasi.

2.3 ISO 31000:2009

Menurut Vincent Gaspersz dalam bukunya All-in-One Bundle of ISO, *International Organization for Standardization* 31000 (ISO 31000) adalah sebuah pedoman untuk menerapkan sistem manajemen risiko, yang akan memberikan prinsip dan petunjuk secara umum mengenai manajemen risiko pada sebuah organisasi atau perusahaan umum.

Secara garis besar, pemaparan manajemen risiko dalam ISO 31000 memiliki tiga bagian, yaitu prinsip, kerangka kerja dan proses. Selain itu, terdapat proses penilaian yang akan menentukan bagaimana penanganan risiko tersebut, berdasarkan tingkat *likelihood* (L) atau kemungkinan, *impact* (I) atau dampak dan skor deteksi (D). Sehingga, dari hasil penilaian dan perhitungan yang ada akan menghasilkan nilai risiko (*Risk Score*) dan *Risk Priority Number* (RPN).



Gambar 2. 1 Hubungan antara Prinsip, Kerangka dan Proses Manajemen Risiko (ISO 31000, 2009)

2.3.1 Proses dan Tahapan Manajemen Risiko berdasarkan ISO 31000

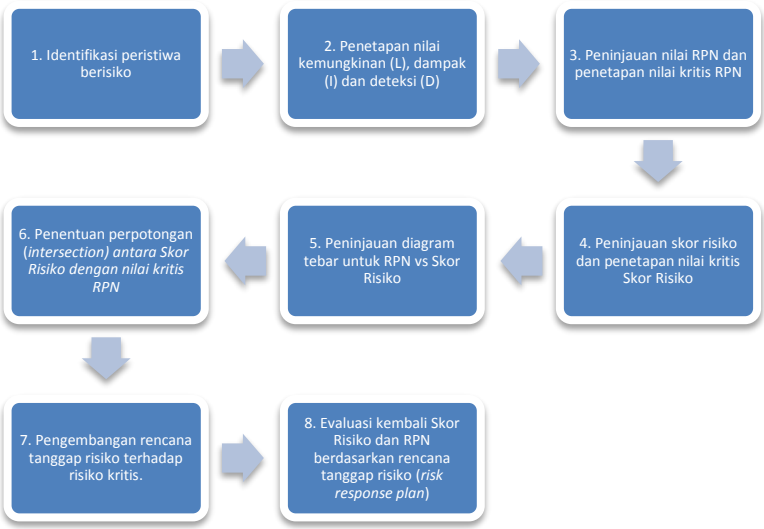
Proses manajemen risiko yang terdapat pada ISO 31000:2009 terdapat pada Klausa 5. Proses dan tahapan tersebut adalah sebagai berikut.

1 Umum
2 Komunikasi dan konsultasi
3 Menetapkan konteks
  3.1 Umum
  3.2 Menetapkan konteks eksternal
  3.3 Menetapkan konteks internal
  3.4 Menetapkan konteks dari proses manajemen risiko
  3.5 Mengembangkan kriteria risiko
4 Menilai risiko (*risk assessment*)
  4.1 Umum
  4.2 Identifikasi Risiko
  4.3 Analisis Risiko
  4.4 Evaluasi Risiko
5 Perlakuan Risiko (*risk treatment*)
  5.1 Umum
  5.2 Seleksi pilihan-pilihan perlakuan risiko
  5.3 Persiapan dan implementasi rencana-rencana perlakuan risiko
6 Pemantauan dan peninjauan ulang (*monitoring and review*)
7 Perekaman atau pencatatan proses manajemen risiko

Pada penelitian ini fase yang digunakan sesuai dengan ISO 31000 adalah fase penilaian risiko (identifikasi, analisis dan evaluasi risiko) serta fase perlakuan risiko (seleksi pilihan perlakuan risiko dan persiapan dan implementasi rencana perlakuan risiko). Fase inilah yang akan tercakup dalam kerangka kerja BCP yang sesuai dengan kebutuhan perusahaan studi kasus.

2.4 Metode FMEA (Failure Mode and Effect Analysis)

Menurut Vincent Gaspersz dalam bukunya All-in-One Bundle of ISO, analisis pengaruh dan mode kegagalan risiko (*risk FMEA*) adalah alat utama yang digunakan untuk melakukan penghitungan pada manajemen risiko. Dalam implementasinya, langkah-langkah dari alat penghitungan ini adalah sebagai berikut.



Gambar 2. 2 Langkah Implementasi Risk FMEA (Sumber: FMEA)

FMEA memiliki beberapa perangkat yang membantu perusahaan atau organisasi dalam menghasilkan penilaian risiko yang akurat, yaitu skor *likelihood, impact* dan *detection.* Ketiganya akan dibahas sebagai berikut.

2.4.1 Petunjuk Pemberian Skor Kemungkinan (Likelihood = L)

Likelihood adalah kemungkinan terjadinya sebuah risiko. Berikut ini dipaparkan mengenai skala dari skor *likelihood*, sekaligus dengan kemungkinan peristiwa yang dapat terjadi.

Tabel 2. 1 Skor Likelihood (Sumber: FMEA)

Skor Likelihood	Peluang atau Kemungkinan terjadi peristiwa
9 atau 10	Hampir pasti akan terjadi, peluang 90-100%
7 atau 8	Akan terjadi, peluang sekitar 70-80%
5 atau 6	Mungkin terjadi atau mungkin tidak terjadi, peluang 50%
3 atau 4	Sangat mungkin tidak akan terjadi, Peluang 30-40%
1 atau 2	Hampir pasti tidak akan terjadi, Peluang 10-20%

2.4.2 Petunjuk Pemberian Skor Dampak (Impact = I)

Impact berkaitan erat dengan dampak atau besar pengaruh risiko terhadap aspek-aspek tujuan proyek, seperti jadwal *(timeline)*, biaya (*cost*) dan teknikal (*technical / operational*).

Tabel 2. 2 Skor Dampak (Sumber: FMEA)

Skor Impact	Dampak yang akan terjadi (Aspek jadwal, biaya, teknis)
9 atau 10	• Jadwal: Berpengaruh besar terhadap *milestone* proyek, >20% dari *critical path.* • Biaya: Meningkatkan total biaya proyek lebih besar dari 20%. • Teknis: Berdampak pada produk akhir proyek, sehingga tidak dapat digunakan lagi.
7 atau 8	• Jadwal: Berpengaruh besar terhadap *milestone* proyek, 10%-20% dari *critical path.* • Biaya: Meningkatkan total biaya proyek 10%-20% • Teknis: Berdampak pada produk akhir proyek, sehigga tidak dapat digunakan oleh klien.
5 atau 6	• Jadwal: Berpengaruh sekitar 5%-10% dari *critical path.*

Skor Impact	Dampak yang akan terjadi (Aspek jadwal, biaya, teknis)
	• Biaya: Meningkatkan total biaya proyek 5%-10%. • Teknis: Berdampak pada produk akhir proyek, yang membutuhkan persetujuan klien, apakah mau menerima produk tersebut atau tidak.
3 atau 4	• Jadwal: Berpengaruh <5% dari *critical path.* • Biaya: Meningkatkan total biaya proyek <5%. • Teknis: Berdampak pada produk akhir proyek, yang cukup membutuhkan persetujuan internal perusahaan, apakah akan diserahkan kepada klien atau tidak.
1 atau 2	• Jadwal: Tidak berpengaruh pada *critical path.* • Biaya: tidak meningkatkan total biaya proyek. • Teknis: tidak berdampak pada produk akhir sebuah proyek.

2.4.3 Petunjuk Pemberian Skor Deteksi (Detection = D)

Detection adalah tingkat efektivitas metode atau kemampuan untuk mendeteksi terjadinya suatu risiko. Deteksi berkaitan dengan kemampuan dari teknik deteksi untuk mendeteksi peristiwa yang memiliki risiko secara tepat, sehingga perusahaan/organisasi dapat melakukan perencanaan dan melakukan tindakan terhadap risiko yang terdeteksi tersebut.

Tabel 2. 3 Skor Deteksi (Sumber: FMEA)

Skor Detection	Kemampuan Metode Deteksi terhadap risiko
9 atau 10	Tidak ada metode deteksi atau metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi

Skor Detection	Kemampuan Metode Deteksi terhadap risiko
7 atau 8	Metode deteksi tidak terbukti atau tidak andal, atau efektivitas metode deteksi tidak diketahui untuk mendeteksi tepat waktu
5 atau 6	Metode deteksi memiliki tingkat efektifitas yang rata-rata (medium)
3 atau 4	Metode deteksi memiliki tingkat efektifitas yang tinggi
1 atau 2	Metode deteksi sangat efektif dan hampir pasti risiko akan terdeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi.

2.4.4 Penentuan Level Risiko

Pada metode perhitungan FMEA, nilai RPN (*Risk Priority Number*) digunakan sebagai penentu level dari setiap risiko. Berikut ini adalah penentuan level risiko berdasarkan nilai RPN.

Tabel 2. 4 Penentuan Level Risiko

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

Skala RPN dari setiap risiko yang ada akan digunakan sebagai penentu level, di mana perusahaan dapat menilai risiko manakah yang bernilai paling tinggi. Perusahaan perlu melakukan antisipasi, mitigasi dan strategi terhadap risiko yang memiliki tingkatan paling tinggi, sehingga operasional bisnis perusahaan dapat tetap berjalan dengan optimal meskipun terjadi gangguan atau bencana.

2.5 Business Continuity Management Systems

Business Continuity Management Systems (BCMS) adalah bagian dari keseluruhan pengelolaan sistem yang mendirikan, mengimplementasikan, mengoperasikan, memantau, meninjau, mengelola dan meningkatkan keberlanjutan bisnis (ISO 22301:2012).

Dalam literatur lainnya, istilah ini juga dikenal dengan sebutan *Business Continuity Management* (BCM). BCM menyediakan ketersediaan proses-proses dan sumber daya yang dibutuhkan, untuk memastikan keberlanjutan dari pencapaian tujuan kritis perusahaan (HB 221:2004 *Business Continuity Management*).

Dalam penelitian ini, BCM erat kaitannya dengan BCP. Di mana, BCP menjadi salah satu bagian di dalam BCM. Namun pada penelitian ini, peneliti memilliki fokus terhadap penelitian BCP untuk perusahaan studi kasus yang telah ditetapkan.

2.6 Business Continuity Planning (BCP)

Business Coninuity Plan (BCP) adalah prosedur yang telah terdokumentasi sebagai petunjuk untuk menanggapi, memulihkan, melanjutkan proses setelah adanya interupsi atau gangguan serta mengaktifkan sistem kembali (*respond, recover, resume, restore*) pada gangguan operasional tingkat standar (yang telah ditetapkan sebelumnya) tersebut. (ISO 22301:2012)

Dipaparkan oleh *Purdue University United States*, *Business Conituity Plan* adalah bagaimana kelanjutan proses bisnis kritis pada sebuah perusahaan, ketika muncul bencana yang mengganggu kemampuan dalam memproses data. Hal yang dilakukan antara lain persiapan, pengujian hingga perawatan tindakan yang spesifik, untuk bisa memulihkan sistem kembali ke keadaan normal.

Federal Financial Institutions Examination Council (FFIEC) *Business Continuity Planning Handbook* memiliki definisi tentang *Business Continuity Plan* yaitu merupakan proses

perencanaan yang meliputi pemulihan, pengembalian keadaan sistem dan pemeliharaan seluruh unit bisnis, bukan hanya dari komponen teknologi. Kerangka pemulihan (*recovery framework*) harus mencakup rencana pemulihan jangka pendek dan jangka panjang.

Berdasarkan Peraturan Bank Indonesia PBI 9/15/PBI 2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, *Business Continuity Planning* adalah kebijakan dan prosedur yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah pengurangan risiko, penanganan dampak bencana/gangguan dan proses pemulihan, agar kegiatan operasional Bank dan pelayanan kepada nasabah tetap dapat berjalan.

2.7 Disaster Recovery Plan (DRP)

Disaster Recovery Plan (DRP) adalah kumpulan dari serangkaian prosedur, kebijakan dan proses yang berkaitan dengan persiapan untuk melakukan pemulihan yang berkelanjutan dari infrastruktur teknologi setelah bencana (alam dan manusia). Setiap perusahaan memiliki kebutuhan yang spesifik atas proses dan tujuan bisnis yang dilakukannya. Oleh karena itulah DRP dibuat di perusahaan, sesuai dengan kebutuhan masing-masing perusahaan (Caroline, 2008).

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

Penyusunan DRP memiliki langkah yang harus dijalankan seperti pemahaman tujuan bisnis, identifikasi kebutuhan spesifik, identifikasi sumber daya manusia yang bertanggung jawab dan melakukan identifikasi *Single Points of Failure* atau kegagalan dengan satu poin (Consulting Solution, 1999). Di mana, *single points of failure* merupakan sebuah bagian dari sistem yang ketika

mengalami kegagalan, akan menghentikan seluruh sistem atau tidak memiliki relokasi alternatif (Dooley, 2002).

2.7.1 Hubungan BCP dengan DRP

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

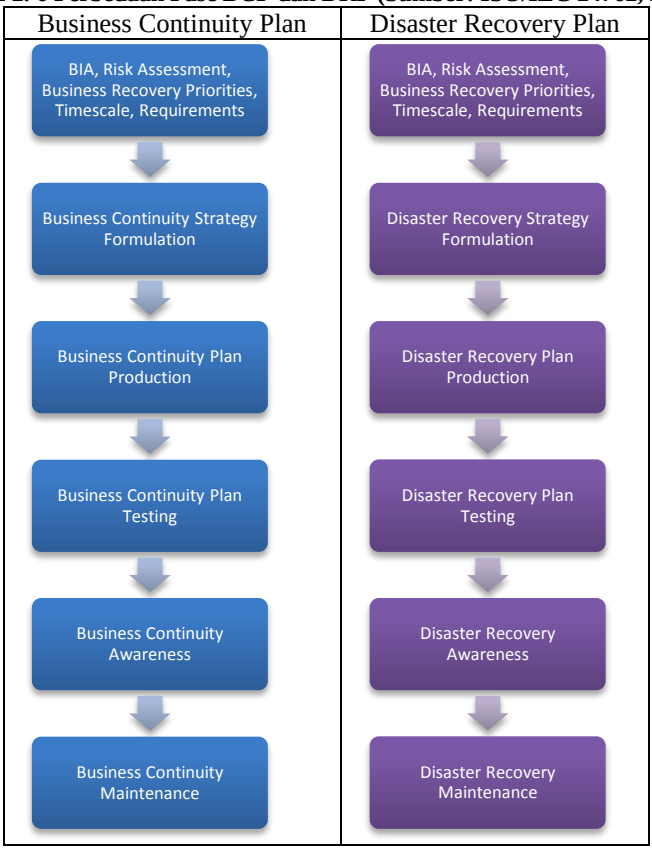
Tabel 2. 5 Perbedaan BCP dan DRP (Sumber: NIST, 2010)

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

Berdasarkan penjelasan dari NIST, disimpulkan bahwa DRP mendukung BCP dengan memulihkan sistem pendukung untuk proses bisnis atau tujuan paling kritis dalam sebuah fungsi pada lokasi pengganti (*alternate location*). Perencana BCP harus berkoordinasi dengan bagian sistem informasi, agar ekspektasi BCP sesuai dengan kemampuan daya dukung sistem informasi pada perusahaan.

ISO/IEC 24762:2008 tentang petunjuk untuk layanan pemulihan bencana teknologi informasi dan komunikasi, mengemukakan pendekatan untuk melakukan pemulihan ketika terjadi bencana atau gangguan yang mengganggu sistem pada sebuah perusahaan atau organisasi. Pendekatan ini dibuat untuk mengemukakan teori mengenai *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP).

Tabel 2. 6 Perbedaan Fase BCP dan DRP (Sumber: ISO/IEC 24762, 2012)



Pada dasarnya secara konseptual kedua perencanaan tersebut memiliki fase yang serupa, berdasarkan ISO/IEC 24762 tersebut. Namun secara teknis, hal ini akan menjadi sangat berbeda. Di mana, DRP hanya berfokus pada teknologi dan sistem informasi sedangkan BCP memiliki konsentrasi pada proses bisnis yang paling kritis pada perusahaan atau organisasi di setiap fungsional bisnis yang ada.

Penjelasan dari setiap fase adalah sebagai berikut.

1. *BIA, Risk Assessment, Recovery Priorities, Timescale, Requirements*

   Merupakan fase penggalian data dampak, prioritas proses bisnis, perkiraan waktu untuk pemulihan dan kebutuhan minimal yang dibutuhkan.
2. *Strategy Formulation*

   Melakukan formulasi dalam bentuk pertemuan dengan pihak yang bersangkutan mengenai prioritas, jangka waktu, kebutuhan minimal dan rekomendasi.
3. *Plan Production*

   Perencanaan, organisasi, pertanggungjawaban, logistik, daftar tindakan secara terperinci.
4. *Plan Testing*

   Strategi serta perencanaan pengujian yang disertakan bukti.
5. *Awareness*

   Membangun kesadaran dari semua karyawan perihal implementasi BCP/DRP.
6. *Maintenance*

   Aktivitas perawatan atau peninjauan BCP/DRP selama implementasi berlangsung.

2.8 Kerangka Kerja BCMS ISO 22301:2012

ISO (*the International Organization for Standardization*) adalah sebuah badan yang mengatur standar nasional di seluruh dunia. ISO 22301:2012 merupakan sebuah standar internasional yang dibuat untuk mengatur dan mengelola sistem pengelolaan keberlangsungan bisnis atau *Business Continuity Management Systems* (BCMS) yang efektif. BCMS adalah bagian dari keseluruhan pengelolaan sistem yang mendirikan, mengimplementasikan, mengoperasikan, memantau, meninjau, mengelola dan meningkatkan keberlanjutan bisnis (ISO 22301:2012).

Penerapan ISO 22301:2012 dinilai cukup generik, di mana dalam hal ini dapat diterapkan pada semua organisasi, dan tingkat

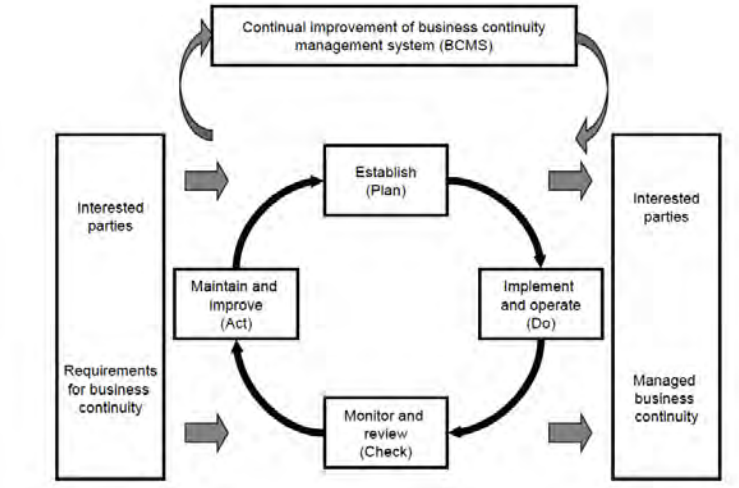
penerapannya tergantung dan dapat disesuaikan dengan lingkungan operasi serta kompleksitas permasalahan di perusahaan.

ISO 22301:2012 diluncurkan untuk melengkapi standar dari *Business Continuity Managements* yang sebelumnya yaitu, BS 25999-1:2006 yang dikeluarkan oleh British Standards (BS) pada tahun 2006 dan BS 25999-2:2007 yang dikeluarkan oleh institusi yang sama pada tahun 2007.

Standar ini digunakan dalam penelitian ini karena pada standar internasional ini juga tercakup mengenai proses BCP (*Business Continuity Plan*) di dalamnya. Di mana, BCP adalah prosedur yang terdokumentasi sebagai petunjuk untuk menanggapi, memulihkan, melanjutkan proses setelah adanya interupsi atau gangguan serta mengaktifkan sistem kembali (*respond, recover, resume, restore*) pada gangguan operasional tingkat standar (yang telah ditetapkan sebelumnya) tersebut (ISO 22301:2012).

Alasan penggunaan kerangka BCP pada standar ini adalah, peneliti meyakini bahwa standar ini merupakan standar yang komperhensif dan diakui secara internasional. Selain itu, ISO (*International Standard Organization*) menjadi sumber dari penggunaan standar di seluruh dunia, karena standar yang dibuat selu berkembang dan dinamis sesuai dengan kebutuhan dan kondisi pasar.

Standar internasional ini menerapkan model PDCA (*Plan-Do-Check-Act*) untuk merencanakan, mendirikan, mengimplementasikan, mengoperasikan, memantau, meninjau, mengelola dan meningkatkan efektivitas secara terus-menerus dalam BCMS organisasi atau perusahaan. Berikut ini adalah model PDCA yang diaplikasikan pada proses BCMS.



Gambar 2. 3Model PDCA (Sumber: ISO 22301, 2012)

Penjelasan dari model tersebut adalah sebagai berikut.

1. *Plan (Establish)*
   Pembuatan kebijakan keberlanjutan bisnis (*business continuity*), objektif, target, kontrol, proses dan prosedur yang relevan untuk meningkatkan keberlanjutan bisnis, dalam rangka penyelarasan dengan kebijakan dan tujuan organisasi atau perusahaan.
2. *Do (Implement and Operate)*
   Mengimplementasi dan mengoperasikan kebijakan keberlanjutan bisnis (*business continuity*), kontrol, proses dan prosedur.
3. *Check (Monitor and Review)*
   Memantau dan meninjau performa yang bertentangan dengan kebijakan dan tujuan keberlanjutan bisnis (*business continuity*), melaporkan hasil ke manajemen untuk peninjauan dan menetapkan serta mengesahkan tindakan untuk memperbaiki dan meningkatkan performa.

4. *Act (Maintain and Improve)*
   Pemeliharaan dan peningkatan BCMS dengan mengambil perbaikan tindakan, berdasarkan hasil dari peninjauan pengelolaan. Tindakan ini juga melingkupi penilaian ulang ruang lingkup BCMS dan kebijakan serta tujuan dari keberlanjutan bisnis (*business continuity*).

Pada model PDCA tersebut, terdapat beberapa masukkan (input) sebelum model PDCA tersebut dijalankan, yaitu adalah pihak yang bersangkutan (*interested parties*) dan kebutuhan untuk keberlanjutan bisnis (*requirement for business continuity*). Kedua hal tersebut menjadi input yang dibutuhkan untuk menjalankan proses yang ada pada model tersebut, yaitu perencanaan-pengerjaan-pemeriksaan-tindakan (*plan-do-check-act*).

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

ISO 22301:2012 terdiri dari 10 klausa yang menjelaskan hal-hal yang terkait dengan BCMS serta penyusunan BCP untuk sebuah organisasi atau perusahhaan. Klausa-klausa tersebut merepresentasikan setiap fase pada model PDCA yang telah dibahas sebelumnya. Namun untuk klausa 1, 2 dan 3 tidak terkait dengan fase-fase pada model tersebut. Di mana, klausa 1 menjelaskan tentang ruang lingkup dari ISO 22301:2012, klausa 2 menjelaskan tentang referensi yang digunakan dalam standar tersebut, serta klausa 3 menjelaskan istilah dan definisi yang digunakan pada standar internasional tersebut.

Klausa yang terkait langsung dengan fase model PDCA adalah klausa 4, 5, 6, 7 dan 8. Berikut ini adalah penjelasan dari

korelasi antara fase pada model PDCA dengan masing-masing klausa yang terkait langsung dengan model tersebut.

Tabel 2. 7 Pemetaan Fase dengan Klausa (Sumber: ISO 22301,2012)

FASE	KLAUSA	KETERANGAN KLAUSA
PLAN	4	Klausa ini mengenalkan kebutuhan yang diperlukan dalam membuat konteks BCMS yang akan digunakan sesuai dengan kebutuhan organisasi. Klausa ini juga menjelaskan mengenai kebutuhan pihak ketiga dan ruang lingkup dari BCMS (inisiasi).
	5	Klausa 5 menjelaskan kebutuhan spesifik mengenai peran dari pihak manajemen tertinggi di organisasi atau perusahaan dalam BCMS, serta kebijakan yang dibuat oleh pimpinan untuk mengatur BCMS (Sumber Daya Manusia)
	6	Klausa 6 mendeskripsikan kebutuhan untuk membuat tujuan strategis dan prinsip BCMS.
	7	Klausa 7 berisi tentang bagian-bagian yang mendukung operasional BCMS, seperti pembuatan kompetensi dan komunikasi dengan pihak-pihak terkait serta pendokumentasian terkait seluruh informasi dalam BCMS.
DO	8	Klausa 8 menjelaskan kebutuhan atau persyaratan keberlanjutan bisnis (*business continuity*), menentukan bagaimana pertanggungjawaban atas apa yang terjadi (sumber daya), serta mengembangkan prosedur-prosedur yang digunakan untuk mengelola kerusakan atau gangguan yang terjadi pada perusahaan atau organisasi. Klausa ini juga menjelaskan beberapa proses penting yang terkait dengan penyusunan BCMS. 1. Perencanaan dan kontrol operasional. 2. BIA (*Business Impact Analysis*) dan

FASE	KLAUSA	KETERANGAN KLAUSA
		Penilaian risiko (*Risk Assessment*). 3. Strategi keberlanjutan bisnis. 4. Penyusunan dan implementasi prosedur keberlanjutan bisnis. 5. Pelatihan dan pengujian BCMS.
CHECK	9	Klausa 9 menjelaskan tentang kebutuhan yang digunakan untuk mengukur performa pengelolaan bisnis keberlanjutan (*Business Continuity Management*), kesesuaian BCMS dengan ISO 22301:2012 (standar yang digunakan), ekspektasi atau keinginan pihak manajemen serta mengumpulkan *feedback* dari manajemen terkait ekspektasi yang ditetapkan.
ACT	10	Klausa 10 menjelaskan tentang tindakan yang dilakukan atas ketidaksesuaian BCMS dengan hal-hal yang telah ditetapkan. Tindakan yang ada dapat berupa perbaikan, ataupun peningkatan yang berkelanjutan (*continual improvement*).

Berdasarkan korelasi antara fase pada model PDCA dengan klausa dalam ISO 22301:2012, maka selanjutnya akan dijelaskan mengenai masing-masing proses yang terdapat dalam klausa-klausa tersebut.

2.8.1 Fase Perencanaan (Plan)

Fase perencanaan pada model PDCA, terdapat pada klausa 4,5,6 dan 7 di ISO 22301:2012. Berikut ini adalah gambaran umum dari masing-masing isi klausa.

Klausa 4 Konteks Organisasi/Perusahaan

4.1 Pemahaman konteks organisasi

Pada bagian ini, organisasi harus memahami hal-hal yang mempengaruhi organisasinya baik dari segi internal maupun eksternal. Di mana, hal-hal tersebut berkaitan dengan tujuan

organisasi dan faktor yang mempengaruhi pencapaian BCMS di organisasi tersebut.

Organisasi perlu mengidentifikasi dan mendokumentasikan hal-hal berikut.

1. Aktivitas, fungsi, layanan, produk, mitra kerja, rantai pasok, hubungan dengan pihak yang bersangkutan serta potensial dampak yang terjadi ketika muncul gangguan pada organisasi.
2. Keterkaitan antara kebijakan keberlanjutan bisnis dengan tujuan maupun kebijakan lain di organisasi
3. Potensial risiko di organisasi.

4.2 Pemahaman kebutuhan dan ekspektasi pihak yang berkepentingan

4.2.1 Penjelasan umum

Dalam penyusunan BCMS, organisasi diharapkan dapat menentukan pihak-pihak yang terkait dengan organisasi beserta kebutuhan-kebutuhan atau persyaratan yang dibutuhkan oleh pihak-pihak tersebut.

4.2.2 Hukum dan Regulasi

Organisasi diharapkan dapat menyusun, mengimplementasi dan mengelola prosedur yang sesuai dengan hukum dan regulasi yang berlaku untuk aktivitas operasional, produk dan layanan pada organisasi tersebut. Selain itu, setiap pelaku BCMS atau organisasi yang bersangkutan dapat memastikan bahwa BCMS yang dibuat, diimplementasikan dan dipelihara dapat sesuai dengan hukum, regulasi dan persyaratan lainnya yang berlaku di organisasi maupun eksternal organisasi.

Semua informasi mengenai hukum harus didokumentasikan oleh organisasi sesuai dengan waktu maupun kejadiannya (kronologis).

4.3 Penetapan ruang lingkup BCMS

4.3.1 Penjelasan umum

Organisasi diharapkan dapat menentukan ruanglingkup BCMS sesuai dengan hal-hal yang berpengaruh di

organisasi baik secara internal dan eksternal, serta kebutuhan atau persyaratan yang dibutuhkan oleh pihak yang bersangkutan (ref 4.1 dan 4.2)

4.3.2 Ruang lingkup BCMS

Pada bagian ini, organisasi diharapkan dapat:

1. Membentuk tim yang merupakan bagian dari organisasi yang akan berkecimpung di dalam BCMS.
2. Menyusun kebutuhan BCMS berdasarkan hal-hal penting terkait organisasi seperti, tujuan organisasi, obligasi internal dan eksternl, pihak yang bersangkutan serta hukum dan regulasi yang berlaku.
3. Mengidentifikasi produk serta layanan di organisasi yang masuk ke dalam ruang lingkup BCMS.
4. Mengidentifikasi pihak yang bersangkutan seperti pelanggan, investor, pemegang saham, masyarakat umum dan lainnya.
5. Menjelaskan ruang lingkup BCMS agar sesuai dengan ukuran dan kompleksitas organisasi.

4.4 *Business Continuity Management Systems*

Organisasi diharapkan dapat menyusun, mengimplementasai, memelihara dan melakukan peningkatan keberlanjutan pada BCMS dan seluruh proses yang terkait, agar sesuai dengan standar internasional ini.

Klausa 5 Kepemimpinan (Leadership)

5.1 Komitmen dan Kepemimpinan

Seluruh pihak yang ada pada manajemen tertinggi di perusahaan harus mendukung terwujudnya BCMS di organisasi yang bersangkutan.

5.2 Komitmen Manajemen

Pihak manajemen dapat menunjukkan kepemimpinan dan komitmennya melalui beberapa hal:

- Memastikan kebijakan dan tujuan BCMS telah sesuai dengan arahan strategis organisasi.

- Memastikan adanya integrasi antara kebutuhan BCMS dengan proses bisnis organisasi.
- Memastikan ketersediaan sumber daya BCMS.
- Mengkomunikasikan pentingnya efektivitas BCMS dan kesesuaiannya dengan kebutuhan BCMS.
- Memastikan BCMS dapat mencapai manfaat yang diinginkan.
- Mengarahkan dan mendukung pihak-pihak untuk berkontribusi pada efektivitas BCMS.
- Mempromosikan peningkatan keberlanjutan
- Mendukung peran manajemen yang berkaitan, untuk menunjukkan kepemimpinan dan komitmen pada area tanggung jawabnya masing-masing.

Pihak manajemen harus menyediakan bukti dari komitmen untuk menyusun, mengimplementasi, operasi, pemantauan, peninjauan, pemeliharaan dan peningkatan BCMS melalui beberapa hal:

- Penyusunan kebijakan bisnis keberlanjutan
- Memastikan tujuan dan perencanaan BCMS dapat tersusun dengan baik.
- Menyusun peran, tanggung jawab dan kompetensi untuk penegelolaan keberlanjutan bisnis.
- Menunjuk orang-orang untuk bertanggung jawab pada BCMS dengan kewenangan yang sesuai dan kompetensi yang dapat dipertanggungjawabkan untuk implementasi dan pemeliharaan BCMS.

5.3 Kebijakan

Kebijakan keberlanjutan bisnis yang disusun oleh pihak manajemen harus sesuai dengan hal-hal berikut.

- Sesuai dengan tujuan organisasi
- Menyediakan kerangka kerja untuk mengatur tujuan keberlanjutan bisnis.
- Komitmen untuk memenuhi kebutuhan yang dapat digunakan.

- Komitmen untuk melakukan peningkatan yang berkelanjutan pada BCMS.

Kebijakan BCMS harus memenuhi beberapa hal sebagai berikut.

- Dapat tersedia sebagai informasi yang terdokumentasi.
- Dapat mengkomunikasikan pesan kepada organisasi.
- Dapat tersedia untuk pihak-pihak yang bersangkutan.
- Dapat ditinjau ulang untuk kelanjutan kesesuaian dengan organisasi.

5.4 Peran, tanggung jawab dan kewenangan organisasi

Pihak manajemen harus memastikan tanggung jawab dan kewenangan peran yang berkaitan yang ditugaskan oleh organisasi.

Pihak manajemen harus menetapkan tanggung jawab dan kewenangan untuk:

- Memastikan bahwa sistem manajemen sesuai dengan kebutuhan standar internasional.
- Melaporkan performa BCMS kepada pihak manajemen tertinggi.

Klausa 6 Perencanaan (Plan)

6.1 Tindakan penunjukkan risiko dan kesempatan

Ketika merencanakan BCMS, organisasi memastikan hal-hal pada klausa 4.1 dan kebutuan yang terdapat pada 4.2, dan penetapan risiko dan kesempatan yang diperlukan untuk ditujukan untuk:

- Memastikan sistem manajemen dapat mencapai manfaat yang diinginkan.
- Mencegah atau mengurangi efek yang tidak diinginkan.
- Mencapai peningkatan berkelanjutan.

Organisasi harus merencanakan:

- Tindakan untuk penunjukkan risiko dan kesempatan.
- Evaluasi efektivitas tindakan tersebut.

6.2 Tujuan dan perencanaan keberlanjutan bisnis

pihak manajemen harus memastikan bahwa tujuan keberlanjutan bisnis disusun dan dikomunikasukan untuk fungsi yang relevan dan tingkatan dalam organisasi.

Tujuan keberlanjutan bisnis adalah:

a. Konsisten dengan kebijakan keberlanjutan bisnis.
b. Memperhitungkan tingkat minimum dari produk dan jasa yang sesuai dengan tujuan organisasi.
c. Dapat diukur.
d. Memperhitungkan kebutuhan yang dapat diaplikasikan.
e. Dapat dipantau dan diperbaharui sesuai dengan kebutuhan.

Organisasi perlu menetapkan beberapa hal, agar tujuan dari keberlanjutan bisnis dapat tercapai. Berikut ini adalah hal-hal yang perlu diperhatikan.

- Siapa yang bertanggung jawab
- Apa yang akan dilakukan
- Sumber daya apa saja yang dibutuhkan
- Kapan hal tersebut dapat selesai
- Bagaimana hasil dari evaluasi yang dilakukan.

Klausa 7 Pendukung (Support)

7.1 Sumber daya

Organisasi perlu menetapkan dan menyediakan sumber daya yang dibutuhkan untuk menyusun, mengimplementasi, memelihara dan melakukan peningkatan yang berkelanjutan pada BCMS.

7.2 Kompetensi

Organisasi harus dapat :

a. Menentukan kompetensi orang-orang yang bekerja di bawah pengawasan, yang mempengaruhi performa.
b. Memastikan orang-orang ini memiliki pendidikan, pelatihan dan pengalaman yang kompeten di bidangnya.

c. Pengambilan tindakan untuk mendapatkkan kompetensi yang dibutuhkan dan evaluasi efektivitas dari tindakan yang diambil.
d. Pendokumentasian informasi sebagai bukti tingkat kompetensi.

7.3 Kesadaran

Ada beberapa hal yang perlu disadari oleh orang-orang yang bekerja di bawah pengawasan organisasi, yaitu:

a. Kebijakan keberlanjutan bisnis.
b. Kontribusi yang diberikan untuk mengefektifkan BCMS, termasuk dari keuntungan peningkatan performa pengelolaan keberlanjutan bisnis.
c. Implikasi atau dampak dari ketidaksesuaian dengan kebutuhan BCMS.
d. Peran dari masing-masing individu ketika terjadi gangguan.

7.4 Komunikasi

Organisasi harus menetapkan kebutuhan berkomunikasi internal dan eksternal yang relevan dengan BCMS, yaitu:

a. Pada bagian apa hal tersebut akan dikomunikasikan
b. Kapan akan berkomunikasi
c. Dengan siapa hal tersebut dikomunikasikan.

Organisasi perlu menyusun, mengimplementasi dan memelihara prosedur dengan tujuan:

- Komunikasi internal di antara pihak yang berkaitan dan karyawan di organisasi.
- Komunikasi eksternal dengan pelanggan, mitra kerja, komunitas lokal dan pihak terkait lainnya, termasuk media.
- Menerima, mendokumentasikan dan merespon komunikasi dari pihak lainnya.

- Menyesuaikan dan mengintegrasikan sistem penasihat ancaman nasional atau regional, atau setara dengan perencanaan dan operasional.
- Memastikan ketersediaan komunikasi selama terjadinya gangguan.
- Memfasilitasi komunikasi terstruktur dengan kewenangan yang sesuai dan memastikan kemampuan bertukar informasi di organisasi
- Mengoperasikan dan menguji kemampuan komunikasi selama gangguan.

7.5 Pendokumentasian informasi

7.5.1 Penjelasan umum

BCMS pada organisasi memerlukan:

a. Pendokumentasian informasi yang dibutuhkan oleh standar internasional.
b. Pendokumentasian informasi yang ditetapkan oleh organisasi untuk efektivitas BCMS.

7.5.2 Pembuatan dan pembaharuan

Dalam proses pembuatan dan pembaharuan pendokumentasian informasi, organisasi perlu memastikan:

a. Identifikasi dan deskripsi
b. Format, media, peninjauan serta persetujuan kesesuai.

7.5.3 Kontrol pendokumentasian informasi

Pendokumentasian informasi yang dibutuhkan oleh BCMS dan standar internasional ini dibutuhkan untuk mengontrol:

a. Ketersediaan dan kesesuaian penggunaan, di mana dan kapan hal tersebut dibutuhkan.
b. Kesesuaian proteksi.

2.8.2 Fase Pengerjaan (Do)

Fase pengerjaan pada model PDCA terdapat di klausa 8 pada ISO 22301:2012. Berikut ini adalah penjelasan dari klausa 8.

Klausa 8 Operasional (Operation)

8.1 Perencanaan dan pengawasan operasional

Organisasi harus merencanakan, mengimplementasi dan mengawasi proses agar sesuai dengan kebutuhan, serta untuk memenuhi perencanaan yang terdapat pada klausa 6.1. Hal tersebut dapat terwujud dengan cara berikut.

a. Menyusun kriteria untuk proses
b. Implementasi pengawasan proses berdasarkan kriteria
c. Menjaga pendokumentasian informasi untuk tetap melaksanakan setiap rencana yang telah dibuat.

Organisasi perlu mengawasi perubahan terhadap rencana yang telah dibuat, konsekuensi terhadap perubahan tersebut, serta tindakan untuk melakukan mitigasi terhadap pengaruh atau efek yang merugikan.

Organisasi harus memastikan bahwa proses yang berada di luar yang telah ditetapkan, tetap diawasi oleh organisasi.

8.2 *Business Impact Analysis (BIA)* dan *Risk Assessment*

8.2.1 Penjelasan umum

Organisasi perlu menyusun, mengimplementasi dan memelihara proses formal dan proses yang terdokumentasi untuk analisis dampak bisnis serta penilaian risiko yang:

a. Menyusun konteks dari penilaian, pendefinisian kriteria serta evaluasi dampak yang potensial saat terjadinya gangguan.
b. Memperhitungkan dasar hukum dan kebutuhan lainnya dari organisasi.
c. Mencantumkan analisis yang sistematik, prioritisasi perlakuan risiko serta biaya yang terkait di dalamnya.

d. Pendefinisian hasil yang diinginkan dari analisis dampak bisnis dan penilaian risiko
e. Menetapkan kebutuhan agar tetap mendapatkan informasi terbaru dan informasi yang bersifat rahasia organisasi.

8.2.2 *Business Impact Analysis (BIA)*

Organisasi perlu menyusun, mengimplementasi dan memelihara proses evaluasi yang formal dan terdokumentasi untuk menentukan prioritas pemulihan dan keberlanjutan, tujuan serta target. Pada proses pembuatan BIA, juga terdapat proses penilaian dampak dari gangguan yang terjadi pada aktivitas atau proses bisnis di organisasi. BIA terdiri dari beberapa hal berikut ini.

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

8.2.3 *Risk Assessment*

Organisasi perlu menyusun, mengimplementasi dan memelihara dokumentasi proses penilaian risiko yang teridentifikasi secara sistematis, analisis dan evaluasi risiko terhadap gangguan yang terjadi pada organisasi.

Organisasi memerlukan beberapa hal sebagai berikut.

a. Identifikasi risiko yang mengganggu proses dan aktivitas bisnis yang paling kritis (prioritas utama),

sistem, informasi, orang, aset, mitra kerja dan sumber daya lainnya yang mendukung.

b. Melakukan analisis risiko secara sistematis.
c. Melakukan evaluasi terhadap gangguan yang berhubungan dengan perlakuan risiko
d. Mengidentifikasi perlakuan risiko yang sesuai dengan tujuan keberlanjutan bisnis.

8.3 Strategi keberlanjutan bisnis

8.3.1 Penetapan dan Pemilihan

Penentuan dan pemilihan strategi berdasarkan hasil dari BIA dan penilaian risiko. Organisasi perlu menentukan strategi keberlanjutan bisnis yang sesuai dengan:

a. Proteksi aktivitas prioritas.
b. Stabilisasi, berkelanjutan, resume dan pemulihan aktivitas utama, ketergantungan serta sumber daya pendukung.
c. Mitigasi, tanggapan dan pengelolaan dampak.

Penentuan strategi keberlanjutan bisnis didasari pada persetujuan prioritisasi waktu untuk kelanjutan aktivitas. Organisasi perlu melakukan evaluasi terhadap kapabilitas keberlanjutan bisnis dari pemasok (s*uppliers*).

8.3.2 Penentuan kebutuhan sumber daya

Organisasi perlu menentukan kebutuhan sumber daya untuk implementasi strategis yang telah dipilih. Berikut ini adalah beberapa sumber daya yang dibutuhkan dalam penyusunan strategi keberlanjutan bisnis.

- Sumber daya manusia
- Data dan informasi
- Bangunan, lingkungan bekerja dan peralatan.
- Fasilitas, perlengkapan dan kebutuhan sehari-hari.
- Sistem teknologi informasi dan komunikasi.
- Transportasi
- Keuangan

- Mitra kerja dan pemasok

8.3.3 Proteksi dan mitigasi

Untuk mengidentifikasi perlaukan risiko yang perlu dilakukan, organisasi harus mempertimbangkan ukuran-ukuran terhadap beberapa hal berikut ini.

a. Pengurangan kemungkinan (*likelihood*) dari gangguan yang terjadi.
b. Pengurangan lama (periode) gangguan
c. Pengurangan dampak yang terjadi pada proses bisnis kritis di organisasi.

Organisasi perlu melakukan pemilihan perlakuan risiko yang sesuai dengan risiko yang terjadi di organisasi.

8.4 Pembuatan dan implementasi prosedur keberlanjutan bisnis

8.4.1 Penjelasan umum

Pada bagian ini organisasi perlu menyusun, mengimplementasi dan memelihara prosedur keberlanjutan bisnis untuk mengelola gangguan dan melanjutkan aktivitas yang ada berdasarkan tujuan pemulihan yang terdapat pada BIA. Di mana prosedur yang ada harus memenuhi persyaratan berikut.

a. Membuat protokol komunikasi internal dan eksternal.
b. Spesifik dalam menentukan langkah cepat yang harus diambil ketika terjadi gangguan.
c. Fleksibel dalam menanggapi ancaman yang tidak diantisipasi sebelumnya dan kondisi internal dan eksternal yang berubah-ubah.
d. Fokus pada dampak yang dapat berpotensi mengganggu operasional bisnis organisasi.
e. Dapat dikembangkan berdasarkan analisis yang saling berkaitan.
f. Efektif dalam meminimalkan konsekuensi melalui implementasi yang sesuai dengan strategi mitigasi.

8.4.2 Struktur respon pada peristiwa

Pada bagian ini organisasi perlu menyusun, mendokumentasi dan mengimplementasi prosedur dan struktur manajemen untuk menanggapi gangguan.

Struktur tanggapan harus memenuhi beberapa hal berikut ini.

a. Identifikasi dampak yang mempertanggungjawabkan respon formal.
b. Melakukan penilaian terhadap kondisi sekitar untuk melihat potensi gangguan atau dampak yang terjadi.
c. Mengaktivasi tanggapan keberlanjutan bisnis yang sesuai.
d. Memiliki proses dan prosedur untuk aktivasi, operasi, koordinasi dan komunikasi terhadap tanggapan selama masa gangguan.
e. Memilliki sumber daya yang tersedia untuk mendukung proses dan prosedur dalam pengelolaan gangguan untuk mengurangi dampak gangguan.
f. Berkomunikasi dengan pihak yang bersangkutan dan pihak yang berwenang.

8.4.3 Peringatan dan Komunikasi

Pada bagian ini organisasi perlu menyusun, mengimplementasi dan memelihara prosedur untuk:

a. Mendeteksi gangguan.
b. Pemantauan peristiwa
c. Komunikasi internal pada organisasi, menerima, mendokumentasikan dan menanggapi komunikasi dari pihak yang bersangkutan.
d. Menerima, mendokumentasi dan menanggapi nasional atau regional sistem penasihat risiko.
e. Menjamin ketersediaan komunikasi selama gangguan.
f. Memfasilitasi komunikasi yang terstruktur dengan responden darurat.

g. Melakukan pencatatan informasi penting mengenai gangguan, tindakan yang diambil oleh organisasi, serta keputusan yang dibuat. Berikut ini merupakan hal-hal yang perlu dipertimbangkan dan diimplementasikan lebih lanjut, yaitu:
   - Menyiagakan pihak terkait yang berpotensi terkena dampak saat terjadi gangguan.
   - Menjamin interoperabilitas atau kemampuan berkomunikasi terhadap tanggapan beragam yang muncul dari organisasi maupun personal.
   - Melakukan kegiatan operasional pada fasilitas komunikasi.

Untuk memastikan kelancaran dalam implementasinya, organisasi perlu mengadakan pelatihan untuk prosedur komunikasi dan peringatan.

8.4.4 *Business Continuity Plans*

Organisasi diharapkan dapat menyusun dokumentasi untuk prosedur dalam menanggapi gangguan dan tindakan untuk pemulihan aktivitas terhadap gangguan.

Perencanaan keberlanjutan bisnis berisi tentang:

a. Mendefinisikan peran dan tanggung jawab untuk pihak-pihak serta tim yang berwenang terhadap gangguan.
b. Proses untuk mengaktivasi tanggapan.
c. Penjelasan detail mengenai konsekuensi yang harus dilakukan secara cepat ketika terjadi gangguan, untuk:
   - Kesejahterhaan individu.
   - Pilihan secara strategi, taktikal dan operasional untuk menanggapi gangguan.
   - Pencegahan kerugian atau ketidaktersediaan aktivitas prioritas.

d. Penjelasan detail mengenai kejadian yang terjadi pada organisasi, mengenai komunikasi organisasi dengan karyawan, mitra kerja, pihak yang bersangkutan dan kontak darurat.
e. Bagaimana organisasi tersebut akan berlanjut atau bagaimana memulihkan aktivitas yang menjadi prioritas utama dari waktu yang telah ditentukan.
f. Penjelasan detail mengenai tanggapan media organisasi terhadap gangguan, melalui:
    - Strategi komunikasi.
    - Antarmuka media yang lebih disukai.
    - Petunjuk atau *template* untuk menyusun pernyataan-pernyataan untuk media.
    - Pembicara yang bersangkutan.

g. Proses ketika gangguan itu berakhir.
    - Setiap perencanaan yang ada perlu menjelaskan beberapa hal sebagai berikut.
    - Tujuan dan ruang lingkup.
    - Nilai objektif
    - Kriteria dan prosedur
    - Implementasi prosedur
    - Peran, tanggung jawab dan kewenangan
    - Kebutuhan komunikasi dan prosedur
    - Ketergantungan internal dan eksternal serta interaksi di dalamnya.
    - Kebutuhan sumber daya
    - Alur informasi dan proses pendokumentasian

8.4.5 Pemulihan

Organisasi perlu mendokumentasikan prosedur untuk memulihkan pengembalian aktivitas bisnis dari untuk mendukung kebutuhan bisnis normal setelah terjadinya gangguan.

8.5 Pelatihan dan pengujian

Organisasi perlu melakukan pelatihan dan pengujian terhadap prosedur keberlanjutan bisnis untuk memastikan bahwa prosedur tersebut konsisten dengan tujuan keberlanjutan bisnis.

Organisasi perlu menjalankan pelatihan dan pengujian yang memenuhi beberapa hal berikut.

a. Pelatihan dan pengujian yang konsisten dengan ruang lingkup dan tujuan dari BCMS.
b. Pelatihan dan pengujian berdasarkan skenario yang sesuai dengan perencanaan.
c.
d. Meminimalisasi risiko dari setiap gangguan operasional.
e. Menyusun laporan pasca pelatihan yang berisi tentang hasil, rekomendasi serta tindakan untuk melakukan perbaikan.
f. Pelatihan dan pengujian ditinjau dari konteks peningkatan yang berkelanjutan
g.

2.8.3 Fase Pemeriksaan (Check)

Fase pemeriksaan pada model PDCA terdapat pada klausa 9. Berikut ini adalah penjelasan dari klausa 9.

Klausa 9 Evaluasi Perfoma (Performance Evaluation)

9.1 Pemantauan, pengukuran, analisis dan evaluasi

9.1.1 Penjelasan umum

Organisasi perlu menetapkan beberapa hal, yaitu:

a. Apa yang diperlukan untuk dipantau dan diukur.
b. Metode untuk pemantauan, pengukuran, analisis dan evaluasi untuk memastikan hasil tersebut telah valid.
c. Kapan pemantauan dan pengukuran harus ditampilkan
d. Kapan hasil dari pemantauan dan pengukuran perlu dianalisis serta dievaluasi.

Proses ini perlu didokumentasikan oleh organisasi sebagai bukti bahwa pemantauan dan pengukuran telah dilakukan.

Evaluasi performa BCMS menjadi hal yang cukup penting pada proses ini, di mana hal tersebut dapat menjadi perbaikan performa dari segi efektivitas dan efisiensi BCMS.

9.1.2 Evaluasi prosedur keberlanjutan bisnis

a. Organisasi perlu melakukan evaluasi kapabilitas dan prosedur keberlanjutan bisnis untuk memastikan kesesuaian, kecukupan dan tingkat efektivitas prosedur yang telah dibuat.
b. Evaluasi ini dikerjakan melalui peninjauan secara periodik, pelatihan, pengujian, pelaporan pasca gangguan dan evaluasi performa. Perubahan signifikan yang terjadi, dapat disertakan pada prosedur melalui evaluasi.
c. Organisasi perlu melakukan evaluasi secara periodik yang sesuai dengan hukum dan regulasi yang berlaku, *best-practices*, serta kesesuaian dengan kebijakan serta tujuan keberlanjutan bisnis organisasi.
d. Organisasi perlu melakukan evaluasi yang direncanakan pada jangka waktu tertentu dan ketika munculnya perubahan yang signifikan yang akan mempengaruhi prosedur yang ada.

Organisasi perlu melakukan peninjauan pasca terjadinya gangguan serta pencatatan hasil, ketika muncul insiden yang akan mempengaruhi prosedur keberlanjutan bisnis.

9.2 Audit Internal

Organisasi perlu melakukan audit internal yang telah direncanakan pada jangka waktu tertentu. Internal audit dilakuan untuk memastikan bahwa BCMS memenuhi hal-hal berikut.

a. Sesuai dengan
    1) Kebutuhan atau persyaratan dari organisasi untuk penyusunan BCMS.
    2) Kebutuhan dari standar internasional yang digunakan.
b. Dapat diimplementasi dan dipelihara secara efektif.

Organisasi perlu melakukan beberapa hal di bawah ini.

- Merencanakan, menyusun, mengimplementasi serta memelihara program audit, termasuk frekuensi, metode, pertanggungjawaban, serta kebutuhan perencanaan dan pelaporan.
- Menentukan kriteria dan ruang lingkup audit.
- Memilih auditor beserta kriteria yang dibutuhkan untuk memastikan objektivitas dari proses audit yang berjalan.
- Memastikan hasil audit dilaporkan kepada pihak manajemen yang bersangkutan.
- Mendokumentasikan informasi audit sebagai bukti atas pelaksanaan program audit dan hasil audit.

9.3 Peninjauan manajemen

Pihak manajemen perlu melakukan peninjauan terhadap BCMS yang dimiliki oleh organisasi tersebut dalam jangka waktu tertentu. Hal ini dimaksudkan untuk memastikan kesesuaian, kecukupan serta tingkat efektivitas dari BCMS tersebut.

Peninjauan yang dilakukan oleh pihak manajemen diharapkan dapat mempertimbangkan hal-hal berikut ini.

a. Kondisi kekinian (status) dari kegiatan yang telah ditinjau oleh pihak manajemen terdahulu.
b. Perubahan yang terjadi di eksternal maupun internal organisasi yang mempengaruhi BCMS.
c. Informasi performa keberlanjutan bisnis, yang berupa:
    1) Ketidaksesuaian dan nilai pembenaran.
    2) Pemantauan dan pengukuran hasil evaluasi
    3) Hasil audit

d. Kesempatan untuk melakukan peningkatan yang berkelanjutan.

Peninjauan dari manajemen perlu mempertimbangkan performa organisasi yang bersangkutan, yaitu:

- Tindak lanjut dari kegiatan yang telah ditinjau oleh pihak manajemen sebelumnya.
- Kebutuhan untuk mengubah isi BCMS, termasuk kebijakan serta tujuan di dalamnya.
- Kesempatan untuk melakukan peningkatan.
- Hasil dari audit dan peninjauan BCMS
- Teknik dan prosedur yang digunakan untuk meningkatkan performa dan efektivitas BCMS.
- Status dari tindakan perbaikan
- Hasil pelatihan serta pengujian BCMS
- Ketidaksesuaian penempatan risiko pada penilaian risiko.
- Perubahan lain yang dapat mempengaruhi BCMS, baik pada internal atau eksternal ruang lingkup BCMS.
- Kecukupan kebijakan
- Rekomendasi untuk melakukan peningkatan
- Pembelajaran serta tindakan yang dilakukan pada saat terjadi gangguan
- Munculnya petunjuk serta praktik yang dapat diimplementasikan dengan baik di organisasi.

2.8.4 Fase Tindakan (Act)

Fase tindakan pada model PDCA terdapat pada klausa ke 10. Berikut ini adalah penjelasan dari klausa 10.

Klausa 10 Peningkatan (Improvement)

10.1 Ketidaksesuaian dan tindakan perbaikan

Ketika muncul ketidaksesuaian dalam implementasi BCMS, maka organisasi perlu melakukan beberapa hal di bawah ini.

a. Identifikasi ketidaksesuaian yang terjadi
b. Melakukan tindakan atas ketidaksesuaian tersebut, seperti:
    1) Mengambil tindakan untuk mengawasi serta memperbaikinya
    2) Menjalankan konsekuensi atas ketidaksesuaian yang terjadi.

c. Evaluasi dengan tujuan untuk mengurangi penyebab dari ketidaksesuaian yang terjadi, yang dilakukan dengan cara:
    1) Peninjauan terhadap ketidaksesuaian
    2) Mencari penyebab ketidaksesuaian
    3) Mencari ketidaksesuaian sejenis yang terjadi atau berpotensi untuk terjadi.
    4) Evaluasi yang dilakukan untuk memastikan bahwa ketidaksesuaian tersebut tidak akan terjadi lagi
    5) Menentukan dan mengimplementasi tindakan perbaikan
    6) Meninjau efektivitas tindakan perbaikan yang dilakukan
    7) Membuat perubahan pada BCMS
d. Implementasi tindakan yang dibutuhkan
e. Meninjau efektivitas tindakan perbaikan yang dilakukan
f. Membuat perubahan BCMS

10.2 Peningkatan secara terus-menerus

Organisasi perlu melakukan peningkatan yang berkelanjutan untuk melihat kesesuaian, kecukupan serta tingkat efektivitas BCMS.

2.9 Kerangka Kerja BCP Bank of Japan

Bank of Japan (BOJ) adalah sebuah perbankan millik pemerintah Jepang. Perusahaan ini memiliki prinsip bahwa sebuah institusi keuangan perlu memiliki BCP (*Business Continuity Plan*) untuk melindungi proses kritis perusahaan dari serangan teroris, bencana alam, permasalahan komputer atau gangguan lainnya yang dapat mengganggu keamanan sistem di perusahaan tersebut. Perhatian Bank of Japan akan BCP sangat tinggi, karena melihat peristiwa 11 September yaitu adanya serangan pada gedung WTC di Amerika serikat. Di mana, Bank

of Japan melihat bahwa BCP untuk institusi keuangan adalah mutlak harus direncanakan serta diimplementasikan pada setiap perusahaan untuk menanggulangi setiap gangguan yang ada.

Alasan penggunaan kerangka ini sebagai studi komparasi adalah, karena kerangka BCP ini dikhususkan untuk diterapkan pada institusi keuangan. *Bank of Japan* merupakan bank sentral yang dimiliki oleh negara Jepang, di mana Jepang merupakan negara yang memiliki teknologi tercanggih di dunia (The Top Ten List Hub, 2014). Selain itu, karena letak geografis Jepang yang berada di cincin api pasifik, maka negara ini cukup memberikan perhatian terhadap manajemen risiko.

2.9.1 Sudut pandang Bank of Japan terhadap BCP

Berikut ini adalah beberapa hal yang menjadi pertimbangan dari BCP mengapa setiap institusi keuangan perlu memiliki BCP untuk melindungi proses bisnis kritis di institusi keuangan pada khususnya.

2.9.1.1 Tujuan BCP

BCP pada institusi keuangan menjadi salah satu hal yang penting karena didasari oleh beberapa hal sebagai berikut.

1. **Memelihara aktivitas ekonomi penduduk di daerah bencana**

   Aktivitas ekonomi menjadi hal yang begitu krusial di lingkungan masyarakat. BCP memungkinkan setiap institusi keuangan dapat tetap melakukan aktivitas finansial dan pelayanan kepada masyarakat selama dan setalah gangguan atau bencana berlangsung. Hal-hal yang tidak diinginkan ketika terjadi gangguan seperti, masyarakat di daerah bencana yang tidak dapat melakukan penarikan tunai, penyetoran tunai ke rekening atau terhambatnya kegiatan jual-beli di kalangan masyarakat, diharapkan dapat tetap berjalan di setiap institusi keuangan yang ada.
2. **Mencegah pembayaran secara luas dan gangguan pada penyelesaian pembayaran**

Pembayaran secara luas (*widespread payment*) adalah jenis pembayaran yang umum dan luas digunakan seperti tunai, menggunakan kartu debet atau kredit, kliring dan cek. Gangguan penyelesaian pembayaran (*settlement disorder*) adalah penyelesaian proses pembayaran yang tidak tuntas, sehingga memunculkan adanya kesalahan atau penggelapan (*fraud*).

BCP dapat berfungsi untuk mencegah *widespread payment* dan *settlement disorder*. Sehingga kegiatan ekonomi dan seluruh transaksi dapat berjalan dengan baik di lingkungan masyarakat.

3. **Mengurangi risiko manajerial**

   Terhambatnya proses operasional dalam perusahaan ketika munculnya gangguan atau bencana, membuat perusahaan sulit mengambil peluang keuntungan, penurunan reputasi di mata pelanggan serta dampak kerugian lainnya pada manajemen perusahaan. BCP diharapkan dapat membantu setiap institusi keuangan dalam mengurangi risiko manajerial yang terjadi.

2.9.1.2 Hal-hal yang perlu diperhatikan dalam BCP

Beberapa hal yang perlu diperhatikan dalam penyusunan BCP adalah sebagai berikut.

1. **Perencanaan, pengujian dan peninjauan**

   Perencanaan dilakukan untuk dapat melancarkan proses keberlanjutan bisnis ketika terjadi gangguan atau bencana pada perusahaan. Rencana yang dibuat hendaknya dapat menjadi solusi efektif yang akan menghasilkan respon yang tepat di fungsi bisnis utama atau proses bisnis kritis dalam perusahaan. Rencana perlu diuji dan ditinjau secara berkala untuk memastikan bahwa rencana tersebut dapat diimplementasikan secara praktis dan layak untuk dilakukan.

2. **Fokus kepada kegiatan operasional yang kritis di perusahaan**

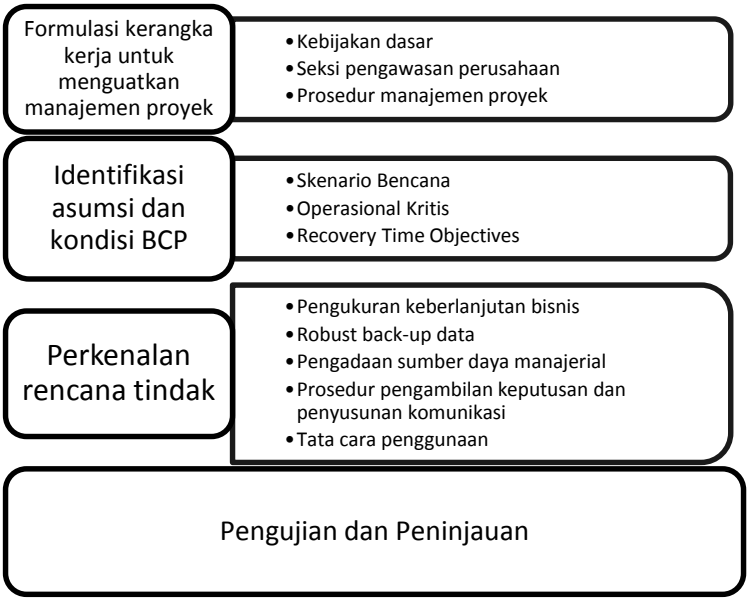
   Bencana atau gangguan yang datang mengakibatkan terbatasnya akses ke sumber daya manajerial perusahaan

dalam skala waktu tertentu. Perusahaan, khususnya institusi keuangan di sini perlu menetapkan proses bisnis kritis yang ada, sehingga kegiatan transaksi tetap dapat berjalan dan mengusahakan pelayanan bank kepada nasabah tetap optimal selama dan setelah munculnya gangguan.

3. **Mempertimbangkan keadaan khusus dalam gangguan skala besar**
   Institusi keuangan perlu mempertimbangkan keadaan khusus ketika terjadi gangguan, seperti melakukan proses secara manual, beralih kepada fasilitas *back-up* atau mempercayakan proses operasional ke pihak ketiga.
4. **Koordinasi BCP dengan pihak yang berkaitan**
   Koordinasi dengan pihak di luar perusahaan diperlukan ketika terjadinya gangguan atau bencana. Hal ini dilakukan agar institusi keuangan dapat melakukan pembayaran dan penyelesaian operasional serta keseluruhan aktivitas bisnis dengan pelaku pasar lainnya.
5. **Mengerahkan kepemimpinan yang kuat**
   Manajemen perusahaan perlu mengerahkan kepemimpinan yang kuat serta terlibat dalam setiap proses yang ada pada BCP, untuk memastikan keberlanjutan bisnis di perusahaan tetap berjalan secara optimal.

2.9.2 Aspek Business Continuity Plan

Untuk menyusun BCP yang efektif diimplementasikan pada institusi keuangan, *Bank of Japan* menyusun serangkaian proses yang memperhatikan aspek-aspek praktis pada institusi keuangan. Gambar di bawah ini adalah urutan proses yang dilakukan oleh *Bank of Japan* dalam menyusun *Business Continuity Plan.*



Gambar 2. 4 Kerangka BCP Bank of Japan (Sumber: BCP Bank of Japan)

Ada tiga fase utama yang dipaparkan dalam proses tersebut, yaitu formulasi kerangka kerja untuk menguatkan manajemen proyek, identifikasi asumsi dan kondisi BCP serta perkenalan rencana tindak untuk menanggulangi segala gangguan yang dapat mengancam kelancaran operasional bisnis perusahaan. Berikut ini akan dijelaskan lebih terperinci mengenai sub-proses pada setiap fase utama tersebut.

2.9.2.1 Fase 1: Formulasi kerangka kerja untuk menguatkan manajemen proyek

Ada tiga proses yang terdapat pada fase pertama ini. Proses tersebut adalah pembentukan kebijakan dasar, dibentuknya seksi atau bagian untuk mengawasi perusahaan secara luas serta penyusunan prosedur manajemen proyek.

Kebijakan dasar

Pihak manajemen institusi keuangan dinilai perlu mengembangkan kebijakan dasar dan pedoman untuk menyusun BCP serta penjelasan-penjelasan detail mengenai perusahaan secara luas. Dokumen ini nantinya diharapkan dapat menjelaskan perlunya BCP di perusahaan tersebut, konsep yang digunakan dalam mengidentifikasi operasional bisnis yang kritis serta pejabat eksekutif atau pihak manajemen yang bertanggung jawab dalam penyusunan BCP.

Formulasi dokumen ini akan mendorong perusahaan lebih sadar akan kebutuhan untuk mengelola krisis yang terjadi. Dokumen ini diharapkan dapat menjadi acuan untuk perusahaan agar lebih efisien dalam melaksanakan pekerjaan selanjutnya.

Bagian pengawasan perusahaan

Institusi keuangan diharapkan dapat menunjuk satu bagian yang bertugas mengawasi perusahaan secara luas. Bagian atau seksi ini bertanggung jawab untuk merumuskan prosedur khusus bekerja, penentuan pekerjaan (*job description*) untuk masing-masing departemen, serta koordinasi antar departemen yang dilaksanakan berdasarkan kebijakan serta pedoman yang ada.

Bagian pengawasan ini dapat melakukan perencanaan serta melaksanakan program pengujian dan peninjauan berkala setelah rencana tersebut ditetapkan.

Prosedur manajemen proyek

BCP adalah proyek yang sangat besar serta melibatkan begitu banyak pihak yang berkepentingan di dalamnya. Hal ini mendorong pihak manajemen untuk dapat menerapkan kontrol kemajuan atas segala proses yang ada, termasuk pelaporan ke level eksekutif atau pimpinan perusahaan. Prosedur ini diharapkan dapat membantu pihak manajemen perusahaan dalam menentukan keputusan secara tepat waktu dan fleksibel sesuai dengan sumber daya serta prioritas pekerjaan yang ada.

2.9.2.2 Fase 2: Identifikasi asumsi dan kondisi BCP

Pada fase kedua ini, terdapat proses lanjutan yaitu penyusunan skenario bencana, penentuan proses bisnisn atau kegiatan operasional yang kritis di perusahaan serta penentuan RTO yang merupakan waktu yang diperlukan oleh sistem selama masa pemulihan dari masing-masing operasional kritis tersebut.

Skenario Bencana

Penyusunan skenario bencana dibagi menjadi beberapa tahap, yaitu mengenali ancaman yang potensial, menganalisis frekuensi (*frequency*) dan tingkat keparahan (*severity*), serta identifikasi material risiko dan skenario kerusakan.

Untuk mengenali ancaman potensial, pihak institusi keuangan perlu mengidentifikasi segala bentuk potensi ancaman yang mungkin terjadi berdasarkan lokasi, dan keadaan lingkungan bisnis perusahaan. Ancaman yang umum terjadi dibagi menjadi tiga jenis yaitu:

- Bencana alam (*natural disaster*)
  Bencana yang muncul dari kondisi alam sekitar, seperti gempa bumi, taifun, tsunami dan bencana alam lainnya.
- Bencana yang dibuat oleh manusia (*man-made disaster*)
  Bencana yang muncul akibat ulah manusia, seperti terorisme, dan kejahatan komputer (*hacking, cracking*)
- Bencana secara teknis (*technical disaster*)
  Bencana yang muncul di sisi teknis, seperti kelumpuhan sistem dan matinya sumber daya listrik.

Skenario selanjutnya adalah melakukan analisis frekuensi dan tingkat keparahan bencana yang mungkin muncul. Analisis ini mengacu kepada asumsi tingkat kerusakan pada perusahaan dan *data center* yang disebabkan oleh bencana. Pada bagian ini, institusi keuangan perlu menganalisis dampak yang terjadi pada nasabah dan lembaga lainnya yang terkait dengan perusahaan tersebut.

Langkah selanjutnya adalah melakukan identifikasi material risiko serta skenario kerusakan. Setelah perusahaan melakukan identifikasi ancaman yang potensial dan tingkat keparahan atau

kerusakan yang terjadi, institusi keuangan perlu menyusun skenario dengan risiko material. Skenario tersebut dapat berupa: a) gangguan pada komputer karena adanya serangan di *data center*, b) hilangnya fungsi kantor pusat karena adanya gangguan di kantor pusat, c) penghentian operasional bisnis di berbagai lokasi dikarenakan bencana alam gempa bumi. Skenario ini dibuat dengan pertimbangan munculnya aspek material dari setiap risiko yang mungkin muncul.

Operasional Kritis

Bencana atau gangguan mengakibatkan terbatasnya akses ke sumber daya perusahaan. Institusi keuangan hendaknya perlu mengidentifikasi operasional bisnis di perusahaan yang memiliki status paling penting atau kritis, sehingga perusahaan fokus untuk melakukan pemulihan pada prioritas operasional bisnis yang utama terlebih dahulu.

Recovery Time Objective (RTO)

RTO adalah target waktu yang dibutuhkan untuk melanjutkan operasional bisnis dengan cara sementara (alternatif), misalnya untuk pengolahan data atau proses di *back-up center*.

Target ini memperhitungkan waktu yang dibutuhkan untuk berpindah ke sistem *back-up*, mendapatkan data akurat yang dibutuhkan untuk melanjutkan sistem *online*, serta waktu untuk perpindahan karyawan atau sumber daya manusia yang bertanggung jawab terhadap proses BCP.

2.9.2.3 Fase 3: Perkenalan rencana tindak

Fase ketiga membahas mengenai beberapa proses seperti pengukuran keberlanjutan bisnis, *robust back-up data*, pengadaan sumber daya manajerial, prosedur pengambilan keputusan dan penyusunan komunikasi serta tata cara penggunaan BCP.

Pengukuran Keberlanjutan Bisnis

Penentuan pengukuran spesifik pada perencanaan dilakukan berdasarkan asumsi dan kondisi untuk BCP.

Pengukuran ini harus memperhitungkan volume proses administrasi yang terlibat, waktu yang dibutuhkan pada setiap transaksi, serta waktu yang dibutuhkan untuk menyelesaikan operasional bisnis pada hari terjadinya bencana. Pada bagian ini perusahaan perlu menentukan apakah fasilitas *back-up* perlu digunakan, apakah proses manual diperlukan atau apakah ada karyawan tambahan yang dibutuhkan selama terjadinya bencana.

Robust Back-up Data

Penyimpanan data sebelum terjadinya bencana diperlukan untuk mempercepat proses pengembalian operasional bisnis (*recovery*) pada saat terjadi bencana. Mekanisme pemeliharaan data *back-up* dibutuhkan dalam bagian ini. Selain itu, pihak institusi keuangan perlu mengidentifikasi data-data yang dibutuhkan untuk menjalankan operasional bisnis yang paling kritis di perusahaan, seperti data transaksi mentah, data neraca, data *ledger* terbaru serta rincian transaksi yang belum terselesaikan.

Back-up data perlu ditransmisikan oleh jaringan telekomunikasi ke tempat penyimpanan yang letaknya cukup jauh dari *data center*. Perusahaan perlu memastikan bahwa *back-up data* dapat diakses dengan mudah selama masa terjadinya bencana atau gangguan.

Pengadaan Sumber Daya Manajerial

Pada bagian ini dibagi menjadi dua tahap yaitu penentuan sumber daya manajerial serta ketersedian infrastruktur publik.

- Sumber daya manajerial
  Institusi keuangan perlu menentukan kapasitas yang dibutuhkan selama proses pemulihan operasional bisnis yang kritis, seperti karyawan, kapasitas komputer dan telekomunikasi yang dibutuhkan.
- Ketersediaan infrastruktur publik
  Operasional bisnis perusahaan dapat dilakukan dengan asumsi bahwa listrik, gas, air, transportasi, telekomunikasi dan infrastruktur publik lainnya dapat digunakan dalam

kondisi normal. Dengan demikian, BCP yang disusun harus memperhitungkan ketersediaan seluruh infrastruktur dalam keadaan darurat atau selama terjadinya gangguan atau bencana.

Prosedur pengambilan keputusan dan penyusunan komunikasi

Tahapan ini dibagi menjadi dua yaitu, penyusunan prosedur pengambilan keputusan dan struktur pemberian perintah serta daftar kontak darurat dan daftar alat komunikasi darurat yang diperlukan selama terjadinya bencana.

- Prosedur pengambilan keputusan dan struktur pemberian perintah

  Pengambilan keputusan yang cepat dan tepat diperlukan selama terjadinya bencana. Untuk mendukung misi tersebut, perusahaan perlu menyusun prosedur pengambilan keputusan dan strukturisasi pemberian perintah untuk menghindari adanya kesalahan dalam mengambil keputusan. Institusi keuangan perlu melakukan konfirmasi darurat ketika bencana atau gangguan terjadi di perusahaan tersebut, dengan membentuk tim khusus, yaitu tim manajemen krisis atau tim lainnya yang ditunjuk secara langsung oleh pimpinan eksekutif perusahaan tersebut. Tim ini bertugas untuk mengumpulkan informasi serta melakukan pengambilan keputusan untuk memastikan proses pemulihan berjalan dengan lancar.
- Daftar kontak darurat dan alat komunikasi darurat

  Sebuah komunikasi dengan pihak yang bertanggung jawab menjadi sangat penting ketika perusahaan ingin memberikan respon yang tepat terhadap setiap gangguan atau bencana yang datang. Perusahaan institusi keuangan perlu memiliki daftar kontak darurat serta menyediakan alat komunikasi yang dapat digunakan di saat darurat. Alat komunikasi yang disediakan harus sesuai dengan kebutuhan dan kemampuan masing-masing perusahaan. Contoh alat komunikasi yang dapat digunakan ketika terjadinya gangguan adalah *fixed line telephone, mobile telephone, e-mail* atau *direct hotlines.*

Tata cara penggunaan

Penyusunan tata cara penggunaan pada prosedur operasional yang mudah dipahami adalah cara yang efektif untuk memastikan kelayakan BCP. Hal ini membantu setiap departemen atau fungsional bisnis untuk dapat melaksanakan tindakan yang sesuai dengan tugas masing-masing.

2.9.2.4 Fase 4: Pengujian dan Peninjauan

Pada fase berikut ini akan dijelaskan mengenai pengujian dan peninjauan perencanaan yang telah dibuat. Hal ini dilakukan untuk memastikan bahwa dokumen BCP yang dibuat sesuai dengan kebutuhan serta layak untuk diimplementasikan.

Pelaksanaan pengujian dan peninjauan secara berkala sangat penting dilakukan untuk dapat memastikan kelayakan BCP di perusahaan. Pengujian yang dilakukan akan menunjukkan ketercapaian RTO (*Recovery Time Objectives*), identifikasi tantangan selama proses berlangsung dan memungkinkan institusi keuangan melakukan peninjauan terhadap kecukupan peralatan yang digunakan selama terjadinya bencana atau gangguan.

Pengujian dapat dilakukan sesuai dengan kebutuhan setiap perusahaan. Pengujian secara total kepada seluruh fungsional bisnis perusahaan dinilai cukup sulit untuk diimplementasikan, mengingat institusi keuangan harus terus berhubungan dengan nasabah dan pihak terkait perusahaan. Pengujian secara parsial bisa menjadi pilihan yang efektif, di mana pengujian hanya dilakukan pada bagian-bagian tertentu saja. Pengujian dengan luar pihak institusi keuangan juga perlu dilakukan untuk melihat bagaimana koneksi yang dibangun antara perusahaan tersebut dengan mitra kerja pada saat terjadi gangguan atau bencana.

2.9.2.5 Isu-isu lain

Pada bagian isu-isu lain ini, akan dibahas mengenai hal-hal lain yang terkait dengan penyusunan BCP di institusi keuangan.

- **Pencegahan dan mitigasi kerusakan bencana**
  Risiko dan kerusakan dapat dicegah dan dimitigasi untuk mengurangi kerugian di perusahaan. Hal-hal yang termasuk

pencegahan dan mitigasi ini dapat berupa, pemindahan kantor ke lokasi anti-gempa atau lokasi yang aman dari bencana, melakukan instalasi pada *back-up generators*, peningkatan kontrol untuk mengakses daerah terlarang, atau memperkuat *firewall* untuk mencegah serangan *hacker*.

- **Pembangunan lokasi fasilitas *back-up***
  Perusahaan perlu membangun fasillitas *back-up* yang lokasinya berjauhan dengan kantor pusat (*data center*) untuk menghindari pengaruh bencana atau gangguan yang terjadi. Hal yang perlu dipastikan adalah fasilitas *back-up* tidak berbagi jaringan telekomunikasi atau berada di rute yang sama untuk pasokan tenaga listrik dengan kantor pusat. Perusahaan juga perlu memperhitungkan kebutuhan karyawan untuk fasilitas *back-up*.
- **Bekerja sama dengan penyedia layanan di luar perusahaan**
  Institut keuangan dapat mengelola fasilitas *back-up* secara mandiri atau mempercayakannya kepada pihak ketiga. Kerja sama yang dibangun oleh perusahaan dengan pihak ketiga dapat membantu perusahaan dalam menangani gangguan atau bencana yang menyerang perusahaannya. Namun ada beberapa hal yang perlu diperhatikan, yaitu terkait dengan kemanan informasi yang diberikan kepada penyedia layanan atau pihak ketiga. Terutama untuk informasi rahasia atau informasi penting milik perusahaan yang dapat menjadi kesempatan untuk kompetitor, apabila informasi tersebut terbongkar.

2.10 Kerangka Kerja BCP Dutch Financial Sector

Kerangka ini dibuat oleh keanggotaan perbankan di Belanda, yang terdiri dari ABN AMRO, ABN AMRO Clearing Bank, Currence, DNB, EMCF, Equens, Euroclear Nederland, ING, KAS BANK, LCH.Clearnet SA, Ministerie van Financiën, NVB, NYSE Euronext, Rabobank, RBS, SNS Bank, dan SWIFT Bank.

Prinsip-prinsip dalam kerangka atau standar ini dibuat untuk mempermudah setiap institusi keuangan dalam mengelola BCM (*Business Continuity Management*) di perusahaannya masing-masing. Kerangka ini juga disusun secara umum dan dapat diaplikasikan secara nyata oleh institusi keuangan.
Dalam implementasinya, penyusunan kerangka ini mengacu kepada beberapa standar internasional seperti:

- British Continuity Institute-Good Practice Guideline (GPG)
- British Standard Institute BS25999 part 1 dan 2
- US Disaster Recovery Institute-Generally Accepted Practices (GAP)
- US National Fire Protection Association-NFPA 1600

Prinsip-prinsip ini merupakan standar minimal yang dibutuhkan dalam melakukan penyusunan BCM di masing-masing perusahaan. Prinsip ini djelaskan di level tertinggi perusahaan, dengan harapan bahwa setiap perusahaan dapat mengambil tanggung jawab serta mendukung dan menerapkan prinsip-prinsip yang ada, sesuai dengan kebutuhan masing-masing perusahaan. Prinsip yang telah tersusun ini disediakan dalam bentuk kerangka kerja secara umum yang mendukung institusi keuangan dan penyedia layanan teknologi informasi dan telekomunikasi.

Alasan penggunaan kerangka BCP dari *Dutch Financial Sector* adalah karena kerangka ini disusun oleh perbankan untuk institusi keuangan di Jerman. Selain itu, Jerman merupakan negara yang cukup maju dan menjadikan riset dan teknologi sebagai perhatian utama dari negara ini. Berikut ini akan dipaparkan mengenai penjelasan dari masing-masing prinsip yang ada di kerangka BCP ini.

2.10.1 Prinsip 1 : Kebijakan

Pendahuluan

Dalam implementasinya, penyusunan kebijakan menjadi fondasi utama yang paling kuat untuk menyusun BCM di

perusahaan masing-masing. Kebijakan BCM menjelaskan poin-poin dan parameter yang digunakan untuk mengimplementasi keberlanjutan bisnis.

Tujuan

Kebijakan BCM dibuat dengan tujuan untuk memberikan penjelasan mengenai tujuan BCM itu sendiri di perusahaan. Kebijakan BCM menjadi dokumentasi bagi perusahaan untuk dapat mengukur kapabilitas dari keberlanjutan bisnis yang direncanakan.

Kebutuhan/persyaratan

Perusahaan perlu membuktikan bahwa kebijakan BCM telah diimplementasikan, dipelihara serta dinilai atau ditinjau secara periodik. Kebijakan BCM disusun oleh pihak manajemen tertinggi perusahaan, seperti Dewan Direksi atau pimpinan di masing-masing fungsional bisnis. Ruang lingkup dari kebijakan BCM adalah mengenai hukum serta obligasi dan batasan-batasan yang ada di perusahaan masing-masing.

Produk dari prinsip pertama ini adalah sebuah dokumen prinsip yang telah diterima dan ditandatangani oleh manajemen tertinggi di perusahaan.

Prinsip 1 ini berisi hal-hal di bawah berikut.

- Penentuan ruang lingkup BCM di perusahaan
- Sumber daya BCM yang dibutuhkan mengenai pertanggungjawaban dan akuntabilitas BCM (RACI)
- Penjelasan prinsip BCM, petunjuk serta standar minimal untu perusahaan seperti ruang lingkup (geografi, organisasi), risiko yang mungkin muncul, kebijakan mitigasi risiko, kategori dampak (perhitungan kualitatif dan kuantitatif) serta kebutuhan regulasi.
- Standar, regulasi atau kebijakan acuan yang digunakan sebagai studi komparasi untuk dapat tetap menghasilkan kebijakan yang terbaik bagi perusahaan.

2.10.2 Prinsip 2 : Business Continuity Governance

Pendahuluan

Efektivitas pengelolaan dan tata kelola keberlanjutan bisnis menjadi bagian yang sangat penting dalam pencapaian perusahaan terhadap keberlanjutan bisnis yang dibuatnya. Partisipasi dari pihak manajemen tertinggi dapat memastikan bahwa proses BCM di perusahaan telah dikenalkan dengan benar, mendukung kebutuhan perusahaan serta menjadi bagian dari budaya perusahaan.

Tujuan

Penyusunan, implementasi dan pemeliharaan struktur tata kelola keberlanjutan bisnis dapat memastikan pemantauan, peninjauan, pemeliharaan serta peningkatan efektivitas dan efisiensi implementasi BCM.

Kebutuhan/persyaratan

Perusahaan harus dapat membuktikan bahwa kebijakan BCM telah diimplementasikan, dipelihara dan dinilai secara periodik. Selain itu, perlu diadakan pengujian dan audit untuk memberikan penjaminan yang cukup, yang selaras dengan kebijakan BCM di perusahaan.

Perusahaan perlu melakukan peningkatan berkelanjutan, yang diharapkan dapat meningkatkan efektivitas dan efisiensi BCM di perusahaan, melalui peninjauan berkala yang dilakukan oleh pihak manajemen.

Produk dari prinsip kedua ini adalah laporan tinjauan secara periodik, yang di dalamnya terdapat tindakan peningkatan atau perbaikan yang dilakukan.

2.10.3 Prinsip 3 : Business Impact Analysis

Pendahuluan

Business Impact Analysis (BIA) merupakan sebuah pendokumentasian yang dilakukan untuk mengidentifikasi kunci

utama dalam rantai nilai perusahaan, proses, produk dan layanan, aktivitas kritis serta sumber daya yang dibutuhkan oleh perusahaan yang selaras dengan tujuan bisnis.

Tujuan

Tujuan dari BIA adalah mengidentifikasikan rantai nilai kritis, proses dan sumber daya dengan cara penentuan dampal dari kerusakan dalam periode maksimal selama gangguan/bencana yang masih dapat ditoleransi oleh perusahaan atau *Maximum Tolerable Period of Disruption* (MTPD). Hal ini dilakukan untuk dapat menentukan kebutuhan minimal yang digunakan untuk melanjutkan rantai nilai dan proses kritis serta sumber daya yang dibutuhkan pada saat terjadinya gangguan.

Kebutuhan/persyaratan

Pada dokumentasi BIA perlu dilakukan penilaian seluruh aktivitas bisnis dan sumber daya yang ada di perusahaan.

Produk dari prinsip ketiga ini adalah penjelasan mengenai seluruh rantai nilai yang kritis, produk serta sumber daya yang dibutuhkan oleh perusahaan (termasuk MTPD).

Bagian ini setidaknya memiliki isi sebagai berikut.

- Identifikasi aktivitas bisnis kritis dan sumber daya yang dibutuhkan.
- Penentuan M*aximum Tolerable Period of Disruption* (MTPD), yaitu maksimal *downtime* atau maksimal waktu kerusakan, di mana waktu ini merupakan waktu yang dapat ditoleransi oleh perusahaan ketika produk dan layanan yang disampaikan tidak dapat dimulai lagi.
- Penentuan *Recovery Time Objective* (RTO), yaitu target waktu yang dibutuhkan untuk kembali meneruskan proses atau aktivitas setelah terjadi gangguan.
- Penentuan *Recovery Point Objective* (RPO), yaitu poin waktu dari mana (sejak kapan) data kritis pada proses bisnis dan aktivitas harus dipulihkan setelah terjadi gangguan.

- Kebutuhan minimal yang dibutuhkan selama menjalankan proses bisnis seperti jumlah karyawan, jumlah fasilitas, sistem informasi dan aplikasi, tingkat pelayanan minimal (*minimal services levels)* untuk internal dan nasabah, serta hubungan dengan pihak ketiga (mitra kerja internal dan eksternal).

2.10.4 Prinsip 4 : Risk Assessment/Analysis

Pendahuluan

Hasil yang diharapkan dari BIA adalah perusahaan dapat fokus terhadap penilaian risiko dari aktivitas kritis yang ada di perusahaan tersebut. Penilaian risiko ini meliputi identifikasi risiko, analisis dan evaluasi.

Tujuan

Tujuan dari penilaian risiko adalah mengidentifikasi ancaman internal dan eksternal, kewajiban serta eksposur, termasuk konsentrasi risiko yang dapat menyebabkan gangguan atau kerugian pada aktivitas bisnis yang kritis. Analisis risiko perlu memperhatikan tingkat ketergantungan perusahaan terhadap fasilitas utama yang ada (listrik, gas, air, dan telekomunikasi) serta penyedia layanan eksternal.

Kebutuhan/persyaratan

Dalam penilaian risiko dibutuhkan pendefinisian tingkatan risiko, aksi mitigasi dan risiko lain yang juga berpengaruh.

Produk dari prinsip ini adalah penilaian risiko dan laporan analisis. Perusahaan perlu melakukan beberapa hal di bawah ini dalam mengimplementasi prinsip ini, yaitu:

- Ruang lingkup penelitian, termasuk area risiko (misal: faktor manusia, aset dan fasilitas).
- Kriteria untuk evaluasi risiko (model 4T : *take*, *treat*, *transfer, terminate*).
- Tingkat kerentanan dan penjelasan (kemungkinan atas kejadian) ancaman yang terjadi di perusahaan.

- Konsentrasi risiko.
- Peniliaian dan analisis risiko (dihubungkan dengan BIA).
- Fokus prioritas BCM dan kontrol risiko.
- Manajemen strategi kontrol risiko dan rencana tindak.
- Tingkat kemungkinan munculnyaa risiko (probabilitas atau frekuensi).
- Tingkat kerentanan perusahaan terhadap berbagai jenis ancaman, penentuan prioritas serta manajemen kontrol perusahaan.
- Dasar untuk menyusun *risk appetite*, program kontrol manajemen risiko dan rencana tindak.

2.10.5 Prinsip 5 : Business Continuity Strategy

Pendahuluan

Analisis strategi yang baik menjadi sesuatu hal yang sangat penting untuk mengukur tingkat efektivitas pembiayaan yang berkelanjutan. Strategi yang dibuat harus sesuai dengan nilai-nilai yang ada pada obyek, hasil dari BIA dan analisis risiko. Strategi yang berkelanjutan dapat dibagi menjadi dua yaitu, strategi pengawasan serta strategi pemulihan.

Tujuan

Menentukan pengurangan risiko serta strategi pemulihan untuk mengurangi kemungkinan serta dampak dari bencana atau gangguan yang terjadi.

Kebutuhan/persyaratan

Produk dari prinsip ini adalah dokumen strategi keberlanjutan bisnis. Perusahaan diharapkan dapat mengimplementasikan beberapa hal berikut.

- Kebutuhan utama yang sesuai dengan nilai obyek, hasil BIA dan penilaian risiko.
- Strategi pencegahan
- Strategi pemulihan

- Strategi kontrol atau pengawasan
- Strategi risiko residu atau risiko lain yang berpengaruh.

2.10.6 Prinsip 6 : Business Continuity Plan

Pendahuluan

Setiap perusahaan memiliki risiko dari gangguan atau bencana yang potensial yang dapat menyebabkan kehilangan karyawan, infrastruktur publik dan swasta, bangunan/gedung, proses bisnis kritis, infrastruktur TIK, data (elektronik dan fisik) serta komunikasi. Pembuatan dan pemeliharaan *Business Continuity Plan* (BCP) memastikan bahwa perusahaan memiliki informasi dan sumber daya untuk menangani bencana yang muncul.

Tujuan

BCP adalah seperangkat prosedur dan informasi yang dirancang untuk memastikan pemulihan dari efek yang mungkin muncul berdasarkan skenario ancaman. Pembahasan ini terdiri dari langkah pemulihan ketika terjadi bencana atau gangguan hingga pada saat seluruh layanan kritis dan fungsi operasional pendukung dapat pulih kembali.

Dalam BCP, perlu diadakan kesepakatan antara perusahaan dengan penyedia layanan mengenai ukuran penyedia layanan serta performa yang terkait dengan SLA (*Service Level Agreement*).

Kebutuhan/persyaratan

Sebuah perencanaan yang menjelaskan langkah-langkah yang dibutuhkan untuk memulihkan rantai nilai, proses dan produk yang terkena gangguan.

Produk dari prinsip ini adalah dokumen BCP. Berikut ini adalah isi dari prinsip-prinsip ini.

- Deskripsi ruang lingkup
- Penanggungjawab atau sumber daya manusia yang dibutuhkan.

- Peninjauan secara berkala
- Deskripsi prosedur pemulihan BCM, seperti informasi dan peringatan, deksripsi tindakan pertama dan tindakan langsung, mobilisasi, respon (skenario risiko), penentuan skala, evaluasi seta pelaporan.
- Informasi terkait yang berisi mengenai beberapa hal berikut.
    1. Hasil BIA, penilaian risiko dan strategi keberlanjutan bisnis.
    2. Manajemen krisis (peran, wewenang dan tanggung jawab), lokasi, prosedur yang berkaitan dengan informasi, pengambilan keputusan serta tindakan yang dilakukan.
    3. Komunikasi krisis (prosedur pemanggilan, alur komunikasi, strategi komunikasi untuk setiap pemangku kepentingan, media serta juru bicara dari perusahaan.

2.10.7 Prinsip 7 : Pelatihan BCM

Pendahuluan

Perencanaan BCM (*Business Continuity*-BC, *Disaster Recovery*-DR, *Crisis Management*-CM) tidak dapat dianggap kuat dan dapat diandalkan sebelum masuk ke dalam tahapan pelatihan. Tujuan dari pelatihan dan evaluasi adalah untuk menentukan kecukupan rencana, mekanisme untuk mempertahankan dan memperbarui rencana, pemenuhan persyaratan peraturan dan bukan untuk menilai performa personal.

Tujuan

Tujuan dari pelatihan BCM adalah untuk memastikan bahwa setiap rencana keberlanjutan yang dibuat dapat divalidasi melalui pelatihan dan peninjauan untuk meningkatkan kompetensi manajemen krisis perusahaan.

Kebutuhan/persyaratan

Setiap perencanaan keberlanjutan (*BC, DR, CM*) untuk rantai nilai, fungsi bisnis, produk serta aktivitas bisnis yang kritis perlu dipelihara dan diuji secara periodik, sesuai dengan pelatihan dan tingkat uji yang telah ditetapkan.

Produk untuk prinsip 7 ini adalah perencanaan pelatihan serta pengujian BCM, termasuk kesenjangan, permasalahan serta langkah-langkah penyelesaiannya. Prinsip ini setidaknya berisi hal-hal di bawah ini.

- Pelatihan
  Pelatihan diadakan untuk memastikan bahwa keberlanjutan bisnis yang telah dibuat memenuhi persyaratan yang telah ditetapkan sebelumnya.
- Pengelolaan pelatihan
  Bagian ini dikhususkan untuk pengalokasian peran dan tanggung jawab yang tepat pada masing-masing individu yang terlibat terhadap BCM di perusahaan.
- Perencanaan pelatihan
  Pelatihan dilakukan secara terencana, realistis dan disetujui oleh pemangku kepentingan, sehingga akan meminimalisasi risiko yang mungkin muncul pada proses bisnis.
- Pelatihan dan tingkat pengujian
  Pelatihan keberlanjutan bisnis (BC, DR, CM) tidak dapat dilakukan dalam satu pelatihan. Pelatihan perlu dijalankan secara progresif untuk dapat melihat tingkat ketergantungan serta hubungan dengan pengguna terkait.
- Penandatanganan
  Perencanaan keberlanjutan bisnis yang dibuat dan telah melalui tahapan pengujian dan pelatihan perlu ditandatangani oleh manajemen senior perusahaan.

2.10.8 Prinsip 8 : Manajemen Krisis

Pendahuluan

Manajemen krisis adalah sebuah proses di mana perusahaan dapat mengatasi ancaman yang dapat menghancurkan perusahaan. Kunci dari krisis dan manajemen krisis adalah:

- Ancaman perusahaan dan sektor keuangan
- Elemen lain di luar ekspektasi atau perencanaan
- Waktu pengambilan keputusan yang singkat

Tujuan

Perusahaan perlu menjalankan dan memelihara kecukupan struktur manajemen krisis yang berisi tim manajemen krisis dan perencanaan manajemen krisis.

Kebutuhan/persyaratan

Perusahaan harus dapat membuktikan bahwa tujuan sudah diimplementasikan, dipelihara, dinilai secara periodik dan diuji serta selaras dengan kebijakan BCM perusahaan.

Produk untuk prinsip 8 ini adalah laporan tinjauan manajemen krisis secara periodik, termasuk tindakan peningkatan atau perbaikan. Laporan ini dapat berisi beberapa hal di bawah ini.

- Tanggal peninjauan terakhir
- Tanggal pengujian terakhir
- Tanggal audit terakhir
- Perencanaan pengujian
- Pencarian masalah atau celah
- Batas waktu untuk mengatasi permasalahan dan celah yang terjadi

2.11 Bank Perkreditan Rakyat (BPR)

Berdasarkan UU Perbankan nomor 10 tahun 1998, bank adalah badan usaha yang menghimpun dana dari masyarakat dan menyalurkan kembali ke masyarakat dalam bentuk kredit, untuk meningkatkan taraf hidup masyarakat. Perbankan adalah segala sesuatu yang menyangkut bank, kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan usaha.

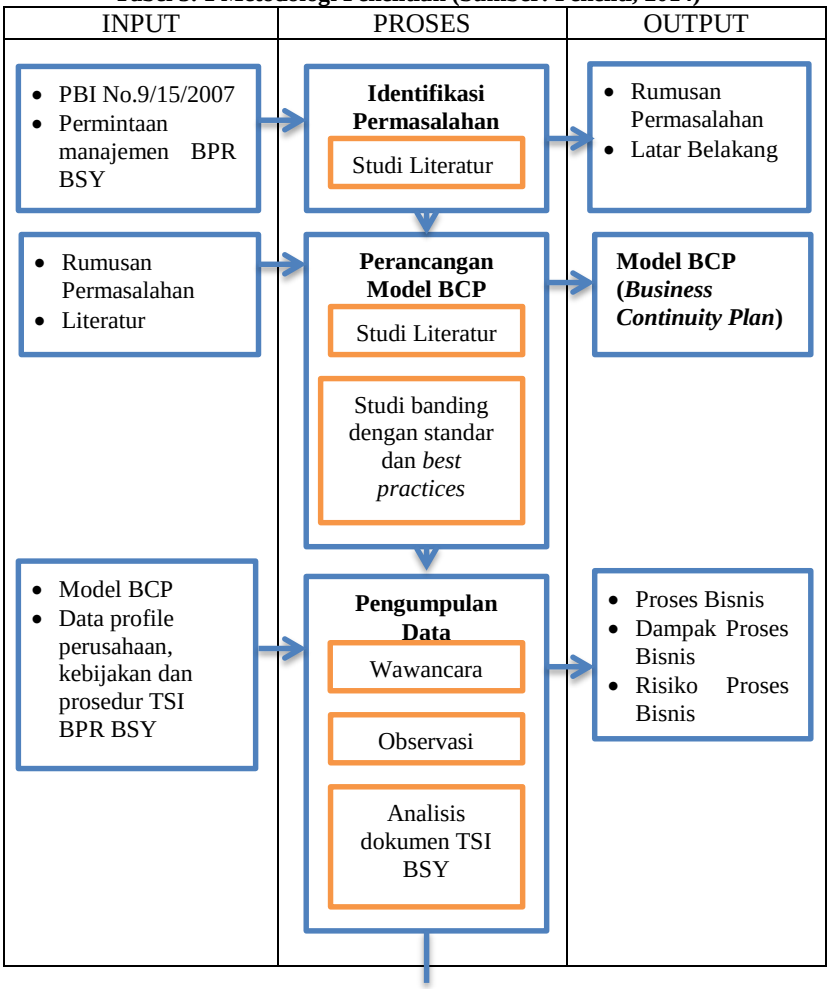
Perbankan yang memiliki segmentasi pasar lebih banyak kepada pengusaha UMKM (Usaha Mikro Kecil dan Menengah), disebut dengan Bank Perkreditan Rakyat (BPR) atau *rural bank.* Menurut Ali Suyanto pada tahun 2013, dalam bukunya yang berjudul Pengelolaan BPR dan Lembaga Keuangan Pembiayaan Mikro, Bank Perkreditan Rakyat adalah lembaga keuangan bank yang menerima simpanan hanya dalam bentuk deposito berjangka, tabungan dan menyalurkan dana melalui bentuk kredit atau bentuk lainnya untuk meningkatkan taraf hidup masyarakat. Usaha ini dilakukan untuk membantu masyarakat dalam menjalankan usahanya melalui prinsip konvensional atau prinsip syariah , di mana dalam kegiatannya tidak memberikan jasa dalam lalu lintas pembayaran.

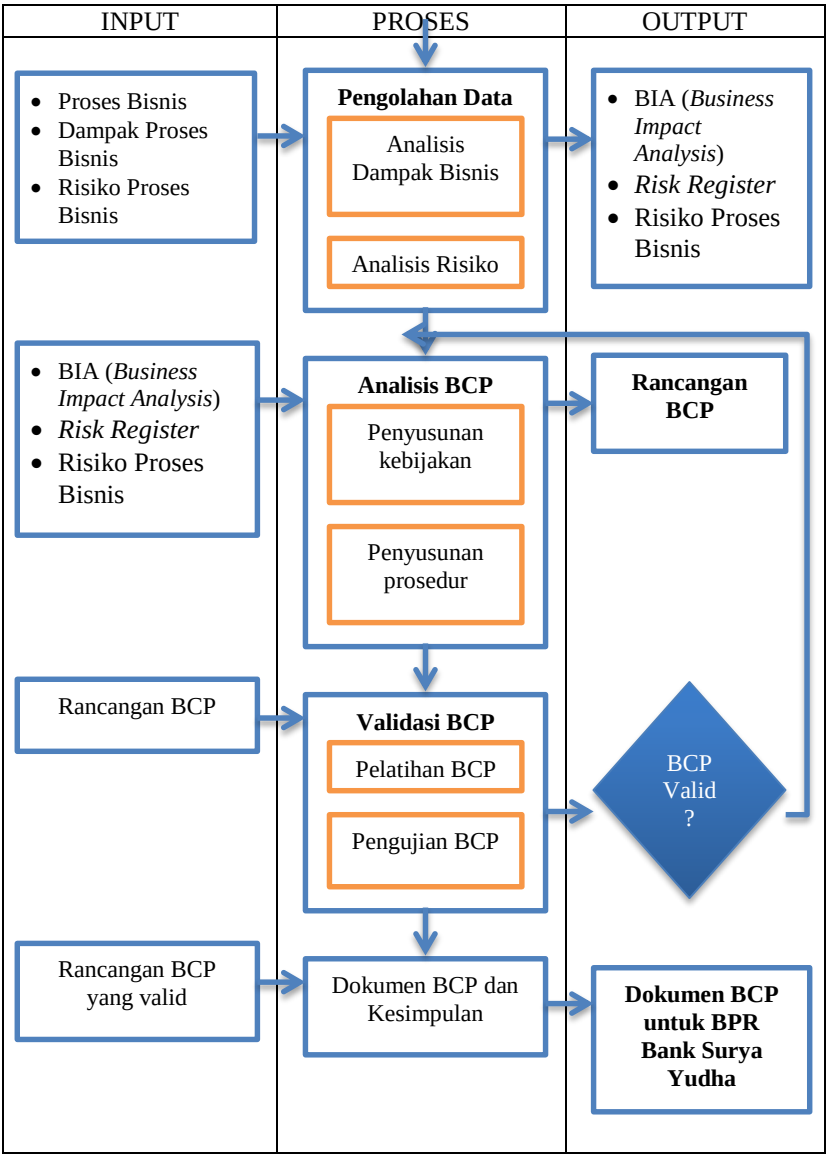
Sesuai dengan pasal 33 UUD 1945 tentang sistem ekonomi, BPR melaksanakan usaha dengan berasaskan pada demokrasi ekonomi, dengan menggunakan prinsip kehati-hatian (*prudential banking*). Payung hukum untuk BPR adalah PBI No. 8/26/PBI/2006 tanggal 8 September 2006 tentang Bank Perkreditan Rakyat. Sedangkan untuk BPR Syariah adalah Pendirian Bank Pembiayaan Rakyat Syariah PBI No.11/23/PBI/2009.

BAB III
METODOLOGI PENELITIAN

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

Tabel 3. 1 Metodologi Penelitian (Sumber: Peneliti, 2014)




INPUT
PROSES
OUTPUT
Proses Bisnis
Dampak Proses Bisnis
Risiko Proses Bisnis
Pengolahan Data
Analisis Dampak Bisnis
Analisis Risiko
BIA (Business Impact Analysis)
Risk Register
Risiko Proses Bisnis
BIA (Business Impact Analysis)
Risk Register
Risiko Proses Bisnis
Analisis BCP
Penyusunan kebijakan
Penyusunan prosedur
Rancangan BCP
Rancangan BCP
Validasi BCP
Pelatihan BCP
Pengujian BCP
BCP Valid ?
Rancangan BCP yang valid
Dokumen BCP dan Kesimpulan
Dokumen BCP untuk BPR Bank Surya Yudha

3.1 Identifikasi Permasalahan

Tahapan ini merupakan langkah awal untuk memulai penyusunan tugas akhir ini. Masukkan dari permasalahan yang ada adalah datang dari permintaan manajemen perusahaan, mengenai pentingnya manajemen risiko teknologi informasi serta implementasi BCP (*Business Continuity* Plan) bagi Bank Perkreditan Rakyat. Selain itu, gagasan ini diperkuat dengan adanya Peraturan Bank Indonesia (PBI) Nomor 9/15/2007 tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum.

Proses identifikasi permasalahan ini didukung dengan adanya studi literatur yang dilakukan untuk memperkuat data dan sebagai referensi untuk memberikan aspek integritas pada penelitian ini. Studi literatur dilakukan dari buku, jurnal, paper, dan informasi yang digunakan di internet. Tahapan ini akan menghasilkan rumusan permasalahan serta latar belakang penelitian yang dijadikan sebagai bahan dasar untuk memulai penelitian ini.

3.2 Perancangan Model BCP

Berdasarkan rumusan masalah dan literatur yang ada, proses selanjutnya adalah perancangan model BCP berdasarkan studi literatur dan studi banding dengan standar serta *best practices* yang ada, untuk menghasilkan model BCP terbaik yang sesuai dengan kebutuhan BPR Bank Surya Yudha Banjarnegara. Standar yang digunakan adalah berdasarkan ISO 22301:2012 dan *best practices* yang digunakan adalah berdasarkan penerapan BCP pada perusahaan perbankan lainnya.

3.3 Pengumpulan Data

Proses pengumpulan data dilakukan dengan cara wawancara terstruktur dan tidak terstruktur, observasi peneliti serta mempelajari prosedur, kebijakan dan laporan tahunan

perusahaan yang telah dilakukan sebelumnya. Validasi kepada pihak perusahaan penting untuk dilakukan, dengan tujuan untuk menjunjung aspek kebenaran (*correctness*) dan integritas dari sebuah penelitian. Berikut ini adalah penjelasan dari masing-masing metode pengumpulan data.

3.3.1 Wawancara terstruktur dan tidak terstruktur

Wawancara terstruktur akan dilakukan oleh pimpinan Teknologi dan Sistem Informasi, Bagian Operasional, Pembukuan, Personalia, Kredit dan Direksi BPR Bank Surya Yudha Banjarnegara. Hal ini dilakukan sebagai bentuk penggalian data dan informasi, sekaligus validasi ats penelitian yang dilaksanakan di perusahaan tersebut.

Wawancara tidak terstruktur dilaksanakan kepada karyawan Divisi Teknologi dan Sistem Informasi BPR Bank Surya Yudha serta perwakilan bagian teknologi informasi (*IT Back Office*) di beberapa kantor cabang dan kantor kas yang ada, sebagai bentuk penggalian data dan informasi secara langsung di lapangan.

3.3.2 Observasi Peneliti

Observasi peneliti dilakukan terutama pada saat peneliti mengumpulkan data untuk menganalisis risiko. Di mana, pada tahapan identifikasi risiko, diperlukan pengamatan untuk bisa mengidentifikasikan dengan tepat, risiko teknologi informasi apa sajakah yang mungkin muncul pada perusahaan tersebut.

Observasi dilakukan juga untuk mengamati kinerja Divisi Teknologi dan Sistem Informasi, untuk menentukkan BCP yang sesuai bagi perusahaan BPR Bank Surya Yudha Banjarnegara.

3.3.3 Mempelajari Dokumen Perusahaan

Mempelajari dokumen perusahaan seperti kebijakan, prosedur, laporan tahunan, dan regulasi eksternal yang diikuti oleh perusahaan merupakan salah satu bentuk usaha peneliti untuk tetap membuat penelitian ini relevan dengan lingkungan operasi, atau kebutuhan perusahaan.

Proses pengolahan data ini akan menghasilkan data dan informasi mengenai proses bisnis fungsional bisnis di perusahaan, dampak proses bisnis ketika terjadi gangguan serta risiko pada proses bisnis yang muncul atas gangguan atau bencana yang terjadi.

3.4 Pengolahan Data

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

3.4.1 Analisis Dampak Bisnis

Tahapan ini dilakukan untuk mengidentifikasi proses bisnis perusahaan beserta dampak yang terjadi pada bisnis ketika terjadi gangguan. Baik dampak ke nasabah, dampak secara finansial maupun dampak secara hukum. Analisis ini dilakukan untuk melihat proses bisnis manakah di perusahaan yang paling kritis dan menjadi sangat fundamental bagi operasional bisnis perusahaan. Proses ini nantinya akan menghasilkan tabel *Business Impact Analysis* (BIA).

3.4.2 Analisis Risiko

Identifikasi risiko dilakukan pada tahapan ini dengan acuan ISO 31000:2009. Risiko IT/IS pada perusahaan ini akan dicari dan dipastikan, bahwa risiko tersebut benar menjadi sebuah ancaman yang dapat melumpuhkan sistem serta operasional bisnis perusahaan. Proses identifikasi risiko dilakukan berdasarkan lima komponen sistem informasi, yaitu perangkat keras, perangkat lunak, data, prosedur, dan sumber daya manusia.

Setelah melakukan identifikasi risiko, maka selanjutnya adalah melakukan penilaian risiko dengan metode FMEA (*Failure Mode and Effect* Analysis). Nilai untuk kecenderungan

(*likelihood*), dampak (*impact*), dan deteksi (*detection*) diberikan untuk setiap risiko IT/IS yang ada. Kemudian setelah dilakukan pemberian nilai, maka langkah selanjutnya adalah penghitungan skor risiko (kecenderungan x dampak) dan RPN atau *Risk Priority Number* (kecenderungan x dampak x deteksi). Setelah penilaian dilakukan maka akan terbentuk grafik yang menggambarkan urutan skor risiko dan RPN, serta posisi dari masing-masing risiko IT/IS, apakah berada pada kondisi yang *critical*, *high*, *medium* atau *low*. Maka selanjutnya, BCP difokuskan untuk menyelesaikan permasalahan untuk risiko IT/IS yang berada pada kondisi *critical* dan *high.*

Proses ini akan menghasilkan tabel analisis risiko atau *risk register* yang dapat dijadikan bahan untuk membuat analisis BCP.

3.5 Analisis BCP

Analisis BCP dilakukan dengan menerapkan model BCP yang telah dibuat dalam bentuk sebuah kerangka atau *template* yang dapat diimplementasikan oleh perusahaan. Analisis ini dimulai dari melakukan penentuan tujuan, ruang lingkup serta sumber daya manusia dalam perusahaan, baik dari level strategis (*top management*) hingga level teknis. Analisis BCP dibagi menjadi penyusunan kebijakan dan penyusunan prosedur.

3.5.1 Penyusunan Kebijakan

Pada tahapan ini disusun kebijakan yang dilakukan perusahaan untuk dapat menanggulangi proses bisnis dan risiko kritis di perusahaan.

3.5.2. Penyusunan Prosedur

Pada tahapan ini disusun prosedur teknis yang dilakukan untuk menangani dan menanggulangi risiko kritis di fungsional bisnis yang merupakan pemilik dari risiko tersebut.

3.6 Validasi BCP

Untuk memastikan bahwa BCP yang dibuat sudah benar dan dapat diterima oleh perusahaan, maka proses validasi dinilai menjadi hal yang sangat penting dalam penelitian ini. Proses ini meliputi pelatihan BCP dan pengujian BCP kepada seluruh karyawan yang terkait dengan sistem pada BPR Bank Surya Yudha Banjarnegara.

3.6.1 Pelatihan BCP

Pelatihan BCP dilaksanakan untuk setiap karyawan yang memiliki tugas dan wewenang yang berhubungan dengan teknologi dan sistem informasi pada operasional bisnis perusahaan. Pelatihan ini dapat diinisiasi dari bagian Teknologi dan Sistem Informasi, yang selanjutnya diikuti oleh fungsional bisnis lainnya di perusahaan tersebut.

3.6.2 Pengujian BCP

Pengujian BCP dilakukan melalui sebuah aktivitas simulasi di perusahaan. Simulasi ini dapat dibedakan menjadi simulasi total dan simulasi parsial.

3.6.2.1 Simulasi Total

Simulasi total dilakukan ketika seluruh sistem yang menjadi tumpuan dari operasional perusahaan dimatikan dalam suatu waktu (*system down*). Hal ini akan membuktikan apakah BCP yang dirancang dapat mengatasi permasalahan selama sistem tersebut mati, ataukah ada beberapa bagian yang belum sesuai, sehingga perlu diperbaiki dan disesuaikan dengan kebutuhan operasional bisnis perusahaan.

3.6.2.2 Simulasi Parsial

Simulasi parsial dilakukan pada proses bisnis sebuah fungsional bisnis perusahaan yang terkait dengan teknologi dan sistem informasi. Simulasi parsial dilakukan hanya pada satu bagian saja, untuk melihat

tanggapan dan penerapan BCP yang dilakukan oleh pengguna ketika terjadi kegagalan sistem pada satu modul atau aktivitas di fungsional bisnis tersebut.

3.7 Dokumentasi BCP

Pendokumentasian tugas akhir adalah hal yang sangat penting, karena dengan adanya pendokumentasian yang rapi dan jelas, akan menjadi acuan yang baik bagi perusahaan. Selain itu, pendokumentasian tugas akhir dilakukan untuk memudahkan peneliti dalam memeriksa kekurangan atau hal-hal yang belum sesuai dengan tujuan atau alur penyusunan tugas akhir.

BAB IV
PROFIL PERUSAHAAN & FORMULASI KERANGKA BCP

Bab ini menjelaskan profil dari perusahaan yang menjadi studi kasus dalam penelitian ini. Perusahaan yang dituju adalah sebuah industri perbankan yaitu BPR (Bank Perkreditan Rakyat) yang bernama BPR Bank Surya Yudha Banjarnegara.

4.1 BPR Bank Surya Yudha Banjarnegara

Studi kasus pada penelitian ini adalah BPR Bank Surya Yudha Banjarnegara. Bank Perkreditan Rakyat ini terletak di Kabupaten Banjarnegara, Jawa Tengah. Semenjak didirikan pada tahun 1992, BPR ini selalu mendapat predikat SEHAT dari Bank Indonesia dan menjadikannya sebagai BPR peringkat pertama se-Jawa tengah dan ketiga se-Indonesia (Infobank, 2011). Berikut ini adalah penjelasan lebih lanjut mengenai BPR Bank Surya Yudha Banjarnegara.

4.1.1 Profil dan Sejarah Perusahaan

BPR Bank Surya Yudha didirikan pada tanggal 12 April 1992 dalam bentuk Perseroan Terbatas berdasarkan izin dari Departemen Keuangan Republik Indonesia No.Kep. 066/KM.13/92. Kehadiran BPR Bank Surya Yudha di tengah-tengah masyarakat menjadi perwujudan dari kebutuhan akan pelayanan jasa perbankan yang lebih baik dengan berbasis budaya masyarakat lokal.

Sebagai sebuah Bank Perkreditan Rakyat, BPR Bank Surya Yudha percaya dengan adanya metode pelayanan perbankan dalam bentuk jemput bola. Melalui pelayanan perbankan ini, BPR Bank Surya Yudha telah berhasil memperoleh perhatian masyarakat luas melalui produk tabungan, deposito dan kredit. Dengan didukung tenaga kerja yang profesional dan produk perbankan yang aman dan menguntungkan, kini BPR Bank Surya Yudha telah menjadi BPR yang terpercaya dan dapat diandalkan.

Upaya restrukturisasi yang mencakup aspek manajemen, karyawan, organisasi, sistem, nilai-nilai dan identitas perusahaan dilakukan secara bertahap oleh perusahaan untuk mendukung pertumbuhan berdasarkan prinsip-prinsip transparansi, tanggung jawab, integritas dan profesionalisme. BPR Bank Surya Yudha secara konsisten terus memperkokoh struktur permodalan dan meningkatkan kinerja keuangannya secara terpadu, untuk terus-menerus mengembangkan pangsa pasarnya.

Selama 20 tahun sejak berdirinya, BPR Bank Surya Yudha senantiasa berupaya membangun dan meningkatkan reputasi serta kepercayaan yang diperoleh dalam kancah industri perbankan. Dimulai dengan Kantor Cabang Utama di Banjarnegara, BPR Bank Surya Yudha kini memiliki jaringan sebanyak 16 kantor cabang, 32 kantor kas dan 1 Payment Point yang tersebar di wilayah Kabupaten Banjarnegara, Purbalingga, Purwokerto, Cilacap dan Pekalongan.

Sejak awal berdirinya, BPR Bank Surya Yudha selalu memperoleh predikat SEHAT dari Bank Indonesia dan pada perayaan 20 tahun melayani masyarakat, per akhir 2012 jumlah total asset BPR Bank Surya Yudha telah mencapai Rp.821,9 milyar yang menjadikannya BPR peringkat pertama Se-Jawa Tengah dan ketiga Se-Indonesia.

Tabel 4. 1 Profil Perusahaan (Sumber: Profil BSY Diolah, 2014)

PROFIL PERUSAHAAN	
Nama Perusahaan	PT. BPR Bank Surya Yudha Banjarnegara
Lokasi Perusahaan	Rejasa, Banjarnegara
Tahun Berdiri	1992
Jenis Usaha	Perbankan (Bank Perkreditan Rakyat)
Status	Perseroan Terbatas
Jumlah Kantor	1 Kantor Pusat, 16 Kantor Cabang, 32 Kantor Kas, 1 Payment Point
Logo Perusahaan	BPR BANK SURYA YUDHA

4.1.2 Visi dan Misi Perusahaan

BPR Bank Surya Yudha menerapkan visi dan misi perusahaan sebagai berikut.

Visi

Menjadi BPR Regional di Jawa Tengah dan terkemuka di Indonesia.

Misi

1. Menjadi infrastruktur keuangan yang berorientasi pada pengembangan UMKM menuju kesejahterahaan bersama rakyat.
2. Suatu organisasi yang terpusat pada nasabah, menawarkan nilai lebih berdasarkan keunggulan pelayanan melalui sumber daya manusia profesional dan teknologi yang mutakhir.
3. Menjadi perusahaan pilihan untuk berkarya dan yang dihormati oleh nasabah, karyawan, pemegang saham, regulator dan komunitas di mana kami berada.

4.1.3 Produk BPR Bank Surya Yudha Banjarnegara

BPR Bank Surya Yudha memiliki produk-produk yang ditujukan untuk meningkatkan pelayanan kepada nasabah secara optimal. Produk-produk ini menjadi sarana pengelolaan dana masyarakat sesuai dengan tujuan pendirian BPR di Indonesia. Berikut ini adalah penjelasan masing-masing produk BPR Surya Yudha yang terdiri dari tabungan, tabungan arisan, deposito dan kredit.

4.1.3.1 Tabungan

Berikut ini adalah produk tabungan dari BPR Bank Surya Yudha Banjarnegara.

1. Tabungan Surya

   Produk tabungan dengan setoran terjangkau yang memberikan kemudahan bertransaksi. Tabungan Surya disajikan dengan memberikan pelayanan tanpa biaya administrasi bulanan, transaksi yang dapat dilakukan di semua kantor, dan penjaminan dana yang dikelola secara profesional oleh Lembaga Penjamin Simpanan (LPS) milik

pemerintah. Produk ini memiliki minimal saldo sebesar Rp 25.000,00.

2. Tabunganku
   Produk tabungan ini ditujukan untuk perorangan Warga Negara Indonesia, yang diselenggarakan secara bersama oleh bank-bank di Indonesia guna menumbuhkan budaya menabung serta meningkatkan kesejahterahaan masyarakat. Tabunganku merupakan produk yang dimiliki oleh perusahaan, di mana diwajibkan setiap bank yang ada di Indonesia untuk memiliki produk Tabunganku. Produk ini memiliki minimal saldo Rp 10.000,00.
3. ATM Tabungan Surya
   Produk tabungan berkualitas dari BPR Bank Surya Yudha yang dikelola secara profesional, aman, terpercaya, menguntungkan dan praktis. Produk ini dilengkapi dengan fasilitas ATM (*Auto Teller Machine*) yang memberikan kemudahan dalam bertransaksi untuk para nasabah bank. Transaksi dapat dilakukan di seluruh Indonesia melalui ATM Bank Syariah Mandiri dan Bank Mandiri.

4.1.3.2 Tabungan Arisan Surya (TAS)

Tabungan Arisan Surya (TAS) adalah produk penggabungan antara tabungan dan deposito. Di mana dana nasabah disimpan dalam bentuk tabungan, tetapi tidak dapat diambil sewaktu-waktu sebelum masa keanggotannya berakhir.

Jangka waktu pelaksanaan TAS selama 36 bulan. Jumlah peserta TAS dibagi ke dalam beberapa kelompok, yang terdiri atas 200 orang, 100 orang dan 50 orang. Pengocokan TAS akan dilaksanakan secara terbuka di depan para peserta, dan menghasilkan 1 nama pemenang. Peserta TAS tidak dikenakan biaya administrasi pada setiap bulannya, namun peserta akan membayar biaya administrasi tutup buku pada setiap akhir tahun sebesar Rp 10.000,00.

4.1.3.3 Deposito

Deposito BPR Bank Surya Yudha adalah simpanan berjangka yang memberikan bunga kompetitif, agar investasi yang dilakukan oleh nasabah memperoleh hasil yang menguntungkan. Produk deposito ini memiliki berbagai pilihan jangka waktu sesuai kebutuhan para nasabah yaitu 1 bulan, 3 bulan, 6 bulan dan 12 bulan.

Suku bunga deposito yang kompetitif menjadikan investasi lebih cepat berkembang. Bunga deposito dapat ditransfer ke rekening tabungan, digabung ke pokok atau penarikan secara tunai. Produk ini pada saat jatuh tempo dapat diperpanjang secara otomatis (*Automatic Roll Over*/ ARO) atau tidak otomatis (non-ARO).

4.1.3.4 Kredit

Produk kredit yang dimiliki mampu bersaing dan memiliki keuntungan lebih kepada para debitur. Perusahaan ini menawarkan suku bunga kredit yang ringan, proses yang cepat dan mengusahakan pelayanan yang optimal untuk para nasabah. Produk kredit di BPR Bank Surya Yudha terdiri dari lima produk yang akan dijelaskan sebagai berikut.

1. Kredit Modal Kerja
   Kredit modal kerja melayani para pengusaha kecil dan menengah di berbagai bidang dalam rangka pengembangan usaha melalui penambahan modal kerja. Produk ini merupakan fasilitas kredit yang diberikan untuk memenuhi kebutuhan akan modal kerja yang habis dalam satu siklus usaha atau kebutuhan modal kerja yang bersifat khusus, seperti pembiayaan persediaan/piutang/proyek atau kebutuhan khusus lainnya, sesuai dengan evaluasi Bank bahwa usaha tersebut layak untuk dibiayai.
2. Kredit Investasi
   Produk ini merupakan kredit yang diberikan untuk membiayai kebutuhan barang modal dalam rangka rehabilitasi, modernisasi, perluasan, pendirian proyek baru atau kebutuhan khusus yang terkait dengan investasi.

3. Kredit Agunan Deposito
   Produk ini merupakan kredit yang diberikan dengan jaminan Bilyet Deposito Berjangka dan/atau tabungan yang diterbitkan oleh BPR Bank Surya Yudha.
4. Kredit Motor
   Kredit kepemilikan sepeda motor dengan berbagai *merk* dan tipe motor yang ditujukan untuk masyarakat umum maupun pegawai dengan fasilitas bunga kecil dan keleluasan penentuan jumlah uang muka dan jangka waktu yang sesuai dengan kemampuan debitur.
5. Kredit Pegawai
   Kredit yang melayani pegawai negeri maupun swasta yang ditujukan untuk memberdayakan penggunaan gaji dengan baik dan bermanfaat secara optimal melalui sistem potong gaji di setiap bulannya.

4.1.4 Prestasi BPR Bank Surya Yudha Banjarnegara

BPR Bank Surya Yudha Banjarnegara mendapatkan beberapa prestasi baik dalam kancah nasional dan internasional. Berikut ini adalah prestasi-prestasi yang diperoleh oleh BPR Bank Surya Yudha, dalam kurun waktu 4 tahun terakhir.

1. Penghargaan dari Kantor Pelayanan Pajak Pratama Purbalingga sebagai wajib pajak pembayar terbesar tahun 2011, Kategori Badan Hukum.
2. Predikat A dari MICRA (*Microfinance Institution Rating and Investor Report/International Professional Rating Institution*) tahun 2011.
3. Predikat "Sangat Bagus" atas Kinerja Keuangan dari INFOBANK BPR Award tahun 2011.
4. Predikat A dari MICRA (*Microfinance Institution Rating and Investor Report/International Professional Rating Institution*) tahun 2010.
5. Predikat "Sangat Bagus" atas Kinerja Keuangan dari INFOBANK BPR Award tahun 2010.
6. Best Information Technology Award pada Asia Pacific Conference and Exhibition JCC Jakarta tahun 2010.

7. Best Performance Award pada Asia Pacific Conference and Exhibition JCC Jakarta tahun 2010.

4.2 Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara

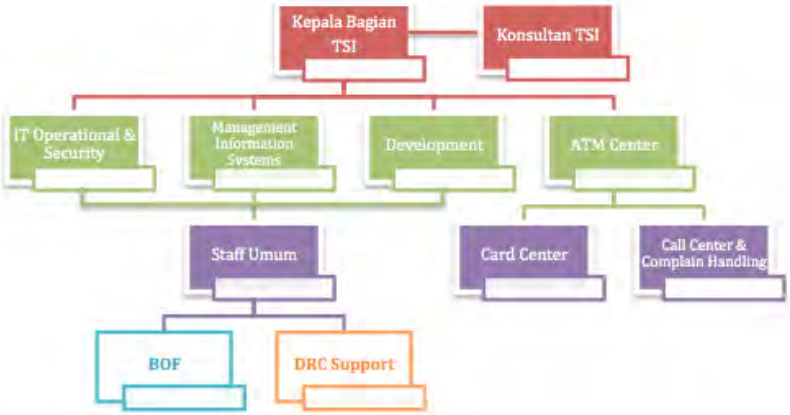
Pada penelitian ini, Bagian Teknologi dan Sistem Informasi menjadi bagian utama Teknologi dan Sistem Informasi diyakini dapat memperkuat daya saing industri perbankan. BPR Bank Surya Yudha memutuskan untuk melakukan investasi teknologi informasi sejak tahun 2006, yang diawali dengan implementasi buku tabungan yang dilengkapi dengan sistem *passbook*, hingga implementasi sistem *Core Banking* yang *real time* dan *online* pada tahun 2009, dengan menggunakan mesin IBM AS-400 *i-series* dan aplikasi *Win Core.*

Bagian Teknologi dan Sistem Informasi (TSI) memegang peranan penting dalam perusahaan. Bagian yang beranggotakan 11 karyawan ini, berada di bawah pimpinan dewan direksi, yaitu Direktur Umum (Non-Kredit). Meskipun menjadi salah satu bagian yang termuda di BPR Bank Surya Yudha Banjarnegara, Teknologi dan Sistem Informasi telah menyumbangkan prestasi yang sangat membanggakan untuk perusahaan ini di tingkat Asia-Pasifik. Berkat kerja sama yang solid, kategori "*Best Information Technology Award"* berhasil diraih pada *Asia Pacific Conference and Exhibition* pada tahun 2010 di Jakarta.

4.2.1 Struktur Organisasi

Sumber daya manusia menjadi bagian yang sangat penting dalam implementasi teknologi dan sistem informasi di perusahaan. Karena meskipun perusahaan memiliki teknologi dan sistem yang canggih, apabila tidak didukung dengan sumber daya manusia yang peduli dan dapat mengimplementasi teknologi dan sistem dengan baik, maka investasi yang dilakukan tidak dapat berjalan secara optimal. Berikut ini adalah susunan sumber daya manusia atau struktur organisasi yang mendukung bagian

Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara.



Gambar 4. 1 Struktur Organisasi TSI BPR Bank Surya Yudha Banjarnegara (Sumber: Struktur TSI Diolah, 2014)

4.2.2 Fungsi Bagian TSI

Bagian Teknologi dan Sistem Informasi pada perusahaan ini memiliki tugas untuk mengadakan teknologi dan sistem informasi yang sesuai dengan kebutuhan proses bisnis di setiap bagian perusahaan. Proses bisnis yang berjalan di bagian ini terdapat di beberapa bagian yaitu:

4.2.2.1 Perencanaan dan Pengembangan Sistem

Aplikasi yang diimplementasikan pada perusahaan ini, sebagian besar dirancang dan dikembangkan secara mandiri (*in-house*). Bagian TSI selalu berupaya untuk dapat memenuhi kebutuhan teknologi dan sistem informasi dari setiap fungsional bisnis perusahaan, dengan adanya sebuah forum yang bernama *IT Steering Committee* (ITSC). Dalam forum tersebut, akan dibahas mengenai usulan aplikasi atau infrastruktur (kebutuhan teknologi informasi) yang dapat mendukung proses bisnis dari setiap fungsional bisnis yang ada serta pemantauan pengembangan dan proses bisnis teknologi informasi yang berjalan.

Forum ITSC dihadiri oleh pimpinan TSI, Dewan Direksi, beserta pimpinan fungsional bisnis yang terkait.

Bagian TSI membuat Rencana Kerja Jangka Pendek dan Jangka Panjang, yang dapat digunakan sebagai acuan dalam menjalankan tugas selama beberapa waktu ke depan, serta menjadi sebuah bukti perencanaan serta pengembangan teknologi dan sistem informasi pada BPR Bank Surya Yudha Banjarnegara.

4.2.2.2 Operasional Teknologi Informasi dan Keamanan Jaringan

Untuk menghasilkan pelayanan teknologi informasi yang optimal, hal ini didukung dengan adanya kegiatan operasional yang terkait dengan proses bisnis bagian TSI dan keamanan jaringan yang akan melindungi sistem dari serangan internal maupun eksternal.

Kegiatan operasional teknologi informasi terkait dengan beberapa fungsional bisnis, seperti bagian operasional, kredit, pembukuan, personalia dan bagian umum. Kegiatan ini merupakan proses bisnis yang terdapat di masing-masing fungsional bisnis yang ada, dengan bantuan teknologi dan sistem informasi yang ada.

Infrastruktur jaringan menjadi perhatian pihak manajemen TSI. Hal ini disebabkan oleh sistem perbankan yang berbasis *real-time* dan *online*. Dengan adanya infrastruktur jaringan yang teruji keamanannya, akan mengoptimalkan pelayanan bank kepada nasabah dan melancarkan seluruh proses bisnis perbankan yang terkait dengan teknologi dan sistem informasi.

Untuk mendukung keamanan jaringan, BPR Bank Surya Yudha berusaha membangun topologi jaringan yang sesuai untuk melayani hubungan koneksi antara kantor pusat, 16 kantor cabang, 32 kantor kas dan 1 *payment point*. Topologi jaringan yang dibuat juga akan menghubungkan antara BPR Bank Surya Yudha dengan Kantor Pusat Bank Indonesia di Jakarta.

4.2.2.3 Management Information Systems (MIS)

Bagian Teknologi dan Sistem Informasi (TSI) memiliki sebuah fungsi yang bertugas untuk mengelola seluruh informasi yang dibutuhkan oleh pihak perbankan, baik secara internal maupun eksternal. Fungsi ini bernama *Management Information Systems* (MIS). Informasi yang dikelola dapat digunakan sebagai penentu pengambilan keputusan oleh pihak manajemen perbankan. MIS menjadi fungsi yang begitu penting dalam sebuah perusahaan khususnya bagi perbankan, di mana perbankan memiliki *stakeholder* atau keterkaitan dengan banyak pihak, seperti Bank Indonesia, Kantor Pajak, nasabah, pemerintah, sektor lembaga keuangan dan pihak terkait lainnya.

4.2.2.4 Automatic Teller Machine (ATM)

Automatic Teller Machine (ATM) adalah salah satu pengembangan produk berbasis teknologi informasi untuk meningkatkan kualitas pelayanan kepada para nasabah bank. Fasilitas ATM dibangun dengan bekerja sama secara aktif dengan Bank Syariah Mandiri (BSM) melalui *co-branding* ATM.

4.2.3 Perangkat Kerja Bagian TSI

Bagian TSI memiliki beberapa perangkat keras dan perangkat lunak yang mendukung fungsi dari bagian ini serta *Data Center* di mana *Server* AS/400, *Server PC* dan peralatan jaringan ditempatkan.

4.2.3.1 Advance Systems 400 (AS-400)

Proses bisnis perbankan yang tidak lagi dapat dipisahkan dari teknologi dan sistem informasi membuat perusahaan ini selalu berusaha untuk mengembangkan bidang tersebut. Teknologi dan sistem informasi yang digunakan adalah mesin *Advance Systems 400* atau AS-400. Mesin ini digunakan untuk menjalankan aplikasi *core banking systems*. Mesin AS-400 dibedakan menjadi tiga kategori, yaitu perangkat lunak, perangkat keras dan *database*.

1. Perangkat Lunak

Pada kategori perangkat lunak, AS-400 memliki Operating System 400 (OS/400) dan beberapa bahasa pemrograman seperti RPG, COBOL dan C. OS/400 adalah salah satu sistem operasi yang dibuat untuk mengaplikasikan data yang spesifik pada sektor tertentu, seperti perbankan. Efisiensi pekerjaan menjadi hal yang diutamakan pada sistem operasi ini, karena sistem ini akan membantu untuk mempermudah proses bisnis yang ada di perusahaan serta memiliki sistem keamanan yang sangat andal hingga saat ini.

Jangkauan AS-400 dinilai sangat luas, karena dirancang secara khusus untuk dapat membaca semua bahasa komputer maupun sistem lain. AS-400 juga dapat mengakses produk-produk lain seperti ATM, *Mobile Banking* dan ATM Bersama yang terhubung secara *online* dengan jarak yang sangat jauh.

2. Perangkat Keras
   Perangkat keras mesin AS-400 memiliki tipe sistem power 520 Double Processor 4300 CPW (*Commercial Processing Workload / sebanding dengan cpu speed 4,3 GigaHertz*), 32 GB RAM, 28X139.5 HDD dan OS V5R4. Perangkat keras yang digunakan berupa mesin AS-400, Monitor AS-400 dan Printer AS-400. Mesin ini digunakan oleh hampir seluruh Bank Umum maupun Bank Asing di seluruh dunia.
3. Database
   AS-400 memiliki database yang disebut DB/2. Kemampuan database ini di atas database yang biasa digunakan pengembang PC seperti MySql, SQL, Oracle. Dapat menyimpan data yang besar dan mempunyai kecepatan akses yang tinggi. Sehingga sangat cocok untuk aplikasi perbankan yang juga didukung dengan keamanan data yang handal serta mempunyai integritas data yang sangat baik.

4.2.3.2 Aplikasi WinCore

WINCore adalah aplikasi yang terintegrasi, fleksibel, terbuka dan merupakan *real-time online core banking systems* yang memiliki tingkat pengawasan terbaik untuk mendukung

operasional perbankan (Forex dan Non-Forex Bank). WINCore Sistem Perbankan didesain dan dikembangkan berdasarkan beberapa konsep sebagai berikut.

1. *Customer Relationship Management*
2. Fleksibel (tabel parameter)
3. *User-friendly* (mudah digunakan oleh pengguna)
4. Terbuka (mudah diintegrasikan dengan pihak ketiga sistem)
5. *Scalable* (dapat ditingkatkan selama pertumbuhan bank)
6. Pemenuhan dan pendukung regulasi Bank Indonesia
7. *Report Design Generator*
8. *Online and Real-time Processing*
9. Pemantauan dan keamanan sistem.

Aplikasi WINCore yang berjalan pada mesin teknologi IBM i-*Series* bersifat terbuka, yaitu mudah untuk dihubungkan dengan sistem yang lain seperti *tax-online*, *host-to-host* dengan pihak pembayaran seperti PLN dan Telkom, sistem *ATM Switching* serta layanan ATM Bersama.

Aplikasi ini dinilai memiliki tingkat keamanan yang tinggi, karena didukung oleh IBM *i-Series* yang teruji keamanannya dari ancaman virus hingga saat ini. Selain itu, aplikasi ini dapat dijalankan dari model terkecil IBM *i-Series* hingga model terbesar, serta dapat disesuaika modelnya sesuai dengan pertumbuhan bank.

4.2.3.3 Aplikasi Non-Core Banking

Aplikasi yang ada pada BPR Bank Surya Yudha menjadi tanggung jawab penuh Bagian TSI. Hingga tahun 2014, ada beberapa aplikasi yang telah dikembangkan, direncanakan dan saat ini sedang dalam masa tunggu. Aplikasi-aplikasi ini merupakan aplikasi yang mendukung proses bisnis dari fungsional bisnis lain yang ada di perusahaan. Aplikasi ini berada di luar dari pengembangan aplikasi dari mesin AS-400.

Aplikasi *non-core banking* yang dikembangkan oleh bagian TSI adalah sebagai berikut.

Tabel 4. 2 Aplikasi Non-Core Banking (Sumber: TSI BSY Diolah, 2014)

APLIKASI PENDUKUNG	FUNGSIONAL BISNIS	STATUS
Human Resource Department (HRD)	Personalia	Tahap Modifikasi
Salary Systems	Personalia	Tahap Implementasi
SVS (Signature Verfication Systems)	Operasional	Tahap Instalasi
Suspicious Transaction ATM	ATM Center	Tahap Pengembangan
Rekonsiliasi	ATM Center, Pembukuan	Tahap Pengembangan
Inventori	Umum	Tahap Pengembangan
Aplikasi SKAI (Satuan Kerja Audit Intern)	SKAI	Tahap Pengembangan
Mobile Banking	Nasabah	Tahap Pengembangan

4.2.3.4 Data Center

Data center AS-400 berfungsi untuk menempatkan sistem komputer dan komponen yang terkait, seperti Server AS-400, perangkat jaringan, sistem telekomunikasi dan penyimpanan data. Selain itu fasilitas ini juga berfungsi untuk menempatkan *power supply* serta alat pengontrol lingkungan seperti *Air Conditioner* (AC) maupun ventilasi udara.

4.3 Fungsional Bisnis dan Proses Bisnis BPR Bank Surya Yudha Banjarnegara

BPR Bank Surya Yudha memilliki fungsional bisnis yang digunakan untuk mencapai tujuan perusahaan. Puncak tertinggi di perusahaan ini adalah keputusan RUPS (Rapat Umum Pemegang Saham), Komisaris, Dewan Direksi, dan selanjutnya merupakan fungsional bisnis yang dibagi menjadi kantor cabang dan kantor kas yang berada di bawah Kawil (Kepala Wilayah), serta divisi, bagian dan seksi yang berada di kantor pusat.

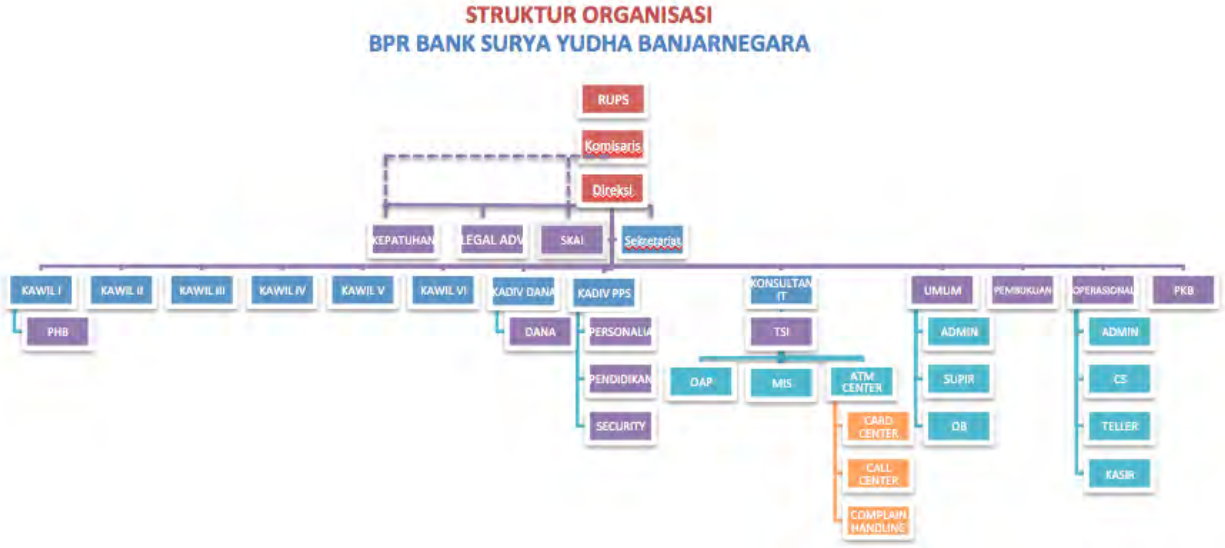
Kepala Wilayah dibagi menjadi 5, berdasarkan pembagian wilayah jangkauan BPR Bank Surya Yudha Banjarnegara. Berikut ini adalah pembagian tugas dari masing-masing Kepala Wilayah.

- KAWIL I : membawahi bagian PHB (Pengembangan Hubungan Bank Kelompok Instansi dan Sekolah), Kantor Cabang Utama, Singamerta dan Pasar Besar, beserta kantor kas di sekitar wilayah tersebut.
- KAWIL II : membawahi Kantor Cabang Klampok, Purwonegoro, Mandiraja, Wanadadi beserta kantor kas di sekitar wilayah tersebut.
- KAWIL III : membawahi Kantor Cabang Batur, Karangkobar, Dieng, Pagentan beserta kantor kas di sekitarnya.
- KAWIL IV : membawahi Kantor Cabang Kalibening, Pekalongan beserta kantor kas di sekitarnya.
- KAWIL V : membawahi Kantor Cabang Purbalingga, Bobotsari beserta kantor kas di sekitarnya.
- KAWIL VI : membawahi Kantor Cabang Purwokerto, Cilacap beserta kantor kas di sekitarnya.

Perusahaan ini memiliki fungsional bisnis yang dibagi menjadi bagian, divisi dan seksi yang berada terpusat di Kantor Pusat BPR Bank Surya Yudha Banjarnegara. Bagian, divisi dan seksi yang menjalankan fungsinya di perusahaan ini adalah:

Tabel 4. 3 Fungsional Bisnis BPR Bank Surya Yudha Banjarnegara (Sumber: Peneliti, 2014)

Divisi	1. Dana
	2. PPS (Personalia, Pendidikan dan Security)
Bagian	1. Kepatuhan
	2. Legal Advisor
	3. SKAI (Satuan Kerja Audit Intern)
	4. PHB (Pengembangan Hubungan Bank Kelompok Instansi dan Sekolah)
	5. Personalia
	6. Pendidikan
	7. Security
	8. TSI (Teknologi dan Sistem Informasi)
	9. Umum
	10. Pembukuan
	11. Operasional
	12. (PKB) Penyselesaian Kredit Bermasalah
Seksi	1. OAP (Operasional PC, AS400, Pengembangan)
	2. MIS *(Management Information Systems)*
	3. ATM Center (*Auto Teller Machine*)



Gambar 4. 2 Struktur Organisasi BSY (Sumber: Struktur Organisasi BPR Bank Surya Yudha Diolah, 2014)

4.3.1 Fungsional Bisnis yang Terlibat dalam Penelitian

Pada penelitian ini hanya 5 fungsional bisnis yang dilibatkan dalam penyusunan BCP perusahaan, yaitu bagian TSI, Pembukuan, Personalia, Operasional dan Kredit. Alasan pemilihan 5 fungsional bisnis ini adalah berdasarkan tingkat ketergantungan proses bisnis yang berada di masing-masing fungsional tersebut. Kelima fungsional bisnis ini memiliki tingkat ketergantungan yang tinggi terhadap layanan teknologi dan sistem informasi yang ada, terutama dalam sistem *core* banking. Fungsional bisnis yang terkait dalam pembuatan BCP di penelitian ini adalah:

1. Teknologi dan Sistem Informasi
   Bagian teknologi dan sistem informasi berfungsi sebagai penyedia dan pemelihara layanan teknologi informasi dan sistem informasi yang ada di perusahaan. Bagian ini bertanggung jawab penuh kepada pengembangan layanan teknologi dan sistem informasi yang ditujukan untuk internal maupun eksternal perusahaan, serta memastikan operasional bank dapat berjalan lancar atau sebagai *helpdesk* jika terjadi permasalahan teknologi dan sistem informasi di sisi pengguna.
2. Operasional
   Bagian operasional terkait dengan proses bisnis sehari-hari yang dilakukan oleh bank sebagai bentuk pelayanan kepada nasabah. Bagian operasional terkait secara langsung dengan produk bank seperti pembukaan rekening bank, tabungan, kredit dan deposito.
3. Pembukuan
   Bagian pembukuan merupakan bagian yang terkait dengan neraca keuangan bank dan segala bentuk aktivitas pembukuan yang ada di bank. Bagian ini juga bertanggungjawab terhadap pelaporan bulanan ke Bank Indonesia maupun ke kantor Pajak. Selain itu, bagian pembukuan memiliki kewajiban untuk melakukan pemantauan dan penyelesaian transaksi antar bank.

4. Kredit
   Bagian kredit adalah bagian yang mengelola pelayanan dan pemantauan kredit kepada para debitur.
5. Personalia
   Bagian personalia adalah bagian yang bertugas untuk mengurus sumber daya manusia yang terlibat dalam aktivitas dan proses bisnis bank secara internal.

4.3.2 Proses Bisnis yang Terlibat dalam Penelitian

Berdasarkan kelima fungsional bisnis yang telah disebutkan sebelumnya, pada bagian ini akan dijelaskan mengenai proses bisnis yang terkait dengan sistem, yang terdapat pada masing-masing fungsional bisnis yang ada. Proses bisnis yang akan dijelaskan merupakan, proses-proses yang memiliki ketergantungan sangat tinggi terhadap teknologi dan sistem informasi secara langsung, dan berdampak terhadap kesehatan bank serta pelayanan kepada nasabah. Berikut ini adalah proses bisnis dari masing-masing fungsional bisnis yang ada.

Tabel 4. 4 Proses Bisnis yang Terlibat (Sumber: Peneliti, 2014)

FUNGSIONAL BISNIS	PROSES BISNIS TERKAIT SISTEM
TSI	Proses End-of-Day
	Input Tabel Parameter
	Modul User AS400
	LAPBUL (Laporan Bulanan)
	Sistem Informasi Debitur (SID)
	Pemasangan Perangkat Jaringan
	Disaster Recovery Center (DRC)
	Perawatan Perangkat Keras
Operasional	Input Data Nasabah
	Tarik Tunai
	Setoran Tunai
	Pembukaan Tabungan
	Pembukaan Deposito dan Realisasi Kredit
	Pembayaran Angsuran

FUNGSIONAL BISNIS	PROSES BISNIS TERKAIT SISTEM
Pembukuan	Pemindahbukuan Rekening Internal
	Pemindahbukuan Multi Jurnal
	Posting Backdate
	Pembentukan PPAP
	Pembentukan Amortisasi
	Neraca
	LAPBUL (Laporan Bulanan)
Kredit	Informasi Kolektabilitas dan NPL
	Sub Modul LAPBUL
	Sistem Informasi Debitur (SID)
Personalia	Pengelolaan Data Karyawan
	Sistem Penggajian Karyawan

4.4 Formulasi Kerangka Kerja BCP BPR Bank Surya Yudha Banjarnegara

Untuk melakukan formulasi kerangka kerja *Business Continuity Plan* di BPR Bank Surya Yudha Banjarnegara, peneliti menggunakan pendekatan mundur. Pendekatan mundur di sini berarti, peneliti berusaha menggali kebutuhan dan keinginan dari pihak perusahaan terlebih dahulu. Kebutuhan yang digali berdasarkan keinginan dari pihak manajemen, khususnya bagian Teknologi dan Sistem Informasi (TSI) selaku penanggung jawab pengembangan teknologi informasi di perusahaan ini. Kebutuhan ini diambil dari Rencana Jangka Panjang Teknologi Sistem Informasi BPR Bank Surya Yudha Banjarnegara yang dibuat pada tahun 2013.

Setelah melakukan penggalian kebutuhan dan keinginan perusahaan, langkah berikutnya adalah peneliti melakukan penyesuaian dengan studi komparasi kerangka kerja BCP yang dilakukan, dalam kasus ini adalah komparasi terhadap ISO 22301:2012, *Bank of Japan* dan *Dutch Financial Sector.* Dengan adanya penggabungan antara studi komparasi kerangka kerja BCP

dengan kebutuhan dan keinginan perusahaan tersebut, maka akan dihasilkan sebuah kerangka kerja BCP yang sesuai dengan kebutuhan BPR Bank Surya Yudha Banjarnegara. Berikut ini adalah skema pendekatan mundur pada penelitian ini.

Gambar 4. 3 Skema Pendekatan Mundur (Sumber: Peneliti, 2014)

4.4.1 Penggalian Kebutuhan Perusahaan

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

1. Wawancara dengan pimpinan di bagian TSI.

2. Penyesuaian dengan Rencana Jangka Panjang Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara.

Berikut ini adalah hasil dari penggalian kebutuhan perencanaan keberlanjutan bisnis BPR Bank Surya Yudha Banjarnegara.

Tabel 4. 5 Kebutuhan Perusahaan (Sumber: Peneliti, 2014)

KEBUTUHAN DAN KEINGINAN PERUSAHAAN	STATUS
1. BCP yang dibuat harus mencakup risiko di bidang teknologi informasi di perusahaan.	Terverifikasi
2. BCP yang dibuat harus dapat mengurangi risiko yang timbul dari implementasi teknologi informasi.	Terverifikasi
3. BCP yang dibuat dapat digunakan dalam waktu jangka panjang.	Terverifikasi
4. BCP yang dibuat harus memperhatikan aspek kemudahan dan kesederhanaan desain.	Terverifikasi
5. BCP yang dibuat harus dapat sesuai dengan teknologi yang sudah diterapkan.	Terverifikasi
6. BCP yang dibuat harus melibatkan perusahaan, dalam hal Sumber Daya Manusia (SDM) secara utuh.	Terverifikasi
7. BCP yang dibuat harus memperhatikan keberlanjutan operasional bisnis perusahaan.	Terverifikasi
8. BCP yang dibuat untuk perbankan, harus dapat mengatasi kebutuhan sistem keamanan yang tinggi di perusahaan.	Terverifikasi
9. BCP yang dibuat harus dapat mendukung tata kelola teknologi informasi yang diterapkan di perusahaan (prosedur di DRC, DRP dan *Contingency Plan*).	Terverifikasi
10. BCP yang dibuat harus dinamis, yaitu dapat mengikuti perkembangan dunia teknologi informasi.	Terverifikasi

Dokumen tersebut telah diverifikasi oleh pihak Pimpinan Bagian TSI BPR Bank Surya Yudha Banjarnegara, dengan menggunakan surat verifikasi yang dibuat oleh peneliti, yang terdapat dalam Lampiran A Halaman A-1.

4.4.1.1 Verifikasi Penggalian Kebutuhan Perusahaan

Berdasarkan kebutuhan yang telah digali di atas, verifikasi dilakukan untuk memastikan keabsahan penyusunan BCP. Verifikasi dilakukan dengan metode penyesuaian dengan rencana jangka panjang teknologi dan sistem informasi BPR Bank Surya Yudha Banjarnegara. Di samping itu, untuk memperkuat kebenaran penelitian, peneliti akan mengajukan surat kesesuaian kebutuhan dan keinginan perusahaan (konfirmasi) kepada pimpinan bagian TSI. Berikut ini adalah pemetaan kesesuaian kebutuhan dan keinginan perusahaan dengan isi kebijakan dan Rencana Jangka Panjang Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara.

Gambar 4. 4 Pemetaan Kebutuhan dengan Isi Kebijakan (1) (Sumber: Peneliti diadopsi dari Rencana Jangka Panjang TSI, 2014)

Gambar 4. 5 Pemetaan Kebutuhan dan Isi Kebijakan (2) (Sumber: Sumber: Peneliti diadopsi dari Rencana Jangka Panjang TSI, 2014)

Untuk memastikan kebenaran dari kebutuhan perusahaan tersebut, maka peneliti mengajukan surat konfirmasi kesesuaian kepada pihak pimpinan bagian TSI, yang akan dilampirkan pada Lampiran A Halaman A-1.

4.4.2 Sintesis Kerangka Kerja BCP

Metode yang digunakan dalam penyusunan kerangka BCP dalam penelitian ini adalah melakukan sintesis dari masing-masing kerangka BCP yang digunakan sebagai literatur, untuk disesuaikan dengan kebutuhan dan keinginan perusahaan.

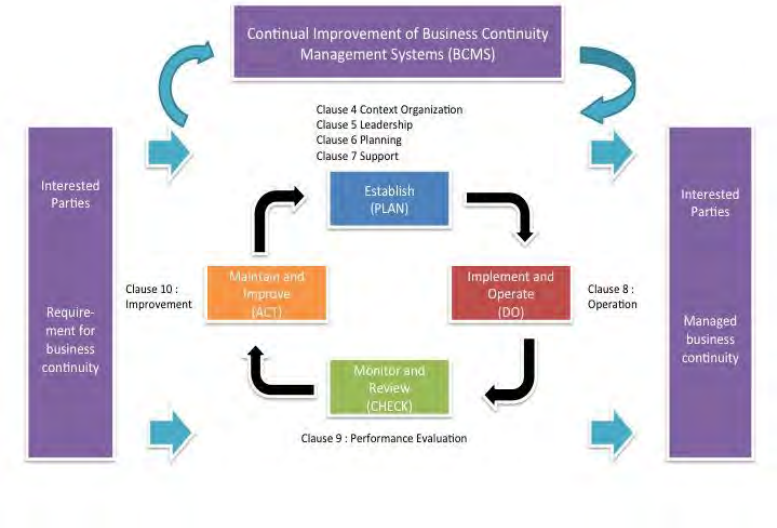
Penjelasan dari masing-masing kerangka kerja standar yang digunakan sebagai studi komparasi terdapat pada Bab II Tinjauan Pustaka di buku penelitian ini. Sintesis dan analisis dilakukan dengan menggunakan model atau kerangka dari beberapa standar yaitu berdasarkan ISO 22301:2012, *Bank of Japan* dan *Dutch*

Financial Sector. Berikut ini adalah kerangka BCP yang digunakan sebagai acuan dalam penelitian ini untuk menyusun kerangka BCP yang sesuai dengan BPR Bank Surya Yudha Banjarnegara.

4.4.2.1 ISO 22301:2012

ISO 22301:2012 adalah sebuah kerangka BCMS (*Business Continuity Management Systems*) atau sebuah sistem pengelolaan keberlanjutan bisnis, yang terpetakan menjadi model PDCA (*Plan-Do-Check-Act*). Model ini dianggap sebagai suatu bentuk model keberlanjutan bisnis yang cukup komprehensif, di mana perusahaan dapat terus melakukan peningkatan secara terus-menerus (*Continuous Improvement)* yang dapat meningkatkan kualitas model itu sendiri.

Pada standar internasional ini, pelaksanaan BCP dimulai dari klausa 4 hingga klausa ke-10, yang terpetakan ke dalam setiap fase (lihat selengkapnya di Bab II Tinjauan Pustaka).



Gambar 4. 6 Model PDCA ISO 22301:2012 (Sumber: ISO 22301:2012 Diolah, 2014)

Berikut ini adalah penjelasan dari masing-masing fase model PDCA yang berisi klausa-klausa yang dapat digunakan untuk melakukan implementasi BCP di perusahaan.

Gambar 4. 7 Rincian Fase PDCA (Sumber: ISO 22301:2012 diolah, 2014)

Pewarnaan seperti pada gambar di atas menunjukkan bahwa dalam penelitian ini, peneliti mengklasifikasikan setiap fase PDCA menjadi beberapa warna, yaitu sebagai berikut.

Gambar 4. 8 Pemberian Warna pada Fase PDCA (Sumber: Peneliti 2014)

Kelebihan dari kerangka BCP ini adalah ISO 22301:2012 adalah sebuah kerangka yang komprehensif, di mana pada setiap fasenya memiliki proses-proses yang melingkupi seluruh lini dari sebuah proses keberlanjutan bisnis di perusahaan.

Namun, kerangka ini tidak bisa sepenuhnya langsung diimplementasikan di BPR Bank Surya Yudha Banjarnegara, karena salah satu kebutuhan di perusahaan tersebut menyatakan bahwa kerangka BCP yang dibuat harus sederhana dan mudah dimengerti. Hal ini tidak sesuai dengan kondisi kerangka ini melihat tingkat kompleksitas yang begitu tinggi dan konteks kalimat yang terlalu teoritis membuat kerangka ini tidak nampak sederhana dan sulit untuk dimengerti oleh orang awam.

4.4.2.2 Bank of Japan

Bank of Japan (BOJ) membuat sebuah kerangka kerja untuk melakukan BCP pada institusi keuangan yang ada di Jepang. Kerangka BCP yang dimiliki oleh *Bank of Japan* terlihat lebih operasional, jika dibandingkan dengan ISO 22301:2012, di mana institusi ini menjelaskan setiap fasenya secara lebih teknis.

Hal ini dipengaruhi oleh sudut pandang *Bank of Japan* terhadap suatu BCP untuk bisa memelihara aktivitas ekonomi masyarakat sekitar bencana. Di mana, kondisi ini adalah kondisi yang cukup kritis untuk ditangani. Sehingga BOJ berupaya untuk dapat memulihkan kondisi operasional kritis di perusahaan secara efektif dan efisien. Berikut ini adalah fase dari kerangka BCP di *Bank of Japan* (selengkapnya lihat Bab II Tinjauan pustaka).

Gambar 4. 9 Kerangka Kerja BCP Bank of Japan (Sumber: Bank of Japan Diolah, 2014)

Pada dasarnya kerangka ini sudah cukup operasional dan cukup sesuai dengan implementasi di dunia perbankan. Namun kerangka ini tidak bisa sepenuhnya diimplementasikan secara langsung tanpa pengubahan di BPR Bank Surya Yudha Banjarnegara. Hal ini dikarenakan, adanya kebutuhan BPR Bank Surya Yudha Banjarnegara yang menyatakan bahwa kerangka BCP yang dibuat harus dinamis dengan perkembangan teknologi informasi atau dengan kata lain perlu adanya upaya untuk melakukan peningkatan secara terus-menerus (*continuous improvement*) dalam fase BCP yang akan diimplementasikan di perusahaan tersebut.

Jika dibandingkan dengan kerangka sebelumnya, kerangka ini hanya mencakup fase perencanaan (*plan*), pengerjaan (*do*) dan sebagian pemeriksaan (*check*) saja, yaitu hanya sampai tahap pengujian dan peninjauan. Dalam kerangka ini belum terdapat

fase tindakan (*act*) untuk melakukan peningkatan secara terus-menerus yang sesuai dengan kebutuhan perusahaan.

4.4.2.3 Dutch Financial Sector

Dutch Financial Sector adalah sebuah asosiasi institusi keuangan yang ada di Belanda. Institusi ini menyusun sebuah kerangka keberlanjutan bisnis untuk institusi keuangan. Kerangka ini terlihat lebih sederhana dan lebih mudah untuk dipahami. Penyajiannya dokumen pun dipaparkan dengan cukup sederhana, dengan hanya menampilkan poin-poin yang merupakan fase yang bisa dilakukan dalam proses keberlanjutan bisnis. Berikut adalah kerangka BCP dari *Dutch Financial Sector* (selengkapnya lihat Bab II Tinjauan Pustaka).

Gambar 4. 10 Kerangka Kerja BCP Dutch Financial Sector (Sumber: Dutch Financial Sector Diolah, 2014)

BPR Bank Surya Yudha tidak dapat secara langsung mengimplementasikan kerangka ini di perusahaan. Hal ini dikarenakan adanya beberapa unsur dari kebutuhan perusahaan yang belum terdapat di kerangka ini, seperti kebutuhan untuk pembahasan khusus mengenai konteks perusahaan, sumber daya yang dibutuhkan serta belum adanya fase tindakan (*act*) untuk melakukan peningkatan secara terus-menerus (*continuous improvement*).

Baik kerangka BCM atau BCP yang dijadikan sebagai studi analisis dan sintesis memiliki kelebihan dan kekurangan pada masing-masing bagian. Untuk menghasilkan kerangka terbaik yang juga sesuai dengan kebutuhan perusahaan yang akan dilibatkan dalam penelitian ini, peneliti berusaha menyusun kerangka yang sesuai berdasarkan hasil sintesis ketiga standar kerangka yang digunakan, yang akan disesuaikan dengan kebutuhan dan keinginan perusahaan terkait keberlanjutan bisnis di BPR Bank Surya Yudha Banjarnegara.

Dari ketiga standar kerangka BCP yang dijadikan acuan dalam penelitian ini, peneliti menghasilkan sebuah kesimpulan berdasarkan ISO 22301:2012, hal yang dapat diimplementasikan adalah berdasarkan penerapan model PDCA dan tata urutan penyusunan BCP yang komprehensif. Dari Bank of Japan, peneliti dapat mengambil isi yang terdapat di beberapa fase yang ada, terutama perihal alur komunikasi, serta dari *Dutch Financial Sector* hal yang paling berbeda adalah perihal fondasi tata kelola teknologi informasi yang harus didirikan di dalam suatu BCP di perusahaan. Hal ini akan digunakan sebagai bahan, untuk melakukan formulasi dan kesesuaian antara ketiga standar tersebut dengan kebutuhan keberlanjutan bisnis yang dimiliki oleh perusahaan.

4.4.3 Kesesuaian Kerangka Kerja BCP BPR Bank Surya Yudha Banjarnegara dengan Kebutuhan Perusahaan

Peneliti melakukan pemetaan terhadap kebutuhan perusahaan dengan sebuah model iteratif manajemen, yang dikenal dengan nama Model PDCA (*Plan-Do-Check-Act*) atau

Deming Cycle atau *Shewart Cycle*. Model PDCA dipopulerkan oleh Dr. W. Edwards Deming, yang dikenal sebagai bapak *modern quality control* atau pengawasan kualitas moderen (Chris, 2011). Alasan pemilihan bentuk model ini adalah, karena ini akan memudahkan perusahaan dalam memantau, mengembangkan serta mengingat fase dari kerangka kerja BCP yang harus ditingkatkan secara terus-menerus untuk mendapatkan performa yang optimal. Selain itu, oleh karena risiko selalu berkembang dan perkembangan teknologi informasi yang sangat cepat dan dinamis, hal ini membutuhkan peran perusahaan yang selalu mau berkembang dan meningkatkan kualitas secara terus-menerus.

Jika diperhatikan kebutuhan yang diinginkan oleh perusahaan, maka kebutuhan tersebut dapat dibagi menjadi 4 fase yaitu, perencanaan (*plan*), pengerjaan (*do*), pemeriksaan *(check*) dan tindakan *(act*). Berikut ini adalah pemetaan kesesuaian kerangka kerja BCP dengan Kebutuhan Perusahaan.

Tabel 4. 6 Kesesuaian Kerangka Kerja dengan Kebutuhan Perusahaan (Sumber: Peneliti, 2014)

FASE	KEBUTUHAN PERUSAHAAN	KERANGKA BCP
PLAN	BCP yang dibuat harus melibatkan perusahaan, dalam hal Sumber Daya Manusia (SDM) secara utuh.	Profil Perusahaan
		SDM (Karyawan dan Pimpinan) yang terlibat
	BCP yang dibuat harus dapat mendukung tata kelola teknologi informasi yang diterapkan di perusahaan	Tata Kelola Teknologi Informasi
	BCP yang dibuat harus dapat sesuai dengan teknologi yang sudah diterapkan.	Perangkat Sumber Daya
DO	BCP yang dibuat harus mencakup risiko di bidang teknologi informasi	Analisis Dampak Bisnis

FASE	KEBUTUHAN PERUSAHAAN	KERANGKA BCP
	di perusahaan.	Manajemen Risiko
	BCP yang dibuat harus dapat mengurangi risiko yang timbul dari implementasi teknologi informasi.	Penilaian Risiko
		Perlakuan Risiko (Mitigasi)
	BCP yang dibuat harus memperhatikan keberlanjutan operasional bisnis perusahaan.	Prosedur Keberlanjutan Bisnis
	BCP yang dibuat untuk perbankan, harus dapat mengatasi kebutuhan sistem keamanan yang tinggi di perusahaan.	Prosedur Keamanan Informasi
CHECK	BCP yang dibuat dapat digunakan dalam waktu jangka panjang.	Peninjauan Manajemen
		Internal Audit
ACT	BCP yang dibuat harus dinamis, yaitu dapat mengikuti perkembangan dunia teknologi informasi.	Peningkatan secara terus menerus (*Continuous Improvement*)

Untuk mendapatkan hasil yang paling tepat dan sesuai, maka peneliti akan mencoba untuk melakukan formulasi antara kebutuhan perusahaan dengan korelasi ketiga kerangka kerja BCP yang digunakan dalam penelitian ini.

Gambar 4. 11 Formulasi Kebutuhan Perusahaan dengan Kerangka Kerja BCP (Sumber: Peneliti, 2014)

Dalam proses formulasi ini, peneliti berusaha untuk melakukan analisis dan sintesis terhadap ketiga standar kerangka BCP yang digunakan, di mana peneliti akan menyesuaikan dengan mengambil bagian-bagian yang sesuai dengan kebutuhan perusahaan dan tidak menggunakan bagian-bagian yang tidak sesuai dengan kebutuhan perusahaan di setiap kerangka yang ada.

Bagian-bagian atau fase yang sesuai dengan kebutuhan perusahaan tersebut akan diformulasi menjadi suatu bentuk kerangka BCP yang unik dan memenuhi atau sesuai dengan 10 kebutuhan perusahaan yang telah diverifikasi pada tahapan sebelumnya. Hal ini akan membantu perusahaan untuk lebih efektif dan efisien dalam menjalankan perencanaan dan proses keberlanjutan bisnis, agar operasional bisnis tetap berjalan dengan

lancar meskipun terjadi gangguan atau bencana yang menimpa perusahaan.

4.5 Kerangka Business Continuity Plan (BCP) BPR Bank Surya Yudha Banjarnegara

Berdasarkan kebutuhan perusahaan yang telah ditetapkan, dan analisis sintesis dari 3 standar kerangka BCP yang digunakan (ISO 22301:2012, *Bank of Japan, Dutch Financial Sector*), maka peneliti melakukan formulasi untuk menyusun sebuah Kerangka BCP yang dibuat sesuai dengan kebutuhan BPR Bank Surya Yudha Banjarnegara. Berikut ini adalah gambar kerangka BCP BPR Bank Surya Yudha Banjarnegara.

Gambar 4. 12 Kerangka BCP di BPR Bank Surya Yudha Banjarnegara (Sumber: Peneliti, 2014)

Setiap fase atau tahapan proses dalam kerangka BCP tersebut, tidak terlepas dari kebutuhan perusahaan dan acuan yang digunakan, yaitu 3 standar kerangka BCP (ISO 22301:2012, *Bank of Japan, Dutch Financial Sector*) yang ada di penelitian ini. Berikut ini adalah pemetaan setiap fase kerangka BCP dengan acuan yang digunakan.

Tabel 4. 7 Pemetaan Kerangka BCP dengan Acuan yang Digunakan (Sumber: Peneliti 2014)

FASE	SUB-FASE	ACUAN
PLAN (PERENCANAAN)	Profil Perusahaan	ISO 22301:2012
	Ruang Lingkup BCP	ISO 22301:2012 Dutch Financial Sector
	Tujuan BCP	ISO 22301:2012 Bank of Japan Dutch Financial Sector
	Sumber Daya	ISO 22301:2012 Bank of Japan Dutch Financial Sector
	Tata Cara Komunikasi	ISO 22301:2012 Bank of Japan
	Tata Kelola TI	Dutch Financial Sector
DO (PENGERJAAN)	Analisis Dampak Bisnis	ISO 22301:2012 Bank of Japan Dutch Financial Sector
	Manajemen Risiko	ISO 22301:2012 Bank of Japan Dutch Financial Sector

FASE	SUB-FASE	ACUAN
	Strategi Keberlanjutan Bisnis	ISO 22301:2012 Dutch Financial Sector
	Prosedur Keberlanjutan Bisnis	ISO 22301:2012 Bank of Japan Dutch Financial Sector
	Pelatihan dan Pengujian	ISO 22301:2012 Bank of Japan Dutch Financial Sector
CHECK (PEMERIKSAAN)	Audit Internal TI Bagian	ISO 22301:2012
	Audit Internal TI Perusahaan	ISO 22301:2012
	Peninjauan Manajemen	ISO 22301:2012
ACT (TINDAKAN)	Peningkatan Secara Terus-Menerus	ISO 22301:2012

Berdasarkan pemetaan di atas, dapat diamati pada setiap fase di Kerangka BCP BPR Bank Surya Yudha Banjarnegara, ada yang sepenuhnya mengacu dari 3 standar yang digunakan, namun ada fase yang hanya mengacu kepada 1 atau 2 standar kerangka saja. Hal tersebut dilakukan agar setiap fase yang ada benar-benar sesuai dengan kebutuhan perusahaan.

Penyusunan kerangka BCP dengan menggunakan pendekatan mundur memerlukan proses peningkatan secara terus-menerus (*continuous improvement*) secara periodik dan terukur. Hal ini disebabkan adanya kemungkinan perubahan pada kebutuhan perusahaan terkait dengan keberlanjutan bisnis, yang dipengaruhi oleh perkembangan teknologi informasi, adanya perubahan regulasi dari Bank Indonesia atau institusi terkait

lainnya, maupun perubahan keputusan manajemen. Oleh karena itu, *continuous improvement* menjadi isu yang penting dalam penelitian ini.

BAB V
PEMBAHASAN KERANGKA BCP PERUSAHAAN

Bab ini menjelaskan proses penyusunan kerangka BCP di BPR Bank Surya Yudha Banjarnegara, dengan menggunakan metode komparasi secara teoritis dan empiris.

5.1 Kerangka BCP BPR Bank Surya Yudha Banjarnegara

Pada bagian ini akan dipaparkan mengenai implementasi model BCP untuk menyusun *Business Continuity Planning* di BPR Bank Surya Yudha Banjarnegara. Setiap fase yang terdapat pada model BCP akan menunjang peneliti untuk mendapatkan hasil terbaik yang sesuai dengan kebutuhan perusahaan. Namun rincian hasil dari penelitian ini secara keseluruhan dilampirkan pada Dokumen BCP BPR Bank Surya Yudha Banjarnegara, demi keamanan informasi perusahaan yang bersangkutan.

5.1.1 Plan (Perencanaan)

Fase perencanaan menuntut perusahaan untuk dapat menyusun keberlanjutan bisnis yang selaras dengan kebijakan dan tujuan bisnis perusahaan. Dalam fase ini, perusahaan akan menentukan kebutuhan perusahaan terkait BCP, ruang lingkup dan tujuan BCP, seluruh sumber daya yang dibutuhkan dan perencanaan cara berkomunikasi selama proses keberlanjutan bisnis, serta peran tata kelola Teknologi Informasi baik secara internal maupun eksternal yang mendukung proses keberlanjutan bisnis di perusahaan tersebut.

1. PROFIL PERUSAHAAN

Bagian ini akan menjelaskan informasi perusahaan yang terlibat dalam penyusunan BCP (perusahaan studi kasus), serta keinginan dan kebutuhan perusahaan terkait dengan proses keberlanjutan bisnis, yang dalam penelitian ini adalah BPR Bank Surya Yudha Banjarnegara.

1.1 Perusahaan

Bank Perkreditan Rakyat ini terletak di Kabupaten Banjarnegara, Jawa Tengah. Semenjak didirikan pada tahun 1992, BPR ini selalu mendapat predikat SEHAT dari Bank Indonesia dan menjadikannya sebagai BPR peringkat pertama se-Jawa tengah dan ketiga se-Indonesia (Infobank, 2011). Berikut ini adalah identitas yang akan melakukan perencanaan keberlanjutan bisnis dalam dokumen BCP ini.

Tabel 5. 1 Profil Perusahaan (Sumber: Profil BSY, 2014)

PROFIL PERUSAHAAN	
Nama Perusahaan	PT. BPR Bank Surya Yudha Banjarnegara
Lokasi Perusahaan	Rejasa, Banjarnegara
Tahun Berdiri	1992
Jenis Usaha	Perbankan (Bank Perkreditan Rakyat)
Status	Perseroan Terbatas
Jumlah Kantor	1 Kantor Pusat 16 Kantor Cabang 32 Kantor Kas 1 Payment Point
Logo Perusahaan	

Untuk profil selengkapnya tentang BPR Bank Surya Yudha Banjarnegara dapat kembali dilihat pada Bab IV, sub-bab 4.1.

1.2 Kebutuhan dan Keinginan Perusahaan

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

1. Wawancara dengan pimpinan di bagian TSI.

2. Penyesuaian dengan Rencana Jangka Panjang Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara.

Berikut ini adalah hasil dari penggalian kebutuhan perencanaan keberlanjutan bisnis BPR Bank Surya Yudha Banjarnegara, yang telah terverifikasi oleh Pimpinan Bagian TSI , untuk menyatakan persetujuan atas kebutuhan dan keinginan perusahaan mengenai penyusunan BCP di perusahaan, Lihat Lampiran A halaman A-1.

Tabel 5. 2 Kebutuhan dan Keinginan Perusahaan (Sumber: Peneliti 2014)

KEBUTUHAN DAN KEINGINAN PERUSAHAAN	STATUS
1. BCP yang dibuat harus mencakup risiko di bidang teknologi informasi di perusahaan.	Terverifikasi
2. BCP yang dibuat harus dapat mengurangi risiko yang timbul dari implementasi teknologi informasi.	Terverifikasi
3. BCP yang dibuat dapat digunakan dalam waktu jangka panjang.	Terverifikasi
4. BCP yang dibuat harus memperhatikan aspek kemudahan dan kesederhanaan desain.	Terverifikasi
5. BCP yang dibuat harus dapat sesuai dengan teknologi yang sudah diterapkan.	Terverifikasi
6. BCP yang dibuat harus melibatkan perusahaan, dalam hal Sumber Daya Manusia (SDM) secara utuh.	Terverifikasi
7. BCP yang dibuat harus memperhatikan keberlanjutan operasional bisnis perusahaan.	Terverifikasi
8. BCP yang dibuat untuk perbankan, harus dapat mengatasi kebutuhan sistem keamanan yang tinggi di perusahaan.	Terverifikasi
9. BCP yang dibuat harus dapat mendukung tata kelola teknologi informasi yang diterapkan di perusahaan (prosedur di DRC, DRP dan *Contingency Plan*).	Terverifikasi
10. BCP yang dibuat harus dinamis, yaitu dapat mengikuti perkembangan dunia teknologi informasi.	Terverifikasi

Berdasarkan kebutuhan dan keinginan perusahaan, maka peneliti memulai untuk menyusun BCP yang sesuai dengan kebutuhan dan tujuan dari perusahaan.

2. RUANG LINGKUP BCP

Pada bagian ini perusahaan perlu menentukan beberapa hal yang berpengaruh terhadap penyusunan BCP baik secara internal maupun eksternal, seperti:

1. Ruang lingkup BCP secara umum.
2. Mengidentifikasi fungsional bisnis serta proses bisnis yang masuk ke dalam ruang lingkup BCP.
3. Mengidentifikasi pihak yang terkait ke dalam ruang lingkup BCP.

Berikut ini adalah penjelasan dari masing-masing poin tersebut.

2.1 Ruang Lingkup BCP secara Umum

Penyusunan kerangka BCP di perusahaan ini, melibatkan beberapa fungsional bisnis dan proses bisnis yang memiliki ketergantungan sangat tinggi terhadap teknologi dan sistem informasi dalam memaksimalkan pelayanannya kepada pengguna lain/nasabah bank. BCP yang dibuat melibatkan beberapa pihak internal yang memiliki kewenangan untuk bisa bertanggung jawab atas setiap proses dan memberikan keputusan pada saat proses mitigasi atau penanganan kondisi darurat. Penyusunan BCP dilakukan untuk mematuhi peraturan perbankan, yaitu himbauan pada saat pemeriksaan BI tahun 2013 yang menyatakan bahwa BPR dengan kondisi teknologi informasi yang sudah mumpuni, disarankan untuk memiliki manajemen risiko, termasuk BCP di dalamnya.

2.2 Fungsional Bisnis dan Proses Bisnis yang Terlibat

Berdasarkan struktur organisasi perusahaan BPR Bank Surya Yudha Banjarnegara, terdapat 2 Divisi, 12 Bagian dan beberapa seksi yang ada di masing-masing bagian pada sistem kantor pusat yang akan diimplementasikan di kantor cabang dan kantor kas yang tersebar di beberapa wilayah. Dari keseluruhan fungsional bisnis tersebut, hanya 5 fungsional bisnis yang akan dilibatkan dalam penelitian ini. Kelima fungsional bisnis ini memiliki tingkat ketergantungan yang tinggi terhadap layanan teknologi dan sistem informasi yang ada, terutama dalam sistem *core* banking. Fungsional bisnis tersebut adalah bagian Teknologi dan Sistem Informasi (TSI), Operasional, Pembukuan, Kredit dan Personalia.

Dalam penyusunan BCP ini, hanya akan ada beberapa proses bisnis yang dilibatkan di dalam masing-masing fungsional bisnis yang telah dipilih. Proses bisnis yang dilibatkan juga merupakan proses bisnis yang paling bergantung kepada layanan teknologi dan sistem informasi serta berpengaruh terhadap pemberian layanan kepada nasabah secara langsung. Berikut ini adalah fungsional bisnis dan proses bisnis yang terlibat di dalam penyusunan BCP ini.

Tabel 5. 3 Fungsional Bisnis dan Proses Bisnis Terkait Sistem (Sumber: Penelit, 2014)

Fungsional Bisnis	Proses Bisnis Terkait Sistem
TSI	Proses End-of-Day
	Input Tabel Parameter
	Modul User AS400
	LAPBUL (Laporan Bulanan)
	Sistem Informasi Debitur (SID)
	Pemasangan Perangkat Jaringan
	Disaster Recovery Center (DRC)
	Perawatan Perangkat Keras
Operasional	Input Data Nasabah
	Tarik Tunai
	Setoran Tunai
	Pembukaan Tabungan

Fungsional Bisnis	Proses Bisnis Terkait Sistem
	Pembukaan Deposito dan Realisasi Kredit
	Pembayaran Angsuran
Pembukuan	Pemindahbukuan Rekening Internal
	Pemindahbukuan Multi Jurnal
	Posting Backdate
	Pembentukan PPAP
	Pembentukan Amortisasi
	Neraca
	LAPBUL (Laporan Bulanan)
Kredit	Informasi Kolektabilitas dan NPL
	Sub Modul LAPBUL
	Sistem Informasi Debitur (SID)
Personalia	Pengelolaan Data Karyawan
	Sistem Penggajian Karyawan

2.3 Pihak yang Terlibat dalam BCP

Penyusunan BCP akan melibatkan pihak internal perusahaan , yaitu pimpinan dan karyawan di Bagian TSI, narasumber (Kepala Bagian atau Wakil Kepala Bagian) Pembukuan, Operasional, Personalia dan Kredit serta Dewan Direksi.

3. TUJUAN BCP

Pada bagian ini perusahaan akan memaparkan tujuan dibuatnya BCP. Tujuan ini akan dijadikan sebagai landasan dan acuan pengerjaan BCP yang mendukung operasional dan pencapaian tujuan perusahaan.

Tujuan dari penyusunan BCP ini adalah :

1. Menghasilkan dokumen BCP (*Business Continuity Plan*) yang selaras dengan tujuan dan kebutuhan perusahaan.
2. Menghasilkan dokumen BCP yang dapat diimplementasikan secara menyeluruh oleh pihak-pihak yang memiliki ketergantungan terhadap teknologi dan sistem informasi.

3. Meminimalisasi risiko teknologi informasi (ancaman alam, internal dan eksternal) yang dapat muncul ketika terjadi gangguan yang dapat menghambat proses operasional bisnis.
4. Memastikan ketersediaan (*availability*), integritas (*integrity*) serta tingkat kehandalan (*reliability*) layanan informasi di bank, untuk menjaga citra perusahaan di mata nasabah.
5. Meningkatkan kesadaran seluruh pihak di perusahaan akan pengembangan teknologi dan sistem informasi, serta pentingnya pengelolaan risiko teknologi informasi di perusahaan.

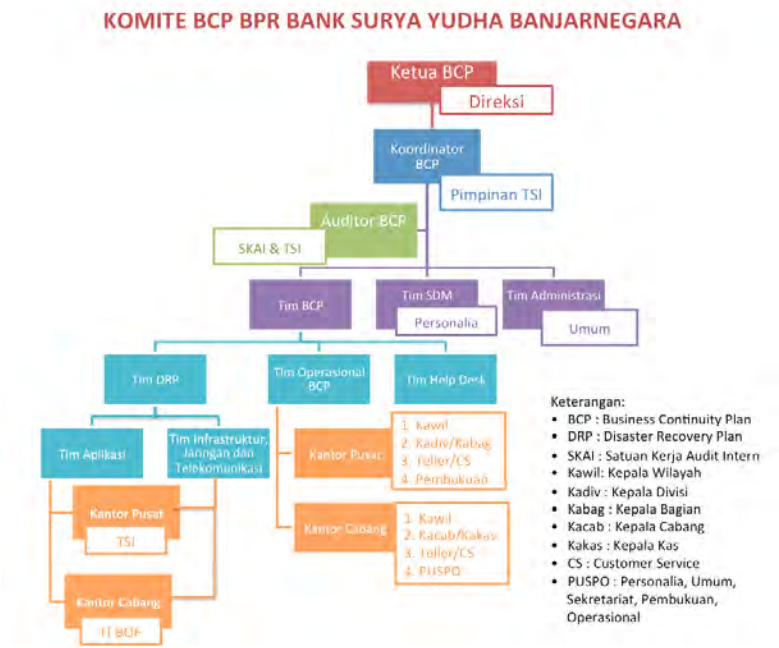
4. SUMBER DAYA

Perusahaan perlu memperhatikan sumber daya yang dibutuhkan selama penyusunan dan implementasi BCP. Sumber daya yang dibutuhkan adalah sumber daya manusia dan perangkat atau infrastruktur atau fasilitas yang akan mendukung tercapainya tujuan BCP.

4.1 Sumber Daya Manusia

Sumber Daya Manusia (SDM) menempati peran yang cukup signifikan dalam penyusunan BCP, karena jika SDM yang diberikan tanggung jawab untuk melakukan penysunan BCP dapat bekerja secara optimal, maka akan menghasilkan BCP yang optimal pula. Untuk memastikan bahwa SDM yang ada dapat berjalan secara optimal, maka perlu dibuat adanya sebuah komite atau kepanitiaan.

Komite BCP berhubungan dengan Tim DRP (*Disaster Recovery* Plan) yang sudah terbentuk di BPR Bank Surya Yudha Banjarnegara. Tim DRP akan bertugas untuk menangani secara langsung tindakan teknis atau operasional teknologi informasi. Berikut adalah komite BCP BPR Bank Surya Yudha Banjarnegara.



Gambar 5. 1 Komite BCP BPR Bank Surya Yudha Banjarnegara (Sumber: Peneliti, 2014)

Komite BCP di perusahaan diharapkan dapat mewakili dari setiap divisi dan bagian di setiap kantor, baik kantor pusat, cabang dan kas. Di mana, proses keberlanjutan bisnis di perusahaan ini diharapkan tidak hanya menjadi tanggung jawab Bagian Teknologi dan Sistem Informasi saja, melainkan melibatkan peran dari seluruh fungsional bisnis yang terkait dan bergantung pada teknologi dan sistem informasi dalam operasional bisnisnya.

4.2 Perangkat

Perusahaan perlu melakukan identifikasi terhadap sumber daya yang terkait dengan perangkat dan ketersediaan infrastruktur yang dipergunakan ketika terjadi gangguan/bencana di perusahaan. Perangkat atau infrastruktur

ini diharapkan dapat menunjang operasional kritis di perusahaan.

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

a. Sistem/CPU AS/400.
b. Unit disk/DASD.
c. Panel komunikasi dan modem.
d. *Drive tape* dan *cartridge.*
e. Printer.
f. Terminal (di TSI dan pengguna/kantor-kantor cabang dan kas).
g. Alat komunikasi dan modem di kantor cabang dan kas.

Perencanaan keberlanjutan bisnis untuk aplikasi adalah sebagai berikut.

a. Tersedianya *check list library* atau *check list file system* yang memiliki tingkat urgensi dan ketergantungan yang tinggi terhadap kegiatan operasional.
b. Pelaksanaan kegiatan *back up* data harian agar dapat dilakukan *restore* apabila diperlukan.

Dokumen serta perangkat lain yang dibutuhkan dalam kondisi kritis adalah sebagai berikut.

a. *Checklist* harian
b. *Tape back-up*
c. Rincian proses akhir hari
d. Daftar Vendor Hardware/Software/Komunikasi
e. SOP (*Standard Operating Procedure*)

5. TATA CARA KOMUNIKASI

Pada BCP perusahaan, diharapkan dapat menetapkan komunikasi untuk kelancaran BCP yang dibagi atas komunikasi internal perusahaan dan komunikasi eksternal perusahaan

(nasabah, BI, asuransi, lembaga keuangan lainnya dan mitra kerja perusahaan).

Perusahaan perlu memastikan bahwa alat telekomunikasi tetap bisa digunakan pada saat terjadinya gangguan atau bencana. Daftar kontak darurat dan alat komunikasi darurat perlu dipersiapkan secara khusus di dalam BCP Perusahaan. Selain itu, perlu dibuat adanya suatu tata cara pengambilan keputusan dan struktur pemberian perintah melalui tim khusus yang bertugas memberikan konfirmasi darurat pada saat terjadi gangguan/bencana.

5.1 Alur Komunikasi

Untuk memastikan bahwa penyampaian pesan dan pelaporan kejadian berjalan dengan baik pada saat terjadi gangguan atau bencana, perusahaan perlu mengatur alur komunikasi yang tertib, sehingga dapat menjadi acuan untuk menentukan, kepada siapa / bagian apa harus berkomunikasi dan kapan waktu yang tepat untuk melakukan komunikasi. Berikut ini adalah alur komunikasi dalam BCP perusahaan.

Gambar 5. 2 Alur Komunikasi pada Saat Terjadi Gangguan (Sumber: Peneliti, 2014)

Penjelasan mengenai alur komunikasi pada saat terjadi gangguan/bencana adalah sebagai berikut.

1. Bencana atau gangguan menyerang operasional bisnis dan aset teknologi informasi yang dimilki oleh perusahaan. Bencana atau gangguan yang muncul dikategorikan menjadi dua hal utama, yaitu gangguan yang harus segera ditangani atau yang memerlukan penanganan darurat dan gangguan yang membutuhkan waktu untuk melakukan pertimbangan dan perumusan untuk menyelesaikannya. Gangguan yang harus segera ditangani seperti bencana alam, kebakaran, banjir serta serangan terhadap keamanan jaringan teknologi dan sistem informasi di perusahaan. Untuk jenis gangguan ini, perusahaan akan langsung melakukan penanganan

melalui pihak yang bertanggung jawab. Gangguan yang membutuhkan waktu untuk melakukan pertimbangan dan perumusan untuk penyelesaiannya dapat berupa gangguan operasional bisnis bank atau gangguan yang berhubungan dengan kebijakan internal maupun eksternal perusahaan. Penyelesaian untuk gangguan ini dapat dilanjutkan dengan langkah selanjutnya yaitu melakukan rapat/*briefing* Komite BCP.

2. Rapat/*briefing* Komite BCP dilakukan sebagai sarana untuk merumuskan langkah-langkah yang harus dilakukan untuk menangani dan menyelesaikan gangguan pada operasional bisnis perusahaan serta yang berkaitan dengan kebijakan internal dan eksternal perusahaan. Pertemuan ini juga dilakukan untuk menyusun rencana selanjutnya yang harus dilakukan terhadap gangguan yang harus segera ditangani, setelah dilakukan penanganan pertama oleh pihak yang bertugas (PIC). Pertemuan ini dipimpin oleh Koordinator BCP.
3. Langkah selanjutnya adalah penyampaian hasil rapat/*briefing* yang dipimpin oleh Koordinator BCP kepada Dewan Direksi dan Dewan Komisaris. Pertemuan ini dimaksudkan untuk meminta persetujuan atas hasil pertemuan sebelumnya untuk melaksanakan langkah-langkah penanganan atau penyelesaian. Jika dalam rapat/*briefing* Komite BCP sudah dihadiri oleh Dewan Direksi dan Dewan Komisaris, maka dapat dilangsungkan persetujuan saat itu juga.

4. Koordinator BCP akan menyampaikan hasil persetujuan oleh Dewan Direksi dan Komisaris kepada Tim BCP, Administrasi dan SDM untuk segera menginstruksikan hasil persetujuan dalam rangka menangani dan menyelesaikan bencana/gangguan di bank. Proses eksekusi ini dijalankan oleh tim-tim yang sesuai dengan permaslahan yang muncul, yaitu oleh Tim DRP yang terdiri dari Tim Aplikasi, Tim Infrastruktur, Jaringan dan Komunikasi atau dilaksanakan oleh Tim Operasional BCP.

Komunikasi dapat dilakukan pula secara eksternal, terutama untuk tim yang berhubungan dengan vendor atau intitusi di luar. Pihak TSI dapat menghubungi Vendor WBK (keluhan kerusakan sistem aplikasi), Telkom dan Icon (keluhan atas infrastruktur, jaringan dan telekomunikasi), IBM (keluhan perangkat keras) atau Bank Syariah Mandiri (keluhan atas ATM Center). Komunikasi dapat dilakukan pula dengan Bank Indonesia, terkait permasalahan yang melibatkan LAPBUL (Laporan Bulanan) atau SID (Sistem Informasi Debitur).

5.2 Daftar Alat Komunikasi Darurat

Untuk memastikan bahwa komunikasi tetap dapat dilakukan dengan lancar dan tanpa hambatan, perusahaan perlu mengidentifikasikan alat-alat komunikasi yang dapat digunakan dalam kondisi darurat, atau pada saat terjadi bencana/gangguan. Alat komunikasi ini disediakan oleh tim Komite BCP, yang terdiri dari sebagai berikut.

Tabel 5. 4 Daftar Alat Komunikasi Darurat (Sumber: Peneliti 2014)

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

Alat komunikasi yang terdapat pada tabel di atas menunjukkan bahwa perusahaan minimal perlu memiliki alat-alat komunikasi tersebut di setiap kantor yang ada, baik kantor pusat, cabang maupun kas. Alat-alat komunikasi ini diharapkan dapat menjadi media perantara utama yang membantu pihak-pihak yang bertanggung jawab di perusahaan untuk dapat menginformasikan terkait bencana atau gangguan yang terjadi kepada pihak yang membutuhkan informasi atau kepada seluruh sumber daya manusia di perusahaan.

Koordinator BCP perlu memastikan bahwa seluruh alat komunikasi yang tertera di atas memiliki tingkat ketersediaan dan kehandalan yang tinggi, sehingga ketika dibutuhkan sewaktu-waktu dapat segera digunakan oleh seluruh pihak yang bertanggung jawab.

6. TATA KELOLA TI

Pengelolaan tata kelola TI sebagai salah satu acuan dalam pengelolaan keberlanjutan bisnis, diyakini dapat menjadi bagian yang sangat penting dalam pencapaian suatu perusahaan. Tata kelola ini diharapkan dapat menjawab kebutuhan perusahaan serta menjadi bagian dari budaya perusahaan. Tata kelola keberlanjutan bisnis pada dokumen BCP ini adalah dalam bentuk kebijakan, prosedur dan formulir untuk melakukan proses audit internal. Komite BCP diharapkan dapat melakukan pelaporan tinjauan secara berkala mengenai tindakan peningkatan atau perbaikan yang dilakukan kepada pihak manajemen tertinggi di perusahaan.

Perusahaan harus memastikan bahwa tata kelola teknologi informasi yang diterapkan di perusahaan, baik dari internal maupun eksternal, dapat menjadi sumber yang baik untuk BCP. Pihak manajemen dan Komite BCP perlu memastikan bahwa BCP yang disusun dan akan diimplementasikan dapat selaras dengan tata kelola TI yang diterapkan di perusahaan.

Tata kelola teknologi informasi yang berkaitan erat dengan penyusunan BCP ini adalah:

1. Internal :

   Rencana Jangka Panjang dan Jangka Pendek Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara (Kebijakan) tahun 2013.

2. Eksternal :

   Peraturan Bank Indonesia Nomor: 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

5.1.2 Do (Pengerjaan)

Pada fase ini perusahaan akan mengimplementasikan dan mengoperasikan perencanaan untuk menyusun BCP yang telah dibuat sebelumnya. Perusahaan harus dapat menentukan analisis dampak bisnis untuk menentukan proses bisnis yang bernilai kritis, manajemen risiko yang meliputi penilaian dan perlakuan risiko, penyusunan strategi keberlanjutan bisnis, prosedur serta pelatihan dan pengujian yang dilakukan untuk verifikasi dan validasi BCP di perusahaan tersebut.

7. ANALISIS DAMPAK BISNIS

Perusahaan perlu melakukan analisis dampak bisnis (*Business Impact Analysis*-BIA) yang digunakan untuk menentukan proses bisnis atau operasional bisnis yang paling kritis di perusahaan. Hal ini dilakukan dengan melakukan identifikasi fungsional dan proses bisnis yang terdapat di perusahaan, memperhatikan dampak dan memberikan nilai untuk menentukan proses bisnis di perusahaan yang memiliki nilai dampak tertinggi.

Namun karena dokumen analisis dampak bisnis merupakan sesuatu yang bersifat rahasia (*confidential*), maka seluruh informasi terkait analisis dampak bisnis tidak akan ditampilkan di buku penelitian ini, namun ditampilkan dalam Dokumen BCP BPR Bank Surya Yudha Banjarnegara. Untuk contoh dari proses analisis dampak bisnis yang dilakukan, lihat Lampiran D.

7.1 Penentuan Proses Bisnis Kritis di Perusahaan

Penentuan proses bisnis dan sistem yang kritis, dilakukan dengan mengetahui proses bisnis apa sajakah yang terlibat dalam penyusunan analisis dampak bisnis ini. Berdasarkan proses bisnis yang terlibat, maka perusahaan dapat melakukan penghitungan dampak dari setiap proses bisnis yang ada. Penghitungan dampak tersebut akan menentukan proses bisnis yang bernilai kritis di perusahaan.

7.1.1 Identifikasi Proses Bisnis yang Terlibat

Proses bisnis pada masing-masing fungsional bisnis yang terlibat merupakan proses bisnis yang terkait dengan teknologi dan sistem informasi secara langsung dan memiliki tingkat ketergantungan yang sangat tinggi. Pada penelitian ini, fungsional bisnis yang dilibatkan berjumlah 5 bagian, yaitu:

1. Teknologi dan Sistem Informasi (TSI)
2. Pembukuan
3. Operasional
4. Kredit
5. Personalia

Proses identifikasi proses bisnis dilakukan dengan melakukan wawancara kepada pimpinan atau yang mewakilinya, dari masing-masing bagian tersebut.

Tabel 5. 5 Keterangan Wawancara (Sumber: Peneliti 2014)

NO	BAGIAN	TANGGAL	TEMPAT	NARASUMBER
1	Pembukuan	Selasa, 4 Maret 2014	Ruang TSI BPR Bank Surya Yudha Banjarnegara	Wakil Kepala Bagian Pembukuan
2	Operasional	Rabu, 5 Maret 2014		Kepala Bagian Operasional
3	Personalia	Rabu, 5 Maret 2014		Kepala Seksi di Bagian personalia
4	Kredit	Rabu, 5 Maret 2014		Kepala Wilayah II
5	TSI	Kamis, 6 Maret 2014		Pimpinan TSI

Wawancara dilakukan dengan mengajukan beberapa pertanyaan terkait upaya keberlanjutan bisnis. Pertanyaan diadopsi dengan penyesuaian dari sebuah *paper* yang berjudul *Business Continuity Planning in Bank in Computerized Environment*, oleh Dr. Arvind Tilak. Berikut

ini adalah pertanyaan dalam sesi wawancara di penelitian ini.

Pertanyaan Wawancara :

1. Jelaskan setiap fungsi bisnis (deskripsi proses binsis) dan kaitannya dengan bagian lain.
2. Jelaskan perihal waktu kritis dari proses bisnis tersebut.
3. Jelaskan perihal dampak yang terjadi ketika sistem tidak berfungsi dalam waktu 1jam/4 jam / 1 hari / 1 minggu / 1 bulan.
4. Apakah yang membuat proses ini sangat penting (peran dalam bisnis)?
5. Jelaskan dampak yang terjadi secara hukum.
6. Jelaskan dampak yang terjadi secara finansial.
7. Jelaskan dampak yang terjadi kepada nasabah.
8. Jelaskan dampak yang terjadi ke fungsional bisnis lainnya (internal/eksternal perusahaan).
9. Berapa lama waktu yang dapat digunakan untuk dapat bertahan tanpa sistem di proses bisnis tersebut?

Berdasarkan hasil wawancara tersebut, maka tersusunkah proses identifikasi proses bisnis yang dapat digunakan untuk proses selanjutnya yaitu penghitungan dampak. Untuk contoh dalam proses tersebut, lihat Lampiran D.1 atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

7.1.2 Penghitungan Dampak

Penghitungan dampak dilakukan dengan tujuan untuk dapat mengetahui proses bisnis manakah yang paling kritis ketika terjadi kelumpuhan sistem. Hal ini dimaksudkan, agar penanganan pemulihan sistem ditujukkan untuk proses bisnis dengan estimasi dampak yang paling tinggi, sehingga operasional bisnis perusahaan dan pelayanan kepada nasabah bank tetap dapat berjalan secara optimal.

Untuk melakukan penghitungan dampak, terlebih dahulu perlu ditentukan kategori untuk masing-masing dampak, beserta nilai untuk masing-masing kategorinya. Kategori dan nilai dampak ditentukan berdasarkan kesepakatan antara peneliti dengan pihak manajemen TSI. Kategori dampak terdiri dari beberapa aspek, yaitu:

1. Internal bank

   Ketegori internal bank terkait dengan proses bisnis yang ada di internal fungsional bisnis yang bersangkutan, dan fungsional bisnis lain yang berkaitan dengan proses bisnis tersebut. Contohnya adalah pada proses bisnis Pembukaan Tabungan yang terdapat pada fungsional bisnis Bagian Operasional. Ketika terjadi kelumpuhan sistem pada proses Pembukaan Tabungan, maka dampak yang muncul bukan hanya pada bagian operasional saja, tetapi juga berdampak pada fungsional bisnis lainnya
2. Finansial

   Kategori finansial terkait dengan dampak yang terjadi secara finansial ke perusahaan. Dengan kata lain, dapat dijelaskan bahwa dampak finansial ini adalah kerugian perusahaan secara finansial. Contohnya adalah ketika terjadi keterlambatan pengiriman LAPBUL yang diakibatkan oleh kegagalan sistem pada modul LAPBUL (pengiriman LAPBUL ke BI). Dalam kasus ini, pihak bank akan dikenakan denda maksimal 3 juta rupiah akibat keterlambatan pengiriman LAPBUL tersebut.
3. Hukum

   Kategori hukum ini merupakan dampak yang terjadi ketika muncul gangguan atau bencana, yang secara langsung atau tidak langsung melibatkan bank dalam pelanggaran hukum atau regulasi yang ada. Contohnya adalah ketika terjadi keterlambatan pengiriman SID ke BI dikarenakan kegagalan sistem

pada modul SID. Dalam kasus ini, pihak bank dapat dianggap melakukan pelanggaran hukum, yaitu melanggar Peraturan Bank Indonesia (PBI) PBI 9/14/2007 SID BAB XI Sanksi Pasal 34 dan UU Perbankan no 7 tahun 1992 BAB VIII Ketentuan Pidana dan Sanksi Administratif.

4. Nasabah

   Kategori nasabah ini merupakan dampak yang terjadi pada nasabah bank, baik secara langsung maupun tidak langsung. Contohnya adalah ketika terjadi kelumpuhan sistem sehingga nasabah tidak dapat melakukan penarikan tunai. Hal ini secara langsung berdampak kepada nasabah dan dapat menurunkan kredibilitas bank di mata nasabah.

5. Eksternal Bank

   Kategori eksternal bank merupakan dampak yang terjadi kepada institusi lain di luar perusahaan. Dalam kasus ini, institusi yang dimaksud adalah Bank Indonesia, Kantor Pelayanan Pajak, Dinas Tenaga Kerja, Transmigrasi dan Kesejahterahaan Sosial, Asuransi, serta institusi lainnya.

Proses penilaian ini juga didasari oleh wawancara yang dilakukan oleh peneliti kepada perwakilan dari masing-masing bagian tersebut.

Tabel 5. 6 Skala Dampak (Sumber: FMEA diolah peneliti, 2014)

		KATEGORI DAMPAK			
		Internal Bank	**Finansial**	**Hukum**	**Nasabah**
NILAI DAMPAK	**1 atau 2**	Tidak ada dampak pada internal bank	Tidak ada dampak secara finansial kepada perusahaan	Tidak melanggar regulasi dan hukum internal dan eksternal perusahaan.	Tidak berdampak secara langsung kepada nasabah
	3 atau 4	Menggangu <25% proses bisnis pada internal fungsional bisnis	Menimbulkan kerugian finansial/biaya ekstra <10%	Melakukan pelanggaran regulasi internal perusahaan.	Mengganggu <25% proses pelayanan bank kepada nasabah.
	5 atau 6	Menggangu 25% - 50% proses bisnis pada internal fungsional bisnis dan <25% proses bisnis di fungsional bisnis lainnya.	Menimbulkan kerugian finansial/biaya ekstra sebesar 10% - 20%	Melakukan pelanggaran regulasi internal dan hukum eksternal, namun tidak mempengaruhi tingkat kesehatan bank.	Mengganggu 25% - 50% proses pelayanan bank kepada nasabah.

	KATEGORI DAMPAK			
	Internal Bank	**Finansial**	**Hukum**	**Nasabah**
7 atau 8	Menggangu 51%-71% proses bisnis pada internal fungsional bisnis dan 25%-50% proses bisnis di fungsional bisnis lainnya.	Menimbulkan kerugian finansial/biaya ekstra sebesar 21% - 30%	Melakukan pelanggaran regulasi internal dan hukum eksternal perusahaan, yang berpotensi mempenga-ruhi tingkat kesehatan bank.	Mengganggu 51% - 75% proses pelayanan bank kepada nasabah
9 atau 10	Menggangu >75% proses bisnis pada internal fungsional bisnis dan menggangu >50% proses bisnis di fungsional bisnis lainnya.	Menimbulkan kerugian finansial/biaya ekstra >30%	Melakukan pelanggaran regulasi internal dan hukum eksternal perusahaan, yang secara langsung mempenga-ruhi tingkat kesehatan bank.	Mengganggu >75% proses pelayanan bank kepada nasabah.

7.2 Penentuan Estimasi *Downtime*

Perusahaan atau organisasi perlu menetapkan waktu yang dapat ditoleransi oleh pihak perusahaan ketika terjadi gangguan atau bencana. Waktu tersebut menunjukkan berapa lama proses bisnis mampu terus beroperasi tanpa adanya sistem tersebut. Penentuan estimasi *downtime* dilakukan dengan cara berdiskusi dengan pihak manajemen perusahaan, dalam hal ini pimpinan bagian TSI dan pimpinan di masing-masing fungsional bisnis yang terkait di dalam penelitian ini.

Berikut ini adalah estimasi *downtime* dari masing-masing proses bisnis yang ada, di mana terdiri dari penghitungan waktu sebagai berikut.

- *Recovery Time Objective* (RTO) adalah jumlah waktu lumpuh maksimal untuk seluruh sumber daya sistem yang ada, sebelum terjadi dampak lain kepada sumber daya lainnya. Jika waktu penanggulangan gangguan atau bencana melebihi RTO dapat menyebabkan dampak yang lebih besar bagi bank.
- *Recovery Point Objective* (RPO) adalah waktu yang diperlukan sebelum terjadinya gangguan, untuk memulihkan data setelah terjadinya gangguan. Penekanan RPO adalah data/transaksi sedangkan RTO penekanannya pada waktu. Pada saat terjadi gangguan atau bencana, kapan Backup data terakhir dilakukan. Apakah perlu dilakukan restore data backup terakhir atau tidak. Sehingga dapat diketahui mulai data transaksi jam berapa yang hilang, jumlah data yang hilang dan data/transaksi yang harus diinput ulang serta jumlah waktu yang dibutuhkan untuk menyelesaikan proses tersebut.

Berdasarkan penghitungan waktu tersebut, ada 2 waktu RPO yang ada di BPR Bank Surya Yudha Banjarnegara, yaitu:

1. Jika aplikasi Mirroring (Real Time Online Backup) tidak bermasalah waktu RPO nya maximal hanya 30 menit tergantung dari kecepatan transfer data dari Data Center ke Disaster Recovery Center.
2. Jika saat gangguan atau bencana terjadi, aplikasi Mirroring bermasalah, maka dilakukan restore dari tape backup terakhir yang dilakukan malam sebelumnya. Sedangkan transaksi yang harus diinput ulang adalah transaksi mulai awal jam kerja.

Untuk contoh pelaksanaan proses ini, lihat Lampiran D.2 atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

7.3 Identifikasi Sumber Daya

Identifikasi sumber daya dilakukan pada kantor kas, kantor cabang, kantor pusat dan bagian TSI serta *Disaster Recovery Center* (DRC) secara khusus. Di masing-masing kantor, bagian dan DRC dilakukan identifikasi kebutuhan sumber daya yang berupa :

1. Sumber Daya Manusia (SDM)
   Setiap kantor dan DRC di perusahaan memerlukan SDM dengan kapabilitas pengetahuan teknologi informasi yang memadai. Selain itu, penunjukkan penanggung jawab juga menjadi bagian yang sangat penting untuk memastikan segala proses dapat berjalan dengan lancar.
   Untuk mengatasi gangguan di kantor pusat, pengguna dapat langsung menghubungi ke Tim BCP (Bagian TSI) yang akan langsung mengatasi permasalahan. Namun untuk setiap kantor cabang, kantor kas dan DRC, penanggung jawab yang bertugas adalah IT BOF (IT *Back Office*) yang digunakan sebagai perwakilan Bagian TSI di setiap kantor cabang, kas dan DRC. Jika permasalahan yang dialami tidak dapat terselesaikan oleh

IT BOF, maka dapat langsung menghubungi pimpinan setempat (Kawil/Kacab/Kakas/) untuk segera menghubungi kantor pusat ke Bagian TSI.

2. Teknologi Informasi
   Teknologi Informasi yang dibutuhkan dapat berupa perangkat lunak, serta perangkat keras, perangkat jaringan dan telekomunikasi.
   Tim BCP hendaknya dapat melakukan inventarisasi atas kebutuhan teknologi informasi di masing-masing kantor. Kebutuhan akan teknologi informasi yang selalu muncul pada saat terjadi gangguan adalah sebagai berikut.
   - Perangkat keras
     PC (*Personal Computer*), kabel, printer.
   - Peralatan Jaringan dan Telekomunikasi
     Perangkat jaringan, modem, pesawat telepon, dan HT (*Handy Talkie*)
   - Perangkat Lunak
     Aplikasi AS/400 terinstal pada PC untuk menjalankan aplikasi Core Banking, Software untuk pembuatan laporan, browser internet.

8. MANAJEMEN RISIKO

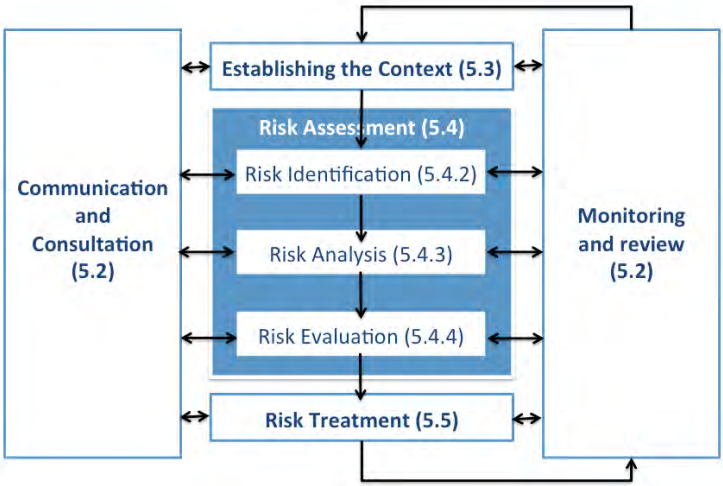
Proses manajemen risiko menjadi hal yang perlu diperhatikan oleh perusahaan. Di mana, perusahaan perlu mengetahui risiko-risiko yang dapat muncul dan memberikan dampak negatif bagi keberlangsungan perusahaan. Proses manajemen risiko dimulai dari proses bisnis paling kritis di perusahaan, yaitu proses bisnis yang memiliki dampak tertinggi sesuai hasil analisis dampak bisnis sebelumnya. Fase manajemen risiko terdiri dari penilaian risiko yang terdiri dari identfikasi, analisis serta evaluasi risiko, dan selanjutnya perlakuan risiko yang terdiri dari aksi mitigasi dan pemilihan risiko.

Namun karena berkas manajemen risiko merupakan sesuatu yang bersifat rahasia (*confidential*), maka seluruh informasi

terkait risiko tidak akan ditampilkan di buku penelitian ini, namun ditampilkan dalam Dokumen BCP BPR Bank Surya Yudha Banjarnegara. Untuk contoh dari proses manajemen risiko yang dilakukan, lihat Lampiran E.

8.1 Penilaian Risiko

Penilaian risiko dilakukan dengan menggunakan standar ISO 31000:2009 dan menggunakan metode penilaian FMEA (*Failure Mode and Effect Analysis*). Penggunaan standar ISO 31000:2009 menitikberatkan pada proses penilaian risiko dan perlakuan risiko. Di mana, untuk urutan proses yang dilakukan dapat dilihat pada gambar berikut.



Gambar 5. 3 Proses Manajemen Risiko (Sumber: ISO 31000,2009)

Gambar tersebut adalah gambar proses manajemen risiko yang diambil dari ISO 31000:2009. Proses penilaian risiko (*risk assessment*) terdiri dari proses identifikasi risiko, analisis risiko dan evaluasi risiko (ISO *Guide* 73, 2009).

Dalam penelitian ini, penilaian risiko didasari dari hasil BIA, yaitu berdasarkan proses bisnis yang memiliki nilai dampak tertinggi (proses bisnis kritis). Berikut ini adalah penjelasan dari tahapan-tahapan yang terdapat pada penilaian risiko, dilanjutkan dengan perlakuan risiko (aksi mitigasi) sehingga dapat menentukan fokus risiko. Fokus risiko merupakan risiko-risiko yang dipilih dari setiap fungsional bisnis perusahaan, untuk dibuat strategi dan prosedur dalam BCP di penelitian ini.

8.1.1 Identifikasi Risiko

Proses bisnis kritis sebagai hasil dari BIA menjadi bahan masukkan untuk melakukan identifikasi risiko. Risiko dalam penelitian ini dibatasi yaitu merupakan risiko teknologi informasi. Identifikasi risiko adalah sebuah proses menemukan, mengenali dan mendeskripsikan risiko (ISO *Guide* 73, 2009).

Proses identifikasi risiko dilakukan berdasarkan proses bisnis yang memiliki nilai dampak tertinggi (proses bisnis tertinggi). Dalam melakukan proses identifikasi risiko ini, peneliti juga melakukan analisis terhadap penyebab risiko itu bisa terjadi serta dampak ketika risiko itu benar-benar terjadi di perusahaan. Untuk mengetahui lebih lanjut, proses identifikasi risiko teknologi infromasi pada BPR Bank Surya Yudha dijelaskan pada tabel Risk Register berdasarkan Nilai Dampak.

8.1.2 Analisis Risiko

Analisis risiko adalah proses untuk memahami sifat dari risiko dan menetapkan tingkatan dari setiap risiko (ISO *Guide* 73, 2009). Metode FMEA (*Failure Mode and Effect Anlysis*) digunakan untuk menilai risiko dalam proses analisis ini. Proses untuk melakukan analisis melibatkan beberapa penghitungan nilai, yaitu terkait *Likelihood* (kemungkinan), *Impact* (dampak) dan *Detection* (deteksi).

Likelihood adalah kemungkinan terjadinya sebuah risiko. Berikut ini dipaparkan mengenai skala dari skor *likelihood*, sekaligus dengan kemungkinan peristiwa yang dapat terjadi.

Tabel 5. 7 Skala Likelihood (Sumber: FMEA, 2014)

SKOR LIKELIHOOD	PELUANG/KEMUNGKINAN TERJADINYA PERISTIWA
9 atau 10	Hampir pasti terjadi, peluang 90% - 100%
7 atau 8	Akan terjadi, peluang sekitar 70%-80%
5 atau 6	Mungkin terjadi/mungkin tidak terjadi, peluang 50%
3 atau 4	Sangat mungkin tidak terjadi, 30%-40%
1 atau 2	Hampir pasti tidak akan terjadi 10%-20%

Impact berkaitan erat dengan dampak atau besar pengaruh risiko terhadap beberapa yang berpengaruh terhadap perusahaan seperti, internal bank, finansial, hukum dan nasabah.

Tabel 5. 8 Skala Dampak (Sumber: FMEA diolah peneliti, 2014)

		KATEGORI DAMPAK			
		Internal Bank	**Finansial**	**Hukum**	**Nasabah**
NILAI DAMPAK	**1 atau 2**	Tidak ada dampak pada internal bank	Tidak ada dampak secara finansial kepada perusahaan	Tidak melanggar regulasi dan hukum internal dan eksternal perusahaan.	Tidak berdampak secara langsung kepada nasabah
	3 atau 4	Mengganggu <25% proses bisnis pada internal fungsional bisnis	Menimbulkan kerugian finansial/ biaya ekstra <10%	Melakukan pelanggaran regulasi internal perusahaan.	Mengganggu <25% proses pelayanan bank kepada nasabah.
	5 atau 6	Mengganggu 25% -50% proses bisnis pada internal fungsional bisnis dan	Menimbulkan kerugian finansial/biaya ekstra sebesar 10% - 20%	Melakukan pelanggaran regulasi internal dan hukum eksternal, namun tidak	Mengganggu 25% - 50% proses pelayanan bank kepada nasabah.

	KATEGORI DAMPAK			
	Internal Bank	**Finansial**	**Hukum**	**Nasabah**
	<25% proses bisnis di fungsional bisnis lainnya.		mempengaruhi tingkat kesehatan bank.	
7 atau 8	Mengganggu 51%-71% proses bisnis pada internal fungsional bisnis dan 25%-50% proses bisnis di fungsional bisnis lainnya.	Menimbulkan kerugian finansial/biaya ekstra sebesar 21% - 30%	Melakukan pelanggaran regulasi internal dan hukum eksternal perusahaan, yang berpotensi mempengaruhi tingkat kesehatan bank.	Mengganggu 51% - 75% proses pelayanan bank kepada nasabah
9 atau 10	Mengganggu >75% proses bisnis pada internal fungsional bisnis dan	Menimbulkan kerugian finansial/biaya ekstra >30%	Melakukan pelanggaran regulasi internal dan hukum eksternal perusahaan, yang	Mengganggu >75% proses pelayanan bank kepada nasabah.

	KATEGORI DAMPAK			
	Internal Bank	**Finansial**	**Hukum**	**Nasabah**
	mengganggu >50% proses bisnis di fungsional bisnis lainnya.		secara langsung mempengaruhi tingkat kesehatan bank.	

Tabel 5. 8 Skala Dampak (Sumber: FMEA diolah peneliti, 2014)

		KATEGORI DAMPAK			
		Internal Bank	**Finansial**	**Hukum**	**Nasabah**
NILAI DAMPAK	**1 atau 2**	Tidak ada dampak pada internal bank	Tidak ada dampak secara finansial kepada perusahaan	Tidak melanggar regulasi dan hukum internal dan eksternal perusahaan.	Tidak berdampak secara langsung kepada nasabah
	3 atau 4	Mengganggu <25% proses bisnis pada internal fungsional bisnis	Menimbulkan kerugian finansial/ biaya ekstra <10%	Melakukan pelanggaran regulasi internal perusahaan.	Mengganggu <25% proses pelayanan bank kepada nasabah.
	5 atau 6	Mengganggu 25% -50% proses bisnis pada internal fungsional bisnis dan	Menimbulkan kerugian finansial/biaya ekstra sebesar 10% - 20%	Melakukan pelanggaran regulasi internal dan hukum eksternal, namun tidak	Mengganggu 25% - 50% proses pelayanan bank kepada nasabah.

	KATEGORI DAMPAK			
	Internal Bank	**Finansial**	**Hukum**	**Nasabah**
	<25% proses bisnis di fungsional bisnis lainnya.		mempengaruhi tingkat kesehatan bank.	
7 atau 8	Mengganggu 51%-71% proses bisnis pada internal fungsional bisnis dan 25%-50% proses bisnis di fungsional bisnis lainnya.	Menimbulkan kerugian finansial/biaya ekstra sebesar 21% - 30%	Melakukan pelanggaran regulasi internal dan hukum eksternal perusahaan, yang berpotensi mempengaruhi tingkat kesehatan bank.	Mengganggu 51% - 75% proses pelayanan bank kepada nasabah
9 atau 10	Mengganggu >75% proses bisnis pada internal fungsional bisnis dan	Menimbulkan kerugian finansial/biaya ekstra >30%	Melakukan pelanggaran regulasi internal dan hukum eksternal perusahaan, yang	Mengganggu >75% proses pelayanan bank kepada nasabah.

	KATEGORI DAMPAK			
	Internal Bank	**Finansial**	**Hukum**	**Nasabah**
	mengganggu >50% proses bisnis di fungsional bisnis lainnya.		secara langsung mempengaruhi tingkat kesehatan bank.	

Detection adalah tingkat efektivitas metode atau kemampuan untuk mendeteksi terjadinya suatu risiko. Deteksi berkaitan dengan kemampuan dari teknik deteksi untuk mendeteksi peristiwa yang memiliki risiko secara tepat, sehingga perusahaan/organisasi dapat melakukan perencanaan dan melakukan tindakan terhadap risiko yang terdeteksi tersebut.

Tabel 5. 9 Skala Deteksi (Sumber: FMEA, 2014)

SKOR DETEKSI	KEMAMPUAN METODE DETEKSI TERHADAP RISIKO
9 atau 10	Tidak ada metode deteksi atau metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi.
7 atau 8	Metode deteksi tidak terbukti (tidak andal) atau efektivitas metode deteksi tidak diketahui untuk mendeteksi tepat waktu.
5 atau 6	Metode deteksi memiliki tingkat efektivitas yang rata-rata (medium).
3 atau 4	Metode deteksi memiliki tingkat efektivitas yang tinggi.
1 atau 2	Metode deteksi sangat efektif dan hampir pasti risiko akan terdeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi.

Berdasarkan beberapa komponen penghitungan nilai tersebut, berikut ini akan dilampirkan mengenai hasil identifikasi risiko dan analisis risiko berdasarkan proses bisnis dengan nilai dampak yang paling tinggi. Hasil identifikasi risiko dilengkapi dengan komponen penyebab risiko dan dampak risiko. Hasil analisis risiko akan menghasilkan nilai risiko (*Risk Score)* dan angka prioritas

risiko (*Risk Priority Number)* yang didapatkan berdasarkan penghitungan berikut.

Risk Score = Likelihood x Impact

Risk Priority Number = Likelihood x Impact x Detection

Berdasarkan perhitungan tersebut, perusahaan akan mengetahui tingkatan (level) dari masing-masing risiko teknologi informasi, sesuai dengan *likelihood, impact* dan deteksinya.

Sebagai contoh dari proses identifikasi dan penilaian risiko, lihat Lampiran E.1 atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

8.1.3 Evaluasi Risiko

Evaluasi risiko adalah proses membandingkan hasil dari analisis risiko dengan kriteria risiko untuk menetapkan risiko beserta besarannya dapat diterima atau ditoleransi oleh perusahaan (ISO *Guide* 73, 2009). Tujuan dari evaluasi risiko adalah untuk membantu dalam membuat keputusan berdasarkan hasil analisis risiko yang telah dilakukan.Untuk menentukan tingkatan dari setiap risiko, maka skala yang digunakan adalah dari FMEA (*Failure Mode and Effect Analysis*). Berikut ini adalah penentuan level risiko berdasarkan nilai RPN dari FMEA.

Tabel 5. 10 Penentuan Level Risiko (Sumber: FMEA, 2014)

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

8.2 Perlakuan Risiko

Perlakuan risiko adalah sebuah proses untuk melakukan modifikasi risiko (ISO *GUIDE* 73, 2009). Strategi yang digunakan untuk mengatasi ancaman atau risiko yang dapat memberikan dampak negatif kepada perusahaan adalah sebagai berikut (PMBOK Guide, 2008).

1. *Avoid*
   Suatu tindakan menghindari risiko dan menghilangkan seluruh ancaman yang potensial. Hal yang dapat dilakukan dalam strategi ini adalah mengubah strategi, meningkatkan komunikasi dalam penggalian informasi, meningkatkan keahlian atau melakukan usaha lainnya untuk dapat menanggulangi ancaman tersebut.
2. *Transfer*
   Tindakan pengalihan atau perpindahan kepemillikan risiko kepada pihak ketiga. Strategi ini dilakukan apabila kemampuan pemilik risiko dalam mengelola risiko lebih kecil/rendah dibandingkan dengan

kemampuan pihak ketiga yang bekerja sama dengan perusahaan.

3. *Mitigate*
   Strategi ini merupakan tindakan mengurangi probabilitas dan minimalisasi dampak yang merugikan untuk perusahaan. Strategi ini membutuhkan pengembangan *prototype* untuk mengurangi risiko. Tindakan meminimalisasi dampak dapat dilakukan melalui aktivitas pemantauan secara berkala.
4. *Accept*
   Tindakan penerimaan risiko dilakukan ketika pemilik risiko tidak dapat mengeliminasi ancaman yang potensial di perusahaan. Tindakan penerimaan risiko ini dibagi menjadi dua yaitu, penerimaan pasif dan aktif. Penerimaan pasif yaitu ketika pemilik risiko tidak melakukan tindakan apapun kecuali pendokumentasian strategi dan menghadapi risiko yang terjadi. Penerimaan aktif yaitu ketika pemilik risiko membuat perencanaan yang digunakan sebagai cadangan. Alokasi cadangan yang dibuat dapat berupa cadangan waktu, biaya dan sumber daya lainnya.

Untuk memperjelas standar tersebut, maka berikut ini peneliti akan memberikan uraian mengenai tanggapan risiko beserta contohnya dari sebuah konsultan dari California Amerika Serikat yang memiliki spesialisasi terhadap strategi, teknologi, manajemen program dan perubahan untuk perusahaan. Konsultan ini bernama Oulixeus *Consulting* Ltd.

Tabel 5. 11 Perlakuan Risiko (Sumber: Oulixeus Consulting, 2010)

PERLAKUAN RISIKO	PENGERTIAN
Avoid	Tujuan : mengurangi kemungkinan (*likelihood*) dan berusaha untuk menghilangkan kemungkinan terjadinya risiko.

PERLAKUAN RISIKO	PENGERTIAN
	Operasional: risiko yang dapat membuat kelebihan anggaran (*over-budget*) karena perusahaan belum berpengalaman terhadap suatu hal.
	Teknologi: Risiko yang mengakibatkan keterlambatan implementasi fitur.
Mitigasi	Tujuan: mengurangi dampak atas terjadinya risiko.
	Operasional: Risiko yang terjadi ketika tidak memiliki kapasitas yang cukup untuk menerima pesanan dari pelanggan.
	Teknologi: Risiko yang terjadi ketika tidak menerima data yang benar dari pelanggan.
Transfer	Tujuan: memindahkan dampak risiko yang terjadi kepada pihak eksternal.
	Operasional: Risiko kebakaran aset perusahaan yang dilakukan oleh pihak internal perusahaan. Transfer dilakukan dengan membeli asuransi kebakaran.
	Teknologi: Risiko adanya pelanggan yang tidak mengerti cara penggunaan produk dan membutuhkan bantuan. Transfer yang dilakukan adalah dengan cara menggunakan *outsourcing* untuk layanan *help-desk.*

PERLAKUAN RISIKO	PENGERTIAN
Accept	Tujuan: proses pembuatan keputusan secara aktif untuk menerima konsekuensi (dampak) ketika risiko terjadi. Respon ini dilakukan ketika dampak risiko jauh lebih kecil daripada biaya untuk menghindari, mengurangi atau transfer risiko.
	Operasional: Risiko keterlambatan pekerjaan yang tidak sesuai dengan tempo waktu.
	Teknologi: Risiko penggunaan teknologi baru yang justru meningkatkan usaha untuk *debugging* (mengeliminasi kesalahan) dan usaha pengujian sistem.

Sebagai contoh proses evaluasi dan perlakuan risiko lihat Lampiran E.2 atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

8.2.1 Aksi Mitigasi

Setelah mengidentifikasi respon atau tanggapan manajemen dari masing-masing risiko, maka langkah selanjutnya adalah menentukan aksi mitigasi yang harus dilakukan dari masing-masing risiko yang ada. Hal ini akan menjadi suatu langkah pencegahan yang bisa meminimalisasi risiko yang mungkin mengganggu jalannya operasional bisnis perusahaan.

Sebagai contoh proses evaluasi dan perlakuan risiko lihat Lampiran E.3 atau lihat Buku Produk BCP BPR

Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

8.2.2 Pemilihan Risiko

Proses pemilihan risiko adalah sebagai tindak lanjut perusahaan dari aksi mitigasi yang direncanakan. Risiko teknologi informasi tersebut akan dipilih dari masing-masing fungsional bisnis yang ada, sehingga perusahaan dapat menentukan fokus risiko dari masing-masing fungsional bisnis yang ada.

8.2.2.1 Risiko per Fungsional Bisnis

Pada bagian ini, akan diklasifikasikan setiap risiko teknologi informasi yang terdapat pada masing-masing fungsional bisnis perusahaan. Berdasarkan penghitungan, berikut ini adalah hasil dari risiko yang terdapat di setiap fungsional bisnis.

Tabel 5. 12 Risiko Setiap Fungsional Bisnis (Sumber: Peneliti, 2014)

FUNGSIONAL BISNIS	LEVEL RISIKO	JUMLAH
Teknologi dan Sistem Informasi	*Very High* *High* *Medium*	12 5 4
Operasional	*Very High* *High* *Medium* *Low*	1 2 5 2
Pembukuan	*High* *Medium*	2 6
Kredit	*High* *Medium*	3 1
Personalia	*High* *Medium* *Low*	2 1 1

Untuk informasi selengkapnya, lihat Dokumen Produk BCP BPR Bank Surya Yudha Banjarnegara.

8.2.2.2 Fokus Risiko

Pada bagian fokus risiko ini, perusahaan akan menentukan risiko TI yang akan ditindaklanjuti dari setiap bagian/fungsional bisnis yang ada. Tindak lanjut yang dilakukan adalah menghasilkan sebuah produk regulasi (dokumen tata kelola) yang akan mengatur hal-hal yang akan membantu perusahaan dalam mengatasi risiko yang muncul tersebut. Regulasi-regulasi tersebut dibuat berdasarkan aksi mitigasi yang telah ditetapkan.

Regulasi yang diusulkan tidak secara keseluruhan dibuat oleh peneliti, dikarenakan regulasi-regulasi tersebut sudah dibuat dan diimplementasikan di perusahaan, sehingga peneliti hanya membuat beberapa regulasi yang belum dibuat di perusahaan ini.

Sebagai contoh proses evaluasi dan perlakuan risiko lihat Lampiran E.4 atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

9. STRATEGI KEBERLANJUTAN BISNIS

Strategi keberlanjutan bisnis dilakukan untuk mengukur tingkat efektivitas dari BCP di perusahaan. Strategi yang dibuat dapat berbentuk strategi pencegahan, pemulihan, pengawasan, maupun strategi untuk mengatasi risiko lainnya. Penyusunan strategi ini juga dapat menjadi alat untuk menetukan aktivitas serta proses yang menjadi prioritas untuk dilanjutkan ke tahapan selanjutnya.

Sebagai contoh kebijakan BCP lihat Lampiran F atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

10. PROSEDUR KEBERLANJUTAN BISNIS

Prosedur keberlanjutan bisnis dilakukan untuk mengelola gangguan dan melanjutkan aktivitas berdasarkan tujuan pemulihan dan proses bisnis kritis pada analisis dampak bisnis. Prosedur ini dapat berupa tanggapan terhadap insiden atau gangguan di perusahaan. Prosedur keberlanjutan bisnis berisi

deskripsi tindakan pertama yang dilakukan, skenario risiko, pelaporan yang ditujukan untuk memulihkan gangguan. Prosedur keberlanjutan bisnis dilengkapi oleh formulir atau *checklist* untuk memeriksa implementasi prosedur pada saat terjadi insiden atau gangguan di perusahaan.

Sebagai contoh prosedurBCP lihat Lampiran G atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

11. PELATIHAN DAN PENGUJIAN

Proses pelatihan dan pengujian dilakukan untuk memastikan bahwa dokumen BCP yang dibuat sesuai dengan kebutuhan serta layak untuk diimplementasikan. Proses pelatihan dapat dijadwalkan oleh perusahaan, untuk memastikan bahwa karyawan atau seluruh SDM di perusahaan tersebut telah memahami strategi serta prosedur yang harus dilakukan ketika terjadi gangguan/bencana.

Pengujian dapat dilakukan sesuai dengan kebutuhan perusahaan. Pengujian dapat dibedakan menjadi pengujian parsial dan pengujian total. Pengujian parsial dilakukan hanya pada unit-unit tertentu atau proses bisnis tertentu saja. Pengujian total dilakukan pada seluruh proses bisnis yang terkait dengan penyusunan BCP perusahaan.

Pengujian juga dapat dilakukan dengan pihak eksternal perusahaan, seperti mitra kerja perusahaan maupun pihak lain yang bersangkutan dengan perusahaan, untuk menjalankan BCP pada saat kondisi kritis.

Dalam penelitian ini, pengujian dilakukan secara parsial pada Bagian Teknologi dan Sistem Informasi, dengan skenario penyerangan sistem *core banking* di BPR Bank Surya Yudha Banjarnegara. Proses ini akan menjadi validasi bagi BCP ini secara parsial, di mana akan diuji implementasi prosedur penanganan serangan penyalahgunaan sistem dan penghitungan nilai lihat Lampiran K sebagai bukti dokumentasi, Lampiran F dan G untuk dokumentasi Kebijakan dan Prosedur atau

selengkapnya lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara.

Tabel 5. 13 Skenario Pengujian BCP (Sumber: Peneliti, 2014)

SKENARIO PENGUJIAN BCP	
Hari/Tanggal	Rabu, 21 Mei 2014
Tempat	Bagian Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara
Pelaku	1. Peneliti 2. Karyawan TSI 3. Pimpinan TSI
Pembagian Peran	1. Peneliti: sebagai pengamat dan dokumentator dari pengujian BCP. 2. Karyawan TSI : Sebagai penyerang sistem *Core Banking* AS-400. 3. Pimpinan Bagian TSI: Sebagai pihak yang menangani serangan.
Skenario	1. Karyawan TSI mencoba untuk masuk ke dalam sistem *Core Banking* AS-400 melalui jaringan. 2. Pimpinan TSI melakukan pemantauan keamanan sistem dengan menggunakan skenario yang terdapat pada Prosedur Pemantauan dan Evaluasi Keamanan Sistem. 3. Pimpinan TSI mencoba menangani adanya serangan yang muncul dengan menggunakan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai. 4. Peneliti mendokumentasikan hasil pengujian BCP.

Hasil pengujian tersebut menjadi bukti verifikasi dan validasi BCP di BPR Bank Surya Yudha Banjarnegara (Lihat Lampiran

C). Untuk informasi selengkapnya, lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara.

5.1.3 Check (Pemeriksaan)

Pada fase ini pemantauan dan peninjauan dilakukan untuk memeriksa seluruh proses yang ada di BCP telah sesuai dengan kebutuhan perusahaan, kebijakan serta tujuan bisnis perusahaan. Perusahaan akan melakukan audit teknologi informasi oleh bagian teknologi informasi itu sendiri sebagai kontrol internal, audit teknologi informasi oleh perusahaan tersebut serta peninjauan manajemen oleh pihak direksi perusahaan.

12. AUDIT TI INTERNAL BAGIAN

Proses audit teknologi informasi pada internal bagian teknologi informasi di perusahaan, akan menjadi peran penting bagi pemeriksaan keberhasilan implementasi BCP di perusahaan. Pemeriksaan ini dilakukan oleh pihak internal bagian untuk memastikan bahwa implementasi BCP berada di bawah pengawasan. Pemeriksaan ini membutuhkan media seperti formulir maupun *checklist* sebagai dokumentasi pengawasan yang dilakukan oleh internal bagian teknologi informasi di perusahaan.

Sebagai contoh kebijakan BCP lihat Lampiran H atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

13. AUDIT TI INTERNAL PERUSAHAAN

Proses audit internal perusahaan akan memeriksa bahwa implementasi BCP di perusahaan sesuai dengan perencanaan yang ada. Proses pemeriksaan ini akan memberikan kesan objektif dan kesadaran dari pihak perusahaan tentang optimalisasi penyusunan BCP di perusahaan.

Pada bagian audit internal perusahaan ini, ada beberapa hal yang perlu dilakukan pemeriksaan yaitu:

1. Kesesuaian BCP dengan kebutuhan dan tujuan perusahaan.
2. Kesesuaian pelaksanaan BCP dengan Kerangka BCP.
3. Kesesuaian peran dan tanggung jawab setiap SDM dalam Komite BCP.
4. Hasil pelatihan dan pengujian BCP sebagai bentuk validasi BCP untuk peningkatan secara terus-menerus.

Sebagai contoh kebijakan BCP lihat Lampiran I atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

14. PENINJAUAN MANAJEMEN

Peninjauan manajemen dilakukan untuk memastikan bahwa BCP telah dijalankan sesuai dengan tujuan perusahaan, kebutuhan perusahaan, tata kelola TI dan regulasi yang diterapkan di perusahaan. Peninjauan dilakukan oleh pihak manajemen dalam jangka waktu tertentu. Hal-hal yang perlu ditinjau oleh pihak manajemen adalah:

1. Kondisi kekinian dari kegiatan yang sudah ditinjau sebelumnya
2. Perubahan internal dan eksternal yang mempengaruhi BCP
3. Informasi performa proses keberlanjutan bisnis yang dapat berupa pemantauan, evaluasi dan hasil audit internal bagian serta perusahaan.

Sebagai contoh kebijakan BCP lihat Lampiran J atau lihat Buku Produk BCP BPR Bank Surya Yudha Banjarnegara untuk informasi selengkapnya.

5.1.4 Act (Tindakan)

Pada fase ini, perusahaan akan melakukan peningkatan secara terus-menerus (*continuous improvement*) untuk BCP Perusahaan. Hal ini dilakukan agar BCP yang

diimplementasikan di perusahaan dapat menjadi hal yang terus-menerus dinamis, mengikuti perkembangan zaman sesuai dengan kebutuhan perusahaan.

15. PENINGKATAN SECARA TERUS-MENERUS

Untuk menghasilkan BCP yang selalu mengalami peningkatan dan perbaikan di setiap fasenya, perusahaan perlu memperhatikan suatu fase yang berpengaruh terhadap penyusunan dan penerimaan BCP di perusahaan. Fase yang dapat dilakukan adalah melalui *Continuous Improvement* (Peningkatan secara terus-menerus). Fase ini mendukung kebutuhan perusahaan, bahwa teknologi informasi yang berkembang harus selalu dinamis dan mengikuti perkembangan TI di dunia.

Proses peningkatan secara terus-menerus atau *continuous improvement* adalah sebuah proses yang dilakukan dari proses-proses sebelumnya seperti:

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

Selain itu, proses *continuous improvement* juga memperhatikan hal-hal yang berada di luar fase kerangka BCP yang dibuat yaitu:

1. Hasil forum komite pengarah TI (*IT Steering Committee*-ITSC) yang akan dilakukan secara periodik.
2. Peraturan Bank Indonesia (baik yang sudah diimplementasikan, maupun rencana yang sudah disosialisasikan oleh pihak BI).
3. Peraturan dari institusi lain yang bersangkutan, seperti Dinas Ketenagakerjaan, Transmigrasi dan Kesejahterahaan Sosial (Disnakertranskesos), Direktorat Jenderal Pajak, Departemen Keuangan maupun institusi lainnya yang erat kaitannya dengan perbankan.

Proses *continuous improvement* menjadi isu yang menarik dalam kerangka BCP ini, karena proses penyusunan BCP ini menggunakan acuan analisis kebutuhan perusahaan (pendekatan

mundur). Sehingga perusahaan harus proaktif untuk terus meningkatkan kualitas dari BCP secara terus-menerus, dan proses ini bisa dilakukan secara periodik (misal 1 tahun 1 kali) dengan pelaporan kepada Ketua BCP (Direksi) dan Komisaris perusahaan.

BAB VI
PENUTUP

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

6.1 Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut.

Kesimpulan Pertama

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

1. Menghasilkan identifikasi risiko teknologi informasi untuk BPR Bank Surya Yudha Banjarnegara (Lihat Buku Komplementer).
2. Menghasilkan penilaian risiko teknologi informasi yang sesuai dengan ISO 31000:2009 di BPR Bank Surya Yudha Banjarnegara (Lihat Buku Komplementer).
3. Menghasilkan Kerangka BCP BPR Bank Surya Yudha Banjarnegara yang sesuai dengan kebutuhan serta keinginan perusahaan terkait keberlanjutan bisnis.

Kesimpulan Kedua

Business Continuity Plan (BCP) adalah sesuatu yang unik. BCP harus dilandasi oleh kebutuhan di perusahaan masing-masing. Karena pada dasarnya tidak ada suatu standar atau *best practice* BCP manapun yang tepat secara keseluruhan untuk sebuah perusahaan. Setiap standar BCP yang ada perlu dilakukan penyesuaian dengan kebutuhan perusahaan,dengan menggunkan analisis sintesis yaitu mengambil yang sesuai dan tidak mengambil yang tidak sesuai dengan kebutuhan perusahaan.

Kesimpulan Ketiga

Kerangka BCP dengan proses pendekatan mundur (melakukan analisis kebutuhan perusahaan terlebih dahulu, baru melakukan sintesis standar kerangka BCP yang digunakan, serta melakukan formulasi standar Kerangka BCP agar sesuai dengan

kebutuhan perusahaan) memerlukan sebuah fase peningkatan secara terus-menerus (*continuous improvement*) yang kuat dan dilakukan secara periodik. Hal ini dilakukan karena kebutuhan perusahaan dapat berubah-ubah sesuai dengan perkembangan teknologi informasi yang dinamis maupun regulasi (peraturan BI, peraturan institusi lainnya) yang berubah atau berkembang sesuai dengan kondisi perbankan di dunia.

6.2 Saran

Saran dari penelitian ini berupa perbaikan untuk keberlanjutan penelitian ini, maupun penelitian selanjutnya. Berikut ini saran yang disampaikan dari penelitian ini.

Saran untuk keberlanjutan penelitian ini

Penelitian ini adalah penelitian yang terus berkembang. Kerangka BCP disusun sesuai dengan kebutuhan perusahaan, di mana kebutuhan tersebut dapat berubah sesuai dengan perkembangan teknologi informasi yang dinamis atau perubahan regulasi perbankan. Oleh karena itulah peningkatan secara terus-menerus (*continuous improvement*) menjadi sangat penting untuk dilakukan demi kualitas dari keberlanjutan penelitian ini.

Saran untuk penelitian selanjutnya

Untuk memastikan bahwa Kerangka BCP ini benar-benar sesuai dengan kebutuhan perusahaan, lakukan langkah-langkah penyusunan BCP ini di BPR (Bank Perkreditan Rakyat) lainnya. Hal ini akan membuka wacana akan pentingnya manajemen risiko di dunia perbankan, khususnya di BPR. Hal tersebut juga dapat membuktikan bahwa Kerangka BCP yang dibuat haruslah unik, sesuai dengan kebutuhan dan tujuan perusahaan setempat.

LAMPIRAN A

Lampiran Dokumen Verifikasi
Kesesuaian Kebutuhan dan Keinginan Perusahaan terhadap
Business Continuity Plan (BPR Bank Surya Yudha Banjarnegara

Surat Konfirmasi

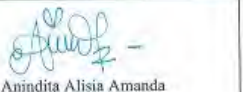
Kesesuaian Kebutuhan dan Keinginan Perusahaan terhadap
Business Continuity Plan (BCP) BPR Bank Surya Yudha Banjarnegara

Dengan hormat,

Saya yang bertanda tangan di bawah ini:
nama : Anindita Alisia Amanda
NRP : 5210100162
pekerjaan : Mahasiswa Sistem Informasi, Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian kebutuhan dan keinginan perusahaan terhadap penelitian penyusunan *Business Continuity Plan* (BCP) atau perencanaan keberlanjutan bisnis di BPR Bank Surya Yudha Banjarnegara kepada pimpinan di Bagian Teknologi Sistem dan Informasi BPR Bank Surya Yudha Banjarnegara.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi terhadap kebutuhan dan keinginan perusahaan yang akan menunjang kerangka kerja atau model BCP yang dibuat secara khusus untuk perusahaan tersebut. Atas perhatian dan kesediaan Bapak/Ibu Pimpinan, saya mengucapkan terima kasih.

PERSETUJUAN KONFIRMASI Banjarnegara, Senin 19 Mei 2014	
Mengetahui, Pimpinan Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara	Peneliti
 Ir. Sri Mulyadi, MBA	 Anindita Alisia Amanda 5210100162

LAMPIRAN B

Lampiran Dokumen Verifikasi
Kesesuaian Kerangka Kerja Business Continuity Plan (BCP)
untuk BPR Bank Surya Yudha Banjarnegara

Surat Konfirmasi

Kesesuaian Kerangka Kerja *Business Continuity Plan* (BCP) untuk
BPR Bank Surya Yudha Banjarnegara

Dengan hormat,

Saya yang bertanda tangan di bawah ini:

nama : Anindita Alisia Amanda
NRP : 5210100162
pekerjaan : Mahasiswa Sistem Informasi, Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian Kerangka Kerja *Business Continuity Plan* (BCP) untuk BPR Bank Surya Yudha Banjarnegara kepada pimpinan di Bagian Teknologi Sistem dan Informasi BPR Bank Surya Yudha Banjarnegara.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi kerangka kerja atau model BCP yang dibuat secara khusus untuk BPR Bank Surya Yudha Banjarnegara

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

PERSETUJUAN KONFIRMASI Banjarnegara, Rabu 21 Mei 2014	
Mengetahui, Pimpinan Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara	Peneliti
Ir. Sri Mulyadi, MBA	Anindita Alisia Amanda 5210100162

LAMPIRAN C

Lampiran Dokumen Verifikasi
Kesesuaian Dokumen BCP BPR Bank Surya Yudha Banjarnegara

Surat Konfirmasi
Kesesuaian Dokumen *Business Continuity Plan* (BCP) untuk
BPR Bank Surya Yudha Banjarnegara

Dengan hormat,

Saya yang bertanda tangan di bawah ini:
nama : Anindita Alisia Amanda
NRP : 5210100162
pekerjaan : Mahasiswa Sistem Informasi, Institut Teknologi Sepuluh Nopember

dengan ini menyatakan permohonan konfirmasi atas kesesuaian Dokumen *Business Continuity Plan* (BCP) untuk BPR Bank Surya Yudha Banjarnegara kepada pimpinan di Bagian Teknologi Sistem dan Informasi BPR Bank Surya Yudha Banjarnegara.

Konfirmasi ini dilakukan sebagai langkah untuk melakukan verifikasi isi dokumen BCP yang dibuat secara khusus, sesuai dengan kebutuhan BPR Bank Surya Yudha Banjarnegara

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

PERSETUJUAN KONFIRMASI Banjarnegara, Rabu 21 Mei 2014	
Mengetahui, Pimpinan Teknologi dan Sistem Informasi BPR Bank Surya Yudha Banjarnegara	Peneliti
Ir. Sri Mulyadi, MBA	Anindita Alisia Amanda 5210100162

LAMPIRAN D

Lampiran Contoh Analisis Dampak Bisnis

D.1 Identifikasi Proses Bisnis dan Penilaian Dampak

FUNGSIONAL BISNIS	PROSES BISNIS	DESKRIPSI PROSES BISNIS	NILAI DAMPAK
PEMBUKUAN	*Posting Backdate*	Melakukan pengembalian tanggal pada sistem kepada tanggal pada akhir bulan sebelumnya, setelah menghitung taksiran pajak pada awal bulan selanjutnya.	7
OPERASIONAL	Input Data Nasabah	Sistem digunakan untuk melakukan input, menyimpan dan menampilkan data nasabah.	5
PE\RSONALIA	HRD (Data Karyawan)	Sistem yang digunakan untuk melakukan input data pribadi karyawan dan dapat menampilkan data pribadi karyawan ketika dibutuhkan. (Data: identitas pribadi, data keluarga, pendidikan, data asuransi, NPWP, mutasi, promosi, rotasi, Foto diri)	4

D.2 Estimated Downtime

FUNGSIONAL BISNIS	PROSES BISNIS	RTO	RPO
PEMBUKUAN	Posting Backdate	< 1 jam	9 jam
OPERASIONAL	Input Data Nasabah	1 jam	9 jam
PERSONALIA	HRD (Data Karyawan)	7 hari	9 jam

LAMPIRAN E

Lampiran Contoh Manajemen Risiko

E.1 Risk Register berdasarkan Nilai Dampak

FUNGSIONAL BISNIS	PROSES BISNIS	DESKRIPSI PROSES BISNIS	NILAI DAMPAK	RISK ID	IDENTIFI-KASI RISIKO	PENYEBAB	DAMPAK	L	I	RS	D	RPN
PEMBUKUAN	*Posting Backdate*	Melakukan pengembalian tanggal pada sistem kepada tanggal pada akhir bulan sebelumnya, setelah menghitung taksiran pajak pada awal bulan selanjutnya.	7	PB06	Sistem tidak dapat melakukan *posting backdate*	- Koneksi jaringan internet yang bermasalah / terputus.	- Tidak bisa melakukan koreksi pada neraca akhir bulan sebelum-nya. - Menggang-gu optimalisa-si laporan keuangan.	4	5	**20**	6	**120**
OPERASIONAL	Input Data Nasabah	Sistem digunakan untuk melakukan input, menyimpan dan menampilkan data nasabah.	5	OP04	Kegagalan sistem pada modul input data nasabah	- Koneksi jaringan internet terputus.	- Penurunan kualitas pelayanan bank kepada	5	5	**25**	4	**100**

FUNGSIONAL BISNIS	PROSES BISNIS	DESKRIPSI PROSES BISNIS	NILAI DAMPAK	RISK ID	IDENTIFI-KASI RISIKO	PENYEBAB	DAMPAK	L	I	RS	D	RPN
							nasabah.					
						- Terjadi kelumpuhan sistem dari pusat (*server down*).	- Nasabah tidak dapat membuka rekening baru.					
							- Nasabah tidak dapat melakukan realisasi kredit.					
				OP05	Kesalahan input data nasabah oleh pengguna sistem.	- Penggunaan sistem yang tidak sesuai dengan SOP. - Kurangnya informasi dan edukasi mengenai input data nasabah oleh pengguna sistem.	- Informasi data nasabah yang tidak sebenarnya.	5	5	**25**	5	**125**
PERSONALIA	HRD (Data Karyawan)	Sistem yang digunakan untuk melakukan input data pribadi	4	PR03	Kesalahan penggunaan sistem oleh karyawan	- Kurangnya edukasi dan penyebaran informasi	- Operasional bank terhambat	8	6	**48**	4	**192**

FUNGSIONAL BISNIS	PROSES BISNIS	DESKRIPSI PROSES BISNIS	NILAI DAMPAK	RISK ID	IDENTIFI-KASI RISIKO	PENYEBAB	DAMPAK	L	I	RS	D	RPN
		karyawan dan dapat menampilkan data pribadi karyawan ketika dibutuhkan. (Data: identitas pribadi, data keluarga, pendidikan, data asuransi, NPWP, mutasi, promosi, rotasi, Foto diri)			perusahaan	mengenai penggunaan sistem dan teknologi informasi. -Ketidak-pedulian karyawan perusahaan terhadap teknologi dan sistem informasi beserta prosedur yang diterapkan (minimum IT awareness) -Budaya teknologi informasi yang masih minim di lingkungan kerja.	- Penyalah-gunaan wewenang sistem - Perkem-bangan teknologi informasi menjadi terhambat. - Proses pengujian dan implementa si sistem menjadi terhambat karena ketidaksiap an pengguna.					

E.2 Evaluasi Risiko

RISK ID	IDENTIFIKASI RISIKO	L	I	RS	D	RPN	LEVEL RISIKO	RISK RESPONSE
PR03	Kesalahan penggunaan sistem oleh karyawan perusahaan	8	6	**48**	4	**192**	*High*	*Avoid*
OP05	Kesalahan input data nasabah oleh pengguna sistem.	5	5	**25**	5	**125**	*High*	*Mitigate*
PB06	Sistem tidak dapat melakukan *posting backdate*	4	5	**20**	6	**120**	*Medium*	*Avoid*
OP04	Kegagalan sistem pada modul input data nasabah	5	5	**25**	4	**100**	*Medium*	*Avoid*

E.3 Aksi Mitigasi

Risk ID	Identifikasi Risiko	Level Risiko	Risk Responses	Aksi Mitigasi
PR03	Kesalahan penggunaan sistem oleh karyawan perusahaan	High	Mitigate	1. Mengadakan pelatihan penggunaan sistem yang efektif dan efisien untuk para karyawan. 2. Mengadakan pengujian sistem (*user testing*) kepada pengguna yang akan menggunakan sistem. 3. Membuat regulasi yang mengatur peran karyawan terhadap perkembangan teknologi di perusahaan. 4. Mengadakan pemantauan dan evaluasi performa karyawan secara berkala.
OP05	Kesalahan input data nasabah oleh pengguna sistem.	High	Avoid	1. Membuat pedoman (*user manual book*) untuk penggunaan sistem input data nasabah. 2. Melakukan sosialisasi dan pembimbingan terhadap pengguna yang akan melakukan input data nasabah ke dalam sistem. 3. Mengatur konsekuesi bagi pengguna (karyawan) yang sering melakukan kesalahan secara individu maupun cabang.

Risk ID	Identifikasi Risiko	Level Risiko	Risk Responses	Aksi Mitigasi
PB06	Sistem tidak dapat melakukan *posting backdate*	Medium	Avoid	1. Melakukan pemantauan dan evaluasi terhadap sistem ketika akan melakukan posting *back date*. 2. Melakukan penyederhanaan proses sehingga tidak dibutuhkan transaksi *backdate.*
OP04	Kegagalan sistem pada modul input data nasabah	Medium	Avoid	Mempersiapkan metode alternatif secara manual untuk dapat melakukan input data nasabah.

E.4 Fokus Risiko

BAGIAN PERSONALIA						
Risk ID	**Identifikasi Risiko**	**Level Risiko**	**Aksi Mitigasi**	**Tindak Lanjut**	**Alasan**	**Status**
PR03	Kesalahan penggunaan sistem oleh karyawan perusahaan	High	1. Mengadakan pendidikan pengembangan teknologi informasi di perusahaan untuk seluruh karyawan. 2. Membuat regulasi yang mengatur peran karyawan terhadap perkembangan teknologi di perusahaan. 3. Mengadakan pelatihan penggunaan sistem yang efektif dan	**1. Regulasi Pendidikan Perkembangan Teknologi Informasi di Perbankan**	Hal ini dapat membantu perusahaan dalam meningkatkan kepedulian karyawan terhadap perkembangan teknologi informasi di perusahaan.	Belum Ada
				2. Regulasi Forum ITSC	Hal ini dapat menunjang perusahaan untuk mengatur	Belum Ada

BAGIAN PERSONALIA						
Risk ID	**Identifikasi Risiko**	**Level Risiko**	**Aksi Mitigasi**	**Tindak Lanjut**	**Alasan**	**Status**
			efisien untuk para karyawan. 4. Melakukan pengembangan aplikasi dengan melibatkan pengguna (karyawan perusahaan).		peran setiap karyawan terhadap perkembangan teknologi di perusahaan.	
				3. Regulasi SDLC (UAT)	Hal ini dapat menunjang pengadaan pelatihan penggunaan sistem yang efektif dan efisien untuk para pengguna, serta secara langsung akan melibatkan	Sudah Ada

BAGIAN PERSONALIA						
Risk ID	**Identifikasi Risiko**	**Level Risiko**	**Aksi Mitigasi**	**Tindak Lanjut**	**Alasan**	**Status**
					pengguna dalam pengembangan aplikasi.	

LAMPIRAN F

Lampiran Contoh Kebijakan Komite Pengarah Teknologi Informasi

BPR Bank Surya Yudha Banjarnegara
KEBIJAKAN KOMITE PENGARAH TEKNOLOGI INFORMASI

Lembar Pengesahan
KEBIJAKAN

Judul	Komite Pengarah Teknologi Informasi
No. Dokumen	K-PRS-002
Revisi	00

Versi	Tanggal Pembuatan	Tanggal Pengesahan

Disahkan Oleh	Dibuat Oleh
(Jabatan)	(Jabatan)
(NAMA)	(NAMA)

F.1 Kebijakan Komite Pengarah Teknologi Informasi

K-PRS-002	No. Revisi	00
Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

1. TUJUAN

Tujuan dari pembuatan kebijakan ini adalah sebagai landasan atau dasar dari penyelenggaraan Komite Pengarah Teknologi Informasi di BPR Bank Surya Yudha Banjarnegara.

2. RUANG LINGKUP

Ruang lingkup dari kebijakan ini adalah akan mengatur komite yang bertugas untuk melakukan tinjauan, penyesuaian, pemantauan dan penentuan prioritas pekerjaan yang sesuai dengan kebutuhan teknologi informasi di BPR Bank Surya Yudha Banjarnegara.

3. PENANGGUNG JAWAB

Penanggung jawab dari kebijakan ini adalah:

3.1 Komisaris
3.2 Direktur Utama
3.3 Direktur Umum
3.4 Kepala Bagian Kepatuhan
3.5 Kepala Bagian Teknologi dan Sistem Informasi (TSI)
3.6 Kepala Seksi Pengembangan Teknologi Informasi Bagian TSI

4. STANDAR ACUAN

Standar yang menjadi acuan dalam kebijakan ini adalah

K-PRS-002	No. Revisi	00
Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

berdasarkan Peraturan Bank Indonesia (PBI) Nomor 9/15/PBI/2007 Pasal 7 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi.

5. ISI KEBIJAKAN

5.1 DEFINISI

Komite **pengarah IT** yang terdiri dari **eksekutif, bisnis, manajemen IT**, untuk menentukan **prioritas program investasi IT** yang sejalan dengan strategi dan prioritas bisnis perusahaan, melihat ***progress*** **proyek** dan menyelesaikan permasalahan sumber daya proyek dan **memantau *service level*** dan ***service improvements***. (COBIT 4.1)

5.2 LANDASAN HUKUM

Peraturan Bank Indonesia nomor 9/15/PBI/2007 pasal 7 tentang Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi.

Pasal 7

1. Bank wajib memiliki Komite Pengarah Teknologi Informasi (*InformationTechnology Steering Committe).*
2. Komite Pengarah Teknologi Informasi sebagaimana dimaksud pada ayat (1) bertanggung jawab memberikan rekomendasi kepada Direksi yang paling kurang terkait dengan:
3. Rencana Strategis Teknologi Informasi (*Information*

K-PRS-002	No. Revisi	00
Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

Technology Strategic Plan) yang searah dengan rencana strategis kegiatan usaha Bank;

4. Kesesuaian proyek-proyek Teknologi Informasi yang disetujui dengan Rencana Strategis Teknologi Informasi;
5. Kesesuaian antara pelaksanaan proyek-proyek Teknologi Informasi dengan rencana proyek yang disepakati (*project charter*);
6. Kesesuaian Teknologi Informasi dengan kebutuhan sistem informasi manajemen dan kebutuhan kegiatan usaha Bank;
7. Efektivitas langkah-langkah meminimalkan risiko atas investasi Bank pada sektor Teknologi Informasi agar investasi tersebut memberikan kontribusi terhadap tercapainya tujuan bisnis Bank;
8. Pemantauan atas kinerja Teknologi Informasi dan upaya peningkatannya;
9. Upaya penyelesaian berbagai masalah terkait Teknologi Informasi, yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara, secara efektif, efisien dan tepat waktu.
10. Komite Pengarah Teknologi Informasi sebagaimana dimaksud pada ayat (1) paling kurang beranggotakan:
11. Direktur yang membawahi satuan kerja Teknologi Informasi;

K-PRS-002	No. Revisi	00
Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

12. Direktur yang membawahi satuan kerja Manajemen Risiko;
13. Pejabat tertinggi yang membawahi satuan kerja penyelenggara Teknologi Informasi;
14. Pejabat tertinggi yang membawahi satuan kerja pengguna utama Teknologi Informasi.

5.3 TUJUAN KOMITE PENGARAH TI

Tujuan dari Komite Pengarah Teknologi Informasi adalah:

1. Untuk memastikan strategi Teknologi Informasi selaras dengan tujuan perusahaan BPR Bank Surya Yudha Banjarnegara.
2. Untuk meningkatkan kesadaran serta kepedulian seluruh bagian perusahaan, terkait perkembangan teknologi informasi yang dapat memberikan dukungan dan perubahan positif kepada operasional bank, baik secara internal maupun eksternal, terutama mendukung *fee base income*.

5.4 MANFAAT KOMITE PENGARAH TI

Manfaat dari Komite Pengarah Teknologi Informasi adalah:

1. Perkembangan teknologi informasi akan mendukung kemudahan dan kelancaran operasional, serta dapat meningkatkan pendapatan dan reputasi bank. Hal ini dikarenakan perkembangan teknologi informasi tidak

K-PRS-002	No. Revisi	00
Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

diarahkan ke solusi bagian TI saja, tetapi juga mengarah kepada solusi bisnis.

2. Mempermudah untuk membuat prioritas pekerjaan yang selaras dengan tujuan perusahaan, kondisi bank dan perkembangan perbankan di Indonesia dan dunia.
3. Meningkatkan komunikasi dan dukungan manajemen terhadap setiap proyek teknologi informasi yang dikerjakan.
4. Meningkatkan transparansi penentuan, prioritas, anggaran dan kemajuan proyek teknologi informasi.
5. Karena forum komite pengarah teknologi informasi melibatkan seluruh bagian di perusahaan, pimpinan dari bagian Non-TI dapat melihat lebih jauh arah pengembangan teknologi informasi serta manfaatnya bagi perkembangan bank.
6. Pimpinan dari Bagian Non-TI diharapkan dapat memberikan masukan yang berhubungan dengan TI untuk efektifitas dan efisiensi operasional maupun pertimbangan laba bank.

5.5 TUGAS DAN TANGGUNG JAWAB KOMITE PENGARAH TI

Tugas dan tanggung jawab Komite Pengarah Teknologi Informasi adalah:

K-PRS-002	No. Revisi	00
Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

1. Menentukan aturan dan tujuan Komite Pengarah TI.
2. Menentukan rencana jangka pendek dan jangka panjang TI perusahaan.
3. Menentukan prioritas pekerjaan atau proyek TI.
4. Melakukan tinjauan dan evaluasi kemajuan proyek.
5. Menentukan anggaran proyek dan evaluasi biaya proyek TI.
6. Menyelesaikan isu dan masalah yang muncul sehubungan dengan pengembangan proyek atau setelah proyek diimplementasikan.
7. Memastikan kelancaran koordinasi dengan bagian operasional, legal dan bagian yang terkait sehingga saat proyek diimplementasikan semua dapat berjalan lancar baik di sisi TI, operasional, prosedur, persiapan di lapangan, serta seluruh proses yang terkait dengan perusahaan.

5.6 ANGGOTA KOMITE PENGARAH TEKNOLOGI INFORMASI

Dalam implementasinya, anggota komite pengarah teknologi informasi dibagi menjadi 3, yaitu :

1. Manajemen

   Manajemen menjadi bagian dari anggota komite pengarah teknologi informasi, karena manajemen yang akan memberikan keputusan atas pengesahan proyek teknologi

K-PRS-002	No. Revisi	00
Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

informasi yang akan diselenggarakan. Manajemen yang ikut serta dalam keanggotaan ini adalah Komisaris dan Dewan Direksi, khususnya Direktur Umum yang membawahi Bagian TSI di BPR Bank Surya Yudha Banjarnegara.

2. Operasional

   Operasional adalah perwakilan dari pengguna yang mengusulkan atau sebagai pemilik teknologi dan sistem informasi yang diusulkan, yang juga mempunyai wewenang untuk memutuskan masalah yang akan dibahas. Anggota operasional terdiri dari Kawil/Kadiv/Kabag yang terkait.

3. Teknologi Informasi

   Keanggotaan teknologi infromasi merupakan peserta dari Bagian TSI. Keanggotaan ini merupakan peserta yang pham betul akan perkembangan teknologi informasi. Dalam forum komite pengarah TI nantinya, keanggotaan ini terdiri dari Pimpinan/Kabag TSI, KaSie di TSI dan staff atau karyawan yang bertanggung jawab atas suatu produk/proyek TI yang akan diimplementasikan.

6. DEFINISI DAN SINGKATAN

6.1 DEFINISI

1. Komite Pengarah Teknologi Informasi

   Komite pengarah teknologi informasi atau *Information Technology Steering Committee* (KOMITE PENGARAH TI) adalah suatu komite terdiri dari **eksekutif, bisnis,**

K-PRS-002	No. Revisi	00
Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

manajemen IT, untuk menentukan **prioritas program investasi IT** yang sejalan dengan strategi dan prioritas bisnis perusahaan, melihat ***progress*** **proyek** dan menyelesaikan permasalahan sumber daya proyek dan **memantau** ***service level*** dan ***service improvements*** (COBIT 4.1).

2. *Fee Based Income*

   Fee Based Income adalah sebuah keuntungan yang didapat dari transaksi yang diberikan dalam jasa-jasa bank lainnya, seperti inkaso, transfer, *safe deposit box,* surat kredit berdokumen, atau *travellers cheque* (Kashmir, 2001).

6.2 SINGKATAN

1. Kawil : Kepala Wilayah
2. Kadiv : Kepala Divisi
3. Kabag : Kepala Bagian
4. KaSie : Kepala Sie

7. DOKUMEN TERKAIT

6.1 Prosedur Mekanisme Forum Komite Pengarah Teknologi Informasi (P-PRS-002)

6.2 Formulir Audit Internal Teknologi Informasi (FAI-PRS-002)

F.2 Kebijakan Keamanan Informasi

<table>
<tr><td colspan="3">  </td></tr>
<tr><td colspan="3">BPR Bank Surya Yudha Banjarnegara
KEBIJAKAN KEAMANAN INFORMASI</td></tr>
<tr><td colspan="3">Lembar Pengesahan
KEBIJAKAN</td></tr>
<tr><td>Judul</td><td colspan="2">Keamanan Informasi</td></tr>
<tr><td>No. Dokumen</td><td colspan="2">K-TSI-001</td></tr>
<tr><td>Revisi</td><td colspan="2">00</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>Versi</td><td>Tanggal Pembuatan</td><td>Tanggal Pengesahan</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>Disahkan Oleh</td><td colspan="2">Dibuat Oleh</td></tr>
<tr><td>(Jabatan)</td><td colspan="2">(Jabatan)</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>(NAMA)</td><td colspan="2">(NAMA)</td></tr>
</table>

K-TSI-001	No. Revisi	00
Keamanan Informasi	Tanggal Pengesahan	
	Halaman	

KEBIJAKAN

1. TUJUAN

Tujuan dari pembuatan kebijakan ini adalah sebagai landasan atau dasar dari sistem keamanan informasi perbankan di BPR Bank Surya Yudha Banjarnegara.

2. RUANG LINGKUP

Ruang lingkup dari kebijakan ini adalah akan mengatur pengamanan informasi pada BPR Bank Surya Yudha Banjarnegara, yang memastikan beberapa hal berikut.

a. Informasi hanya dapat diakses oleh pihak yang berwenang atau memiliki otoritas tertentu (aspek kerahasiaan / *confidentiality*).
b. Informasi tetap akurat dan lengkap tanpa ada pengubahan informasi yang tidak sesuai dengan otoritas (aspek integritas / *integrity*).
c. Informasi dapat diakses oleh pihak yang berwenang (aspek ketersediaan/*availability*).

3. PENANGGUNG JAWAB

Penanggung jawab dari kebijakan ini adalah:

3.1 Komisaris
3.2 Direktur Utama
3.3 Direktur Umum

3.4 Kepala Bagian Kepatuhan
3.5 Kepala Bagian Teknologi dan Sistem Informasi (TSI)

4. STANDAR ACUAN

4.1. Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Pasal 14 tentang Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi.

4.2. Rencana Jangka Panjang Teknologi dan Sistem Informasi, Bagian F.

5. ISI KEBIJAKAN

5.1 DEFINISI

Keamanan informasi adalah penjagaan kerahasiaan, integritas dan ketersediaan informasi. Sifat/keadaan informasi lainnya seperti keaslian, akuntabilitas, bukan tindakan penyangkalan/nirsangkal serta kehandalan termasuk di dalamnya (ISO/IEC 17799:2005). Ketentuan ini dibuat untuk memberikan pedoman mengelola informasi yang dimiliki Bank agar *Confidentiality* (Kerahasiaan), *Integrity* (Integritas) dan *Availability* (Ketersediaan) informasi Bank tetap terjaga.

5.2 LANDASAN HUKUM

Landasan hukum yang digunakan dalam kebijakan keamanan informasi ini adalah sebagai berikut.

5.2.1 Peraturan Bank Indonesia

Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Pasal 14 tentang Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi.

Pasal 14

Bank wajib memastikan pengamanan informasi dilaksanakan secara efektif dengan memperhatikan paling kurang hal-hal sebagai berikut.

a. Pengamanan informasi ditujukan agar informasi yang dikelola terjaga
kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaannya
(*availability*) secara efektif dan efisien dengan

memperhatikan
kepatuhan terhadap ketentuan yang berlaku;

b. Pengamanan informasi dilakukan terhadap aspek teknologi, sumber
daya manusia dan proses dalam penggunaan Teknologi Informasi;

c. Pengamanan informasi mencakup pengelolaan aset bank yang terkait
dengan informasi, kebijakan sumber daya manusia, pengamanan fisik,
pengamanan akses, pengamanan operasional, dan aspek penggunaan
Teknologi Informasi lainnya;

d. Adanya manajemen penanganan insiden dalam pengamanan informasi; dan

e. Pengamanan informasi diterapkan berdasarkan hasil penilaian terhadap
risiko (*risk assessment*) pada informasi yang dimiliki Bank.

5.2.2 Rencana Jangka Panjang Teknologi dan Sistem Informasi, Bagian F.

"Kecanggihan teknologi harus diimbangi dengan keamanan sistem yang baik dan kuat. Pengamanan sistem informasi dapat dilakukan secara *hardware, software* dan pembuatan kebijakan TI.

BPR Bank Surya Yudha telah menggunakan peralatan jaringan standar perbankan dan mempunyai keamanan informasi internal yang kuat. Walaupun demikian setiap saat perlu dilakukan kajian dan analisis terhadap jaringan yang ada karena pesatnya perkembangan dunia TI dan perlu dilakukan peningkatan sesuai dengan perkembangan teknologi jaringan."

5.3 TUJUAN KEAMANAN INFORMASI

Keamanan informasi memiliki tujuan sebagai berikut.

a. Melindungi data dan informasi perbankan dari pengungkapan pihak-pihak yang tidak berwenang.

b. Memastikan bahwa bank dapat menyediakan data dan

informasi untuk pihak-pihak yang memiliki wewenang untuk menggunakannya.

c. Memastikan bank dapat memberikan data yang lengkap dan akurat dari sistem yang dimiliki.

d. Menjaga reputasi bank dari ancaman yang menyerang keamanan informasi perbankan.

5.4 PRINSIP KEAMANAN INFORMASI

Pelaksanaan keamanan informasi memiliki prinsip-prinsip yang harus diterapkan yaitu:

1. Informasi yang dikelola harus terjaga kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaannya (*availability*) secara efektif dan efisien dengan memperhatikan kepatuhan (*compliance*) terhadap ketentuan yang berlaku.
2. Keamanan informasi memperhatikan aspek sumber daya manusia, proses dan teknologi informasi.
3. Pelaksanaan keamanan informasi dilakukan berdasarkan hasil penilaian risiko (*risk assessment*) dengan memperhatikan strategi bank dan ketentuan yang berlaku.
4. Menerapkan pengamanan informasi secara komprehensif dan berkesinambungan dengan beberapa hal sebagai berikut.
   a. Menetapkan tujuan dan kebijakan pengamanan informasi.
   b. Mengimplementasikan pengendalian pengamanan informasi.
   c. Memantau dan mengevaluasi kinerja serta keefektifan kebijakan pengamanan informasi.

5.5 PERANGKAT KEBIJAKAN KEAMANAN INFORMASI

Dalam menerapkan kebijakan keamanan informasi harus mencakup beberapa hal berikut.

1. Keamanan informasi meliputi pengelolaan aset, sumber daya manusia, pengamanan fisik, pengamanan logika

(*logical security*), pengamanan operasional TI, penanganan insiden pengamanan informasi, dan pengamanan informasi dalam pengembangan sistem.

2. Komitmen manajemen terhadap pengamanan informasi yang selaras dengan strategi dan tujuan bisnis perusahaan.
3. Menetapkan pengendalian melalui pelaksanaan manajemen risiko Bank, sebagai bentuk pengendalian keamanan informasi.
4. Kepatuhan terhadap regulasi atau ketentuan yang berlaku beserta sanksi atas pelanggaran regulasi keamanan informasi di perusahaan.
5. Pelatihan dan peningkatan kesadaran atas pentingnya pengamanan informasi kepada seluruh karyawan perusahaan
6. Pembagian tugas dan tanggung jawab pihak-pihak yang terlibat dalam pengamanan informasi;
7. Dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi.

6. DEFINISI DAN SINGKATAN

6.1 DEFINISI

1. Keamanan Informasi

   Keamanan informasi adalah penjagaan kerahasiaan, integritas dan ketersediaan informasi. Sifat/keadaan informasi lainnya seperti keaslian, akuntabilitas, bukan tindakan penyangkalan/nirsangkal serta kehandalan termasuk di dalamnya (ISO/IEC 17799:2005).
2. Kerahasiaan / *confidentiality*

   Informasi hanya dapat diakses oleh pihak yang memiliki wewenang.
3. Integritas / *Integrity*

   Informasi tetap akurat dan lengkap, serta informasi tersebut tidak dimodifikasi tanpa otorisasi yang jelas.
4. Ketersediaan / *availability*

   Informasi dapat diakses oleh pihak yang memiliki

wewenang ketika dibutuhkan.

7. DOKUMEN TERKAIT

7.1 Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001)

7.2 Formulir Audit Internal Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (FAI-TSI-001)

7.3 Prosedur Pemantauan dan Evaluasi Keamanan Sistem (P-TSI-002)

7.4 Formulir Audit Internal Pemantauan dan Evaluasi Keamanan Sistem (FAI-TSI-002)

LAMPIRAN G

G.1 Lampiran Contoh Prosedur Mekanisme Komite Pengarah Teknologi Informasi

BPR Bank Surya Yudha Banjarnegara
PROSEDUR MEKANISME FORUM KOMITE PENGARAH TEKNOLOGI INFORMASI

Lembar Pengesahan
PROSEDUR

Judul	Mekanisme Forum Komite Pengarah Teknologi Informasi
No. Dokumen	P-PRS-002
Revisi	00

Versi	Tanggal Pembuatan	Tanggal Pengesahan

Disahkan Oleh	Dibuat Oleh
(Jabatan)	Peneliti
(NAMA)	(NAMA)

P-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

PROSEDUR

1. TUJUAN

Tujuan dari pembuatan prosedur ini adalah mengatur pelaksanaan Forum Komite Pengarah TI, yang akan menyelaraskan kebutuhan teknologi informasi dengan tujuan dan kebutuhan perusahaan di BPR Bank Surya Yudha Banjarnegara.

2. RUANG LINGKUP

Ruang lingkup dari prosedur ini adalah mengatur mekanisme Forum Komite Pengarah TI untuk melakukan pemilihan dan prioritisasi implementasi sistem dan teknologi informasi serta menyelaraskan kebutuhan teknologi informasi dengan tujuan dan kebutuhan perusahaan di BPR Bank Surya Yudha Banjarnegara.

3. PENANGGUNG JAWAB

Penanggung jawab dari prosedur ini adalah:

3.1 Komisaris
3.2 Direktur Utama
3.3 Direktur Umum
3.4 Kepala Bagian Kepatuhan
3.5 Kepala Bagian Teknologi dan Sistem Informasi (TSI)
3.6 Kepala Seksi Pengembangan Teknologi Informasi

P-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

PROSEDUR

4. STANDAR YANG BERLAKU

berdasarkan Peraturan Bank Indonesia (PBI) Nomor 9/15/PBI/2007 Pasal 7 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi.

5. RINCIAN PROSEDUR

5.1 WAKTU PELAKSANAAN FORUM KOMITE PENGARAH TI

1. Forum Komite Pengarah TI diselenggarakan setiap bulan satu kali (12 kali dalam satu tahun) untuk pemantauan dan evaluasi proyek.
2. Forum Komite Pengarah TI yang diselenggarakan di bulan ke-1 dan ke-7 ditujukan untuk pengajuan usulan proyek TI.

5.2 KEGIATAN FORUM KOMITE PENGARAH TI

1. Penerimaan pengajuan kebutuhan teknologi informasi yang berasal dari setiap fungsional bisnis (bagian) perusahaan.
2. Penyeleksian kebutuhan teknologi informasi yang diajukan oleh masing-masing fungsional bisnis (bagian) perusahaan.
3. Prioritisasi kebutuhan teknologi informasi yang diajukan.
4. Pemantauan dan evaluasi implementasi proyek.

P-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

PROSEDUR

5.3 PERSIAPAN FORUM KOMITE PENGARAH TI

Setiap pihak yang akan mengajukan kebutuhan teknologi informasi, harus membuat dokumen proyek yang berisi:

1. Latar belakang kebutuhan teknologi informasi
2. Tujuan dan manfaat kebutuhan teknologi informasi
3. Cakupan proyek pengadaan atau rancangan kebutuhan teknologi informasi
4. Analisis biaya dan anggaran kebutuhan teknologi informasi
5. Analisis kondisi terkini masing-masing fungsional bisnis sebelum implementasi proyek.
6. *Project Organization* (Struktur organisasi dan penanggung jawab proyek)
7. *User requirement* (kebutuhan pengguna)
8. *Project Time Schedule* (Jadwal atau *milestone* proyek)

5.4 MEKANISME FORUM KOMITE PENGARAH TI

5.4.1 Pengajuan Proyek Teknologi Informasi

1. Forum dilaksanakan pada bulan ke-1 dan bulan ke-7.
2. Setiap fungsional bisnis (bagian) perusahaan yang akan mengajukan perancangan sistem atau pengadaan kebutuhan teknologi informasi membuat dokumen proyek.
3. Dokumen proyek dikumpulkan ke Bagian Teknologi dan

P-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

PROSEDUR

Sistem Informasi.

4. Kepala Sie Perkembangan Teknologi Informasi (*IT Development*) membuat penjadwalan pelaksanaan Forum Komite Pengarah TI selama satu tahun.
5. Kepala Bagian TSI menyampaikan usulan proyek kebutuhan teknologi informasi pada saat forum Komite Pengarah TI berlangsung.
6. Pihak pengusul proyek melakukan presentasi usulan kebutuhan teknologi informasi, sesuai dokumen proyek TI yang telah dibuat.
7. Direktur Utama atau Direktur Umum beserta pimpinan/Kabag TSI melakukan penyeleksian usulan kebutuhan teknologi informasi yang sesuai dengan kebutuhan bisnis perbankan, anggaran keuangan perusahaan dan sistem perundang-undangan perbankan.
8. Direktur Utama atau Direktur Umum beserta pimpinan/Kabag TSI melakukan prioritisasi atau pembobotan usulan kebutuhan teknologi informasi yang akan diimplementasikan terlebih dulu.
9. Keanggotaan Manajemen (Komisaris dan Dewan direksi) melakukan persetujuan proyek.
10. Usulan kebutuhan teknologi informasi yang disetujui diserahkan kepada Bagian TSI untuk melakukan

P-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

PROSEDUR

implementasi dan evaluasi proyek.

5.4.2 Forum Pemantauan dan Evaluasi Komite Pengarah TI

1. Forum diadakan setiap satu bulan satu kali.
2. Forum dihadiri oleh keanggotaan manajemen, operasional dan teknologi informasi yang memiliki kepentingan atau sedang menjalankan proyek teknologi informasi.
3. Pimpinan TSI melaporkan kepada Komisaris atau Dewan Direksi tentang hasil perkembangan rencana kerja teknologi dan sistem informasi, beserta kendala yang ada.
4. Kepala Bagian terkait (pimpinan non-TI) memberikan laporan dan hasil pemantauan selama satu bulan mengenai proyek TI yang sedang/akan/telah berjalan di bagiannya, serta hasil dari implementasi.
5. Komisaris atau Dewan Direksi beserta Pimpinan TSI melakukan pembahasan dan memberikan masukan terhadap rencana kerja teknologi dan sistem informasi yang sedang/akan/telah berjalan di masing-masing bagian.

5.5 DOKUMENTASI

Karyawan TSI membuat dokumentasi forum Komite Pengarah Teknologi Informasi dalam bentuk notulen (*Minute of Meeting*), foto, rekaman suara atau video, yang akan diketahui oleh

P-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

PROSEDUR

pimpinan TSI dan dilaporkan serta disahkan oleh Dewan Direksi.

6. DOKUMEN TERKAIT

Dokumen Kebijakan Komite Pengarah Teknologi Informasi (K-PRS-002)
Formulir Mekanisme Forum Komite Pengarah Teknologi Informasi (FAI-PRS-002)

7. APLIKASI TERKAIT

Tidak ada aplikasi yang terkait di prosedur ini.

8. MATRIK PROSEDUR

Berikut ini adalah matrik prosedur dari

RUANG LINGKUP		FUNGSI				
	K	Dirut	DU	KBK	KB TSI	KS PTI
Mekanisme Forum Komite Pengarah Teknologi Informasi	I	I/A	I/A	C/I	R/A	R

Keterangan: R=*Responsible* ; A=*Accountable* ; C=*Consulted* ; I=*Information*

P-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

PROSEDUR

9. DEFINISI DAN DAFTAR SINGKATAN

9.1 Definisi

1. Komite Pengarah Teknologi Informasi
   Komite **pengarah IT** yang terdiri dari **eksekutif, bisnis, manajemen IT**, untuk menentukan **prioritas program investasi IT** yang sejalan dengan strategi dan prioritas bisnis perusahaan, melihat ***progress*** **proyek** dan menyelesaikan permasalahan sumber daya proyek dan **memantau *service level*** dan ***service improvements***. (COBIT 4.1)
2. *Responsible*
   Responsible adalah pihak yang bertanggung jawab penuh untuk mengerjakan suatu tugas atau pekerjaan.
3. *Accountable*
   Accountable adalah pihak yang memiliki peran untuk membuat keputusan dan sebagai pemilik atas pekerjaan tersebut.
4. *Consulted*
   Consulted adalah pihak yang berperan untuk memberikan konsultasi sebelum membuat keputusan.
5. *Information*
   Information adalah pihak yang harus diberikan informasi setelah melakukan pengambilan keputusan.

9.2 Singkatan

1. K : Komisaris
2. Dirut: Direktur Utama
3. DU : Direktur Umum
4. KBK : Kepala Bagian Kepatuhan

P-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

PROSEDUR

5. KBTSI : Kepala Bagian TSI
6. KSPTI : Kepala Seksi Pengembangan TI

10. CATATAN PERUBAHAN

Belum ada.

G.2 Lampiran Contoh Prosedur Pemantauan dan Evaluasi Keamanan Sistem

<table>
<tr><td colspan="3">  </td></tr>
<tr><td colspan="3">BPR Bank Surya Yudha Banjarnegara
PROSEDUR PEMANTAUAN DAN EVALUASI KEAMANAN SISTEM</td></tr>
<tr><td colspan="3">Lembar Pengesahan
PROSEDUR</td></tr>
<tr><td>Judul</td><td colspan="2">Pemantauan dan Evaluasi Keamanan Sistem</td></tr>
<tr><td>No. Dokumen</td><td colspan="2">P-TSI-002</td></tr>
<tr><td>Revisi</td><td colspan="2">00</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>Versi</td><td>Tanggal Pembuatan</td><td>Tanggal Pengesahan</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>Disahkan Oleh</td><td colspan="2">Dibuat Oleh</td></tr>
<tr><td>(Jabatan)</td><td colspan="2">(Jabatan)</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>(NAMA)</td><td colspan="2">(NAMA)</td></tr>
</table>

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

1. TUJUAN

Tujuan dari pembuatan prosedur ini adalah untuk melakukan pemantauan dan evaluasi keamanan sistem teknologi informasi di BPR Bank Surya Yudha Banjarnegara. Hal ini sebagai suatu langkah untuk mencegah adanya aksi serangan yang dapat mengancam keamanan informasi perusahaan.

2. RUANG LINGKUP

Ruang lingkup dari prosedur ini adalah pemantauan dan evaluasi keamanan sistem pada infrastruktur jaringan, perangkat keras (AS-400) serta sistem *core banking* di BPR Bank Surya Yudha Banjarnegara.

3. PENANGGUNG JAWAB

Penanggung jawab dari prosedur ini adalah:

3.1 Komisaris
3.2 Direktur Utama
3.3 Direktur Umum
3.4 Kepala Bagian Kepatuhan
3.5 Kepala Bagian Teknologi dan Sistem Informasi (TSI)
3.6 Kepala Seksi Pengembangan Teknologi Informasi

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

4. STANDAR YANG BERLAKU

4.1 Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Pasal 14 tentang Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi.

4.2 Rencana Jangka Panjang Teknologi dan Sistem Informasi, Bagian F.

5. RINCIAN PROSEDUR

5.1 Waktu dan Tempat

Pemantauan rutin dilakukan satu kali dalam satu minggu, oleh karyawan Bagian TSI.

5.2 Alat Identifikasi

Periksa lampu indikator pada mesin AS-400Berikut ini adalah indikator lampu berdasarkan warna.

Hijau : Kondisi Normal secara fisik

Kuning : Kondisi tidak normal pada perangkat keras atau jaringan.

5.2.1 Penjelasan Kondisi

1. Ketika lampu indikator berwarna kuning, maka petugas atau penanggung jawab diwajibkan segera memeriksa kondisi perangkat keras dan jaringan, karena hal tersebut

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

mengindikasikan bahwa sistem terkena serangan.

2. Jika terjadi serangan, maka lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).
3. Ketika kondisi lampu indikator berwarna hijau, hal ini menunjukkan bahwa kondisi sistem normal secara fisik.
4. Lakukan pemantauan selanjutnya dengan memeriksa kondisi data melalui *job log* untuk memastikan kondisi data tetap dalam kondisi normal.

5.3 Alur Pemantauan dan Evaluasi

Alur pemantauan keamanan informasi dilakukan berdasarkan kondisi jaringan, kemudian beranjak ke pemantauan mesin AS-400 (perangkat keras) dan aplikasi *core banking* (perangkat lunak).

5.4 Pemantauan dan Evaluasi pada Infrastruktur Jaringan

Petugas harus melakukan pemeriksaan terhadap *router*, untuk memastikan bahwa kondisi jaringan dalam keadaan normal. Berikut ini adalah langkah pemeriksaan pada *router*.

1. Periksa bagian ***User ID Activity***. Periksa dengan teliti, apakah ada *user* lain yang tidak terdaftar di Bagian TSI.
2. Jika terdapat *User ID* yang asing dan tidak terdaftar pada bagian TSI, maka lakukan Prosedur Penanganan Serangan

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).

3. Jika tidak ada permasalahan pada bagian *User ID Activity*, maka selanjutnya periksa bagian ***Setting Automatic E-mail***. Periksa apakah terjadi pengisian alamat e-mail pada *field* yang ada. Di mana hal ini memungkinkan pihak penyerang mendapatkan setiap perubahan pada *username* dan *password* jaringan secara otomatis kepada *e-mail* penyerang.
4. Jika terdapat pengisian *Setting Automatic E-mail* dan alamat e-mail merupakan alamat yang asing, maka lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).
5. Jika tidak ada permasalahan pada bagian *Setting Automatic E-mail*, maka periksa bagian ***Automatic Process***. Dengan melakukan pemeriksaan ini, maka petugas dapat mengetahui kapan *router* dimatikan atau dihidupkan. Sehingga jika terjadi serangan dari luar untuk mematikan *router*, hal ini dapat segera diketahui.
6. Jika pengaturan pada *automatic schedule* dalam keadaan menyala (ON), maka lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).
7. Jika ketiga elemen kontrol yaitu *User ID Activity, Setting Automatic E-mail* dan *Automatic Schedule* dalam kondisi yang baik, maka pemantauan dapat dilanjutkan ke bagian mesin AS-400 (perangkat keras).

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

5.5 Pemantauan dan Evaluasi pada Perangkat Keras (As-400)

Untuk melakukan pemantauan dan evaluasi terhadap perangkat keras AS-400, maka langkah-langkah yang dilakukan adalah sebagai berikut.

1. Periksa bagian lampu indikator.
2. Jika lampu berwarna kuning, maka telah terjadi penyerangan keamanan informasi secara fisik. Lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).
3. Jika lampu berwarna hijau, maka kondisi mesin secara fisik dalam keadaan yang normal. Lakukan pemantauan selanjutnya.
4. Periksa *job log* dan tampilkan dengan memilih fungsi *check display*. *Job Log* akan menampilkan *user ID,* pekerjaan yang dilakukan dan *IP Number.*
5. Periksa dengan teliti, apakah terdapat *User Id* atau *IP Number* yang asing dan tidak terdaftar pada bagian TSI.
6. Jika terdapat *User id* atau *IP Number* yang asing dan tidak terdaftar pada bagian TSI, maka lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

5.6 Pemantauan dan Evaluasi pada Aplikasi *Core Banking*
Pemantauan dilakukan dengan melakukan pemeriksaan terhadap kondisi aplikasi *Core Banking.*

1. *Log in* sebagai pengguna ke aplikasi.
2. Periksa performa aplikasi.
3. Jika Aplikasi *Core Banking* terkena serangan, hal ini memungkinkan penyerang telah melakukan serangan pada jaringan dan perangkat keras perusahaan. Sehingga ketika aplikasi terkena serangan, penyerang dimungkinkan sudah melakukan sesuatu terhadap nilai, data atau sistem di dalamnya. Di mana hal tersebut akan ditangani sesuai dengan kasus yang terjadi, sesuai dengan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).

6. DOKUMEN TERKAIT

6.1. Dokumen Kebijakan Keamanan Informasi (K-TSI-001)
6.2. Dokumen Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penggantian Nilai (P-TSI-001)
6.3. Formulir Pemantauan dan Evaluasi Keamanan Sistem (FAI-TSI-002).
6.4. Berita Acara Pemantauan dan Evaluasi Keamanan Sistem (BA-

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

TSI-002).

7. APLIKASI TERKAIT

Aplikasi yang terkait dengan prosedur ini adalah aplikasi *Core Banking* WIN Core.

8. MATRIK PROSEDUR

Berikut ini adalah matrik prosedur pada prosedur pemantauan dan evaluasi keamanan sistem.

RUANG LINGKUP		FUNGSI				
	K	Dirut	DU	KBK	KB TSI	KS PTI
Pemantauan dan Evaluasi Keamanan Sistem	I	I/A	I/A	C/I	R/A	R

Keterangan: R=*Responsible* ; A=*Accountable* ; C=*Consulted* ; I=*Information*

9. DEFINISI DAN DAFTAR SINGKATAN

9.1 Definisi

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

1. Serangan pada sistem
Serangan (*attack*) adalah aktivitas percobaan untuk menghancurkan, menyingkap, mengubah, mencuri atau mendapatkan akses yang tidak sah atau untuk menggunakan aset secara tidak sah (melawan otoritas). (ISO 27000:2009)
2. *Router*
Router adalah sebuah perangkat yang meneruskan atau mengirimkan paket data di antara jaringan komputer.
3. AS 400
Mesin AS-400 dibedakan menjadi 3 kategori yaitu perangkat lunak, perangkat keras dan *Database*. OS/400 merupakan sistem operasi yang dibuat untuk mengaplikasikan data yang spesifik pada sektor tertentu, misalkan perbankan. Perangkat keras AS-400 terdiri atas mesin AS-400, Monitor AS-400 dan printer AS-400. AS-400 memiliki database yang disebut dengan DB/2.
4. Aplikasi *Core Banking* WIN Core
WINCore adalah aplikasi yang terintegrasi, fleksibel, terbuka dan merupakan *real-time online core banking systems* yang memiliki tingkat pengawasan terbaik untuk mendukung operasional perbankan (Forex dan Non-Forex Bank).
5. *Responsible*
Responsible adalah pihak yang bertanggung jawab penuh untuk mengerjakan suatu tugas atau pekerjaan.
6. *Accountable*

P-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

PROSEDUR

Accountable adalah pihak yang memiliki peran untuk membuat keputusan dan sebagai pemilik atas pekerjaan tersebut.

7. *Consulted*

Consulted adalah pihak yang berperan untuk memberikan konsultasi sebelum
membuat keputusan.

8. Information

Information adalah pihak yang harus diberikan informasi setelah melakukan pengambilan keputusan.

9.2 Singkatan

1. K : Komisaris
2. DU : Direktur Umum
3. KBK : Kepala Bagian Kepatuhan
4. KBTSI : Kepala Bagian TSI
5. KSPTI : Kepala Seksi Pengembangan TI

10. CATATAN PERUBAHAN

Belum ada.

LAMPIRAN H

H.1 Lampiran Contoh Formulir Audit Internal Mekanisme Komite Pengarah Teknologi Informasi

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*				
Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
Waktu	Forum Komite Pengarah TI diselenggarakan setiap bulan satu kali (12 kali dalam satu tahun) untuk pemantauan dan evaluasi proyek.			
	Forum Komite Pengarah TI yang diselenggarakan di bulan ke-1 dan ke-7 ditujukan untuk pengajuan usulan proyek TI.			
Kegiatan Forum Komite Pengarah TI	Penerimaan pengajuan kebutuhan teknologi			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	informasi yang berasal dari setiap fungsional bisnis (bagian) perusahaan.			
	Melaksanakan Penyeleksian kebutuhan teknologi informasi yang diajukan oleh masing-masing fungsional bisnis (bagian) perusahaan.			
	Melaksanakan Prioritisasi kebutuhan teknologi informasi yang diajukan.			
	Melaksanakan Pemantauan dan evaluasi implementasi			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	proyek.			
Isi Dokumen Pengajuan Proyek	Terdapat latar belakang kebutuhan teknologi informasi			
	Terdapat tujuan dan manfaat kebutuhan teknologi informasi			
	Terdapat cakupan proyek pengadaan atau rancangan kebutuhan teknologi informasi			
	Terdapat analisis biaya dan anggaran kebutuhan teknologi informasi			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	Terdapat analisis kondisi terkini masing-masing fungsional bisnis sebelum implementasi proyek.			
	Terdapat *Project Organization* (Struktur organisasi dan penanggung jawab proyek)			
	Terdapat *user requirement* (kebutuhan pengguna)			
	Terdapat *Project Time Schedule* (Jadwal atau *milestone* proyek)			
Mekanisme Forum Komite Pengarah TI	**Pengajuan Proyek Teknologi Informasi**			
	Forum dilaksanakan pada bulan ke-1 dan			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	bulan ke-7.			
	Setiap fungsional bisnis (bagian) perusahaan yang akan mengajukan perancangan sistem atau pengadaan kebutuhan teknologi informasi membuat dokumen proyek.			
	Dokumen proyek dikumpulkan ke Bagian Teknologi dan Sistem Informasi.			
	Kepala Sie Perkembangan Teknologi Informasi (*IT Development*)			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	membuat penjadwalan pelaksanaan Forum Komite Pengarah TI selama satu tahun.			
	Kepala Bagian TSI menyampaikan usulan proyek kebutuhan teknologi informasi pada saat forum Komite Pengarah TI berlangsung.			
	Pihak pengusul proyek melakukan presentasi usulan kebutuhan teknologi informasi, sesuai dokumen proyek TI yang telah dibuat.			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	Direktur Utama atau Direktur Umum beserta pimpinan/Kabag TSI melakukan penyeleksian usulan kebutuhan teknologi informasi yang sesuai dengan kebutuhan bisnis perbankan, anggaran keuangan perusahaan dan sistem perundang-undangan perbankan.			
	Direktur Utama atau Direktur Umum beserta pimpinan/Kabag TSI melakukan prioritisasi atau pembobotan			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	usulan kebutuhan teknologi informasi yang akan diimplementasikan terlebih dulu.			
	Keanggotaan Manajemen (Komisaris dan Dewan direksi) melakukan persetujuan proyek.			
	Usulan kebutuhan teknologi informasi yang disetujui diserahkan kepada Bagian TSI untuk melakukan implementasi dan evaluasi proyek.			
	Pemantauan dan Evaluasi Komite Pengarah TI			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	Forum diadakan setiap satu bulan satu kali.			
	Forum dihadiri oleh keanggotaan manajemen, operasional dan teknologi informasi yang memiliki kepentingan atau sedang menjalankan proyek teknologi informasi.			
	Pimpinan TSI melaporkan kepada Komisaris atau Dewan Direksi tentang hasil perkembangan rencana kerja teknologi dan sistem informasi,			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	beserta kendala yang ada.			
	Kepala Bagian terkait (pimpinan non-TI) memberikan laporan dan hasil pemantauan selama satu bulan mengenai proyek TI yang sedang/akan/telah berjalan di bagiannya, serta hasil dari implementasi.			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	Komisaris atau Dewan Direksi beserta Pimpinan TSI melakukan pembahasan dan memberikan masukan terhadap rencana kerja teknologi dan sistem informasi yang sedang/akan/telah berjalan di masing-masing bagian.			
Dokumentasi	Karyawan TSI membuat dokumentasi forum Komite Pengarah Teknologi Informasi dalam bentuk notulen (Minute of Meeting), foto,			

FAI-PRS-002	No. Revisi	
Mekanisme Forum Komite Pengarah Teknologi Informasi	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Keterangan
	rekaman suara atau video, yang akan diketahui oleh pimpinan TSI dan dilaporkan serta disahkan oleh Dewan Direksi.			

H.2 Lampiran Contoh Formulir Audit Internal Pemantauan dan Evaluasi Keamanan Sistem

FAI-TSI-002		No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem		Tanggal Pengesahan	
		Halaman	
FORMULIR AUDIT INTERNAL (*CHECKLIST*)			
Prosedur	**Detil Prosedur**	**Cek**	**Penanggung Jawab**	**Ket**
Waktu	Pemantauan rutin dilakukan 1 minggu 1 kali oleh karyawan Bagian TSI.			
Alat Identifikasi	Lampu indikator berwarna hijau			
	Lampu indikator berwarna kuning			
Jika lampu indikator berwarna kuning, lanjutkan pemeriksaan jaringan dan perangkat keras. Jika lampu berwarna hijau, lakukan pemeriksaan aplikasi.				
Serangan infrastruktur jaringan	Periksa bagian ***User ID Activity***. Periksa dengan teliti, apakah ada *user* lain yang tidak terdaftar di Bagian TSI.			

FAI-TSI-002		No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem		Tanggal Pengesahan	
		Halaman	
FORMULIR AUDIT INTERNAL (*CHECKLIST*)			
Prosedur	**Detil Prosedur**	**Cek**	**Penanggung Jawab**	**Ket**
	Jika terdapat *User ID* yang asing dan tidak terdaftar pada bagian TSI, maka lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).			
	Periksa bagian ***Setting Automatic E-mail***. Periksa apakah terjadi pengisian alamat e-mail pada *field* yang ada. Di mana hal ini memungkinkan pihak penyerang mendapatkan setiap perubahan pada *username* dan			

FAI-TSI-002		No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem		Tanggal Pengesahan	
		Halaman	
FORMULIR AUDIT INTERNAL (*CHECKLIST*)			

Prosedur	**Detil Prosedur**	**Cek**	**Penanggung Jawab**	**Ket**
	password jaringan secara otomatis kepada *e-mail* penyerang.			
	Jika terdapat pengisian *Setting Automatic E-mail* dan alamat e-mail merupakan alamat yang asing, maka lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).			
	Periksa bagian ***Automatic Process,*** untuk mengetahui kapan router			

FAI-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL (*CHECKLIST*)

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Ket
	dimatikan atau dihidupkan.			
	Jika pengaturan pada *automatic schedule* dalam keadaan menyala (ON), maka lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).			

FAI-TSI-002		No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem		Tanggal Pengesahan	
		Halaman	

FORMULIR AUDIT INTERNAL (*CHECKLIST*)

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Ket
Serangan Perangkat Keras	**Periksa bagian lampu indikator.** Jika lampu berwarna kuning, maka telah terjadi penyerangan keamanan informasi secara fisik. Lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001). Jika lampu berwarna hijau, maka kondisi mesin secara fisik dalam keadaan yang normal. Lakukan pemantauan selanjutnya.			

FAI-TSI-002	No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL (*CHECKLIST*)

Prosedur	Detil Prosedur	Cek	Penanggung Jawab	Ket
	Periksa job log dan tampilkan dengan memilih fungsi check display. Job Log akan menampilkan user ID, pekerjaan yang dilakukan dan IP Number.			
	Jika terdapat User id atau IP Number yang asing dan tidak terdaftar pada bagian TSI, maka lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).			
Serangan Aplikasi *Core*	*Log in* sebagai pengguna ke aplikasi.			
	Periksa performa			

FAI-TSI-002		No. Revisi	
Pemantauan dan Evaluasi Keamanan Sistem		Tanggal Pengesahan	
		Halaman	

FORMULIR AUDIT INTERNAL (*CHECKLIST*)

Prosedur	**Detil Prosedur**	**Cek**	**Penanggung Jawab**	**Ket**
Banking	aplikasi			
	Jika terjadi gangguan pada aplikasi lakukan Prosedur Penanganan Serangan Penyalahgunaan Sistem dan Penghitungan Nilai (P-TSI-001).			

LAMPIRAN I

Lampiran Contoh Formulir Audit Internal Perusahaan BCP

F-AI-001	No. Revisi	
BUSINESS CONTINUITY PLAN BPR BANK SURYA YUDHA BANJARNEGARA	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Kontrol		**Cek**	**Penanggung Jawab**	**Keterangan**
Kebutuhan keberlanjutan bisnis perusahaan	1. BCP yang dibuat harus mencakup risiko di bidang teknologi informasi di perusahaan.			
	2. BCP yang dibuat harus dapat mengurangi risiko yang timbul dari implementasi teknologi informasi.			
	3. BCP yang dibuat dapat digunakan dalam waktu jangka panjang.			
	4. BCP yang dibuat harus memperhatikan aspek kemudahan dan kesederhanaan desain.			

F-AI-001	No. Revisi	
BUSINESS CONTINUITY PLAN BPR BANK SURYA YUDHA BANJARNEGARA	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Kontrol		Cek	Penanggung Jawab	Keterangan
	5. BCP yang dibuat harus dapat sesuai dengan teknologi yang sudah diterapkan.			
	6. BCP yang dibuat harus melibatkan perusahaan, dalam hal Sumber Daya Manusia (SDM) secara utuh.			
	7. BCP yang dibuat harus memperhatikan keberlanjutan operasional bisnis perusahaan.			
	8. BCP yang dibuat untuk perbankan, harus dapat mengatasi kebutuhan sistem keamanan yang tinggi di perusahaan.			

F-AI-001		No. Revisi	
BUSINESS CONTINUITY PLAN BPR BANK SURYA YUDHA BANJARNEGARA		Tanggal Pengesahan	
		Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Kontrol		**Cek**	**Penanggung Jawab**	**Keterangan**
	9. BCP yang dibuat harus dapat mendukung tata kelola teknologi informasi yang diterapkan di perusahaan (prosedur di DRC, DRP dan *Contingency Plan*).			
	10. BCP yang dibuat harus dinamis, yaitu dapat mengikuti perkembangan dunia teknologi informasi.			
Tujuan BCP Perusahaan	1. Dokumen BCP (*Business Continuity Plan*) selaras dengan tujuan dan kebutuhan perusahaan.			

F-AI-001	No. Revisi	
BUSINESS CONTINUITY PLAN BPR BANK SURYA YUDHA BANJARNEGARA	Tanggal Pengesahan	
	Halaman	

FORMULIR AUDIT INTERNAL *(CHECKLIST)*

Kontrol		**Cek**	**Penanggung Jawab**	**Keterangan**
	2. Dokumen BCP yang dapat diimplementasikan secara menyeluruh oleh pihak-pihak yang memiliki ketergantungan terhadap teknologi dan sistem informasi.			
	3.Rrisiko teknologi informasi (ancaman alam, internal dan eksternal) dapat diminimalisasi.			
	4. Terwujudnya ketersediaan (*availability*), integritas (*integrity*) serta tingkat kehandalan (*reliability*) layanan informasi di bank.			

			
F-AI-001		No. Revisi	
BUSINESS CONTINUITY PLAN BPR BANK SURYA YUDHA BANJARNEGARA		Tanggal Pengesahan	
		Halaman	
FORMULIR AUDIT INTERNAL *(CHECKLIST)*			

Kontrol		**Cek**	**Penanggung Jawab**	**Keterangan**
	5. Meningkatkan kesadaran seluruh pihak di perusahaan akan pengembangan teknologi dan sistem informasi, serta pentingnya pengelolaan risiko teknologi informasi di perusahaan.			
Verifikasi dan Validasi BCP	1. Pemeriksaan verifikasi dokumen BCP			
	2. Pelaksanaan pelatihan BCP secara periodik			

LAMPIRAN J

Lampiran Contoh Formulir Peninjauan Manajemen

RAPAT PENINJAUAN MANAJEMEN **BCP BPR BANK SURYA YUDHA BANJARNEGARA**	
Tanggal Peninjauan: / /	
KEHADIRAN	
NAMA	JABATAN
KETIDAKHADIRAN	
NAMA	JABATAN
Disahkan Oleh	Dibuat Oleh

RAPAT PENINJAUAN MANAJEMEN
BCP BPR BANK SURYA YUDHA BANJARNEGARA

NO	KONTROL	TINDAK LANJUT	KET
1	Hasil Audit Internal Bagian		
2	Perubahan internal perusahaan yang mempengaruhi BCP		
3	Perubahan eksternal yang mempengaruhi BCP		
4	Tinjauan Sumber Daya BCP		
	Sumber Daya Manusia		
	Sumber Daya Teknologi Informasi		

RAPAT PENINJAUAN MANAJEMEN
BCP BPR BANK SURYA YUDHA BANJARNEGARA

NO	KONTROL	TINDAK LANJUT	KET
5	Tinjauan efisiensi pelatihan BCP		
6	Tinjauan pihak ketiga, mitra kerja BCP		
7	Tinjauan keselarasan kebutuhan BCP dengan kebutuhan perusahaan		
8	Evaluasi BCP		

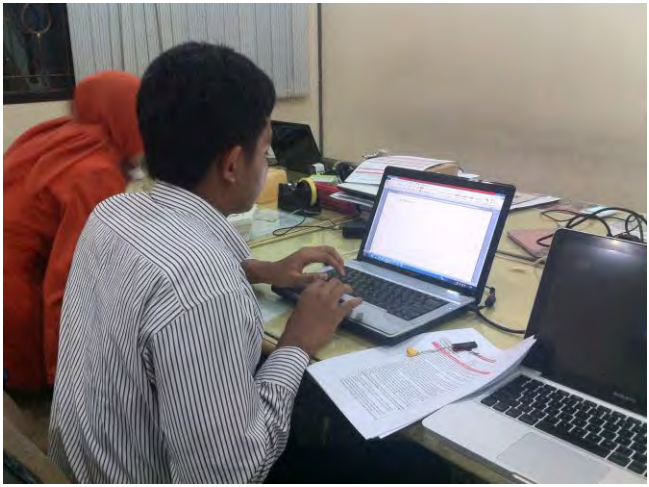
*Referensi: *Management Review Meeting Minutes, Oxebridge.*

LAMPIRAN K

Dokumentasi

Lampiran ini akan menunjukkan dokumentasi saat proses penyusunan BCP di BPR Bank Surya Yudha Banjarnegara

Gambar Lampiran 1 Penyerahan Dokumen Prosedur BCP ke Pimpinan Bagian TSI: Ir. Mulyadi MBA (Sumber: Peneliti, 2014)



Gambar Lampiran 2 Proses Penyerangan Sistem Core Banking (Pengujian BCP) oleh Karyawan TSI (Sumber: Peneliti, 2014)

Gambar Lampiran 3 Proses Penanganan Serangan pada Sistem Core Banking (Pengujian BCP) oleh Pimpinan Bagian TSI (Sumber: Peneliti, 2014)