Jurnal Sistem Informasi dan Sains Teknologi
Vol.3 No.1, Februari 2021
ISSN 2684-8260

PERANCANGAN *BUSINESS CONTINUITY PLAN* PADA PT. XYZ

Ibnu Mas'ud[1)], Rizkya Salsabila[2)] M. Gilvy Langgawan Putra[3)], Dwi Nur Amalia[4)]
[1, 2)]Program Studi Sistem Informasi. Institut Teknologi Kalimantan
Jl. Soekarno Hatta KM 15, Karang Joang, Balikpapan

e-mail: 10171037@student.itk.ac.id[1)], 10171068@student.itk.ac.id[2)]

ABSTRAK

Bencana merupakan kejadian yang secara tiba-tiba dan sangat membahayakan. Bencana dapat terjadi dari berbagai macam aspek antara lain bencana yang disebabkan oleh alam, manusia, dan sebagainya. BCP adalah salah satu metode dalam menjaga keberlangsungan bisnis baik sebelum, selama, dan setelah bencana dan kerusakan pada organisasi terjadi. Cyber crime adalah salah satu bencana yang sangat ditakuti di masa ini. Seluruh aspek organisasi diharuskan untuk menggunakan teknologi dan sistem informasi. Sektor yang paling berisiko terdampak serangan cyber crime adalah perbankan. PT. XYZ, salah satu bank yang terus berevolusi dengan mengambil kebijakan strategis dalam mempertahankan bisnisnya. Dalam menjalankan kegiatan operasionalnya, PT. XYZ menerapkan teknologi informasi diberbagai aspek bisnisnya. Dengan kata lain, apabila cyber crime terjadi akan berdampak pada lumpuhnya operasional perusahaan. Oleh karena itu, pada penelitian ini akan dirancang dokumen perencanaan keberlangsungan bisnis yang dimana dapat membantu PT. XYZ dalam mengatasi bencana baik itu sebelum, di saat, dan setelah terjadinya bencana. Dengan dokumen ini pula, PT. XYZ dapat mengurangi atau mencegah dampak bencana terhadap aktivitas bisnis yang normal.

***Kata Kunci**: Bencana, Cyber Crime, Perencanaan Keberlangsungan Bisnis, PT. XYZ, Teknologi Informasi.*

ABSTRACT

Disasters are sudden and very dangerous events. Disaster can occur from various aspect, including nature-caused disaster, human-caused disaster, and so on. BCP is a method of maintaining business continuity before, during, and after disasters and damage to the organization occur. Cyber crime is one of the most feared disasters at this time. All aspects of the organization are required to use information technology and systems. The sector most at risk of being affected by cyber crime attacks is banking. PT. XYZ, a bank that continues to evolve by taking strategic policies in maintaining its business. In carrying out its personal activities, PT. XYZ applies information technology in various aspects of its business. In other words, if a cyber crime occurs, it will have an impact on the company's operations. Therefore, this research will design a business continuity plan which can help PT. XYZ in overcoming disasters before, during and after the disaster. With this document, PT. XYZ can reduce or prevent the impact of disasters on normal business activities.

***Keywords**: Business Continuity Plan, Cyber Crime, Disaster, Information Technology, PT. XYZ.*

I. PENDAHULUAN

Bencana adalah suatu kejadian yang secara tiba-tiba dan sangat membahayakan dari berbagai aspek mulai dari fungsi, sumber daya manusia, material, dan ekonomi pada organisasi, kelompok, ataupun individu masyarakat. Bencana dapat terjadi dari berbagai macam aspek antara lain bencana yang disebabkan oleh alam, manusia, infrastruktur, dan sebagainya. *Business Continuity Plan* (BCP) adalah salah satu metode dalam menciptakan dan memvalidasi perencanaan dalam menjaga kelanjutan operasional bisnis baik sebelum, selama, dan setelah kejadian bencana dan kerusakan terjadi.

Kejahatan siber (*cyber crime*) adalah salah satu bencana yang dapat terjadi pada organisasi. Pengimplementasian sistem dan teknologi informasi dapat membantu meningkatkan kinerja dan efisiensi organisasi. *Cyber crime* dapat terjadi dikarenakan buruknya keamanan jaringan dan sistem yang ada pada organisasi, kurangnya pemeliharaan teknologi dan jaringan, dan kurangnya perhatian organisasi terhadap infrastruktur yang ada. Salah satu organisasi yang memiliki dampak besar dengan adanya *cyber crime* adalah sektor perbankan.

PT. XYZ sebagai salah satu perusahaan yang bergerak pada bidang perbankan terus meningkatkan kinerja dan efisiensi organisasi. Seiring dengan berjalannya waktu, PT. XYZ terus berevolusi mengikuti perkembangan era saat ini yaitu digitalisasi, perubahan perilaku nasabah dan perkembangan lingkungan bisnis. Dalam merespon perubahan, PT. XYZ mengambil kebijakan strategis dalam mempertahankan keunggulan layanan perbankan dengan selalu berlandaskan pada pemenuhan kebutuhan nasabah melalui penyediaan produk dan layanan yang berkualitas. Semua langkah yang ditempuh memiliki tujuan untuk mengarahkan perubahan dan ancaman yang terjadi pada masa mendatang.

PT. XYZ memiliki proses bisnis utama yaitu memenuhi kebutuhan dana nasabah dengan cara mengelola likuiditas dengan baik. Dalam pelaksanaannya, kendala dan masalah operasional seperti bencana atau kegagalan sistem bisa saja terjadi. PT. XYZ dalam mendukung kegiatan operasional bisnisnya sangat bergantung pada teknologi dan sistem informasi. Semua sektor bisnis yang ada pada PT. XYZ memanfaatkan teknologi informasi. Dengan begitu, apabila teknologi dan sistem informasi yang ada pada PT. XYZ terserang oleh *cyber crime*, besar kemungkinan keseluruhan kegiatan bisnis akan lumpuh atau tidak dapat berjalan. Keamanan data nasabah dan pihak yang berkepentingan menjadi aspek yang paling penting dari pelaksanaan proses bisnis PT. XYZ. Oleh karena itu, diperlukan perancangan XYZ sehingga PT. XYZ dapat mengurangi atau mencegah dampak bencana terhadap aktivitas bisnis yang normal.

II. TINJAUAN PUSTAKA

Pada bagian ini berisi penjelasan terkait pustaka yang digunakan sebagai landasan dalam pengerjaan penelitian ini.

2.1 Profil Perusahaan

PT. XYZ merupakan salah satu bank dengan reputasi tinggi di Indonesia. Adapun visi dari PT. XYZ adalah menjadi Bank pilihan utama andalan masyarakat, yang berperan sebagai pilar penting perekonomian Indonesia. Selain itu, terdapat pula misi dari PT. XYZ adalah sebagai berikut:

1. Membangun institusi yang unggul di bidang penyelesaian pembayaran dan solusi keuangan bagi nasabah bisnis dan perseorangan.
2. Memahami beragam kebutuhan nasabah dan memberikan layanan finansial yang tepat demi tercapainya kepuasan optimal bagi nasabah.
3. Meningkatkan nilai *franchise* dan nilai *stakeholder* XYZ.

PT. XYZ memiliki proses bisnis utama yaitu memenuhi kebutuhan dana nasabah dengan cara mengelola likuiditas dengan baik. Dalam menjalankan kegiatan operasional, proses bisnis utama tersebut dijabarkan ke dalam proses bisnis yang lebih spesifik. Berikut adalah penjabaran dari proses bisnis yang dijalankan oleh PT XYZ:

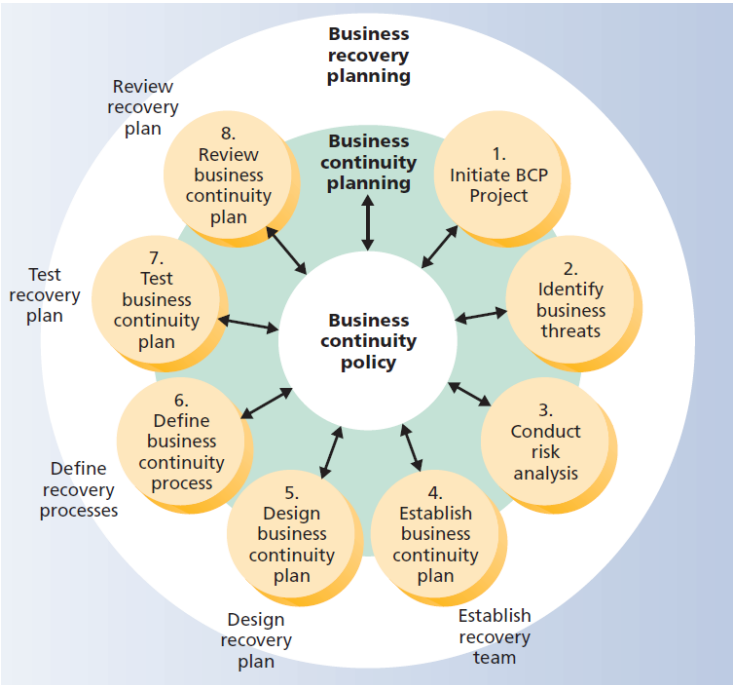
1. Melakukan penghimpunan dana dari masyarakat dalam bentuk simpanan berupa giro, deposito berjangka, sertifikat deposito, tabungan dan/atau bentuk lainnya yang dipersamakan dengan itu.
2. Memberikan layanan kredit untuk masyarakat.
3. Menerbitkan surat pengakuan hutang.
4. Menerima pembayaran dari tagihan atas surat berharga dan melakukan perhitungan dengan atau antar pihak ketiga.
5. Menyediakan tempat untuk menyimpan barang dan surat berharga.
6. Melakukan kegiatan penitipan untuk kepentingan pihak lain berdasarkan suatu kontrak

PT. XYZ selalu berusaha untuk meningkatkan keamanan, kenyamanan, dan kemudahan bagi nasabah dalam melakukan transaksi. Oleh karena itu, PT. XYZ terus mengembangkan layanan perbankan sesuai dengan perkembangan inovasi teknologi dan kebutuhan nasabah.

2.2 *Business Continuity Plan*

Business Continuity Plan (BCP) adalah kerangka kerja yang dapat digunakan dalam mebuat dan memvalidasi rencana dalam mempertahankan operasi secara berkelanjutan baik itu sebelum, saat, dan setelah bencana terjadi. BCP berhubungan dengan bagaimana mengidentifikasi, memeroleh, mengembangkan, mendokumentasi serta menguji sumber daya serta prosedurnya sehingga proses bisnis kritis pada organisasi dapat terjaga apabila terjadi bencana [1].

Dalam merancang BCP terdapat beberapa tahapan yaitu *initiate BCP project, identify business threats, conduct risk analysis, establish business continuity plan, design business continuity plan, define business continuity process, test business continuity plan*, dan *review business continuity plan*. BCP *life cycle* disajikan pada Gambar 2.1 [2].



Gambar 2.1 BCP *cycle*

2.3 *Disaster Recovery Plan*

Disaster Recovery Plan (DRP) terbentuk atas prosedur dan aturan yang memanfaatkan sumber daya solusi yang ditujukan dalam melindungi dan/atau menghidupkan kembali sumber daya, fungsi, atau proses bisnis organisasi (misalnya sistem informasi). Dikarenakan ada beberapa perbedaan jenis bencana yang dapat terjadi, masing-masing dapat memiliki dampak yang berbeda pada sumber daya organisasi. DRP terdiri atas satu set subplan komponen, yang masing-masing ditujukan untuk melindungi/menghidupkan kembali satu set sumber daya dari dampak bencana yang dapat melemahkan proses atau aktivitas organisasi.

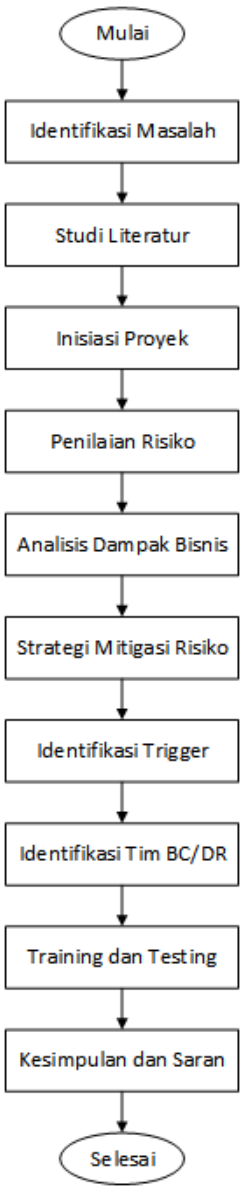
DRP harus memiliki sifat kelayakan, kelengkapan, konsistensi, dan keandalan. Untuk mengembangkan DRP dibutuhkan beberapa tahap antara lain: (1). *vulnerability assessment*; (2). *organizational impact assessment* atau dapat juga *business impact analysis* (BIA); (3). *definition of detailed requirements and* continuity; (4). *Development of alternative subplans*; (5). *The evaluation and selection of the subplans which will constitute the* DRP; (6). *Testing of the* DRP dan; (7). *Maintenance of the* DRP [3].

2.4 *Risk Assessment*

Risk assessment atau penilaian risiko adalah sebuah proses penilaian semua potensi risiko yang dihadapi oleh suatu organisasi. Risiko ini dapat dimulai dari yang biasa hingga yang sangat tidak biasa. Risiko dapat berupa kebakaran atau banjir kecil di ruangan server hingga bencana dengan dampak kerugian yang besar seperti gempa bumi atau badai besar. Penilaian risiko adalah fase dimana semua potensi risiko terhadap bisnis dituliskan dan dievaluasi baik *likelihood* dan dampak dari bencana yang terjadi [4].

III. METODE PENELITIAN

Penelitian ini dilakukan melalui 9 tahapan yang digambarkan melalui diagram alir pada gambar 3.1 berikut:



Gambar 3.1 Diagram Alir Penelitian

3.1 Identifikasi Masalah

Pada tahap ini, penulis mengidentifikasi masalah pada PT. XYZ yang bersumber pada jurnal, *annual report*, *sustainability report*, penelitian terdahulu, dan sumber lainnya. Melalui tahap identifikasi masalah inilah didapatkan latar belakang dan luaran yang akan dihasilkan dari penelitian ini.

3.2 Studi Literatur

Pada tahap ini, penulis mempelajari literatur yang berkaitan dengan objek penelitian dan penelitian terdahulu berupa buku, jurnal, *prosiding*, laporan tahunan, laporan berkelanjutan, skripsi, ataupun sumber lain yang telah terpercaya kualitas dan kevalidan datanya. Studi literatur yang digunakan berkaitan dengan PT. XYZ, BCP, dan DRP.

3.3 Inisiasi Proyek

Pada tahap ini, penulis melakukan identifikasi apa saja yang menjadi potensi bencana pada PT. XYZ. Selain itu, pada tahap ini juga diidentifikasi bagaimana potensi solusi dari setiap bencana yang berpotensi. Pada tahap ini juga dilakukan identifikasi terkait dengan *business*

requirements, functional requirements, technical requirements, success criteria, dan *key contributors* dan *responsibilities*.

3.4 Penilaian Risiko

Pada tahap ini, dilakukan penilaian risiko dari semua bencana yang berpotensi. Risiko yang telah teridentifikasi, dianalisis untuk dilakukan penilaian pada penilaian risiko (*risk assessment*). Penilaian risiko ditentukan berdasarkan *likelihood rating, impact rating*, dan *overall risk rating*. Penilaian risiko ini ditujukan untuk memetakan peringkat dari risiko yang ada mulai dari yang terendah (*very low*) sampai dengan yang tertinggi (*very high*) sehingga didapatkanlah prioritas risiko. Pada penelitian ini, risiko yang memiliki prioritas risiko tertinggi adalah *cyber-crime*.

3.5 Analisis Dampak Bisnis

Pada tahap ini, dilakukan analisis terkait dengan dampak bisnis dari risiko *cyber-crime*. Analisis dilakukan didasarkan pada 6 proses bisnis utama yang ada pada PT. XYZ. Setiap proses bisnis yang ada dianalisis untuk mendapatkan hasil analisa berupa *customer impact, financial impact, reputational impact, operational impact, human impact, critical category,* serta *Maximum Tolerable Downtime* (MTD), *Recovery Time Objective* (RTO), dan *Work Recovery Time* (WRT).

3.6 Strategi Mitigasi Risiko

Pada tahap ini, dilakukan perancangan strategi mitigasi risiko untuk mengeliminasi, mengurangi, atau mengendalikan dampak dari risiko yang diketahui secara intrinsik dengan usaha tertentu sebelum kegagalan terjadi. Hasil pada tahap ini berupa tindakan yang akan dilakukan terhadap risiko utama pada PT. XYZ yaitu *cyber-crime*.

3.7 Identifikasi *Trigger*

Pada tahap ini, dilakukan identifikasi terkait dengan *trigger* dan langkah-langkah pada setiap fase pada BCP. Fase pada BCP terbagi menjadi *activation, recovery, business continuity,* dan *normal operations*. Tujuan dilakukannya tahap ini adalah menentukan langkah-langkah yang akan dilakukan pada 4 fase BCP di saat *cyber-crime* terjadi sampai dengan proses bisnis kembali berjalan normal.

3.8 Identifikasi Tim BC/DR

Pada tahap ini, dilakukan penyusunan tim BC/DR untuk melakukan pembagian peran dan tanggung jawab sumber daya manusia yang jelas sehingga BCP dapat dijalankan dengan efektif dan efisien. Tujuan dibentuknya tim BC/DR adalah untuk memastikan keberlangsungan bisnis perusahaan dan pemulihan dari bencana. Pada tahap ini juga disusun rencana komunikasi (*communication plan*) dengan tujuan untuk mengetahui bagaimana proses komunikasi dan koordinasi tim BC/DR berjalan apabila *cyber-crime* terjadi.

3.9 *Training* dan *Testing*

Pada tahap ini, dilakukan *training* untuk memberikan pemahaman dan tata cara kepada seluruh karyawan PT. XYZ secara khusus tim BC/DR dalam pelaksanaan BCP pada saat *cyber-crime* terjadi dan *testing* dengan tujuan untuk memastikan BCP yang telah dirancang sesuai dengan yang diharapkan, dapat dijalankan, dan apa saja kekurangan dari BCP yang telah dirancang. Perencanaan *training* dilakukan berdasarkan *scope, objectives, timeline,* dan

requirements. Adapun pada tahap ini dilakukan *auditing* untuk memastikan *error* atau kesalahan apa saja yang terjadi serta memberikan prosedur yang jelas dalam pelaksanaan BCP.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini dijelaskan terkait hasil dari tahapan penyusunan dokumen *Business Continuity Planning* untuk PT XYZ. Bagian hasil dibagi menjadi 6 pembahasan yaitu penilaian risiko, analisis dampak bisnis, strategi mitigasi risiko, identifikasi *trigger*, pembentukan tim *Business Continuity/Disaster Recovery*, dan proses *training* & *testing*.

4.1 Hasil Penilaian Risiko

Penilaian risiko dilakukan dengan mengidentifikasi bencana yang berpotensi memengaruhi keberlangsungan bisnis PT XYZ. Proses identifikasi bencana disesuaikan dengan letak perusahaan, proses bisnis, dan layanan yang disediakan oleh perusahaan. Setelah didapatkan potensi bencana, dilanjutkan dengan menentukan tingkat kemungkinan terjadinya bencana dan seberapa besar dampak yang ditimbulkan jika bencana tersebut terjadi. Kemudian, ditentukan pula *risk response* atau langkah apa yang harus diambil perusahaan dalam menghadapi bencana tersebut.

Tabel 4.1 Penilaian Risiko

Threat ID	***Threat Name***	***Threat Source***	***Likelihood***	***Impact***	***Overall Risk Rating***	***Risk Response***
1	Banjir	Eksternal	4	4	16 (Moderate)	*Acceptance*
2	Gempa bumi	Eksternal	2	10	20 (Moderate)	*Transfer*
3	Tsunami	Eksternal	1	10	10 (Low)	*Transfer*
4	Pandemi/wabah	Eksternal	1	6	6 (Low)	*Acceptance*
5	Badai angin/petir	Eksternal	5	5	25 (Moderate)	*Transfer*
6	Kebakaran	Eksternal	2	9	18 (Moderate)	*Transfer*
7	Kebakaran karena kelalaian pegawai	Internal	2	9	18 (Moderate)	*Mitigate*
8	Terorisme (Pengeboman)	Eksternal	1	10	10 (Low)	*Mitigate*
9	Pemadaman Listrik	Eksternal	2	8	16 (Moderate)	*Mitigate*
10	Kegagalan Sistem	Internal	4	9	36 (High)	*Mitigate*
11	Kegagalan jaringan listrik	Eksternal	2	8	16 (Moderate)	*Transfer*
12	Tidak adanya pembaruan dokumen *business continuity planning*	Internal	5	8	40 (High)	*Mitigate*
13	Intensitas penggunaan sistem sangat tinggi sehingga mengalami *downtime*	Internal	4	4	16 (Moderate)	*Mitigate*

14	Terjadinya kesalahan pelaporan dan manipulasi data	Internal	4	8	32 (Moderate)	*Avoid*
15	Pencurian data oleh pegawai	Internal	4	9	36 (High)	*Mitigate*
16	*Cyber-crime*	Eksternal	8	10	80 (Very High)	*Avoid*
17	Koneksi jaringan internet yang lambat	Eksternal	7	4	28 (Moderate)	*Transfer*
18	Kurangnya pengetahuan sumber daya manusia dalam pengoperasian sistem	Internal	4	6	24 (Moderate)	*Mitigate*
19	Infrastruktur jaringan yang kurang memadai	Internal	5	6	30 (Moderate)	*Mitigate*
20	Kerusakan infrastruktur TI	Internal	5	5	25 (Moderate)	*Mitigate*
21	Kerusakan infrastruktur bangunan	Internal	2	8	16 (Moderate)	*Transfer*

Setelah dilakukan penilaian risiko, didapatkan risiko dengan nilai tertinggi yaitu ***cyber crime***. Didapatkan nilai kemungkinan terjadinya *cyber crime* sebesar 8 karena PT XYZ merupakan bank yang mana, hampir seluruh layanan perbankan dilakukan secara digital melalui sistem informasi. Sedangkan untuk dampaknya didapatkan nilai sebesar 10 karena jika terjadi *cyber crime* yang menyerang salah satu sistem maka akan sangat berdampak bagi operasional perusahaan.

4.2 Analisis Dampak Bisnis

Analisis dampak bisnis dilakukan untuk mengidentifikasi dampak apa saja yang dapat memengaruhi proses bisnis perusahaan jika terserang bencana. Dampak yang dianalisis meliputi dampak untuk *customer*, *financial*, *reputational*, *operational* dan *human*. Kemudian dilanjutkan dengan mengidentifikasi waktu-waktu yang diperlukan untuk menoleransi terjadinya bencana dan proses pemulihan. Waktu-waktu tersebut mencakup *Maximum Tolerable Downtime* (MTD), *Recovery Time Objective* (RTO), dan *Work Recovery Time* (WRT)

Tabel 4.2 Analisis Dampak Bisnis

Business Process	***Customer Impact***	***Financial Impact***	***Reputational Impact***	***Operational Impact***	***Human Impact***	***Critical Category***	**MTD**	**RTO**	**WRT**
Melakukan penghimpunan dana dari masyarakat dalam bentuk simpanan berupa giro, deposito berjangka, sertifikat deposito, tabungan dan/atau	Hilangnya data dana masyarakat yang dihimpun	Keluarnya dana perusahaan untuk melakukan ganti rugi terkait hilangnya data dana masyarakat	Perusahaan dianggap lalai dan tidak memiliki langkah preventif dalam pencegahan risiko serta tidak memiliki standar operasional yang jelas	Terhambatnya proses penghimpunan dana dari masyarakat	-	Mission-critical	± 7 jam	± 5 jam	± 2 jam

bentuk lainnya yang dipersamakan dengan itu									
Memberikan layanan kredit untuk masyarakat	Masyarakat tidak dapat melakukan peminjaman dana	Pemasukan perusahaan berkurang diakibatkan tidak adanya pinjaman dana dari nasabah	Perusahaan dianggap tidak mampu memberikan kredit kepada masyarakat sehingga kepercayaan masyarakat untuk melakukan pinjaman kepada perusahaan berkurang	Terhambatnya proses layanan kredit untuk masyarakat	-	Mission-critical	± 7 jam	± 5 jam	± 2 jam
Menerbitkan surat pengakuan hutang	Masyarakat tidak dapat melakukan kredit pada perusahaan	Kurangnya pemasukan perusahaan diakibatkan proses peminjaman dana terhambat	Perusahaan dianggap tidak memiliki rencana cadangan dalam menanggulangi masalah yang ada dan masyarakat beralih ke perusahaan lain untuk mengajukan pinjaman	Terhambatnya proses penerbitan surat pengakuan hutang yang berdampak pada tidak dapat dilakukannya pemberian kredit	-	Mission-critical	± 2 Jam	± 1 Jam	± 1 Jam
Menerima pembayaran dari tagihan atas surat berharga dan melakukan perhitungan dengan atau antar pihak ketiga	-	Besarnya nilai dari surat berharga mengakibatkan kerugian finansial yang besar pula yaitu sebesar nilai surat berharga itu sendiri	Perusahaan dianggap lalai dan tidak memiliki langkah preventif dalam pencegahan risiko serta tidak memiliki standar operasional yang jelas	Terhambatnya proses pembayaran surat berharga dan perhitungannya	Terjadinya kesalahan perhitungan nilai surat berharga dari karyawan perusahaan	Mission-critical	± 3 jam	± 1 jam	± 2 jam
Menyediakan tempat untuk menyimpan barang dan surat berharga	-	Hilangnya barang dan surat berharga mengakibatkan kerugian	Perusahaan dianggap memiliki tingkat keamanan	Tempat penyimpanan barang dan surat berharga melebihi	-	Mission-critical	± 6 jam	± 2 jam	± 4 jam

		finansial yang sangat signifikan bagi perusahaan	yang rendah atau tidak mumpuni dalam melakukan penyimpanan barang dan surat berharga	kapasitas sehingga proses penyimpanan menjadi terhambat					
Melakukan kegiatan penitipan untuk kepentingan pihak lain berdasarkan suatu kontrak	Masyarakat tidak dapat melakukan kegiatan penitipan pada perusahaan	Hilangnya barang atau data masyarakat yang dititip sehingga menyebabkan perusahaan wajib mengganti barang atau data yang dititipkan sesuai dengan kontrak yang telah disepakati	Perusahaan dianggap lalai dalam melakukan penyimpanan barang atau data yang dititip oleh masyarakat dan memiliki tingkat keamanan yang rendah serta standar operasional yang tidak baik	Terhambatnya proses penitipan oleh pihak lain	-	Vital	± 20 jam	± 8 jam	± 18 jam

4.3 Strategi Mitigasi Risiko

Berikut adalah hasil dari identifikasi strategi mitigasi risiko jika terjadi bencana *cyber crime* di PT XYZ:

Tabel 4.3 Strategi Mitigasi Risiko

Business Process	***Option***	***Cost***	***Capability***	***Effort***	***Quality***	***Control***	***Safety***	***Security***	***Desirability***
Melakukan penghimpunan dana dari masyarakat dalam bentuk simpanan berupa giro, deposito berjangka, sertifikat deposito, tabungan dan/atau bentuk lainnya yang dipersamakan dengan itu	**Pre-Arranged**	High	Unknown	Medium	Medium	Medium	Low	Medium	High
Memberikan layanan kredit untuk masyarakat	**Pre-Arranged**	Medium	Meet requirements	Medium	Medium	Medium	Medium	Low	High
Menerbitkan surat pengakuan hutang	**Pre-Arranged**	Medium	Meet requirements	Low	Medium	Medium	High	High	Medium
Menerima pembayaran dari tagihan atas surat berharga dan melakukan perhitungan dengan atau antar pihak ketiga	**Pre-Established**	High	Meet requirements	Medium	High	High	Medium	High	High
Menyediakan tempat untuk menyimpan barang dan surat berharga	**Pre-Established**	High	Meet requirements	Medium	High	High	High	High	High
Melakukan kegiatan penitipan untuk kepentingan pihak lain berdasarkan suatu kontrak	**Pre-Established**	High	Meet requirements	Medium	High	High	High	High	High

4.4 Pengidentifikasian *Trigger*

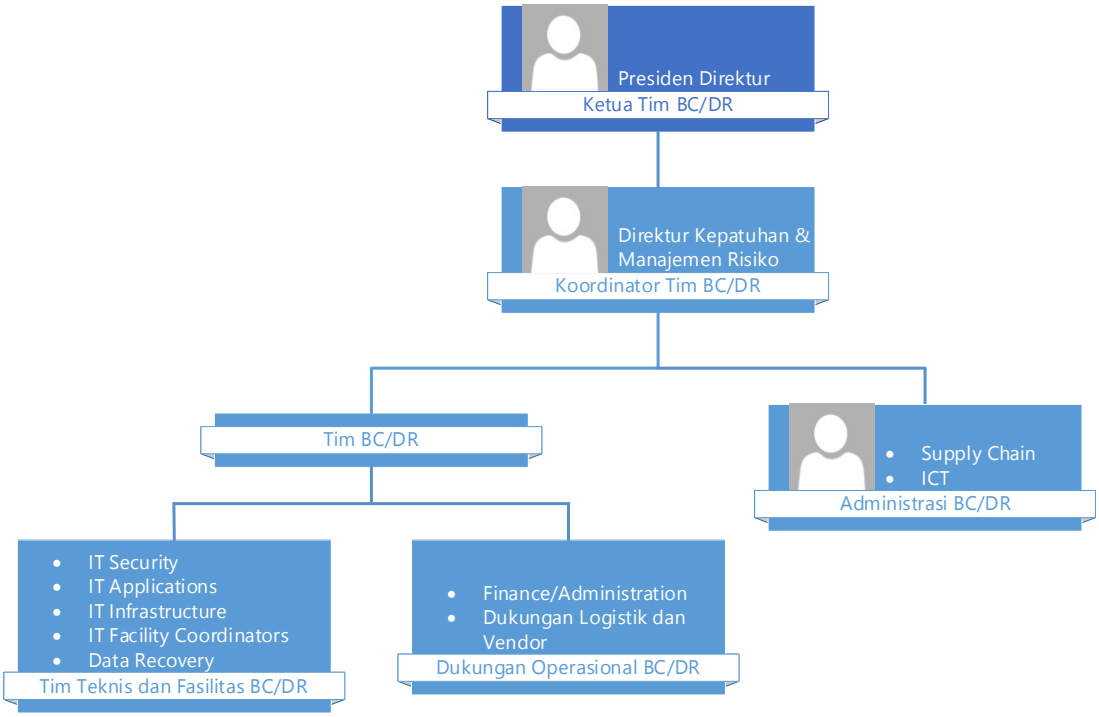
Berikut adalah langka-langkah yang perlu dilakukan jika layanan PT XYZ terserang *cyber crime*:

Tabel 4.4 *Business Continuity Plan*

Trigger	**BCP**	**Pelaksanaan**
Cyber Crime	*Activation*	1. Apabila *cyber crime* terjadi, maka prosedur operasional penanganan dan pencegahan terjadinya dampak secara berkelanjutan harus dijalankan.
	Recovery	2. Mengidentifikasi target dari serangan *cyber crime*.
		3. Mengidentifikasi penyerang
		4. Menentukan kerentanan keamanan yang tidak diketahui
		5. Mengurangi tambahan kerusakan dengan melakukan *routing* ulang *network traffic*.
		6. Melakukan penyaringan atau pemblokiran *traffic*.
		7. Mengisolasi semua atau sebagian jaringan yang menjadi celah dari *cyber crime*.
		8. Melakukan pencatatan secara detail terkait dengan sistem yang terdampak, akun yang diserang, layanan yang terganggu, data dan jaringan yang terdampak, dan jumlah serta kerusakan yang terjadi pada sistem.
		9. Menghubungi organisasi pemerintah atau penegak hukum dalam bidang *cyber crime*
		10. Jika *cyber crime* membahayakan informasi *customer* dan *stakeholder*, berikan pemberitahuan untuk dapat membantu *customer* dalam mengambil langkah untuk segera melindungi diri.
	Business Continuity	11. Melakukan evaluasi dengan mendokumentasikan semua kesalahan atau *error* yang terjadi dan lakukan penilaian bagaimana kesalahan dapat dihindari.
		12. Pastikan *training* selanjutnya termasuk dengan evaluasi yang telah dilakukan.
		13. Mengimplementasikan sistem yang dapat merespon dan mendeteksi ancaman secara efektif.
		14. Melakukan *penetration testing* untuk memastikan keamanan jaringan dipertahankan pada tingkat tertinggi
		15. Melakukan segmentasi jaringan
		16. Mengidentifikasi dampak yang ditimbulkan dari *cyber crime*. Apabila serangan memiliki dampak pada data perusahaan, maka diperlukan proses pemulihan data melalui cadangan data yang disediakan pada *Data Recovery Center*
	Normal Operations	17. Setelah pemulihan data berhasil dilakukan, kegiatan operasional serta proses bisnis yang terdampak langsung pada *cyber crime* dapat dijalankan dengan normal
		18. Melakukan *backup data* secara berkala

4.5 Pembentukan Tim BC/DR

Berikut adalah struktur tim *Business Continuity* (BC)/*Disaster Recovery* (DR) yang dibentuk untuk PT. XYZ:



Gambar 4.1 Struktur Tim BC/DR

4.6 Proses *Training* dan *Testing*

Berikut adalah proses *training* yang perlu dilakukan untuk memastikan seluruh sumber daya manusia pada PT. XYZ memahami langkah-langkah yang harus dijalankan apabila *cyber crime* terjadi.

Tabel 4.5 *Training* Detail

Topik	Detail
Scope	Melakukan pelatihan terhadap seluruh karyawan PT. XYZ terkait dengan langkah dan apa saja yang harus dilakukan pada saat *cyber crime* terjadi.
Objective	• Memahami peran dan tanggung jawab setiap karyawan • Mengetahui tindakan yang akan dilakukan di saat terjadinya *cyber crime* • Mengetahui bagaimana merespon aktivitas jaringan dan sistem yang mencurigakan • Mengetahui bagaimana mendeteksi dini adanya indikasi *cyber crime*
Timeline	• *Training* dilakukan 1 (satu) kali dalam 1 (satu) tahun. • *Training* wajib diikuti oleh seluruh karyawan dan tim BC/DR di PT. XYZ
Requirement	• Tim BC/DR dan karyawan PT. XYZ • Kemampuan dalam mengelola jaringan • Kemampuan dalam mengambil keputusan dan tindakan dalam mengatasi aktivitas jaringan dan sistem yang mencurigakan • Kemampuan dalam mengelola *data center* • Kerja sama dengan Badan Siber dan Sandi Negara (BSSN)

Tabel 4.6 Training

Threat	***Training***
Cyber Crime	Pelatihan dalam menganalisa dan mengindikasi keadaan yang tidak wajar pada sistem dan jaringan sebagai tindakan preventif serta pengurangan risiko terserangnya PT. XYZ
	Pelatihan dalam melakukan *recovery data* ditujukan agar pemulihan berlangsung cepat dan aman.
	Pelatihan terhadap seluruh karyawan terkhusus bagi karyawan yang terspesialisasi pada bidang sistem dan jaringan untuk dapat melakukan pencegahan dan perawatan secara berkala pada sistem dan jaringan PT. XYZ

Tahap *testing* dilakukan dengan menggunakan metode ***Field Exercise***. *Field exercise* dilakukan guna memberikan gambaran nyata dari *cyber-crime.* Metode ini perlu dilakukan karena bank memiliki data-data yang sangat krusial, terutama data nasabah. Sehingga tidak dapat dilakukan *testing* yang hanya didasarkan pada pemahaman dan pengetahuan, namun juga diperlukan pengalaman. Oleh karena itu, harus dilakukan simulasi yang cukup realistis agar SDM yang terlibat untuk menangani *cyber-crime* mendapatkan gambaran nyata terkait apa yang harus dilakukan. Berikut adalah tahapan dari proses testing yang dilakukan:

Tabel 4.7 *Testing*

Threats	**BC/DR Team**	**Testing**
Cyber Crime	Bagian Teknis dan Fasilitas BC/DR, Bagian Operasional BC/DR	Terjadi *cyber-crime* yang menyerang suatu sistem
		Mengidentifikasi target dari serangan *cyber-crime*.
		Mengidentifikasi penyerang
		Menentukan kerentanan keamanan yang tidak diketahui
		Mengurangi tambahan kerusakan dengan melakukan *routing* ulang *network traffic*.
		Melakukan penyaringan atau pemblokiran *traffic*
		Mengisolasi semua atau sebagian jaringan yang menjadi celah dari *cyber-crime*
		Melakukan pencatatan secara detail terkait dengan sistem yang terdampak, akun yang diserang, layanan yang terganggu, data dan jaringan yang terdampak, dan jumlah

		serta kerusakan yang terjadi pada sistem
		Menghubungi organisasi pemerintah atau penegak hukum dalam bidang *cyber crime*
		Jika *cyber-crime* membahayakan informasi *customer* dan *stakeholder*, berikan pemberitahuan untuk dapat membantu *customer* dalam mengambil langkah untuk segera melindungi diri.

V. KESIMPULAN

5.1 Kesimpulan

Adapun kesimpulan dari dilaksanakannya penelitian ini adalah sebagai berikut:

1. Berdasarkan hasil penilaian risiko terhadap potensi ancaman yang ada pada PT. XYZ, dihasilkan risiko bencana dengan tingkat prioritas tertinggi yaitu *cyber-crime*.
2. Dokumen BCP yang dihasilkan pada penelitian ini mampu membantu PT. XYZ dalam merespon dan melakukan pemulihan terhadap bencana.
3. *Training* dan *testing* pada BCP mampu memberikan pemahaman dan gambaran bagaimana BCP dijalankan apabila *cyber-crime* terjadi.

5.2 Saran

Adapun saran dari dilaksanakannya penelitian ini adalah sebagai berikut:

1. Pengambilan data penelitian dilakukan dengan melakukan wawancara dan observasi sehingga penulis dapat memahami kondisi nyata pada PT. XYZ.
2. Penelitian dilakukan dengan jangka waktu yang lebih panjang sehingga luaran yang didapatkan lebih baik lagi.
3. Penelitian ini dilakukan di masa pandemi COVID-19 yang dimana menjadi kendala utama pada pelaksanaan penelitian.
4. Penelitian dilakukan dengan anggota lebih dari 2 orang untuk memudahkan proses analisis pada BCP.

DAFTAR PUSTAKA

[1] M. I. Amirullah and A. P. Subriadi, "Evaluasi Kerangka Kerja Perencanaan Keberlangsungan Bisnis pada PT. Lotte Chemical Titan Nusantara," *Jurnal SISFO,* vol. 8, no. 2, pp. 88-89, 2019.

[2] W. Lam, Ensuring Business Continuity, Los Amitors: IT Pro, 2002.

[3] K.-M. Bryson, H. Millar, J. Anito and A. Mobolurin, "Using formal MS/OR modeling to support disaster recovery planning," *European Journal of Operational Research,* pp. 681-682, 2002.

[4] S. Snedaker, Business Continuity & Disaster Recovery, Burlington: Syngress Publishing Inc, 2007.