

BAB II

TINJAUAN PUSTAKA

2.1 Studi Sebelumnya

Identifikasi penelitian terdahulu yang relevan dengan topik penelitian merupakan salah satu tujuan utama dari tinjauan pustaka. Penelitian-penelitian tersebut berperan sebagai landasan dalam mengembangkan penelitian baru. Berikut adalah beberapa contoh penelitian sebelumnya yang dijadikan sebagai acuan dan informasi latar belakang untuk penelitian ini.

Yenny dkk, melakukan Penelitian ini bertujuan mengembangkan Business Continuity Plan (BCP) untuk ketahanan UMKM dan UKM di masa krisis. Dengan metode kualitatif, data dikumpulkan melalui wawancara dan kuesioner dari pelaku UMKM dan UKM di Bandung, lalu dianalisis menggunakan metode OODA Loop. Hasilnya menunjukkan bahwa UMKM dan UKM dapat bertahan dengan memproduksi produk sesuai kebutuhan pasar, melakukan modifikasi atau pengembangan produk, mengikuti pelatihan, meningkatkan kemampuan penjualan online, bergabung dengan grup, berpartisipasi dalam pameran pemerintah, serta memanfaatkan digital marketing dan kolaborasi. Implementasi siklus OODA melibatkan observasi, orientasi, pengambilan keputusan, dan tindakan. Pelaku usaha juga berupaya menjual produk yang ada, memproduksi berdasarkan permintaan, memasarkan secara digital, dan mencari bantuan modal, penangguhan pinjaman, serta pajak dari pemerintah[11].

Ibnu Mas'ud dkk, bertujuan merancang dokumen perencanaan keberlangsungan bisnis (BCP) untuk membantu PT. XYZ dalam mengatasi bencana, khususnya cyber-crime, baik sebelum, di saat, maupun setelah terjadinya bencana, serta untuk mengurangi atau mencegah dampak bencana terhadap aktivitas bisnis yang normal. Metode penelitian ini melalui sembilan tahapan, yaitu Identifikasi Masalah, Studi Literatur, Inisiasi Proyek, Penilaian Risiko, Analisis

Dampak Bisnis, Strategi Mitigasi Risiko, Identifikasi Trigger, Identifikasi Tim BC/DR, serta Training dan Testing. Data penelitian bersumber dari jurnal, annual report, sustainability report, penelitian terdahulu, dan sumber terpercaya lainnya, serta berkaitan dengan PT. XYZ, BCP, dan DRP. Hasil penelitian menunjukkan bahwa *cyber-crime* adalah risiko bencana dengan tingkat prioritas tertinggi bagi PT. XYZ. Nilai kemungkinan terjadinya *cyber-crime* sebesar 8 karena PT. XYZ merupakan bank yang hampir seluruh layanan perbankannya dilakukan secara digital melalui sistem informasi. Dampaknya memiliki nilai 10 karena jika *cyber-crime* menyerang salah satu sistem, operasional perusahaan akan sangat terpengaruh. Dokumen BCP yang dihasilkan mampu membantu PT. XYZ dalam merespons dan melakukan pemulihan terhadap bencana. *Training* dan *testing* pada BCP terbukti memberikan pemahaman dan gambaran nyata mengenai bagaimana BCP dijalankan apabila *cyber-crime* terjadi[12]

Penelitian Humdiana bertujuan merumuskan Business Continuity Plan (BCP) untuk PT. PAM, mengidentifikasi kondisi internal, dampak risiko bencana, dan menyusun strategi pemulihan sistem. Menggunakan metode kualitatif dan kerangka Sharing Vision, penelitian ini menganalisis data melalui *Risk Assessment* dan *Business Impact Assessment* (BIA) yang melibatkan wawancara dan kuesioner kepada Manajer TI. Hasilnya menunjukkan gempa bumi, kebakaran, dan serangan *hacker* sebagai ancaman tertinggi. BIA mengungkapkan ketergantungan kuat antar proses bisnis yang mayoritas berkategori tinggi hingga moderat. Rekomendasi strategi BCP mencakup *backup hardware*, listrik, data, telekomunikasi, persediaan, personel, *recovery site*, *offsite libraries*, prosedur eskalasi, aktivasi, dan asuransi. Penelitian ini memiliki implikasi penting, baik secara manajerial, sistem, maupun keilmuan. Secara manajerial, BCP membuka kesadaran manajemen akan pentingnya keselamatan dan kelanjutan proses bisnis yang terencana, serta mendorong pembentukan tim kerja BCP formal dengan *job description* dan sistem *reward and punishment* yang jelas. Dari sisi sistem, BCP membuat prosedur lebih detail, membutuhkan biaya tambahan untuk peralatan

cadangan, dan melengkapi sistem dengan infrastruktur pendukung kesehatan, keamanan, dan keselamatan kerja. Ini juga memastikan sistem memiliki perencanaan pemulihan yang jelas dan dapat dilaksanakan semua bagian[13]

Yulhendri melakukan Penelitian ini memiliki implikasi penting, baik secara manajerial, sistem, maupun keilmuan. Secara manajerial, BCP membuka kesadaran manajemen akan pentingnya keselamatan dan kelanjutan proses bisnis yang terencana, serta mendorong pembentukan tim kerja BCP formal dengan job description dan sistem reward and punishment yang jelas. Dari sisi sistem, BCP membuat prosedur lebih detail, membutuhkan biaya tambahan untuk peralatan cadangan, dan melengkapi sistem dengan infrastruktur pendukung kesehatan, keamanan, dan keselamatan kerja. Ini juga memastikan sistem memiliki perencanaan pemulihan yang jelas dan dapat dilaksanakan semua bagian. Penelitian ini memiliki implikasi penting, baik secara manajerial, sistem, maupun keilmuan. Secara manajerial, BCP membuka kesadaran manajemen akan pentingnya keselamatan dan kelanjutan proses bisnis yang terencana, serta mendorong pembentukan tim kerja BCP formal dengan job description dan sistem reward and punishment yang jelas. Dari sisi sistem, BCP membuat prosedur lebih detail, membutuhkan biaya tambahan untuk peralatan cadangan, dan melengkapi sistem dengan infrastruktur pendukung kesehatan, keamanan, dan keselamatan kerja. Ini juga memastikan sistem memiliki perencanaan pemulihan yang jelas dan dapat dilaksanakan semua bagian[14]

Fikri dkk, melakukan penelitian ini dengan tujuan utama untuk mengembangkan dokumen Business Continuity Plan (BCP) bagi PT. XYZ, sebuah perusahaan komunikasi berskala nasional, guna meminimalkan kerusakan akibat gangguan operasional. Metode yang digunakan dalam penelitian ini adalah metodologi Business Continuity Planning, yang mencakup tahapan inisiasi proyek, penilaian risiko (risk assessment), analisis dampak bisnis (business impact analysis), pengembangan strategi mitigasi risiko, pengembangan rencana, pelatihan, pengujian, dan audit. Hasil penelitian ini adalah dokumen BCP yang

dapat digunakan oleh PT. XYZ sebagai respons terhadap berbagai gangguan. Dokumen BCP ini dirancang untuk memungkinkan PT. XYZ merespons gangguan yang terjadi secara efektif dan memulihkan operasi bisnis dengan cepat. Berdasarkan identifikasi dan penilaian risiko, ditemukan bahwa ancaman keamanan siber (cybersecurity threats) memiliki nilai risiko tertinggi (very high) dengan kemungkinan terjadinya tinggi (high) dan dampak yang sangat tinggi (very high). Oleh karena itu, PT. XYZ berupaya merespons risiko ini untuk meminimalkan kemungkinan dan implikasinya. Strategi mitigasi risiko yang paling tepat adalah dengan mempertimbangkan berbagai faktor, yaitu menyusun rekomendasi penanganan serangan siber berdasarkan analisis insiden historis. Dalam menjaga keberlangsungan bisnis, rencana telah disusun mulai dari aktivasi SOP, pemulihan (recovery), keberlangsungan bisnis (business continuity), hingga operasi normal (normal operations). Selain itu, tim BC/DR dibentuk, serta pelatihan dan pengujian dilakukan untuk memastikan BCP dapat berjalan lancar.[15]

Tabel 2. 1 Tabel Perbandingan

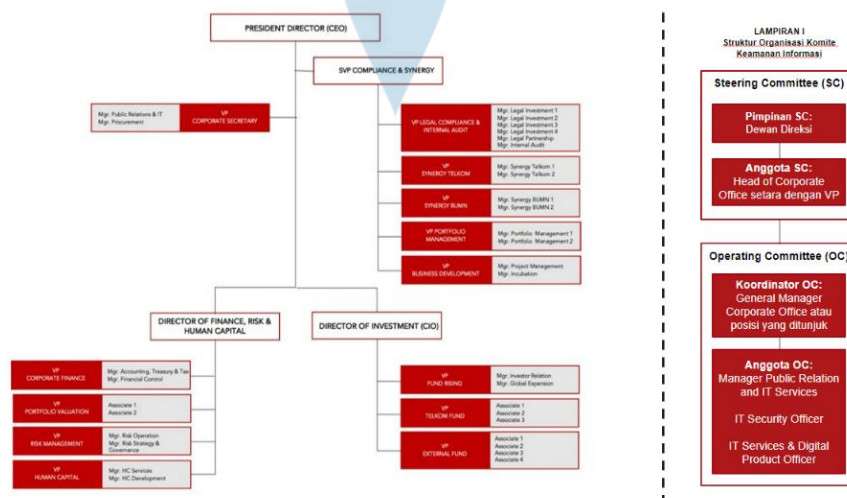
No	Penulis	Tahun	Metode	Hasil	Tujuan
1.	Yenny dkk	2022	Metode kualitatif dengan pengumpulan data melalui wawancara dan kuesioner dari pelaku UMKM dan UKM di Bandung, kemudian dianalisis menggunakan metode OODA Loop (Observasi, Orientasi, Pengambilan Keputusan, dan Tindakan)	UMKM dan UKM bertahan dengan menyesuaikan produk, meningkatkan penjualan online, bergabung grup, ikut pameran, serta memanfaatkan digital marketing dan bantuan pemerintah seperti modal dan keringanan pajak.	Mengembangkan Business Continuity Plan (BCP) untuk meningkatkan ketahanan UMKM dan UKM di masa krisis, khususnya menghadapi dampak pandemi Covid-19
2.	Ibnu dkk	2021	Metode penelitian ini meliputi sembilan tahapan mulai dari identifikasi masalah hingga training dan testing, dengan data dari jurnal, laporan tahunan, dan sumber terpercaya terkait PT. XYZ, BCP, dan DRP, untuk menghasilkan dokumen BCP yang komprehensif dan dapat diimplementasikan efektif.	Hasil penelitian menunjukkan cyber-crime sebagai risiko tertinggi bagi PT. XYZ dengan kemungkinan 8 dan dampak 10, karena ketergantungan tinggi pada sistem digital. Serangan ini dapat mengganggu operasional dan kelangsungan bisnis. Dokumen BCP yang dibuat efektif membantu perusahaan merespons dan memulihkan operasional saat bencana terjadi.	merancang dokumen Business Continuity Plan (BCP) untuk membantu PT. XYZ mengantisipasi, merespons, dan memulihkan operasional bisnis dari ancaman cyber-crime agar aktivitas bisnis tetap berjalan lancar.
3.	Humdiana	2017	Metode kualitatif dengan kerangka Sharing Vision, menggunakan Risk Assessment dan Business Impact Assessment (BIA) melalui wawancara dan kuesioner kepada Manajer TI PT. PAM	Ancaman utama adalah gempa bumi, kebakaran, dan serangan hacker. Analisis BIA menunjukkan ketergantungan tinggi antar proses bisnis dengan dampak dari moderat hingga tinggi. Rekomendasi BCP meliputi backup hardware, listrik, data, telekomunikasi, persediaan, personel, recovery site, offsite libraries, prosedur eskalasi, aktivasi, dan asuransi untuk memastikan kelangsungan operasional dan meminimalkan dampak risiko bencana.	Merumuskan Business Continuity Plan (BCP) untuk PT. PAM dengan mengidentifikasi kondisi internal, dampak risiko bencana, dan menyusun strategi pemulihan sistem
4.	Yulhendri	2021	Metode kualitatif dengan analisis implementasi Business Continuity Plan (BCP) dari sisi manajerial, sistem, dan keilmuan	Secara manajerial, BCP meningkatkan kesadaran manajemen dan mendorong pembentukan tim kerja formal dengan sistem reward-punishment. Dari sisi sistem, BCP memperjelas prosedur, memerlukan biaya tambahan untuk peralatan cadangan, dan melengkapi infrastruktur keselamatan. Secara keilmuan, BCP memastikan perencanaan pemulihan yang jelas dan dapat diimplementasikan di seluruh perusahaan.	Menilai implikasi penerapan BCP dalam meningkatkan keselamatan, kelangsungan bisnis, dan kesiapan sistem di perusahaan
5.	Fikri dkk	2021	: Metodologi Business Continuity Planning yang mencakup tahapan inisiasi proyek, penilaian risiko (risk assessment), analisis dampak bisnis (business impact analysis), pengembangan strategi mitigasi risiko, pengembangan rencana, pelatihan, pengujian, dan audit	Dokumen BCP memungkinkan PT. XYZ merespons gangguan dengan efektif dan memulihkan operasi bisnis cepat. Risiko keamanan siber teridentifikasi sebagai ancaman tertinggi dengan risiko dan kemungkinan sangat tinggi. Strategi mitigasi risiko disusun berdasarkan analisis insiden historis, meliputi aktivasi SOP, pemulihan, keberlangsungan bisnis, pembentukan tim BC/DR, pelatihan, dan pengujian untuk memastikan kelancaran implementasi BCP	Mengembangkan dokumen Business Continuity Plan (BCP) bagi PT. XYZ untuk meminimalkan kerusakan akibat gangguan operasional

2.2 Dasar Teori

2.2.1 MDI Ventures

MDI Ventures adalah perusahaan modal ventura (venture capital) yang dimiliki sepenuhnya oleh PT Telkom Indonesia (Persero) Tbk, salah satu perusahaan telekomunikasi terbesar di Asia Tenggara. Didirikan pada tahun 2015, MDI Ventures memiliki fokus pada pendanaan startup berbasis teknologi yang memiliki potensi pertumbuhan tinggi, baik di dalam negeri maupun secara global. Sebagai bagian dari strategi transformasi digital TelkomGroup, MDI Ventures menjalankan peran ganda sebagai *corporate venture capital* (CVC) dan juga sebagai venture capital tradisional. Artinya, selain mencari keuntungan dari investasi, MDI juga berperan strategis dalam mendorong sinergi antara startup dengan ekosistem bisnis Telkom. Fokus investasinya meliputi sektor-sektor seperti *fintech*, *artificial intelligence* (AI), *software as a service* (SaaS), logistik digital, serta teknologi kesehatan. Perusahaan *venture capital* (VC) beroperasi di lingkungan yang sangat dinamis dan penuh ketidakpastian, di mana tingkat volatilitas pasar sangat tinggi dan perubahan teknologi terjadi dengan cepat.

Untuk susunan struktur pada perusahaan MDI Ventures dapat dilihat Pada Gambar 2.1



Gambar 2. 1 Struktur Organisasi Perusahaan

2.2.2 Risiko

Risiko adalah kemungkinan terjadinya suatu peristiwa yang dapat berdampak pada pencapaian tujuan, baik secara positif maupun negatif. Dalam teori, risiko sering diartikan sebagai kombinasi antara ketidakpastian, kemungkinan terjadinya suatu peristiwa, dan dampaknya terhadap individu, organisasi, atau sistem. Menurut ISO 31000:2018, risiko didefinisikan sebagai efek ketidakpastian pada tujuan, di mana efek ini dapat berupa penyimpangan dari yang diharapkan, baik dalam bentuk peluang maupun ancaman. Elemen utama dari risiko mencakup ketidakpastian, probabilitas terjadinya peristiwa, dan dampak yang dapat timbul. Risiko dapat diklasifikasikan ke dalam beberapa kategori, seperti risiko strategis, operasional, keuangan, reputasi, dan teknologi[16]

Dalam teknologi informasi, risiko sering kali berkaitan dengan ancaman terhadap keamanan data, keberlangsungan operasional, dan kerahasiaan informasi. Contoh risiko di bidang ini mencakup serangan siber, kehilangan data, kegagalan sistem, atau ketidakpatuhan terhadap regulasi keamanan. Untuk mengelola risiko, organisasi biasanya menggunakan pendekatan manajemen risiko yang mencakup identifikasi risiko, penilaian kemungkinan dan dampaknya, mitigasi untuk mengurangi risiko, serta pemantauan dan evaluasi secara berkelanjutan. Dengan memahami dan mengelola risiko secara efektif, organisasi dapat meminimalkan dampak negatif sekaligus memanfaatkan peluang yang mungkin muncul, terutama di era digital yang penuh dengan ketidakpastian.

Manajemen risiko adalah proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko yang dapat memengaruhi pencapaian tujuan organisasi. Proses ini bertujuan untuk meminimalkan dampak negatif dari risiko sekaligus memaksimalkan peluang yang dapat muncul. Menurut ISO 31000:2018, manajemen risiko melibatkan prinsip, kerangka kerja, dan proses untuk mengelola ketidakpastian secara efektif. Elemen utama dari manajemen

risiko meliputi identifikasi risiko, penilaian risiko, mitigasi risiko, serta pemantauan dan evaluasi secara berkelanjutan[17]

Proses manajemen risiko dimulai dengan identifikasi risiko, yaitu upaya untuk mengenali potensi ancaman atau peluang yang dapat memengaruhi organisasi. Setelah risiko teridentifikasi, dilakukan penilaian risiko, di mana kemungkinan terjadinya risiko dan dampaknya dianalisis untuk menentukan prioritas penanganan. Langkah berikutnya adalah mitigasi risiko, yaitu merancang dan menerapkan strategi untuk mengurangi kemungkinan atau dampak risiko. Strategi mitigasi dapat mencakup penerapan kontrol teknis, prosedural, atau administratif. Terakhir, dilakukan pemantauan dan evaluasi risiko secara berkala untuk memastikan bahwa langkah-langkah mitigasi yang diambil efektif dan relevan dengan kondisi terkini[18].

Manajemen risiko sangat penting dalam berbagai konteks, termasuk teknologi informasi, di mana risiko sering kali berkaitan dengan keamanan data, gangguan operasional, atau ancaman siber. Dengan menerapkan manajemen risiko yang efektif, organisasi dapat mengurangi kerugian yang mungkin timbul akibat ancaman, memastikan kelangsungan bisnis, serta meningkatkan kemampuan untuk merespons perubahan dan ketidakpastian di lingkungan operasional[19].

2.2.3 Business Continuity Plan

Business Continuity Plan (BCP) adalah rencana strategis yang dirancang untuk memastikan kelangsungan operasional organisasi dalam menghadapi gangguan atau kejadian yang tidak terduga. BCP bertujuan untuk meminimalkan dampak dari insiden yang dapat mengganggu proses bisnis, seperti bencana alam, serangan siber, kegagalan sistem, atau pandemi. Rencana ini mencakup serangkaian langkah, kebijakan, dan prosedur yang dirancang untuk memulihkan operasional organisasi dengan cepat dan efisien[20].

Proses pembuatan BCP biasanya dimulai dengan identifikasi aset kritis dan risiko yang dapat memengaruhi keberlangsungan bisnis. Langkah ini dilanjutkan

dengan *Business Impact Analysis (BIA)*, yaitu penilaian dampak dari berbagai risiko terhadap operasional bisnis. Setelah itu, organisasi menyusun strategi pemulihan (*recovery strategy*) yang mencakup langkah-langkah untuk memitigasi risiko dan memulihkan operasional. Strategi ini kemudian dituangkan ke dalam dokumen BCP yang berisi panduan tanggap darurat, komunikasi krisis, pemulihan sistem, dan pengelolaan sumber daya. BCP juga harus melalui tahap implementasi dan pengujian untuk memastikan bahwa rencana tersebut memadai dan dapat diandalkan saat diperlukan[20].

BCP sangat penting bagi organisasi karena membantu memastikan kelangsungan layanan dan operasional meskipun terjadi gangguan. Dalam konteks teknologi informasi, BCP sering kali mencakup rencana pemulihan data, pemindahan sistem ke server cadangan, dan koordinasi tim tanggap darurat. Selain itu, BCP juga memberikan panduan komunikasi yang jelas kepada para pemangku kepentingan selama masa krisis. Dengan memiliki BCP yang terencana dengan baik, organisasi dapat mengurangi kerugian finansial, melindungi reputasi, dan meningkatkan kepercayaan pelanggan. Oleh karena itu, BCP menjadi bagian integral dari strategi manajemen risiko dan tata kelola yang baik dalam organisasi[20].

Selain Business Continuity Plan (BCP), terdapat beberapa metodologi lain yang juga banyak digunakan dalam kerangka perencanaan keberlangsungan bisnis, antara lain NIST 800-34, ISO 22301, dan COBIT.

- NIST 800-34 (Contingency Planning Guide for Federal Information Systems) memberikan panduan terstruktur dalam perencanaan kontinjensi khusus untuk sistem informasi. Kelebihannya adalah tahapan yang rinci, mulai dari inisiasi hingga pengujian, sehingga membantu organisasi mengantisipasi gangguan teknologi secara sistematis. Namun, kelemahannya adalah pendekatan ini sangat berfokus pada aspek teknis TI, sehingga kurang menekankan dimensi strategis bisnis secara keseluruhan.

- ISO 22301 (Business Continuity Management System/BCMS) merupakan standar internasional yang komprehensif dengan pendekatan Plan-Do-Check-Act (PDCA). Kelebihannya adalah mampu meningkatkan kredibilitas organisasi di mata stakeholder karena bersertifikasi global dan memberikan kerangka kerja manajemen yang menyeluruh. Kekurangannya, penerapan ISO 22301 membutuhkan biaya, sumber daya, dan komitmen tinggi, sehingga sering dianggap kompleks oleh organisasi berskala kecil hingga menengah.
- COBIT (Control Objectives for Information and Related Technology) berfokus pada tata kelola dan manajemen TI. Kelebihannya adalah mampu menyelaraskan manajemen risiko TI dengan tujuan strategis perusahaan, sehingga memberikan kontrol kuat pada aspek governance. Namun, COBIT tidak secara detail memberikan pedoman pemulihan bisnis saat krisis, melainkan lebih menekankan pengendalian dan pengelolaan TI.

Sehingga BCP menunjukkan keunggulan relatif merata pada semua aspek. BCP tidak hanya memetakan risiko dan kerentanan aset informasi, tetapi juga menghubungkannya dengan strategi bisnis, operasional, serta kebutuhan menjaga kepercayaan investor. Inilah yang menjadikan BCP paling relevan bagi MDI Ventures sebagai perusahaan modal ventura yang sangat bergantung pada keamanan informasi, keberlanjutan operasional, dan reputasi di mata investor.

2.2.3.1 Business Impact Analysis

Business Impact Analysis (BIA) adalah proses sistematis yang digunakan untuk mengidentifikasi dan mengevaluasi dampak dari gangguan terhadap fungsi bisnis organisasi. Proses ini bertujuan untuk menentukan prioritas operasional dan memastikan kelangsungan bisnis dalam menghadapi gangguan, seperti bencana alam, serangan siber, atau kegagalan teknologi. BIA merupakan komponen penting dalam pengembangan *Business Continuity Plan (BCP)* karena memberikan

informasi mendalam tentang proses bisnis kritis yang memerlukan pemulihan segera[21].

a) Identifikasi Proses Kritis

Proses kritis Merupakan serangkaian aktivitas atau fungsi bisnis utama yang apabila terganggu akan menimbulkan dampak signifikan terhadap kelangsungan operasional, reputasi, maupun kondisi finansial organisasi. Proses ini dimulai dengan pemahaman terhadap visi, misi, dan tujuan organisasi, serta struktur

Identifikasi proses kritis dalam *Business Continuity Plan (BCP)* adalah langkah awal yang penting untuk memastikan kelangsungan operasional organisasi saat menghadapi gangguan. Proses ini dimulai dengan pemahaman terhadap visi, misi, dan tujuan organisasi, serta struktur operasionalnya, sehingga aktivitas utama yang mendukung keberlanjutan bisnis dapat dikenali. Selanjutnya, dilakukan pemetaan fungsi-fungsi bisnis utama yang memiliki dampak langsung terhadap operasional, seperti produksi, layanan pelanggan, atau sistem teknologi informasi. Proses ini juga mencakup identifikasi ketergantungan antarproses dan sumber daya yang mendukungnya, termasuk tenaga kerja, infrastruktur, dan teknologi. Selain itu, identifikasi proses kritis juga membantu organisasi menyusun skenario penanganan yang lebih realistis terhadap berbagai potensi gangguan, baik yang berasal dari ancaman internal maupun eksternal. Hasil identifikasi ini menjadi dasar dalam merancang strategi mitigasi risiko, mengalokasikan sumber daya secara memadai, serta memastikan bahwa rencana keberlanjutan bisnis mampu menjaga stabilitas operasional dan kepercayaan pemangku kepentingan.[22].

b) Recovery Time Object (RTO)

Recovery Time Objective (RTO) adalah salah satu elemen penting dalam *Business Continuity Plan (BCP)* yang mengacu pada batas waktu

maksimum yang dapat diterima bagi suatu proses bisnis atau sistem untuk kembali beroperasi setelah terjadi gangguan. RTO membantu organisasi menentukan prioritas pemulihan dan alokasi sumber daya selama situasi darurat, seperti bencana alam, serangan siber, atau kegagalan sistem[23].

RTO ditentukan berdasarkan tingkat kritis dari setiap proses bisnis. Proses yang sangat penting, seperti sistem pembayaran atau layanan pelanggan, biasanya memiliki RTO yang lebih singkat karena dampaknya terhadap organisasi jika tidak segera dipulihkan lebih besar. Sebaliknya, proses yang kurang kritis dapat memiliki RTO yang lebih panjang. Penetapan RTO mempertimbangkan beberapa faktor, seperti dampak finansial dari downtime, risiko terhadap reputasi, dan kepatuhan hukum[23].

Sebagai bagian dari BCP, RTO digunakan untuk mengembangkan strategi pemulihan yang efisien. Misalnya, untuk proses dengan RTO pendek, organisasi dapat menerapkan solusi pemulihan cepat seperti failover sistem otomatis atau penggunaan cadangan data yang diperbarui secara real-time[23].

c) Maximum Tolerable Period Of Disruption (MTPD)

Maximum Tolerable Period of Disruption (MTPD) adalah batas waktu maksimum yang dapat ditoleransi oleh suatu organisasi jika terjadi gangguan pada proses bisnis atau sistem kritis sebelum dampaknya menjadi tidak dapat diterima. MTPD membantu organisasi menentukan sejauh mana toleransi terhadap gangguan dan menjadi panduan dalam menetapkan prioritas pemulihan serta strategi mitigasi risiko dalam *Business Continuity Plan* (BCP)[24].

MTPD mencerminkan tingkat kritis suatu proses atau sistem dalam mendukung operasi organisasi. Proses bisnis yang memiliki dampak besar terhadap keberlanjutan operasional, reputasi, atau kepatuhan hukum biasanya memiliki MTPD yang lebih singkat. Sebagai contoh, sistem

pembayaran online pada perusahaan e-commerce mungkin hanya dapat mentoleransi downtime selama beberapa menit hingga jam, sementara proses pendukung administratif mungkin dapat mentoleransi gangguan selama beberapa hari[24].

Penetapan MTPD melibatkan analisis dampak bisnis (*Business Impact Analysis/BIA*) untuk mengevaluasi konsekuensi finansial, operasional, dan reputasi dari gangguan. MTPD berfungsi sebagai batas maksimum, di mana waktu pemulihan yang ditetapkan melalui *Recovery Time Objective* (RTO) harus berada dalam rentang tersebut. Sebagai ilustrasi, jika MTPD untuk suatu sistem adalah 8 jam, maka RTO untuk pemulihan sistem tersebut harus kurang dari atau sama dengan 8 jam[24].

Dengan menetapkan MTPD, organisasi dapat menyelaraskan strategi pemulihan dengan tingkat toleransi risiko yang dapat diterima, memastikan prioritas yang tepat dalam alokasi sumber daya, dan menjaga kelangsungan operasional meskipun terjadi gangguan signifikan. MTPD juga menjadi acuan dalam pengujian dan pemutakhiran BCP secara berkala untuk memastikan relevansi dan efektivitasnya terhadap kondisi organisasi[24].

d) *Recovery Time Objective* (RPO)

Recovery Point Objective (RPO) adalah salah satu elemen utama dalam *Business Continuity Plan* (BCP) yang menentukan jumlah data maksimum yang dapat diterima untuk hilang selama gangguan sebelum berdampak signifikan pada operasional organisasi. RPO digunakan untuk menetapkan interval pencadangan data dan memastikan bahwa data yang hilang akibat gangguan tetap berada dalam batas toleransi yang telah ditentukan[25].

RPO sangat bergantung pada tingkat kritis data dan kebutuhan operasional organisasi. Misalnya, dalam sistem keuangan *real-time* seperti perbankan *online*, RPO biasanya mendekati nol, artinya data harus

dicadangkan secara terus-menerus atau hampir tanpa kehilangan. Sebaliknya, untuk proses yang tidak terlalu kritis, seperti arsip data historis, RPO dapat lebih panjang, misalnya harian atau mingguan[25].

2.2.3.2 Risk Assessment

Risk Assessment dalam *Business Continuity Plan (BCP)* adalah proses yang bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko yang berpotensi mengganggu operasional bisnis. Proses ini dimulai dengan identifikasi risiko, di mana organisasi mengidentifikasi berbagai ancaman potensial, seperti bencana alam, kegagalan teknologi, serangan siber, atau kelalaian manusia, yang dapat berdampak pada kelangsungan operasional. Setelah itu, dilakukan analisis risiko untuk mengevaluasi probabilitas terjadinya ancaman tersebut dan tingkat dampaknya terhadap bisnis, termasuk aspek finansial, waktu *downtime*, kerusakan infrastruktur, reputasi, dan kepatuhan terhadap regulasi. Analisis ini dapat menggunakan pendekatan kualitatif atau kuantitatif, tergantung pada kebutuhan organisasi. Hasil analisis digunakan untuk mengevaluasi risiko mana yang memerlukan perhatian segera dan prioritas dalam strategi mitigasi. Proses ini memberikan wawasan yang diperlukan untuk merancang langkah-langkah mitigasi, seperti peningkatan keamanan sistem, pelatihan karyawan, atau investasi dalam infrastruktur cadangan, guna memastikan bahwa organisasi dapat mengelola risiko secara memadai dan meminimalkan dampaknya terhadap operasional. Dengan melakukan *Risk Assessment* secara sistematis, organisasi dapat meningkatkan ketahanan dan kesiapan dalam menghadapi berbagai gangguan yang mungkin terjadi[26].

a) Daftar Risiko

Dalam *Business Continuity Plan (BCP)*, penting untuk mengidentifikasi berbagai risiko yang dapat mengganggu operasional bisnis. Risiko teknologi menjadi salah satu yang utama, termasuk kegagalan sistem IT, seperti gangguan pada perangkat keras, perangkat lunak, atau jaringan,

serta ancaman serangan siber, seperti *malware*, *ransomware*, atau peretasan. Selain itu, terdapat risiko fisik, seperti bencana alam (gempa bumi, banjir, atau kebakaran) yang dapat merusak infrastruktur penting organisasi. Risiko operasional juga perlu dipertimbangkan, seperti gangguan rantai pasok, kesalahan manusia, atau kegagalan proses internal. Di sisi lain, risiko finansial, seperti fluktuasi pasar atau kerugian akibat penundaan produksi, juga memiliki dampak signifikan terhadap kelangsungan bisnis. Terakhir, risiko reputasi, yang timbul akibat kegagalan layanan atau pelanggaran data, dapat memengaruhi kepercayaan pelanggan dan mitra bisnis. Identifikasi dan analisis risiko-risiko ini menjadi dasar untuk merancang strategi mitigasi yang sesuai dalam BCP guna memastikan kelangsungan operasional organisasi[27].

b) Peluang Risiko

Dalam konteks *Business Continuity Plan* (BCP), peluang risiko merujuk pada potensi yang timbul dari risiko tertentu yang, jika dikelola dengan baik, dapat memberikan manfaat bagi organisasi. Meskipun risiko biasanya dikaitkan dengan ancaman atau dampak negatif, beberapa risiko juga dapat menciptakan peluang untuk perbaikan, inovasi, atau efisiensi yang sebelumnya tidak dipertimbangkan.

Misalnya, ancaman serangan siber dapat mendorong organisasi untuk mengadopsi teknologi keamanan yang lebih canggih, yang pada akhirnya meningkatkan perlindungan terhadap data dan aset digital. Risiko kegagalan sistem IT dapat memotivasi organisasi untuk memperbarui infrastruktur teknologi mereka, yang tidak hanya mengurangi risiko di masa depan tetapi juga meningkatkan produktivitas operasional. Selain itu, gangguan rantai pasok dapat menjadi peluang untuk mengevaluasi dan mengoptimalkan sumber daya alternatif, sehingga memperkuat ketahanan operasional jangka panjang[28].

c) Risk Map

Risk Map dalam *Business Continuity Plan (BCP)* adalah alat visual yang digunakan untuk memetakan dan memprioritaskan risiko berdasarkan tingkat probabilitas terjadinya dan dampak yang ditimbulkan terhadap operasional bisnis. *Risk Map* biasanya disajikan dalam bentuk matriks dua dimensi, di mana sumbu horizontal menunjukkan tingkat probabilitas (rendah ke tinggi) dan sumbu vertikal menunjukkan tingkat dampak risiko (rendah ke tinggi). Proses pembuatan *Risk Map* dimulai dengan mengidentifikasi semua risiko yang relevan, seperti bencana alam, serangan siber, kegagalan sistem, atau gangguan rantai pasok, melalui analisis risiko. Selanjutnya, setiap risiko dievaluasi berdasarkan kemungkinan terjadinya dan tingkat dampaknya terhadap aspek keuangan, reputasi, atau keberlanjutan operasional. Risiko kemudian dipetakan ke dalam kategori seperti risiko rendah, sedang, tinggi, atau kritis, yang membantu organisasi menentukan prioritas mitigasi. Dengan menggunakan *Risk Map*, organisasi dapat lebih mudah memvisualisasikan risiko utama yang perlu dikelola dan merancang langkah mitigasi yang sesuai untuk memastikan keberlanjutan bisnis meskipun terjadi gangguan. Alat ini menjadi dasar yang kuat dalam pengambilan keputusan terkait prioritas alokasi sumber daya untuk pengelolaan risiko[29].

2.2.3.3 Recovery Strategy Development

Recovery Strategy Development dalam *Business Continuity Plan (BCP)* adalah proses penyusunan strategi untuk memastikan pemulihan fungsi bisnis kritis setelah terjadi gangguan atau bencana. Proses ini bertujuan untuk meminimalkan dampak gangguan dan memastikan bahwa operasional dapat kembali berjalan sesuai dengan *Recovery Time Objective (RTO)* dan *Recovery Point Objective (RPO)* yang telah ditetapkan. Langkah pertama dalam pengembangan strategi ini adalah mengidentifikasi proses bisnis kritis yang harus segera

dipulihkan, termasuk memahami ketergantungan antarproses dan sumber daya yang mendukungnya. Selanjutnya, organisasi menilai sumber daya yang tersedia, seperti tenaga kerja, infrastruktur, dan teknologi, untuk menentukan langkah pemulihan yang paling sesuai. Berdasarkan penilaian ini, organisasi mengembangkan berbagai alternatif strategi pemulihan, seperti pencadangan data, sistem *failover*, atau penggunaan lokasi alternatif untuk operasional darurat. Strategi ini kemudian diuji dan diperbarui secara berkala untuk memastikan efektivitasnya dalam menghadapi berbagai skenario gangguan. Dengan pendekatan yang terencana dan sistematis, *Recovery Strategy Development* membantu organisasi mempersiapkan diri untuk menghadapi gangguan dengan lebih tangguh, menjaga keberlanjutan bisnis, dan melindungi kepentingan pemangku kepentingan[30].

a) Mengidentifikasi Keberlangsungan Bisnis

Mengidentifikasi keberlangsungan bisnis adalah langkah kunci dalam menyusun *Business Continuity Plan (BCP)* untuk memastikan bahwa organisasi mampu tetap beroperasi meskipun terjadi gangguan. Proses ini mencakup analisis terhadap elemen-elemen penting yang mendukung operasional organisasi, seperti fungsi bisnis kritis, sumber daya utama, dan risiko yang berpotensi mengganggu keberlangsungan. Tujuannya adalah untuk memahami kebutuhan organisasi dalam menjaga kelangsungan operasional dan meminimalkan dampak gangguan terhadap aspek finansial, reputasi, serta kepatuhan hukum[31]

Langkah awal dalam proses ini adalah melakukan *Business Impact Analysis (BIA)* untuk mengidentifikasi proses-proses yang paling penting bagi kelangsungan bisnis. Setiap proses dievaluasi berdasarkan dampaknya terhadap operasional jika terjadi gangguan, termasuk penetapan *Recovery Time Objective (RTO)* dan *Recovery Point Objective (RPO)*. Selain itu, dilakukan *Risk Assessment* untuk mengenali ancaman potensial yang dapat

memengaruhi keberlangsungan bisnis, seperti bencana alam, serangan siber, atau kegagalan sistem[31].

Setelah risiko dan kebutuhan bisnis kritis diidentifikasi, organisasi dapat menyusun strategi mitigasi dan pemulihan yang relevan, termasuk pengelolaan sumber daya alternatif, pencadangan data, dan pengembangan sistem *failover*. Identifikasi ini tidak hanya memastikan kesiapan organisasi dalam menghadapi gangguan, tetapi juga memberikan kerangka kerja yang kuat untuk meningkatkan ketahanan bisnis secara keseluruhan. Dengan memahami elemen-elemen yang mendukung keberlangsungan bisnis, organisasi dapat lebih tangguh dalam menghadapi tantangan dan melindungi kepentingan pemangku kepentingan.

b) Mekanisme Manajemen Bencana

Mekanisme manajemen bencana dalam *Business Continuity Plan (BCP)* adalah serangkaian langkah dan prosedur yang dirancang untuk membantu organisasi merespons, mengelola, dan memulihkan diri dari gangguan atau bencana yang dapat menghambat operasional bisnis. Proses ini dimulai dengan langkah mitigasi risiko, di mana organisasi mengidentifikasi potensi risiko dan mengimplementasikan langkah-langkah pencegahan untuk mengurangi kemungkinan terjadinya bencana atau dampaknya, seperti instalasi sistem keamanan, pelatihan karyawan, dan pencadangan data secara rutin. Selanjutnya, perencanaan dan kesiapsiagaan dilakukan dengan menyusun rencana tanggap darurat yang mencakup prosedur evakuasi, lokasi cadangan operasional, dan sumber daya penting berdasarkan hasil *Risk Assessment* dan *Business Impact Analysis (BIA)*, untuk memastikan fokus pada proses bisnis kritis. Ketika bencana terjadi, mekanisme respons darurat diaktifkan, mencakup pelaksanaan prosedur tanggap darurat, komunikasi dengan pemangku kepentingan, dan perlindungan terhadap aset penting. Setelah situasi terkendali, tahap pemulihan dilakukan dengan memulihkan fungsi bisnis

sesuai dengan *Recovery Time Objective (RTO)* dan *Recovery Point Objective (RPO)* yang telah ditetapkan, serta mengevaluasi respons untuk perbaikan di masa depan. Mekanisme ini dirancang untuk memastikan bahwa organisasi mampu bertahan dan pulih secara efektif dari dampak bencana sambil melindungi karyawan, aset, dan reputasi bisnis[32].

c) Fase Tanggap Darurat

Fase tanggap darurat merupakan tahap penting dalam *Business Continuity Plan (BCP)* yang bertujuan untuk merespons bencana atau gangguan secara cepat dan Terstruktur guna melindungi karyawan, aset organisasi, dan keberlanjutan operasional. Pada fase ini, tindakan langsung diambil untuk meminimalkan dampak bencana dan memastikan keselamatan semua pihak yang terlibat[33].

d) Pemulihan Dan Restorasi

Pemulihan dan restorasi dalam *Business Continuity Plan (BCP)* adalah tahap akhir yang bertujuan untuk mengembalikan operasional bisnis ke kondisi normal setelah terjadinya gangguan atau bencana. Tahap ini dimulai dengan pemulihan sementara, di mana fungsi bisnis kritis segera dipulihkan untuk memastikan operasional minimal berjalan sesuai dengan *Recovery Time Objective (RTO)*[34].

2.2.4.4 OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) adalah kerangka kerja yang dirancang untuk membantu organisasi mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi secara strategis. OCTAVE berfokus pada pengelolaan ancaman, aset bisnis, dan kerentanan dengan tujuan melindungi informasi kritis yang mendukung keberlangsungan operasional[35].

Selain OCTAVE, terdapat pula sejumlah metodologi lain yang sering dijadikan acuan dalam penyusunan rencana kesinambungan operasional dan

manajemen risiko. Beberapa di antaranya adalah NIST 800-34 (Contingency Planning Guide for Federal Information Systems), ISO 22301 (Business Continuity Management Systems – BCMS), serta COBIT (Control Objectives for Information and Related Technology). Masing-masing metodologi memiliki karakteristik, kelebihan, serta keterbatasan yang berbeda sehingga perlu dianalisis kesesuaiannya dengan konteks organisasi. Berikut Tabel Perbandingan Analisis pada Tabel 2.2

Tabel 2. 2 Tabel Perbandingan Octave

Metodologi	NIST 800-34 (Contingency Planning Guide for Federal Information Systems)	ISO 22301 (Business Continuity Management Systems – BCMS)	COBIT (Control Objectives for Information and Related Technology)
Kelebihan	Memberikan panduan teknis sangat detail untuk membuat rencana kontinjensi. Fokus pada sistem informasi sehingga cocok untuk risiko TI. Banyak digunakan di sektor publik/teknologi tinggi.	Terlalu teknis, kurang menekankan aspek strategis bisnis. Lebih sesuai untuk instansi pemerintah AS, sehingga adaptasi ke sektor swasta butuh penyesuaian.	Cukup relevan untuk MDI Ventures dalam konteks perlindungan sistem informasi, namun tidak sepenuhnya mencakup aspek strategis dan kepercayaan investor.
Kekurangan	Standar internasional yang diakui global. - Fokus pada manajemen keberlangsungan bisnis secara menyeluruh, bukan hanya TI. Memberikan kredibilitas eksternal (penting untuk investor).	Implementasi kompleks dan membutuhkan biaya besar. Cenderung lebih administratif dan dokumentatif.	Sangat relevan untuk MDI Ventures karena dapat meningkatkan kepercayaan investor dan mendukung tata kelola operasional yang berstandar global.
Relevansi Pada Perusahaan	Framework tata kelola TI yang kuat. Menyelaraskan strategi TI dengan tujuan bisnis. Fokus pada kontrol, audit, dan kepatuhan.	Tidak secara khusus dirancang untuk BCP. Lebih menekankan governance TI daripada manajemen krisis atau pemulihan.	Relevan secara parsial, terutama untuk governance TI di MDI Ventures, namun perlu dikombinasikan dengan metodologi BCP lain agar menyentuh aspek keberlangsungan bisnis.

2.2.3.5 IT Disaster Recovery Plan

IT Disaster Recovery Plan (IT DRP) adalah dokumen strategis yang bertujuan untuk memandu organisasi dalam memulihkan sistem teknologi informasi (TI) yang terpengaruh akibat gangguan, bencana, atau insiden tak terduga. IT DRP berfokus pada meminimalkan *downtime*, memastikan kelangsungan operasional, dan melindungi data kritis. Sebagai bagian dari *Business Continuity Plan (BCP)*, IT DRP dimulai dengan identifikasi sistem, aplikasi, dan infrastruktur TI yang paling penting bagi operasional bisnis, seperti *server*, *database*, jaringan, dan perangkat lunak utama. Proses ini juga melibatkan analisis *Recovery Time Objective (RTO)* dan *Recovery Point Objective (RPO)* untuk menentukan prioritas pemulihan. Strategi pencadangan dan pemulihan data menjadi elemen penting, dengan mencakup pencadangan rutin melalui metode lokal maupun berbasis *cloud*, serta replikasi data *real-time* untuk menjaga ketersediaan informasi terkini selama gangguan. Selain itu, rencana ini mencakup langkah-langkah pemulihan infrastruktur TI, seperti pemulihan perangkat keras, perangkat lunak, dan jaringan melalui solusi *failover server*, virtualisasi, atau pemindahan beban kerja ke lokasi cadangan. Dengan penerapan IT DRP yang memadai, organisasi dapat memastikan bahwa sistem TI dapat pulih dengan cepat, mendukung kelangsungan bisnis, dan mengurangi dampak negatif dari gangguan yang tidak terduga[36].

2.2.3.6 Crisis Communication Plan

Crisis Communication Plan (CCP) adalah strategi yang dirancang untuk mengelola komunikasi organisasi secara Terstruktur selama dan setelah krisis atau gangguan besar. CCP bertujuan memastikan bahwa informasi yang akurat, konsisten, dan tepat waktu disampaikan kepada pemangku kepentingan, seperti karyawan, pelanggan, mitra bisnis, media, dan masyarakat umum. Dalam implementasinya, CCP melibatkan pembentukan tim komunikasi krisis yang

bertanggung jawab atas pengelolaan semua aspek komunikasi selama insiden berlangsung[37].

