



JASA RAHARJA

**KEBIJAKAN
BUSINESS CONTINUITY MANAGEMENT
DAN KELANGSUNGAN LAYANAN TIK**

Nomor Dokumen : K05/TIK
Revisi : 3.0
Tanggal Penyusunan : Jan 2021
Tanggal Berlaku : Mei 2021
Klasifikasi : INTERNAL

**DIVISI TEKNOLOGI INFORMASI DAN KOMUNIKASI
PT JASA RAHARJA**

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 1 dari 16

RIWAYAT PERUBAHAN			
Rev	Tanggal	Uraian Perubahan	Penyusun
1.0	Oktober 2015	Terbitan Pertama	
2.0	Mei 2019	Perubahan: <ul style="list-style-type: none"> Butir 11.15 .4 Strategi pemulihan cool standby dihapus karena tidak digunakan Jasa Raharja 	Wawang Yusdiman
3.0	Jan 2021	Perubahan mengikuti platform baru	Wawang Yusdiman

DOKUMEN TIDAK TERKENDALI

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 2 dari 16

DAFTAR ISI

RIWAYAT PERUBAHAN	1
DAFTAR ISI.....	2
1. Latar Belakang	3
2. Tujuan	4
3. Ruang Lingkup.....	4
4. Istilah dan Definisi	5
5. Persyaratan dan Rencana Kelangsungan Layanan TIK	7
6. Uji Coba	8
7. Pelaporan	8
8. Pengertian RPO, RTO dan MTPD.....	9
9. Prinsip Business Continuity Management	9
10. Hirarki Tata Kelola dan Cakupan BCM.....	10
11. Siklus BCM	12
12. Kebijakan Umum BCM.....	13
13. Kebijakan Business Impact Analysis.....	13
14. Kebijakan Kelangsungan Layanan TIK	14
15. Review dan Audit.....	16

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 3 dari 16

1. Latar Belakang

Sebagai perusahaan yang bidang usahanya lebih fokus pada asuransi sosial PT. Jasa Raharja harus terus menerus meningkatkan kinerjanya agar layanan asuransi prima yang dicanangkan dapat dirasakan masyarakat dan terus mengalami peningkatan. Selain memiliki komitmen untuk menerapkan Tata Kelola Perusahaan yang baik (*Good Corporate Governance* - GCG), Jasa Raharja juga menetapkan dan menerapkan Tata Kelola Teknologi Informasi (*IT Governance*) yang merujuk pada standar-standar yang diakui secara internasional mengingat Teknologi Informasi dan Komunikasi sudah menjadi tulang punggung dalam penyelenggaraan asuransi sosial sebagai program utama yang diemban Jasa Raharja.

Peran teknologi informasi dan komunikasi yang semakin penting dalam penyelenggaraan dan pengembangan usaha (bisnis) Jasa Raharja memunculkan adanya kebutuhan perusahaan agar teknologi informasi yang meliputi seluruh sistem dan infrastrukturnya memiliki keandalan yang tinggi sehingga layanan prima yang dicanangkan tidak terganggu karenanya.

Gangguan terhadap kegiatan usaha Jasa Raharja tidak saja hanya disebabkan oleh faktor teknologi informasi dan komunikasi. Ketidaktersediaan pimpinan, pegawai atau ruang kerja yang sangat vital/penting bagi proses penyelenggaraan layanan asuransi juga dapat menjadi faktor penyebab gangguan kegiatan usaha.

Untuk mengantisipasi berbagai jenis gangguan yang dapat menghambat penyelenggaraan kegiatan usaha, maka Jasa Raharja harus memiliki strategi dan rencana yang mampu memelihara kelangsungan usaha, mencegah atau mengurangi terjadinya gangguan serta mengendalikan dampaknya agar tidak mengganggu kegiatan usaha. Strategi ini juga harus mampu memulihkan kegiatan usaha jika gangguan bersifat mendadak (tak terduga) baik karena bencana alam atau tindakan manusia yang berdampak pada terhentinya sementara kegiatan usaha. Strategi dan rencana seperti ini umumnya disebut sebagai *Business Continuity Management* (BCM) atau Manajemen Kelangsungan Usaha.

Dengan digunakannya sistem dan teknologi informasi dan komunikasi sebagai tumpuan operasional proses utama penyelenggaraan layanan asuransi, maka sistem tata kelola TIK di Jasa Raharja harus dikembangkan agar mencakup strategi dan rencana tentang kelangsungan sistem dan

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 4 dari 16

infrastruktur teknologi informasi dan komunikasi dan ketersediaan sumber daya pendukung (pegawai, ruang kerja) yang diperlukan untuk mengoperasikan dan memfasilitasi sistem dan teknologi informasi dan komunikasi.

Dokumen ini menjelaskan strategi, rencana dan komitmen Jasa Raharja dalam rangka menjamin kelangsungan kegiatan usahanya apabila terjadi keadaan yang tidak dikehendaki (bencana) yang berdampak pada terganggunya kegiatan usaha Jasa Raharja, khususnya untuk aspek-aspek yang langsung berhubungan dengan Tata Kelola Teknologi Informasi dan Komunikasi.

2. Tujuan

- 2.1. Menjaga kelangsungan usaha (bisnis) atau layanan asuransi PT Jasa Raharja saat terjadi bencana, khususnya proses bisnis atau layanan paling penting/vital.
- 2.2. Menetapkan pendekatan terhadap pembangunan, penerapan dan pemeliharaan sistem kelangsungan usaha yang mampu mengatasi dampak gangguan sehingga tidak menghentikan kegiatan usaha.
- 2.3. Memberikan kepastian kepada Pimpinan PT Jasa Raharja serta para pemangku kepentingan (*stakeholder*) akan adanya upaya sungguh-sungguh dan berkelanjutan untuk menjaga kelangsungan bisnis perusahaan, khususnya untuk proses-proses yang mengandalkan dukungan sistem dan teknologi informasi dan komunikasi.

3. Ruang Lingkup

- 3.1. Penyusunan strategi pengelolaan kelangsungan usaha atau *Business Continuity Management* (BCM) dalam penyediaan layanan asuransi yang mengandalkan ketersediaan sumber daya pegawai, penyiapan proses, dan teknologi informasi yang menjadi tanggung jawab Divisi TIK.
- 3.2. Implementasi strategi kelangsungan usaha dalam kebijakan ini difokuskan pada kelangsungan layanan TIK yang akan dituangkan dalam prosedur *Business Continuity Plan* (BCP) dan/atau *Disaster Recovery Plan* (DRP).

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 5 dari 16

Dokumen kebijakan ini tidak membahas masalah *Crisis Management*, yang merupakan strategi perusahaan mengelola kondisi krisis selama terjadinya bencana.

4. Istilah dan Definisi

- 4.1. *Business Continuity Management* (BCM) adalah kerangka kerja yang menunjukkan strategi dan komitmen manajemen dalam rangka menjamin proses bisnis utama PT Jasa Raharja tetap berlangsung.
- 4.2. *Business Continuity Plan* (BCP) adalah seperangkat prosedur dan informasi yang dikembangkan, dirangkum, dan dipelihara agar siap digunakan saat adanya kejadian yang termasuk dalam kategori bencana. BCP dapat berupa proses otomatis atau manual yang dirancang untuk mengurangi dampak dari adanya gangguan terhadap fungsi-fungsi penting perusahaan sehingga menjamin kelangsungan layanan yang penting bagi perusahaan. BCP mencakup fungsi/proses bisnis, orang, infrastruktur, sumber daya, informasi, saling ketergantungan antarproses dan sifat serta skala potensi kerugian sepanjang waktu.
- 4.3. *Business Impact Analysis* (Analisis Dampak Usaha) adalah kegiatan untuk mengidentifikasi dan menganalisis kritikalitas fungsi/proses bisnis perusahaan, mengidentifikasi ketergantungan proses bisnis terhadap sistem informasi dan mengkaji dampak bagi PT Jasa Raharja jika fungsi/proses bisnis utama tidak dapat berfungsi.
- 4.4. *Command Center* adalah fasilitas kerja bagi Tim Pengelolaan Kelangsungan Layanan TIK (Tim BCP/DRP) pada saat terjadi keadaan darurat.
- 4.5. *Disaster Recovery Plan* (DRP) adalah suatu rencana atau prosedur yang diperlukan untuk memulihkan layanan TIK (infrastruktur, data dan aplikasi) dan menjamin kelangsungan fungsi bisnis kritis saat terjadi bencana. DRP merupakan bagian dari *Business Continuity Management* (BCM) yang fokusnya memulihkan kelangsungan layanan TI.
- 4.6. Keadaan Darurat/Bencana adalah keadaan dimana fungsi/proses bisnis utama tidak berfungsi sebagian atau seluruhnya sehingga secara langsung mengganggu penyelenggaraan layanan PT Jasa Raharja. Keadaan darurat dapat disebabkan oleh bencana alam

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 6 dari 16

(banjir, badai, gempa bumi), kecelakaan (kebakaran, epidemi) atau kesengajaan manusia (sabotase, terorisme, kerusakan atau intrusi layanan TIK).

- 4.7. Layanan Teknologi Informasi dan Komunikasi (Layanan TIK) adalah fasilitas yang terdiri dari gabungan komponen teknologi, proses, dan personil dalam rangka penyelenggaraan sistem informasi yang direncanakan, dikembangkan, dioperasikan, dan dipelihara oleh Divisi TIK baik secara terpusat maupun terdistribusi, yang digunakan untuk memenuhi kepentingan pemenuhan tugas pokok dan fungsi unit kerja terkait maupun PT Jasa Raharja pada umumnya.
- 4.8. Layanan TIK Utama adalah kesatuan proses dan sistem yang terdiri dari perangkat keras, perangkat lunak, sarana komunikasi, fasilitas, utilitas, dokumen, data, dan personil TIK yang diselenggarakan dan dikelola secara terpusat untuk mendukung proses bisnis inti PT Jasa Raharja. Layanan TIK utama terdiri dari:
 - 4.8.1. DASI-JR (Basis Data Korporasi)
 - 4.8.2. *Bussiness Inteligence*
 - 4.8.3. Aplikasi HRIS
 - 4.8.4. Aplikasi Keuangan
 - 4.8.5. Aplikasi *Monitoring*
 - 4.8.6. *Webmail*
- 4.9. *Maximum Tolerable Periode of Disruption* (MTPD) adalah periode waktu maksimum berhentinya layanan TI/proses bisnis kritikal yang dapat ditoleransi setelah terjadinya bencana. Istilah ini disebut juga dengan *Maximum Tolerable Outage* (MTO) atau *Maximum Acceptable Outage* (MAO).
- 4.10. Pemangku Kepentingan (*Stakeholder*) adalah pihak yang berkepentingan dengan perusahaan, mencakup organisasi atau orang yang dapat terpengaruh langsung atau tidak terhadap suatu kejadian atau keputusan yang berkaitan dengan bencana.
- 4.11. *Recovery Point Objective* (RPO) adalah jumlah maksimum kehilangan data yang dapat diterima saat terjadinya bencana. RPO = 8 jam artinya *backup* dilakukan setiap 8 jam. Jika *backup* terakhir dilakukan pada jam 04.00 dan bencana terjadi pada jam 11.30, maka kehilangan data yang diterima adalah data yang diproses sejak jam 04.00 sampai jam 11.30 (selama 7 jam 30 menit) yang belum di-*backup*. Jika RPO = 1 jam,

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 7 dari 16

berarti data hilang yang ditoleransi adalah data yang diproses selama kurang dari 1 jam sejak backup terakhir.

- 4.12. *Recovery Time Objective* (RTO) adalah periode waktu pasa terjadinya bencana untuk mulai memulihkan layanan pada tingkat minimum. Istilah ini juga disebut dengan *Minimum Business Continuity Objective* (MBCO). Contoh, jika suatu bencana terjadi pada jam 11.30 (siang) dan RTO = 8 jam, maka layanan TI minimum harus mampu dipulihkan mulai jam 19.30.
- 4.13. Tim Pengelolaan Kelangsungan Layanan TIK terdiri dari unsur-unsur lintas unit organisasi sesuai kebutuhan. Susunan Tim ini akan didefinisikan dalam Prosedur *Business Continuity Plan* (BCP) dan/atau *Disaster Recovery Plan* (DRP).

5. Persyaratan dan Rencana Kelangsungan Layanan TIK

- 5.1. PT Jasa Raharja harus mengkaji risiko termasuk faktor-faktor bencana yang dapat mengancam kelangsungan layanan TIK.
- 5.2. Hasil kajian risiko, bersama persyaratan bisnis perusahaan, persyaratan layanan TIK, dan *Service Level Agreement* (SLA) akan menjadi pertimbangan dalam menyusun dan menetapkan persyaratan kelangsungan layanan TIK.
- 5.3. Divisi TIK akan menyusun rencana kelangsungan layanan TIK yang memuat atau merujuk pada:
 - 5.3.1. Kriteria dan tanggung jawab mengaktifkan kelangsungan layanan TIK.
 - 5.3.2. Prosedur saat terjadi event kehilangan layanan TIK kategori major.
 - 5.3.3. Target ketersediaan layanan saat rencana kelangsungan layanan TIK diaktifkan.
 - 5.3.4. Persyaratan pemulihan layanan TIK.
 - 5.3.5. Prosedur kembali ke kondisi normal.
- 5.4. Dokumen rencana kelangsungan layanan TIK dan daftar kontak penanggung jawab harus dapat diakses saat diperlukan.
- 5.5. Rencana kelangsungan layanan TIK harus memastikan agar kontrol-kontrol keamanan informasi tetap berlaku pada saat kondisi bencana dan saat rencana kelangsungan layanan TIK diaktifkan.

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 8 dari 16

- 5.6. Rencana kelangsungan layanan TIK (*IT Service Continuity*) akan didokumentasikan dalam dokumen terpisah.

6. Uji Coba

- 6.1. Rencana kelangsungan layanan TIK harus diuji coba secara berkala, minimum 1 (satu) tahun sekali untuk memeriksa kesesuaiannya terhadap persyaratan yang ditetapkan. Hasil pengujian harus disimpan untuk kepentingan evaluasi dan perbaikan secara berkelanjutan.
- 6.2. Rencana kelangsungan layanan TIK harus diuji coba kembali jika terjadi perubahan lingkungan yang signifikan dan/atau setelah rencana kelangsungan layanan TIK diaktifkan.

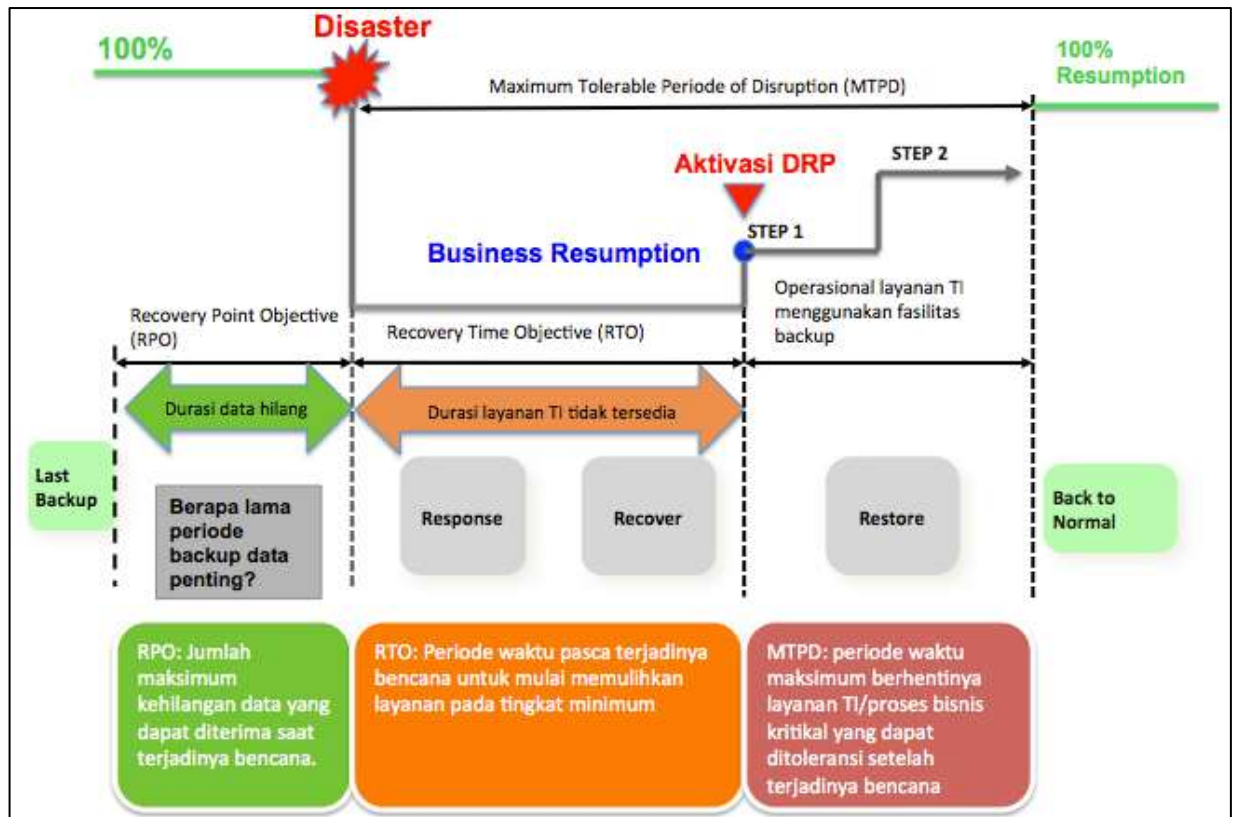
7. Pelaporan

- 7.1. Rencana kelangsungan layanan TIK harus diuji coba secara berkala, Divisi TIK harus melaporkan penyebab, dampak dan pemulihan setelah rencana kelangsungan layanan diaktifkan kepada Komite Pengarah TIK dan Direksi.

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 9 dari 16

8. Pengertian RPO, RTO dan MTPD

RPO, RTO dan MTPD merupakan istilah penting yang harus dipahami dalam menyusun dokumen BCP/DRP. Diagram di bawah ini dapat membantu memahami arti istilah-istilah tersebut.



Gambar 1: RPO, RTO dan MTPD

9. Prinsip Business Continuity Management

PT Jasa Raharja harus memiliki strategi dan rencana yang menjamin fungsi bisnisnya tetap dapat berlangsung saat terjadinya bencana (*disaster*). *Business Continuity Management* (BCM) merupakan kerangka kerja yang akan membantu PT Jasa Raharja tetap beroperasi saat menghadapi atau mengalami gangguan yang dapat menghentikan fungsi bisnisnya.

Prinsip-prinsip utama BCM mencakup:

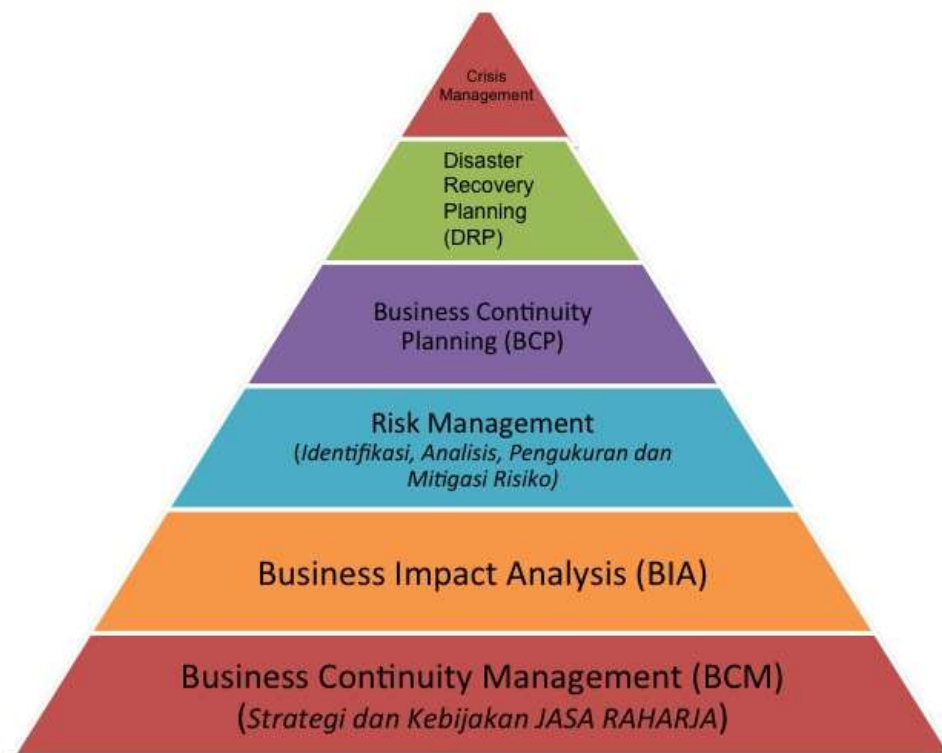
- 9.1. BCM harus menjadi bagian dari strategi, rencana dan proses-proses dalam manajemen perusahaan (PT Jasa Raharja);

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 10 dari 16

- 9.2. Komitmen pimpinan PT Jasa Raharja merupakan prasyarat bagi penerapan strategi dan rencana yang ditetapkan;
- 9.3. Dukungan seluruh unit kerja terkait di setiap tahapan proses sangat diperlukan bagi peningkatan efektivitas BCM.

10. Hirarki Tata Kelola dan Cakupan BCM

Hirarki Tata Kelola dan cakupan BCM secara ringkas digambarkan dalam Gambar 2.



Gambar 2: Cakupan BCM

- 10.1. *Business Continuity Management* (BCM) merupakan strategi dan rencana induk yang menjelaskan komitmen manajemen PT Jasa Raharja dalam menjaga dan memelihara kelangsungan bisnis perusahaan.
- 10.2. *Business Impact Analysis* (BIA) adalah proses menganalisis fungsi bisnis kritis dan dampak terjadinya suatu gangguan yang dapat

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 11 dari 16

dialami oleh fungsi bisnis tersebut. Dalam BIA, data dihimpun melalui wawancara atau dokumen rujukan untuk melakukan identifikasi fungsi/proses bisnis mana yang kritikal/utama dan mana yang merupakan proses pendukung. Fungsi/proses bisnis kritikal akan diprioritaskan agar tetap dapat berlangsung atau jika mengalami gangguan, fungsi/proses bisnis kritikal akan mendapat prioritas untuk dipulihkan.

Berdasarkan identifikasi fungsi/proses bisnis kritikal, BIA kemudian mengidentifikasi sistem informasi utama yang digunakan untuk menopang fungsi/proses bisnis kritikal.

- 10.3. *Risk Management* (manajemen risiko) adalah kegiatan terkoordinasi untuk mengarahkan dan mengendalikan organisasi dalam menangani risiko. Manajemen risiko di sini khususnya mencakup risiko-risiko penggunaan teknologi informasi yang digunakan sebagai pendukung utama fungsi/proses bisnis penyediaan layanan asuransi.
- 10.4. *Business Continuity Plan* (BCP) mencakup tindakan / langkah untuk memindahkan sistem kritikal ke lingkungan yang lain saat perbaikan sistem utama sedang dilakukan, termasuk memindahkan orang yang tepat ke lokasi yang ditetapkan dan melaksanakan bisnis dalam cara yang berbeda sampai kondisi semula berhasil dipulihkan. BCP melibatkan pengelolaan kegiatan kelangsungan dan pemulihan aktivitas bisnis saat terjadi suatu gangguan, dan pengelolaan keseluruhan program melalui pelatihan, latihan dan *review* untuk menjamin agar BCP tetap berlaku dan terkini (*up-to-date*).
- 10.5. *Disaster Recovery Plan* (DRP) mencakup tindakan/langkah untuk mengurangi dampak terjadinya suatu bencana dan menjamin sumber daya TIK dan pegawai yang disiapkan mampu melanjutkan penyediaan layanan TIK pada waktu yang tepat. DRP umumnya lebih fokus pada upaya mengatasi pemulihan fungsi dan layanan TIK yang digunakan sebagai pendukung utama fungsi/proses bisnis dalam hal ini layanan asuransi. Langkah-langkah dalam DRP dapat mulai dilakukan ketika keadaan masih dinyatakan sebagai darurat.
- 10.6. *Crisis Management* merupakan kegiatan merespon suatu keadaan darurat/bencana yang dikoordinasikan oleh suatu Tim di tingkat perusahaan dengan tujuan agar proses penanggulangan bencana dan proses pemulihan tepat dan efektif. Respon ini mencakup tetapi tidak terbatas pada penanganan keselamatan pegawai, penanggulangan

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 12 dari 16

kerusakan fisik gedung, penanganan operasional bisnis perusahaan dan penanganan operasional layanan TIK secara terkoordinasi dengan melibatkan seluruh *stakeholder* perusahaan. *Crisis Management* menyangkut hirarki pelaporan dan pengambilan keputusan penanganan kondisi bencana pada tingkat perusahaan. *Crisis Management* tidak dicakup dalam dokumen ini.

11. Siklus BCM

Business Continuity Management harus menjadi bagian suatu siklus perencanaan manajemen yang dilakukan PT Jasa Raharja. Siklus ini berlaku untuk seluruh tingkatan perencanaan, sejak tingkat perusahaan sampai tingkat unit organisasi pelaksana suatu proses. Siklus BCM digambarkan dalam Gambar 3.



Gambar 3: Siklus *Business Continuity Management*

Dengan memahami dan menerapkan siklus BCM sebagai proses berkelanjutan (*continuous improvement*), maka strategi dan rencana BCM

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 13 dari 16

akan terus menerus mengalami penyempurnaan sesuai dengan kebutuhan dan perubahan karakteristik organisasi dan layanan perusahaan.

12. Kebijakan Umum BCM

- 12.1. Strategi Manajemen Kelangsungan Usaha (*Business Continuity Management - BCM*) harus diterapkan untuk menjamin berlangsungnya proses bisnis utama selama terjadinya bencana/keadaan darurat sesuai dengan kebutuhan, komitmen penyediaan proses bisnis dalam jangka waktu yang ditetapkan.
- 12.2. Strategi Manajemen Kelangsungan Usaha harus mengutamakan keselamatan seluruh pegawai yang terlibat, mengamankan kepentingan dan kewajiban PT Jasa Raharja dalam memenuhi ketentuan undang-undang serta mencegah atau mengurangi dampak terhadap meluasnya gangguan bagi perusahaan.
- 12.3. Setiap unit kerja di lingkungan perusahaan harus mempersiapkan rencana dan/atau prosedur untuk menjaga kelangsungan proses bisnis dan memulihkan proses bisnis sesuai tanggung jawab masing-masing pada saat terjadi bencana.
- 12.4. Dalam hal pemulihan proses bisnis melibatkan layanan TIK, maka unit kerja terkait harus berkoordinasi dengan Divisi TIK.

13. Kebijakan Business Impact Analysis

- 13.1. Divisi TIK harus melakukan kegiatan *Business Impact Analysis* (BIA) untuk memahami dampak keadaan darurat bagi proses bisnis inti. Kegiatan *Business Impact Analysis* mencakup antara lain:
 - 13.1.1. Mengidentifikasi proses bisnis utama perusahaan;
 - 13.1.2. Mengidentifikasi dukungan TIK terhadap proses bisnis utama tersebut;
 - 13.1.3. Mengidentifikasi dampak jika proses bisnis utama tidak dapat dilaksanakan akibat terhentinya layanan TIK;
 - 13.1.4. Menentukan *Maximum Tolerable Periode of Disruption* (MTPD)/*Maximum Tolerable Outage* (MTO), *Recovery Point Objective* (RPO) dan *Recovery Time Objective* (RTO).

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 14 dari 16

- 13.2. *Business Impact Analysis* dilakukan secara berkala minimal 1 (satu) tahun sekali atau jika terjadi perubahan profil risiko (aset, ancaman dan kelemahan) yang dapat memperbesar kerugian terhadap perusahaan.

14. Kebijakan Kelangsungan Layanan TIK

- 14.1. Divisi TIK harus menyusun rencana dan langkah-langkah yang diperlukan untuk menjamin kelangsungan layanan TIK kritis dan harus mampu memulihkan layanan TIK tersebut saat terjadi bencana. Rencana kelangsungan layanan TIK akan didokumentasikan dalam Prosedur *Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP)*.
- 14.2. Keadaan darurat bagi layanan TIK meliputi skenario sebagai berikut:
- 14.2.1. Skenario 1 - Kebakaran *Data Center* PT Jasa Raharja dengan tingkat kerusakan > 50% ruang atau perangkat;
 - 14.2.2. Skenario 2 - Kerusakan struktur bangunan/ruang *Data Center* dengan tingkat kerusakan > 50% (misalnya disebabkan oleh usia bangunan, gempa bumi, bencana alam lainnya dan sebagainya);
 - 14.2.3. Skenario 3 - Gangguan teknis > 50% perangkat pendukung layanan TIK utama (misal: *server*, *core switch*, perangkat jaringan komunikasi, A/C dan sebagainya) selama lebih dari 2 jam.
- 14.3. Gangguan teknis yang diluar skenario keadaan darurat di atas akan ditangani dengan Prosedur *Incident Management*.
- 14.4. Pernyataan keadaan darurat dan kembali ke keadaan normal ditetapkan minimum oleh Direktur terkait atau pejabat ditetapkan perusahaan.
- 14.5. Pengembangan dan penyusunan dokumen BCP/DRP merupakan bagian yang tak terpisahkan dari strategi *Business Continuity Management (BCM)* perusahaan dengan mempertimbangkan:
- 14.5.1. Kebutuhan tingkat ketersediaan informasi dan sistem informasi;
 - 14.5.2. Toleransi *downtime* sistem informasi;
 - 14.5.3. Hasil kajian *business impact analysis (BIA)* dan *IT risk assessment*;
 - 14.5.4. Persyaratan perundang-undangan yang berlaku.

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 15 dari 16

- 14.6. Kontrol-kontrol keamanan informasi sebagaimana ditetapkan dalam kebijakan keamanan informasi dan prosedur terkait harus tetap diberlakukan pada kondisi bencana agar ancaman terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi dapat dikendalikan.
- 14.7. Divisi TIK harus mengidentifikasi sistem dan teknologi informasi utama yang diperlukan bagi pengoperasian layanan TIK sebagai bagian dari strategi Manajemen Kelangsungan Usaha.
- 14.8. *Business Continuity Plan* (BCP)/*Disaster Recovery Plan* (DRP) harus mencakup rencana tindakan untuk pengaktifan kembali (*reactivation*) seluruh layanan TIK kritikal, termasuk penyediaan (*provision*) layanan oleh pihak eksternal yang menjadi bagian dari jaminan kelangsungan proses bisnis utama.
- 14.9. *Business Continuity Plan* (BCP)/*Disaster Recovery Plan* (DRP) harus dikomunikasikan dan disosialisasikan kepada seluruh pegawai terkait khususnya penanggungjawab BCP/DRP secara berkala, dan pihak eksternal terkait yang langsung terlibat dalam penyediaan layanan TIK.
- 14.10. *Business Continuity Plan* (BCP)/*Disaster Recovery Plan* (DRP) akan diuji secara berkala, minimum 1 (satu) kali setahun atau jika terjadi perubahan lingkungan yang signifikan, untuk mengevaluasi dan meningkatkan efektivitasnya.
- 14.11. *Business Continuity Plan* (BCP)/*Disaster Recovery Plan* (DRP) akan mencakup penyediaan fasilitas *redundancy* sebagai solusi backup layanan TIK utama dan memberi kemampuan untuk menghindari adanya *single point of failure* baik dalam infrastruktur (server, perangkat network, storage) maupun aplikasi utama.
- 14.12. Fasilitas *redundancy* yang harus disediakan minimum memiliki spesifikasi dan kemampuan yang sama dengan fasilitas yang akan digantikan.
- 14.13. Hasil uji coba dan langkah pemulihan keadaan darurat harus dievaluasi dan dijadikan sebagai masukan untuk perbaikan dan penyempurnaan BCP/DRP.
- 14.14. PT Jasa Raharja, sepanjang diperlukan, akan mengalokasikan ruang kerja alternatif yang memadai, dilengkapi dengan fasilitas kerja dan sarana komunikasi yang memadai sebagai *Command Center* pada saat terjadi keadaan bencana/darurat.

 JASA RAHARJA	Kebijakan BCM dan Kelangsungan Layanan TIK	No: K05/TIK
		Revisi: 3.0
		Halaman: 16 dari 16

14.15. PT Jasa Raharja menetapkan pilihan strategi pemulihan (*recovery*) layanan TIK utama sebagai berikut:

- 14.15.1. *Hot Recovery*. Untuk layanan dengan tingkat kritikalitas sangat tinggi. Tersedia layanan cadangan di DRC yang bersifat *full redundancy (real time* atau *periodic data replication)* dan sasaran ketersediaan layanan antara 80 - 100% dengan waktu pemulihan maksimum 8 jam;
- 14.15.2. *Warm Standby*. Untuk layanan dengan tingkat kritikalitas tinggi. Tersedia perangkat cadangan di DRC yang meliputi perangkat keras, sistem operasi, aplikasi dan data. Layanan siap digunakan setelah proses restorasi data dan uji fungsi dengan sasaran ketersediaan layanan kurang dari 80% dan waktu pemulihan antara <8 - 24 jam;
- 14.15.3. *Cold Standby*. Untuk layanan dengan tingkat kritikalitas menengah. Tersedia perangkat cadangan di DRC dan siap digunakan setelah instalasi atau restorasi sistem operasi, aplikasi, data dengan sasaran ketersediaan layanan sesuai kebutuhan. Jangka waktu pemulihan antara <24 - 48 jam.

15. Review dan Audit

- 15.1. Divisi TIK harus melakukan tinjauan ulang (*review*) terhadap akurasi proses, prosedur dan petunjuk pelaksanaan secara berkala minimal 1 (satu) kali setahun.
- 15.2. Hasil *review* wajib didokumentasikan dan menjadi bahan rapat Manajemen Review tata kelola TIK.
- 15.3. PT Jasa Raharja harus melaksanakan audit minimal 1 (satu) kali setahun terhadap kepatuhan pelaksanaan Pengelolaan Kelangsungan Layanan TIK.
- 15.4. Audit harus dilaksanakan oleh pihak yang independen, baik dari internal atau eksternal, dan berkompeten melakukan audit.