ISSN:2302-8149
e-ISSN:2540-9719

Usulan Business Continuity Plan Teknologi Informasi menggunakan ISO 22301 dan ISO 27031

Proposed Business Continuity Plan Information Technology using ISO 22301 and ISO 27031

Ari Cahaya Puspitaningrum
Sistem Informasi, Fakultas Teknik dan Desain, Universitas Hayam Wuruk Perbanas
Wonorejo Utara 16, Rungkut, Surabaya, Jawa Timur, 60296, Indonesia
*e-mail: *ari.cahaya@hayamwuruk.ac.id*

(***received*:** 15 Maret 2022, ***revised*:**1 Juli 2022, ***accepted*:** 8 Agustus 2022)

Abstrak

Mayoritas organisasi memiliki ketergantungan yang tinggi terhadap peran teknologi informasi (TI). TI memiliki peran yang sangat penting bagi sebuah bisnis, sehingga implementasi TI perlu dilindungi dari berbagai ancaman dan gangguan untuk menghindari kegagalan TI dan terjadinya risiko TI yang akan berdampak buruk pada aktivitas bisnis organisasi. Penjaminan keberlangsungan bisnis dapat dilakukan dengan membuat perencanaan keberlanjutan bisnis atau dikenal dengan *Business Continuity Plan* (BCP). BCP merupakan seperangkat prosedur yang lengkap untuk merespon gangguan operasi bisnis secara efektif dan efisien, sehingga bisnis dapat terus berlanjut. Selama ini belum banyak organisasi yang memiliki kesadaran akan pentingnya penerapan BCP yang baik. Hal ini disebabkan oleh kurangnya pengetahuan bagaimana merancang dokumen BCP dengan komprehensif, termasuk analisis dampak bisnis dan memprioritaskan proses bisnis kritis. Organisasi yang tidak menerapkan BCP berpotensi merugi, karena tidak memiliki persiapan apapun jika terjadi bencana terkait teknologi informasi yang memiliki peran krusial dalam organisasi bisnis. Hal ini menunjukkan bahwa BCP penting untuk diterapkan di seluruh organisasi agar bisnis dapat terus berlanjut karena mengurangi dampak negatif dari gangguan bisnis. Penelitian sebelumnya, telah membahas BCP namun masih sedikit yang mengusulkan BCP untuk industri minyak dan gas. Hasil dari penelitian ini adalah usulan BCP pada industri minyak dan gas dengan menggunakan acuan ISO 22301:2012, ISO 27031:2011 terkait keberlangsungan bisnis pada teknologi informasi, dan penelitian sebelumnya tentang elemen BCP.

Kata kunci: *Business Continuity Plan (BCP), Proses Bisnis, Business Impact Analysis (BIA)*, ISO 22301: 2012, ISO 27031:2011, Risiko Teknologi Informasi.

Abstract

Majority of organizations have a high dependence on the role of information technology (IT). IT has a very important role for a business, so IT implementation needs to be protected from various threats and disruptions to avoiding IT failures and the occurrence of IT risks that will poor impact to business activities of the organization. To ensure the sustainability of the business, an organization needs to have a business continuity planning (BCP) document. BCP is a complete set of procedures to respond to the disruption of business operations effectively and efficiently, so that business can continue continuously. During all this time, not many organizations have awareness to the importance of good BCP implementation. It is caused by the lack knowledge how to design BCP document with comprehensive, included business impact analysis and prioritize critical business processes. Organizations without BCP implementation, would potentially loss profit, because they did not have any preparation in case of disaster related to information technology which has crusial role in *business organizations. This indicated that BCP is important to be implemented throughout the organization for business to continue continuously as it reduces the negative impact of business interruptions. The output of this research is the proposed BCP in the oil and gas industry using ISO 22301:2012, ISO 27031:2011 references related to business continuity in information technology, and previous research on BCP elements.*

Keywords: *Business Continuity Plan (BCP), Business Impact Analysis (BIA), ISO 22301: 2012, ISO 27031:2011, Information Technology Risks*

1 Pendahuluan

Keberadaan teknologi informasi (TI) dalam suatu organisasi menjadi sangat krusial dalam pengelolaan bisnis. Sebagian besar organisasi tidak dapat menjalankan bisnisnya tanpa implementasi TI. Implementasi TI dalam suatu organisasi perlu dilindungi dari berbagai gangguan ancaman untuk menghindari terjadinya risiko TI yang akan berdampak buruk terhadap kinerja dan operasi bisnis organisasi [1]. Menurut hasil survei yang dilakukan oleh Business Continuity Institute (2018) menunjukkan bahwa terdapat 5 risiko TI teratas yang dapat mengganggu operasi bisnis, antara lain: serangan dunia maya, pelanggaran data, pemadaman TI dan telekomunikasi yang tidak direncanakan, gangguan pasokan utilitas, dan cuaca buruk [2][3]. Risiko TI dalam suatu organisasi dapat terjadi secara tiba-tiba dan dapat merusak keunggulan kompetitif perusahaan, sehingga memerlukan perhatian segera [4]. Untuk memastikan keberlangsungan bisnis dalam situasi kritis atau berisiko tersebut, organisasi perlu memiliki *Business Continuity Plan (BCP)* [5]. Penerapan BCP merupakan hal yang penting, karena BCP terdiri dari kumpulan prosedur lengkap yang digunakan untuk bertahan dalam bencana, gangguan atau perubahan yang tidak terduga. BCP juga memastikan bahwa proses bisnis penting akan terus berfungsi dalam sebagian besar keadaan yang merugikan dengan batasan yang dapat diterima [4][6].

Penerapan BCP perlu dilakukan oleh organisasi kecil-menengah maupun besar, agar organisasi tidak mengalami kerugian besar dalam menghadapi situasi yang krisis. Kenyataannya, masih banyak organisasi yang belum mengimplementasikan BCP. Berdasarkan hasil survei oleh Asian Disaster Reduction Center (ADRC) pada tahun 2011 menyatakan bahwa hanya 28 % organisasi yang telah memiliki BCP, 9% sedang berprogres membuat BCP, 26% tidak membuat BCP, dan terdapat 37% organisasi yang tidak kenal dengan BCP [7]. Selain itu, pada tahun 2020 juga terdapat hasil survei yang menyatakan bahwa 51% organisasi tidak memiliki BCP untuk menghadapi keadaan darurat atau bencana, 31,1 % telah memiliki BCP namun belum diimplementasikan, 17,9 telah mengimplementasikan BCP [8]. Hal ini menunjukkan bahwa kesadaran organisasi tentang pentingnya BCP masih sangat kurang. Pengembangan BCP telah menjadi masalah kritis bagi sebagian besar organisasi dan masih sedikit literatur yang berfokus pada manajemen BCP.

PT. XYZ merupakan salah satu unit pengolahan industri minyak dan gas yang berperan penting dalam menjaga pasokan minyak nasional hingga 33,3%. Adanya peran penting tersebut mendorong PT. XYZ untuk selalu menjaga keberlangsungan usahanya dengan memanfaatkan peran TI. Perusahaan memiliki ketergantungan yang tinggi terhadap aplikasi online, penggunaan internet dan informasi yang up to date. Ketergantungan ini akan menimbulkan potensi risiko TI bagi perusahaan seperti akses internet terputus, kabel LAN putus, informasi rahasia tersebar luas, kegagalan aplikasi. Risiko-risiko tersebut akan berdampak pada bisnis yang kritis dan mengganggu produksi, pengelolaan, dan distribusi bahan bakar minyak, sehingga PT. XYZ perlu menerapkan BCP.

Hasil dari penelitian ini adalah mengusulkan elemen dan rancangan BCP dengan memberikan informasi kepada perusahaan mengenai daftar risiko TI dan dampaknya bagi perusahaan, serta strategi yang perlu dilakukan. Penelitian ini mengacu pada best practice ISO 22301:2012 dan ISO 27031:2011, serta penelitian sebelumnya tentang elemen BCP. Pengumpulan data dalam penelitian ini dilakukan dengan menganalisis dokumen, observasi, dan wawancara dengan pihak pengelola perusahaan.

ISSN:2302-8149
e-ISSN:2540-9719

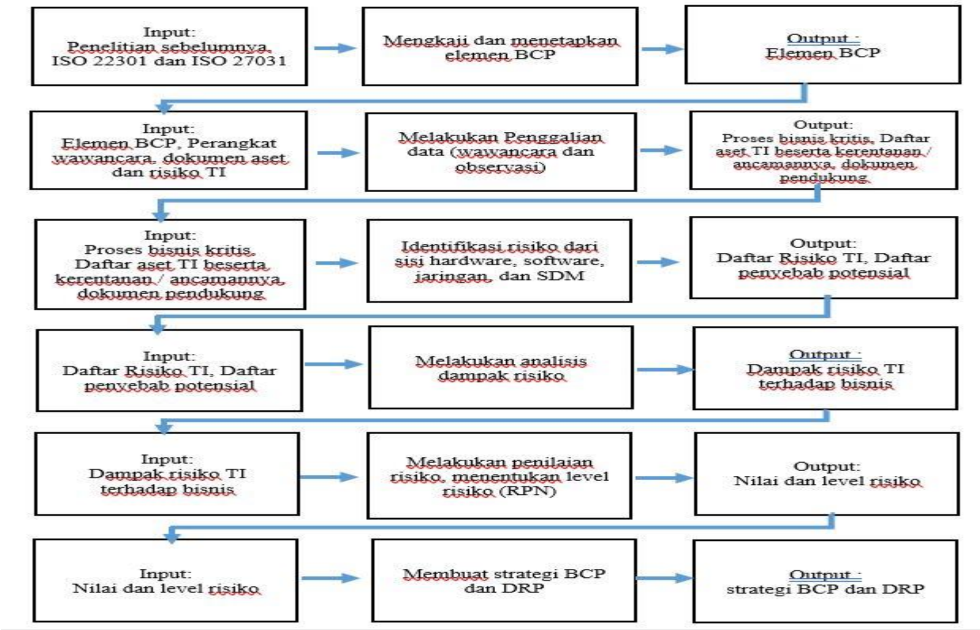
2 Tinjauan Literatur

Pada beberapa penelitian sebelumnya telah mengusulkan model prosedur dan perencanaan business contunity plan (BCP). Pada penelitian [9] memberikan gambaran tentang bagaimana langkah-langkah mengembangkan business continuity plan (BCP) untuk layanan teknologi informasi. Langkah-langkahnya adalah: 1) inisiasi proyek; 2) penilaian risiko/analisis dampak bisnis; 3) desain dan pengembangan BCP; 4) pembuatan BCP; 5) pemeliharaan dan pembaruan. Penelitian lain dilakukan terhadap 4 organisasi di Cape Town Afrika Selatan yang telah memiliki BCP, namun BCP tersebut tidak merinci kegagalan dari segi infrastruktur TI, sehingga ketika terjadi insiden membutuhkan waktu yang lama untuk pemulihannya. Oleh karena itu, penelitian mengusulkan untuk menambahkan pendeteksian titik kritis fase kegagalan dengan mengidentifikasi dan memeringkat setiap kegagalan, sehingga hanya titik-titik penting kegagalan yang akan dimasukkan ke dalam dokumen BCP akhir. Jadi, tahapan lengkap pengembangan BCP dalam penelitian tersebut adalah : 1) persetujuan manajemen; 2) analisis dampak bisnis; 3) Komite BCP; 4) mendeteksi titik kritis kegagalan; 5) mengembangkan BCP; 6) pengujian; 7) pemeliharaan [4]. Pada penelitian [10] telah merancang BCP untuk catatan kesehatan elektronik rumah sakit selama waktu henti. Penelitian tersebut merancang BCP menggunakan siklus PDSA (Plan-Do-Study-Act) dan menghasilkan daftar strategi efektif yang dapat diterapkan ketika catatan kesehatan elektronik terhenti [10]. Penelitian lain telah merancang BCP dengan menggunakan tahapan 1) inisiasi projek, 2) penilaian risiko, 3) analisis dampak bisnis, 4) strategi mitigasi, 5) pengembangan BCP, 6) pengujian dan audit, 7) pemeliharaan, namun penelitian tersebut lebih berfokus pada penilaian dan evaluasi risiko [11]. Selain itu, juga terdapat peneliti yang merancang BCP menggunakan acuan ISO 22301:2102 [12] [13]. Pada ISO 22301:2012, menjelaskan beberapa elemen dari BCP, antara lain : 1) tujuan dan ruang lingkup, 2) pembagian peran, wewenang, dan tanggungjawab, 3) aktivasi rencana, 4) alur komunikasi, 5) kebutuhan sumber daya.

Berdasarkan beberapa penelitian sebelumnya, dapat disimpulkan bahwa telah terdapat beberapa penelitian yang membahas dan merancang BCP untuk sebuah studi kasus dan juga terdapat penelitian yang mengusulkan model / tahapan pengembangan BCP. Elemen BCP yang sering digunakan oleh peneliti sebelumnya mencakup 5 tahap, yaitu 1) inisiasi proyek; 2) penilaian risiko/analisis dampak bisnis; 3) strategi kelangsungan bisnis (strategi BCP & DRP); 4) pelatihan & pengujian; 5) pemeliharaan. Kekurangan pada penelitian sebelumnya adalah masih sedikit yang merancang BCP untuk teknologi informasi dan masih sedikit penelitian yang merancang BCP untuk organisasi besar, terutama untuk industri minyak dan gas.

3 Metode Penelitian

Pendekatan metodologi penelitian ini adalah studi kasus. Penelitian studi kasus adalah studi di mana peneliti mengeksplorasi fenomena (kasus) tertentu dalam waktu dan kegiatan (program, peristiwa, proses, lembaga, atau kelompok sosial) dan mengumpulkan informasi rinci dan mendalam dengan menggunakan berbagai prosedur pengumpulan data selama satu periode [14]. Dengan menggunakan pendekatan studi kasus, peneliti menghabiskan banyak waktu dalam mendeskripsikan konteks atau setting suatu kasus. Menurut Yin, ada 6 bentuk pengumpulan data dalam studi kasus: (1) dokumen; (2) arsip rekaman; (3) wawancara terbuka; (4) pengamatan langsung; (5) observasi partisipan dan (6) peralatan atau instrumen teknologi [15]. Proses pengerjaan penelitian ini mengikuti kerangka kerja metode sebagai berikut:



Gambar 1. Metode Penelitian

Pada Gambar 1 menunjukkan metode atau kerangka penelitian yang dilakukan oleh peneliti, dimana peneliti memulainya dengan melakukan literatur review pada penelitian sebelumnya dan mengkaji ISO 22301 dan 27031 untuk mendapatkan elemen – elemen BCP. Selanjutnya, peneliti melakukan penggalian data melalui wawancara dan observasi. Penggalian data dilakukan untuk mengetahui proses bisnis kritis, daftar aset TI beserta kerentananannya, dan dokumen pendukung.

Penggalian data melalui wawancara dilakukan menggunakan perangkat wawancara yang dengan tujuan dan topik pertanyaan yang ditunjukkan pada Tabel 1. Wawancara ditujukkan kepada penanggung jawab di bagian TI, bagian operasi bisnis dan teknologi, bagian pendukung bisnis dan infrastruktur.

Tabel 1. Perangkat Wawancara

No	Tujuan Pertanyaan	Topik Pertanyaan
1.	Untuk menggali proses bisnis dan daftar layanan TI yang digunakan serta aset TI yang tersedia pada masing – masing bagian.	• Proses bisnis dan layanan TI saat ini • Proses bisnis yang kritikal • Aset TI yang digunakan dalam proses bisnis • Aset TI penting yang dapat menimbulkan ancaman bagi keberlanjutan proses bisnis penting
2.	Untuk menggali informasi tentang risiko pada layanan dan aset TI pada masing – masing bagian.	• Risiko pada layanan dan aset TI • Dampak yang terjadi selama ini ketika risiko TI terjadi.
3.	Untuk menggali informasi tentang praktik pengendalian risiko yang telah diterapkan.	• Bentuk pengendalian risiko yang telah diterapkan

Sedangkan, penggalian data melalui observasi, dilakukan dengan mengkaji dokumen pendukung yang memiliki informasi dan relevansi untuk perancangan BCP, antara lain dokumen aset TI,

 ISSN:2302-8149
e-ISSN:2540-9719

dokumen risiko TI, dokumen analisis dampak bisnis, dokumen rencana mitigasi risiko TI pada tahun sebelumnya yang dimiliki oleh PT. XYZ. Dokumen – dokumen tersebut digunakan untuk kebutuhan identifikasi risiko, analisis risiko, analisis dampak risiko, dan penilaian risiko pada penelitian ini. Peneliti juga melakukan observasi dengan mengamati kondisi kantor perusahaan.Kegiatan terakhir dari metode kerangka kerja penelitian ini adalah membuat strategi BCP dan DRP, sehingga dapat digunakan oleh PT. XYZ.

4 Hasil dan Pembahasan

Proses bisnis yang dimiliki PT. XYZ dapat dibagi menjadi 3 kelompok, yaitu proses identitas, proses prioritas, dan proses penunjang. Proses identitas meliputi: proses eksplorasi, eksploitasi, dan produksi migas & geothermal. Proses prioritas terdiri dari proses pengolahan dan produksi BBM & Non BBM, sedangkan proses penunjang terdiri dari pemasaran produk migas, BBM, non BBM, serta produk energi lainnya dan jasa. Adapun proses bisnis kritikal yang dimiliki oleh PT. XYZ yang memiliki peranan penting dalam keberlangsungan bisnis, yaitu: perencanaan proses pengolahan, pengolahan dan produksi BBM dan non BBM, distribusi produk BBM dan non BBM, pengendalian dan pemeliharaan peralatan kilang, pengeloaan keselamatan lingkungan kerja. Pada penelitian ini mengambil salah satu proses bisnis kritikal, yaitu perencanaan proses pengolahan, sehingga dilakukan analisis risiko pada aset dan layanan TI pada proses bisnis tersebut (lihat Tabel 2). Saat ini, PT. XYZ sudah menerapkan pengendalian pada risiko TI namun belum dilakukan secara maksimal.

Usulan BCP dimulai dengan menentukan elemen – elemen penyusunan yang digunakan. Elemen BCP pada penelitian ini didasarkan pada penelitian sebelumnya dan ISO 22301:2012, serta ISO 27031:2011. Berdasarkan kajian dari beberapa penelitian sebelumnya, ditemukan beberapa elemen yang sering digunakan dalam tahap penyusunan BCP, antara lain: 1) inisiasi proyek; 2) penilaian risiko/analisis dampak bisnis; 3) strategi kelangsungan bisnis (strategi BCP & DRP); 4) pelatihan & pengujian; 5) pemeliharaan. Sedangkan, berdasarkan ISO 22301:2012 dan ISO 27031:2011, dalam penyusunan BCP dapat dilakukan dengan menggunakan siklus PDCA (*plan-do-check-act*) dan elemen BCP yang terdapat di *best practice* tersebut meliputi: tujuan dan ruang lingkup, pembagian peran dan tanggung jawab, daftar kontak, rencana aktivasi, analisis risiko dan analisis dampak bisnis, strategi BCP dan DRP [16] [17]. Dengan demikian, pada penelitian ini mengusulkan elemen – elemen yang dapat digunakan untuk menyusun BCP adalah sebagai berikut:

1. Inisiasi BCP (perencanaan, tujuan, dan ruang lingkup)
2. Pembagian peran dan tanggung jawab
3. Daftar kontak
4. Penilaian risiko dan analisis dampak bisnis
5. Strategi BCP dan DRP
6. Pelatihan dan pengujian
7. Pemeliharaan

Batasan pada penelitian ini adalah peneliti melakukan penilaian risiko dan analisis dampak bisnis pada aset dan layanan TI yang digunakan di proses bisnis perencanaan proses pengolahan, kemudian mengusulkan strategi BCP dan DRP yang dapat diterapkan oleh PT. XYZ.

Identifikasi Risiko dan Analisis Dampak Bisnis

Aset dan layanan TI pada perencanaan proses pengolahan dapat dibagi menjadi lima kategori, yaitu data, *software, hardware*, jaringan, data, dan sumber daya manusia. Identifikasi risiko yang dilakukan mencakup daftar aset TI yang digunakan, penyebab potensial terjadinya risiko pada aset TI, dan risiko TI yang dapat terjadi. Selanjutnya, dilakukan analisis dampak bisnis atau yang dikenal dengan *business impact analysis* (BIA). BIA merupakan elemen dasar untuk pengembangan BCP [18]. BIA dapat digunakan untuk menentukan prioritasi proses operasional bisnis yang paling dianggap kritis pada suatu organisasi. Selain itu, hasil dari BIA ini selanjutnya juga digunakan sebagai dasar proses penilaian risiko [19].

ISSN:2302-8149
e-ISSN:2540-9719

Tabel 2. Identifikasi Risiko dan Analisis Dampak Bisnis

Kategori	Nama Aset	Penyebab Potensial	ID Risiko	Risiko	Dampak Bisnis
Software	• LIMS • Saprodu • SIMOPS • mySAP • P2P *(procure to pay)* • E-Corr • *Material Catalogue* • *Monitoring of data purchasing* • *fingerprint*	Pertahanan sistem tidak cukup kuat untuk mencegah serangan dari luar Serangan dari sumber yang tidak diketahui	S.01.01	Ancaman dunia maya	Layanan tidak bisa berjalan dengan baik, dan banyak keluhan dari pengguna yang akan mengurangi citra positif.
		Sistem tidak dapat menerima semua permintaan Bug dan kesalahan dari sistem default	S.01.02	Kegagalan aplikasi	Loading aplikasi akan menjadi sangat lambat hingga dampak terburuk dari aplikasi tersebut tidak dapat digunakan. Mengganggu aktivitas bisnis karena proses yang biasanya dilakukan secara otomatis harus dilakukan secara manual.
Hardware	• *Phone* • *Handy Talkie* • *Modem* • *Network* • *Intercom* • *PC* • *Camera* • *CCTV* • *AP*	Pengguna membawa minuman ke kantor (cair)	H.01.01	Kerusakan perangkat keras	Mengganggu aktivitas bisnis perusahaan dan menimbulkan keluhan dari pengguna.
		Terjadinya konsleting atau hubungan pendek arus listrik	H.01.02	Kebakaran	Kebakaran akan berdampak pada rusaknya hardware dan lokasi kantor

ISSN:2302-8149
e-ISSN:2540-9719

Kategori	Nama Aset	Penyebab Potensial	ID Risiko	Risiko	Dampak Bisnis
Jaringan	Kabel LAN dan WAN	Tikus yang menggigit kabel	J.01.01	Kerusakan kabel LAN dan WAN	Terganggunya kabel LAN dan WAN secara otomatis akan mengganggu aktivitas bisnis karena hampir semua aplikasi yang digunakan bergantung pada koneksi jaringan.
	Internet	Topologi LAN masih full star, dengan area yang luas	J.01.02	Lambatnya akses jaringan	Mengganggu aktivitas bisnis karena hampir semua aplikasi yang digunakan bergantung pada koneksi jaringan
Data	• Pemantauan kegiatan laboratorium • Lisensi Distribusi / Pemompaan / Pengiriman • Pembayaran Pengadaan Barang/Jasa • Kode dan nama bahan yang digunakan • Pergerakan tangki	Akses yang tidak sah	D.01.01	Informasi rahasia tersebar luas	Menderita kerugian dan merusak citra perusahaan, juga kehilangan kepercayaan dari pelanggan
		Kapasitas Penyimpanan overload	D.01.02	Kehilangan data	Kehilangan data tentu saja merugikan perusahaan serta mengganggu operasional bisnis perusahaan.
Sumber Daya Manusia	• Manajer • Asisten Manajer • Karyawan	Akses yang tidak sah	P.01.01	Penyebaran data dan informasi rahasia	Informasi rahasia perusahaan yang terserbar luas akan merugikan karena merusak citra positif. Selain itu juga menurunkan kepercayaan masyarakat.
		Tidak ada SOP untuk pengelolaan ase	P.01.02	Kesalahan pengelolaan aset	Kesalahan pengelolaan aset akan berdampak pada usia

ISSN:2302-8149
e-ISSN:2540-9719

Kategori	Nama Aset	Penyebab Potensial	ID Risiko	Risiko	Dampak Bisnis
					aset. Aset yang tidak dikelola dengan baik akan memperpendek umur aset serta merugikan perusahaan dalam bidang finansial

Pada Tabel 2, menunjukkan bahwa terdapat berbagai aset dan layanan TI yang dimiliki oleh perencanaan proses pengolahan dalam menjalankan operasi bisnisnya. Setiap aset dan layanan TI tersebut tentunya tidak terbebas dari segala ancaman. Berdasarkan hasil wawancara dan analisis, ditemukan 10 risiko TI yang telah teridentifikasi pada proses bisnis perencanaan proses pengolahan. Risiko-risiko tersebut dapat terjadi karena terdapat penyebab potensial yang mendorong terjadinya risiko. Pada Tabel 2, masing – masing risiko juga telah dianalisis terkait dampak risiko apa saja yang terjadi yang dapat mempengaruhi kelangsungan bisnis.

Penilaian Risiko TI

Setelah mengidentifikasi risiko, langkah selanjutnya adalah melakukan penilaian risiko untuk mengukur nilai risiko yang dihasilkan dengan mempertimbangkan penyebab dan dampaknya. Proses penilaian didasarkan pada hasil observasi, wawancara, dan penilaian subjektif peneliti. Dalam proses penilaian risiko menggunakan metode Failure Mode and Effect Analysis (FMEA), menggunakan tiga komponen penilaian antara lain tingkat keparahan (*Severity* (S)), tingkat kejadian (*Occurrence* (O)), dan deteksi kegagalan (*Detection* (D)) [20]. Ketiga nilai tersebut digunakan untuk menghitung nilai *risk priority number* (RPN) untuk menghasilkan prioritas risiko. Rumus untuk menghitung RPN adalah S x O x D. Nilai RPN akan dikelompokkan menjadi prioritas risiko sangat tinggi (*very high*), tinggi (*high*), sedang (*medium*), rendah (*low*) dan sangat rendah (*very low*).

Tabel 3. Level Risiko

No	ID Risiko	Risiko	RPN	Level Risiko
1.	J.01.02	Lambatnya akses jaringan	S = 5 O =10 D =4 RPN = 200	*Very High*
2.	J.01.01	Kerusakan fisik kabel LAN and WAN	S = 7 O =4 D =5 RPN = 140	*High*
3.	S.01.02	Kegagalan aplikasi	S = 4 O =4 D =6 RPN = 96	*Medium*
4.	D.01.02	Kehilangan Data	S = 8 O =2	*Medium*

ISSN:2302-8149
e-ISSN:2540-9719

			D =5 RPN = 80	
5.	S.01.01	Ancaman dunia maya	S = 5 O =2 D =3 RPN = 30	*Low*
6.	H.01.02	Kebakaran	S = 7 O =2 D =2 RPN = 28	*Low*
7.	H.01.01	Kerusakan perangkat lunak	S = 3 O =6 D =3 RPN = 54	*Low*
8.	D.01.01	Informasi rahasia tersebar luas	S = 7 O =2 D =4 RPN = 56	*Low*
9.	P.01.01	Penyebaran data dan informasi rahasia	S = 7 O =2 D =4 RPN = 56	*Low*
10.	P.01.02	Kesalahan pengelolaan aset	S = 4 O =3 D =3 RPN = 36	*Low*

Pada Tabel 3, menunjukkan hasil perhitungan RPN yang didapatkan dari *severity* (S)) x *occurrence* (O) x *detection* (D). Penentuan nilai S, O, dan D, didapatkan dari hasil wawancara dan analisis dari peneliti. Setelah mengetahui nilai RPN pada masing – masing risiko, maka selanjutnya dapat menentukan level dari risiko tersebut. Pada Tabel 3, terdapat 4 level risiko, yaitu *very high*, *high*, *medium*, dan *low*.

Penentuan level didasarkan pada teori metode FMEA, yang mengklasifikasikan skala RPN sebagai berikut [20]:

RPN ≥ 200: very high
RPN = 120-199: high
RPN = 80-119: medium
RPN = 20-79: Low
RPN = 0-19: very low

Risiko TI yang memiliki nilai RPN paling tinggi adalah risiko lambatnya akses jaringan (ID risiko : J.01.02), sehingga risiko ini merupakan risiko yang perlu diprioritaskan penanganannya, agar operasi bisnis tidak terhenti. Perlakuan yang sama juga perlu diterapkan pada risiko dengan level RPN tinggi.

 ISSN:2302-8149
e-ISSN:2540-9719

Setelah mengetahui level risiko, maka selanjutnya dapat dilakukan perancangan strategi BCP dan DRP.

Strategi BCP dan DRP

Menurut ISO 27031: 2011, BCP perlu fokus pada pengembangan strategi untuk BCP dan DRP [17]. DRP merupakan bagian dari BCP yang berfungsi untuk menangani gangguan sistem informasi/teknologi informasi [21].

Strategi BCP ditentukan berdasarkan hasil analisis risiko dan analisis dampak bisnis. Strategi BCP ini dibuat dengan tujuan untuk menjaga kelangsungan proses bisnis yang diprioritaskan oleh organisasi, serta sebagai bentuk mitigasi manajemen risiko. Menurutnya, strategi BCP terdiri dari 3 strategi, yaitu: 1) strategi pencegahan, bertujuan untuk mengurangi kemungkinan terjadinya bencana / gangguan; 2) strategi respon, strategi yang dilakukan ketika bencana terjadi ; 3) strategi pemulihan, strategi yang dilakukan untuk memulai kembali bisnis, setelah mendapat bencana.

Strategi BCP berfokus pada nilai input risiko TI yang sangat tinggi (RPN> 200) dan tinggi (200> RPN> 120) dengan asumsi bahwa risiko benar-benar terjadi dan mengganggu aktivitas yang ada dalam proses bisnis kritis. RPN dengan nilai rendah dan sedang diabaikan pada penelitian ini. Berdasarkan prioritas Risiko TI, terdapat 2 risiko TI yang termasuk dalam kategori sangat tinggi dan tinggi, yaitu:

1. Lambatnya akses jaringan
2. Kerusakan fisik kabel LAN dan WAN

Strategi BCP dari ke-2 risiko TI tersebut telah didefinisikan pada Tabel 4.

Tabel 4. Strategi BCP

Risiko TI	Strategi BCP
Lambatnya akses jaringan	Strategi Pencegahan : • Pemberlakuan kebijakan penggunaan internet dalam lingkungan kantor Strategi Respon : • Pemindahan proses dari automasi ke proses manual • Identifikasi penyebab gangguan • Memperbaiki kesalahan system • Penyelamatan data dan informasi • Restorasi data Strategi Pemulihan : • Sinkronisasi data • Melakukan evaluasi terkait penyebab gangguan • Melakukan evaluasi prosedur penanganan gangguan
Kerusakan fisik kabel LAN dan WAN	Strategi Pencegahan : • Penyusunan prosedur pengkabelan dan peralatan listrik • Pemberlakuan prosedur backup data secara rutin pada proses bisnis kritikal • Melakukan monitoring secara berkala Strategi Respon : • Pemindahan proses dari automasi ke proses manual

- Identifikasi penyebab gangguan
- Memperbaiki kesalahan system
- Penyelamatan data dan informasi
- Restorasi data

Strategi Pemulihan :

- Sinkronisasi data
- Melakukan evaluasi terkait penyebab gangguan

Melakukan evaluasi prosedur penanganan gangguan

Sedangkan, strategi DRP adalah rencana pemulihan layanan TI jika terjadi bencana atau gangguan untuk mengurangi risiko kerugian perusahaan ke tingkat yang dapat diterima oleh manajemen. Strategi DRP berfokus pada penggunaan teknologi, proses dan sumber daya manusia yang ditujukan untuk memenuhi tujuan tingkat layanan yang diwujudkan dalam bentuk kesepakatan nilai.

Dalam strategi DRP, perlu mengidentifikasi layanan/proses kritis dan periode gangguan maksimum yang dapat ditoleransi (*Maximum tolerable period of disruption* (MTPoD)), seperti *Recovery Time Objective* (RTO), dan *Recovery Point Objective* (RPO). Strategi DRP dalam penelitian ini berfokus pada layanan TI yang memiliki tingkat kritis yang tinggi. Strategi tersebut adalah strategi pecadangan (*backup*) dan strategi pemulihan (*restore*) pada layanan aplikasi TI.

Tabel 5. Strategi DRP

No	Aplikasi TI	Level RTO	Maks. RPO	Strategi *Backup*	Strategi *Restore*
1	LIMS	*High*	< 1 jam	*Mirroring*	*Electronic Vaulting (Active-Active)*
2	MySAP	*High*	< 1 jam	*Mirroring*	*Electronic Vaulting (Active-Active*
3	Monitoring Data Purchasing	*High*	4 jam	*Incremental Backup - Scheduled*	*Electronic Vaulting (Active-Active*
4	ROAS	*High*	< 1 jam	Mirroring	*Electronic Valuting (Active- Active)*
5	Material Catalog	*High*	1 hari	*Incremental Backup - Scheduled*	*Electronic Valuting (Active- Active)*

Pada Tabel 5 dapat diketahui bahwa ada 5 aplikasi TI yang memiliki risiko dengan tingkatan tertinggi. Berikut ini uraian masing-masing opsi strategi yang terdapat dalam penelitian ini:

Mirroring

Mirroring adalah proses menduplikasi database ke lokasi lain (server lain) atau melakukan snapshot dari seluruh status sistem pada suatu titik waktu untuk mencegah gangguan pada database. Misalnya crash, data tidak bisa diakses, atau datanya corrupt [1].

Incremental backups

Incremental backup hanya mencadangkan data / database yang telah dibuat, ditambahkan, atau berubah sejak terakhir kali [1].

Electronic Vaulting

Strategi pencadangan dengan perangkat pencadangan di lokasi lain. Metode ini cocok untuk layanan TI yang digunakan pada proses bisnis yang membutuhkan *backup* dan saat *downtime* harus segera diaktifkan kembali. *Electronic Vaulting* terbagi menjadi 2 jenis, yaitu: 1) *Active-Standby*: metode ini berarti perangkat berada di 2 lokasi, tetapi jika terjadi bencana aktivasi harus secara manual; 2) *Active - active*: metode ini berarti perangkat berada di 2 lokasi dan aktif, jika terjadi bencana secara otomatis failover ke server cadangan.

Pada penelitian ini mengusulkan beberapa elemen yang diperlukan dan hasil BCP yang yang mengacu pada beberapa penelitian sebelumnya dan *best practice* ISO. Peneliti telah mengkaji beberapa penelitian sebelumnya, namun masih sedikit penelitian yang mengusulkan elemen BCP serta masih sedikit yang mengusulkan strategi BCP dan DRP untuk perusahaan yang bergerak di bidang minyak dan gas.

5 Kesimpulan

BCP merupakan dokumen penting yang harus dimiliki dan dilaksanakan oleh seluruh organisasi untuk mendukung kelangsungan bisnis secara berkesinambungan dan meminimalkan gangguan dan kerugian ekonomi akibat bencana atau insiden. BCP memiliki karakteristik yang unik, sehingga setiap organisasi perlu mengembangkan BCP yang komprehensif berdasarkan kondisi unik dalam organisasinya. Penelitian ini menghasilkan usulan elemen BCP dan usulan strategi BCP dan DRP untuk PT. XYZ dengan menggunakan elemen BCP yang telah ditemukan pada penelitian sebelumnya dan ISO 22301:2012, ISO 27031:201 Bagi internal, penelitian ini dapat memberikan pengetahuan kepada PT.XYZ terkait daftar risiko TI beserta dampaknya bagi perusahaan. Selain itu memberikan usulan strategi BCP dan DRP aplikasi layanan TI yang dapat diterapkan oleh PT.XYZ untuk menjaga keberlangsungan proses bisnis kritisnya. Bagi eksternal, penelitian ini memberikan pengetahuan tentang apa saja elemen BCP dan bagaimana proses Menyusun BCP, serta memberikan pengetahuan tentang bagaimana melakukan analisis risiko dan dampak bisnis dari risiko teknologi informasi.
Keterbatasan dari penelitian ini adalah BCP yang telah dikembangkan hanya untuk 1 proses bisnis kritikal, yaitu perencanaan proses pengolahan pada PT. XYZ. Usulan BCP belum sampai pada pelatihan, pengujian dan pemeliharaan. Saran yang dapat diajukan untuk penelitian selanjutnya adalah mengeksplor pembuatan BCP di industri minyak dan gas untuk beberapa proses bisnis kritikal (lebih dari 1 proses bisnis), kemudian dilakukan simulasi pelatihan, pengujian, dan pemeliharaan terhadap strategi BCP dan DRP yang telah dihasilkan, untuk mengetahui apakah strategi tersebut dapat diimplementasikan dengan baik dan maksimal.

Referensi

[1] J. J. Kassema, “Information Technology (IT) Contingency Plan as part of the Business Continuity Plan: Case of IT Services Delivery Industry,” *SSRN Electron. J.*, Dec. 2019, doi: 10.2139/ssrn.3496143.

[2] P. Kirvan, “Ten Business Continuity Risks to Monitor In 2018,” *2018*. .

[3] S. Fani and A. Subiadi, “Trend of Business Continuity Plan: A Systematic Literature Review,” Feb. 2020, doi: 10.4108/eai.13-2-2019.2286164.

[4] F. Sambo and F. O. Bankole, “A Normative Process Model For ICT Business Continuity Plan for Disaster Management in Small, Medium and Large Enterprises,” *Int. J. Electr. Comput. Eng.*, vol. 6, no. 5, pp. 2425–2431, 2016, doi: 10.11591/ijece.v6i5.11461.

[5] J. Botha and R. Von Solms, “A Cyclic Approach to Business Continuity Planning,” *Inf. Manag. Comput. Secur.*, vol. 12, no. 4, pp. 328–337, 2004, doi: 10.1108/09685220410553541.

[6] IEEE Computer Society., "Business Continuity Planning (BCP) Methodology – Essential For Every Business," 2011.
[7] ADRC, "Business Continuity Planning (BCP) Survey Results and Analysis for the APEC Region," *Asian Disaster Reduct. Cent.*, no. Aug, 2011.
[8] Mercer's Business Responses to the COVID-19 Outbreak Survey, "51% of Organizations Have No Business Continuity Plan to Combat Coronavirus," 2020. [Online]. Available: https://solutionsreview.com/backup-disaster-recovery/51-of-organizations-have-no-business-continuity-plan-to-combat-coronavirus/.
[9] M. Niemimaa and J. Järveläinen, "IT service continuity: Achieving embeddedness through Planning," *Proc. - 2013 Int. Conf. Availability, Reliab. Secur. ARES 2013*, pp. 333–340, 2013, doi: 10.1109/ARES.2013.45.
[10] K. Roush, A. Opsahl, K. Parker, and J. Davis, "Business Continuity Planning:: An Effective Strategy During an Electronic Health Record Downtime," *Nurse Lead.*, vol. 19, no. 5, pp. 525–531, 2021, doi: 10.1016/j.mnl.2021.01.003.
[11] A. Setiawan, A. Wibowo, and A. H. Susilo, "Risk Analysis on the development of a Business Continuity Plan," *Proc. 2017 4th Int. Conf. Comput. Appl. Inf. Process. Technol. CAIPT 2017*, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/CAIPT.2017.8320736.
[12] I. Setiawan, R. Waluyo, and W. A. Pambudi, "Perancangan Business Continuity Plan dan Disaster Recovery Plan Teknologi dan Sistem Informasi Menggunakan ISO 22301," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 3, no. 2, pp. 148–155, 2019, doi: 10.29207/resti.v3i2.911.
[13] G. W. Pramudya and A. N. Fajar, "Business Continuity Plan using ISO 22301:2012 in IT solution company (pt. ABC)," *Int. J. Mech. Eng. Technol.*, vol. 10, no. 2, pp. 865–872, 2019.
[14] J. W. Creswell, "Qualitative Inquiry And Research Design: Choosing Among Five Traditions," SAGE Publications, London., 1998.
[15] Yin, R.K., "Case Study Research Design and Methods," COSMOS Corporation, Washington., 1989.
[16] International Standards Organization, "ISO/IEC 22301," 2011.
[17] T. S. Preview, "International Standard ISO / IEC Information Technology — Security Techniques — Information Security Management Systems— Guidance iTeh Standard Preview iTeh Standard Preview," 2017.
[18] R. L. Tammineedi, "Business Continuity Management: A Standards-based Approach," *Inf. Secur. J.*, vol. 19, no. 1, pp. 36–50, 2010, doi: 10.1080/19393550903551843.
[19] S. A. Torabi, R. Giahi, and N. Sahebjamnia, "An Enhanced Risk Assessment Framework for Business Continuity Management Systems," *Saf. Sci.*, vol. 89, pp. 201–218, 2016, doi: 10.1016/j.ssci.2016.06.015.
[20] S. V. Seyed Shamseddin Alizadeh, Y Rasoulzadeh, P Moshashaie, "Failure Modes and Effects Analysis (FMEA) Technique: A Literature Review," *Sci. J. Rev.*, no. January, 2015, doi: 10.14196/sjr.v4i1.1805.
[21] S. Snedaker, *Business Continuity And Disaster Recovery Planning for IT Professionals*, 2nd ed. USA: Elsevier Inc, 2014.