Rancangan Business Continuity Planning (BCP) Perlindungan Data untuk Bank

Nurani Buaty[1], Rama Dutasmara[2], Mardiana Purwaningsih[3]

[123] Program Studi Sistem Informasi, Perbanas Institute, Jakarta, Indonesia 12940

** E-mail korespondensi: mardiana@perbanas.id*

Kata kunci:
Bussines Countinuity Planning
BCP
Keamanan Data
Risiko Bank

Diterima: 11 Agustus 2024
Disetujui: 20 Oktober 2024
Diterbitkan: 30 Desember 2024

Penerbit:
Perbanas Institute

ABSTRAK

Kegiatan operasional bank sangat bergantung pada sistem teknologi informasi dan pengelolaan data yang aman. BCP adalah pendekatan yang dapat diterapkan oleh bank dalam memastikan kelangsungan operasional bisnisnya dalam menghadapi gangguan yang tidak terduga pada data termasuk melindungi data pelanggan. Salah satu hal yang penting dalam BCP adalah perlindungan data. Setiap bank harus mengamankan data pelanggan yang sensitif dan menghindari kerugian finansial serta reputasi yang dapat terjadi akibat kebocoran atau penyalahgunaan data. Penelitian ini menganalisis tantangan yang dihadapi oleh bank dalam melindungi data, mengidentifikasi kelemahan yang ada dalam sistem keamanan yang ada saat ini, dan merancang strategi BCP yang komprehensif untuk mengatasi risiko yang mungkin terjadi. Metode penelitian yang digunakan dalam penelitian ini melibatkan studi literatur, analisis kebutuhan, serta pengumpulan dan analisis data. Metode wawancara sebagai data primer dengan unit terkait untuk mendapatkan informasi mendalam mengenai permasalahan yang ada.

I. PENDAHULUAN

Dalam era digital, teknologi informasi telah memberikan dampak positif di berbagai bidang (Hermawan et al., 2022). Perlindungan data menjadi aspek penting bagi organisasi, terutama dalam sektor perbankan tiga dimensi yang mempengaruhi keamanan sistem informasi yaitu *confidentiality, integrity dan availability* merupakan faktor yang berpengaruh positif dan dominan pada keamanan sistem informasi (Dianta & Zusrony, 2019) (Hermawan et al., 2022) (Dianta & Zusrony, 2019). Semua bank wajib menyadari betapa pentingnya rancangan *Business Continuity Planning (BCP)* untuk melindungi data pelanggan dan menjaga kelangsungan bisnisnya. Rancangan BCP yang efektif dan komprehensif menjadi tantangan yang kompleks bagi setiap bank. Ancaman keamanan data seperti serangan siber, bencana alam, dan kegagalan sistem dapat mengganggu operasional dan mempengaruhi reputasi serta kepercayaan nasabah (Tutuhatunewa & Purwaningsih, 2013). Perusahaan harus memahami setiap ancaman dan proaktif dalam menanggapinya (Chandra, 2017) Oleh

karena itu, penting untuk merancang rencana yang terstruktur dan terencana guna mengatasi potensi risiko dan mengurangi dampak negatif yang mungkin terjadi. Penelitian ini bertujuan untuk mengusulkan rancangan BCP yang efektif untuk perlindungan data pada bank. Dalam penelitian ini, penulis juga menganalisis tantangan yang dihadapi oleh bank dalam melindungi data, mengidentifikasi kelemahan yang ada dalam sistem keamanan yang ada saat ini, dan merancang strategi BCP yang komprehensif untuk mengatasi risiko yang mungkin terjadi.

Metode penelitian yang akan digunakan dalam penelitian ini melibatkan studi literatur, analisis kebutuhan, serta pengumpulan dan analisis data dari sebuah bank. Penulis juga melakukan wawancara dengan unit terkait untuk memperoleh informasi mendalam mengenai permasalahan yang ada.

Hasil dari penelitian ini diharapkan dapat memberikan masukan bagi bank dalam merancang dan mengimplementasikan BCP yang efektif. Dengan adanya rencana yang terstruktur dan terencana, maka setiap bank dapat memitigasi risiko yang terkait dengan perlindungan data, menjaga kelangsungan bisnis, serta meningkatkan kepercayaan nasabah.

Penelitian ini memiliki signifikansi praktis yang besar, tidak hanya bagi bank saja tetapi juga bagi institusi keuangan lainnya yang ingin meningkatkan keamanan dan keandalan sistem mereka. Selain itu, penelitian ini juga dapat memberikan kontribusi terhadap peningkatan kesadaran tentang pentingnya BCP dalam melindungi data dan menjaga kelangsungan bisnis di era digital ini. Dalam penelitian ini, penulis membahas secara rinci langkah-langkah yang diambil dalam merancang BCP, termasuk identifikasi risiko, analisis dampak bisnis, perencanaan pemulihan, serta pengujian dan evaluasi BCP yang telah diimplementasikan (Abrams, 2021) (Muparadzi & Rodze, 2021). Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang berarti bagi perkembangan dan peningkatan keamanan data di sektor perbankan serta mendorong kesadaran akan pentingnya BCP dalam melindungi data dan menjaga kelangsungan bisnis.

II. KAJIAN TEORI

Pada bagian ini dibahas mengenai beberapa rujukan yang menjadi dasar penyusunan rancangan BCP pada bank.

2.1. ISO 22301:2012

ISO 22301:2012 adalah salah satu standar internasional berisi aturan dan pengelolaan rancangan keberlanjutan bisnis, *Business Continuity Management Systems (BCMS)* yang efektif (Steen et al., 2023) (Amanda & Subriadi, 2014). *Plan-Do-Check-Act* merupakan salah satu standar model penerapan yaitu, perencanaan (*plan*), pengerjaan (*do*), pemeriksaan (*check*) dan tindakan (*act*).

2.2. PERATURAN BANK INDONESIA

BI sendiri membuat ketentuan-ketentuan tentang Penerapan Manajemen Risiko Bagi Bank Umum yang mengatur tuntutan dan persyaratan manajemen risiko operasional termasuk *Business Continuity*. BI mampu menjadi salah satu tolak ukur dalam penyusunan pedoman BCP selain itu BI melakukan pengawasan terhadap bank-bank di Indonesia untuk memastikan kepatuhan terhadap persyaratan BCP BI mengharuskan bank-bank untuk

menyampaikan informasi terkait BCP secara teratur. Bank diwajibkan melaporkan rencana BCP mereka, hasil uji coba, dan tindakan pemulihan yang dilakukan dalam situasi darurat kepada BI. Hal ini memungkinkan BI untuk memantau dan mengevaluasi tingkat kesiapan bank dalam menghadapi risiko dan kejadian darurat.

2.3. Peraturan Otoritas Jasa Keuangan Nomor 46/POJK.03/2013

Peraturan Nomor 46/POJK.03/2013 tentang Manajemen Risiko Operasional Bank Umum mengatur tentang Manajemen Risiko Operasional bagi bank umum di Indonesia. Peraturan ini mewajibkan bank umum untuk membentuk Komite Manajemen Risiko, melakukan penilaian risiko operasional secara berkala, mengelola risiko melalui kebijakan dan prosedur yang memadai, serta memiliki rencana kontinuitas bisnis guna menjaga kelangsungan operasional dan mengurangi potensi kerugian. Tujuannya adalah memastikan bank umum memiliki sistem manajemen risiko yang efektif dalam menghadapi risiko operasional dan menjaga stabilitas dalam kegiatan operasional mereka. Manajemen risiko merupakan suatu upaya untuk mengetahui, menganalisis, dan mengendalikan risiko pada seluruh kegiatan perusahaan atau entitas yang bertujuan untuk mendapatkan tingkat efektivitas dan efisiensi yang lebih baik (Muslih & Marbun, 2020).

III. METODE

Penelitian ini menganalisis tantangan yang dihadapi oleh bank dalam melindungi data, mengidentifikasi kelemahan sistem keamanan saat ini, serta merancang strategi BCP yang komprehensif untuk mengatasi risiko. Metode yang digunakan mencakup studi literatur, analisis kebutuhan, serta pengumpulan dan analisis data dari sebuah bank BUMN. Wawancara dengan unit terkait juga dilakukan untuk memperoleh informasi mendalam mengenai permasalahan yang ada. Usulan rancangan BCP untuk bank disusun selain dari hasil wawancara juga diadopsi dari beberapa model BCP pada penelitian pendahulu.

IV. HASIL DAN DIKUSI

4.1. SEKILAS TENTANG OBYEK PENELITIAN

Bank yang digunakan sebagai tempat untuk pengambilan data dan melakukan rancangan dari hasil tersebut merupakan salah satu bank BUMN terbesar di Indonesia yang didirikan pada tahun 1998. Bank ini merupakan hasil merger dari empat bank milik pemerintah Indonesia. Bank ini didirikan dengan tujuan untuk memperkuat sistem perbankan nasional dan mendukung pertumbuhan ekonomi Indonesia.

Seperti halnya dengan bank lainnya, maka bank menyediakan berbagai produk dan layanan perbankan kepada nasabahnya, termasuk layanan perbankan konvensional dan syariah. Produk dan layanan yang ditawarkan mencakup tabungan, deposito, kredit, kartu kredit, investasi, treasury, dan layanan perbankan korporasi. Selain itu, juga menawarkan layanan perbankan elektronik, seperti internet banking, mobile banking, dan ATM, untuk memberikan kemudahan akses perbankan kepada nasabahnya.

Sebagai bank terbesar di Indonesia, bank tersebut memiliki jaringan yang luas, baik melalui kantor cabang maupun jaringan ATM yang tersebar di seluruh Indonesia. Bank tersebut juga memiliki kehadiran global melalui kantor perwakilan dan anak perusahaan di beberapa

negara. Selain itu juga pernah memperoleh berbagai penghargaan dan sertifikasi atas kualitas layanannya.

4.2 PEMETAAN PROSES BISNIS DAN KAITANNYA DENGAN *BUSINESS CONTINUITY*

Bank merupakan lembaga keuangan yang besar dan kompleks, sangat bergantung pada sistem teknologi informasi dan pengelolaan data yang aman. BCP adalah pendekatan yang diterapkan oleh bank untuk memastikan kelangsungan operasional bisnisnya dalam menghadapi situasi darurat atau gangguan tidak terduga pada data, termasuk melindungi data pelanggan.

Salah satu hal yang penting dalam BCP adalah perlindungan data. Sehingga dari pengumpulan data, maka semua bank harus mengamankan data pelanggan yang sensitif dan menghindari kerugian finansial serta reputasi yang dapat terjadi akibat kebocoran atau penyalahgunaan data. Oleh karena itu, perencanaan dan implementasi langkah-langkah perlindungan data yang efektif menjadi bagian penting dari rancangan BCP pada bank. Untuk mendukung perlindungan data, bank dapat mengadopsi kebijakan keamanan data yang ketat, termasuk enkripsi data, akses terbatas, dan pemantauan keamanan secara terus-menerus. Selain itu, bank juga perlu memiliki infrastruktur teknologi yang andal dan backup data yang berkualitas untuk memastikan ketersediaan dan integritas data yang penting (Dianta & Zusrony, 2019) (Hermawan et al., 2022).

4.3. PENGENALAN *BUSINESS CONTINUITY* DI BANK

Kegiatan operational pada bank selalu bergantung pada teknologi, hal ini merupakan hal yang harus diperhatikan karena semua kegiatan operational pada bank selalu melibatkan data. Saat ini, semua teknologi bank menggunakan akses internet dalam kegiatan operationalnya, sehingga aktivitas tersebut menjadi rentan terkena gangguan yang disebabkan oleh alam maupun manusia. Rancangan BCP merupakan rencana untuk memastikan kelangsungan operasional bisnis tetap berjalan pada kondisi darurat atau bencana. BCP ini dibuat untuk meminimalkan dampak yang mungkin terjadi pada bisnis dan pelanggan.

Secara umum penyusunan rancangan BCP pada bank mencakup beberapa aspek, sebagai berikut.

1. Identifikasi risiko
2. Pemetaan proses bisnis kritis
3. Pengembangan rencana pemulihan
4. Pengujian secara berkala.

Dalam rancangan BCP juga terdapat tiga tingkatan kesiapan, yaitu: Tingkat siaga 1 yaitu kondisi normal, sedangkan tingkat siaga 2 dan 3 adalah kondisi darurat.

Keberadaan rancangan BCP ini, diharapkan dapat membantu setiap bank dapat tetap menjalankan bisnisnya dengan lancar dan memberikan pelayanan yang optimal kepada pelanggan, meskipun dalam kondisi darurat atau bencana. Jika penyusunan BCP ini tidak tepat, maka dapat berdampak pada kelangsungan operasional bisnis dan layanan kepada pelanggan. Hal ini dapat terjadi karena BCP yang tidak tepat dapat mengakibatkan kesalahan dalam identifikasi risiko dan pemetaan proses bisnis kritis, sehingga rencana

pemulihan yang dikembangkan tidak efektif dan tidak dapat meminimalkan dampak yang mungkin terjadi pada bisnis dan pelanggan. Selain itu, BCP yang tidak tepat juga dapat mengakibatkan bank tidak siap menghadapi situasi darurat atau bencana dengan baik, sehingga dapat mengganggu kelangsungan operasional dan layanan kepada pelanggan.
Manajemen risiko bencana menjadi tanggung jawab berbagai unit dan fungsi yang bekerja sama untuk mengidentifikasi, mengelola, dan memitigasi risiko terkait bencana. Secara umum, beberapa manajemen pada bank yang terlibat dalam penanganan risiko bencana, adalah sebagai berikut.

1. Divisi Manajemen Risiko, Divisi Manajemen Risiko bertanggung jawab dalam pengelolaan risiko secara keseluruhan yang ada di bank.
2. Divisi Keamanan, Divisi Keamanan bertanggung jawab untuk menjaga keamanan fisik dan operasional bank.
3. Divisi Teknologi Informasi (TI), Divisi TI memiliki peran penting dalam manajemen risiko bencana terkait dengan sistem teknologi informasi.
4. Divisi Operasional, Divisi Operasional bertanggung jawab untuk mengidentifikasi risiko operasional terkait bencana, merencanakan langkah-langkah pemulihan operasional, dan melibatkan staf dalam pelatihan dan pengujian BCP secara berkala.
5. Tim Krisis dan Pemulihan, setiap bank memiliki tim khusus yang bertugas merespons keadaan darurat dan mengkoordinasikan pemulihan operasional setelah terjadinya bencana.

Manajemen risiko bencana pada bank melibatkan kolaborasi antar unit dan fungsi yang berbeda untuk memastikan bahwa risiko bencana diidentifikasi dengan baik, mitigasi yang tepat diimplementasikan, dan pemulihan operasional yang efisien dilakukan dalam situasi darurat. Strategi mitigasi risiko untuk memastikan keamanan dan stabilitas bisnis mereka. Salah satu strategi yang dapat diterapkan pada bank adalah penggunaan teknologi informasi dan sistem manajemen risiko yang canggih untuk memantau dan mengelola risiko pencurian data secara efektif. Setiap bank biasanya juga memiliki kebijakan manajemen risiko yang ketat dan prosedur pengawasan yang ketat untuk memastikan kepatuhan terhadap peraturan dan standar keamanan yang berlaku. Selain itu, setiap bank juga harus memiliki program pelatihan dan pengembangan untuk meningkatkan kesadaran dan pemahaman karyawan tentang risiko dan tindakan yang harus diambil untuk mengurangi risiko bencana yang dapat terjadi kapan saja. Untuk memitigasi seluruh risiko yang dihadapi bank, khususnya risiko operasional, bank sangat penting untuk memiliki mitigasi operasional bank.

BCP salah satu bentuk pencegahan dari risiko operasional bank, yang bersifat terpadu dan menyeluruh ditunjukkan untuk memastikan kelangsungan operasional pada bank dalam menjalankan bisnis dan melayani nasabah.

4.4. GARIS BESAR PROSES *BUSINESS CONTINUITY* PADA BANK

Berdasarkan insiden-insiden yang menimpa bank, maka penyusunan BCP difokuskan untuk keamanan data karena data sangat rentan mengalami kebocoran. Menggunakan perangkat lunak keamanan seperti antivirus dan *firewall* pada komputer dan perangkat *mobile*. Perangkat lunak keamanan akan membantu mencegah serangan malware dan virus yang dapat merusak atau mencuri data. Memperbarui perangkat lunak dan sistem operasi secara

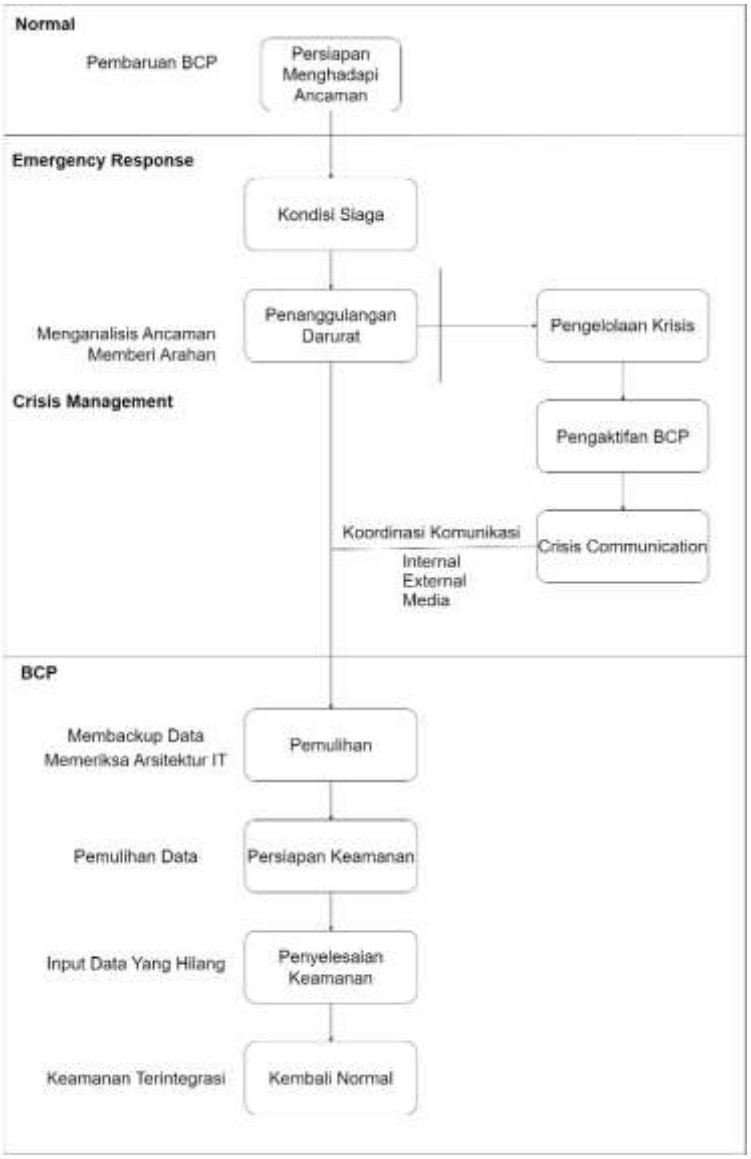
teratur, memperbarui perangkat lunak dan sistem operasi akan membantu memperbaiki kerentanan keamanan yang ditemukan pada perangkat tersebut. Membuat salinan cadangan data secara teratur dan menyimpannya di tempat yang aman, salinan cadangan data akan membantu mengembalikan data yang hilang atau rusak akibat serangan atau kesalahan. Melakukan evaluasi risiko secara berkala dan menyusun strategi keamanan data yang tepat. Menggunakan teknologi keamanan seperti enkripsi data dan pemantauan aktivitas pengguna. Enkripsi data akan membantu melindungi data dari akses yang tidak sah, sedangkan pemantauan aktivitas pengguna akan membantu mendeteksi aktivitas yang mencurigakan atau tidak wajar. Mengedukasi karyawan dan pelanggan tentang praktik keamanan data yang baik. Edukasi akan membantu meningkatkan kesadaran tentang pentingnya keamanan data dan mengurangi risiko kebocoran data akibat kesalahan manusia. Melakukan tes penetrasi secara berkala untuk menguji keamanan sistem dan jaringan. Tes penetrasi akan membantu mengidentifikasi kerentanan keamanan yang mungkin dapat dimanfaatkan oleh penyerang untuk melakukan kebocoran data. Menjalin kemitraan dengan penyedia layanan keamanan data yang terpercaya. Kemitraan dengan penyedia layanan keamanan data yang terpercaya akan membantu bank memperoleh akses ke teknologi dan keahlian keamanan terbaru. Selain ini perlu juga untuk dilakukan audit atau evaluasi secara berkala untuk memastikan penanganan risiko (Dewi et al., 2023).

Secara umum Prosedur *Business Continuity Plan* dibagi menjadi 4 tahap seperti yang ditunjukkan oleh Tabel 1.

Tabel 1. Tahapan BCP

Kondisi	Tahapan	Pengertian
Sebelum	Normal	Kondisi operasional normal.
Sesudah	Presedur *Recovery*	Tahapan di mana unit kerja melakukan evakuasi data.
	Prosedur *Resume*	Tahapan aktivitas operational dilakukan menggunakan back-up prosedur secara manual.
	Prosedur Restorasi	Tahapan transaksi dilakukan menggunakan komputer (Data Center sudah on-line).

Berikut gambaran Proses *Emergency Response* dalam kaitannya dengan *Business Continuity Plan* yang diusulkan untuk bank, yang ditunjukkan pada Gambar 1. Model ini disusun daro penelitan pendahulu yang dilakukan oleh (Chandra, 2017) dan hasil wawancara pada obyek penelitian.



Gambar 1. Proses *Emergency Response*

Setiap proses kerja akan mengalami perubahan sebagai bentuk penyesuaian perkembangan bisnis maka kebijakan dan strategi *Business Continuity Plan* selalu mengalami pembaharuan agar rancangan *Business Continuity Plan* tetap relevan(Mudholkar, 2013) (Steen et al., 2023). Perubahan-perubahan ini akan disampaikan oleh kantor pusat dalam bentuk Surat Keputusan (SK) kepada kantor cabang, sedangkan perubahan yang berhubungan dengan ketentuan dan prosedur pelaksanaan akan dikirimkan melalui Surat Edaran (SE). Namun selain pihak bank itu sendiri SK dan SE dapat bersumber dari pemerintah.

4.5. ROADMAP BC AWARENESS

Peran BCP pada bank juga menjadi pertimbangan masyarakat dalam memilih bank. Saat ini, setiap manajemen bank telah melakukan beberapa program yang bertujuan agar seluruh pemilik risiko sadar dan paham akan pentingnya BCP. Dengan demikian perlu untuk disusun

Roadmap kesadaran pentingnya BCP dan menjadi bagian dari budaya organisasi (Sawalha et al., 2012).

4.6. BUSINESS RESILIENCE METHODOLOGY

Metodologi ketahanan bisnis adalah pendekatan yang digunakan untuk membangun keuletan dan ketahanan sebuah organisasi dalam menghadapi ancaman dan gangguan yang dapat mempengaruhi operasionalnya.

Manajemen Risiko dikelola menjadi tiga bagian, yaitu *Low Risk*, *Medium Risk* dan *High Risk* (Pratama, 2018). Kerangka kerja dan tata kelola manajemen risiko pada bank biasanya terdiri dari Dewan Komisaris yang menjalankan fungsi pengawasan risiko (*risk oversight*) melalui Komite Audit, Komite Pemantau Risiko dan Komite Tata Kelola Terintegrasi, serta Dewan Direksi yang menjalankan fungsi kebijakan risiko (*risk policy*) melalui *Executive Committee* terkait manajemen risiko yaitu *Risk Management & Credit Policy Committee*, *Asset and Liabilities Committee*, *Capital and Subsidiaries Committee*, dan *Integrated Risk Committee*. Di tingkat operasional, Satuan Kerja Manajemen Risiko bersama Unit Bisnis dan Unit Kerja Kepatuhan melakukan fungsi identifikasi risiko, pengukuran risiko, mitigasi risiko serta pengendalian risiko.

Dengan adanya rancangan BCP ini, maka setiap bank harus menjalankan Proses Identifikasi, Pengukuran, Pemantauan, dan Pengendalian Risiko, serta Sistem Informasi Manajemen Risiko melalui kerangka kerja *Enterprise Risk Management (ERM). Enterprise Risk Management (ERM)* mampu meningkatkan berbagai peluang, mengidentifikasi dan mengelola risiko di seluruh entitas, meningkatkan hasil positif dan keuntungan sambil mengurangi kejutan negatif, mengurangi variabilitas kinerja, memperbaiki pemanfaatan sumber daya, dan meningkatkan ketahanan perusahaan (Otero González et al., 2020).

Implementasi ERM di bank menggunakan pendekatan *two-prong*, untuk memastikan bahwa risiko tidak hanya dimitigasi dengan baik melalui proses bisnis sehari-hari, namun juga pada kondisi yang tidak terduga (*downturn*) melalui pencadangan modal. Dengan menerapkan manajemen risiko, semua risiko yang dapat menghambat pencapaian tujuan perusahaan dapat diantisipasi sejak awal (Muslih & Marbun, 2020). Setiap bank secara berkesinambungan wajib mengelola semua risiko secara terukur dan komprehensif dengan mekanisme tertentu sehingga risiko-risiko tersebut bisa dihindari, atau meminimalkan dampak yang timbul apabila risiko tersebut terjadi. Selanjutnya, setiap bank juga harus melakukan asesmen atas pengelolaan risiko tersebut.

Setelah rancangan BCP selesai, maka setiap bank senantiasa melakukan evaluasi atas efektivitas sistem manajemen risiko. Evaluasi meliputi penyesuaian strategi dan kerangka risiko sebagai bagian dari kebijakan manajemen risiko, kecukupan sistem informasi manajemen risiko serta kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko. Salah satu bentuk evaluasi pada kebijakan manajemen risiko adalah evaluasi tahunan terhadap Kebijakan Manajemen Risiko dan Standar Prosedur. Dewan Komisaris berperan aktif dalam pelaksanaan evaluasi sistem manajemen risiko dengan me-*review* hasil evaluasi yang telah dilakukan oleh Direksi sebagai orang yang bertanggung jawab atas efektivitas penerapan sistem manajemen resiko.

V. KESIMPULAN DAN REKOMENDASI

BCP ini dibuat untuk meminimalkan dampak yang mungkin terjadi pada bisnis dan pelanggan. Dalam BCP pada perbankan, terdapat tiga tingkatan kesiapan, yaitu: Tingkat siaga 1 adalah kondisi normal, sedangkan tingkat siaga 2 dan 3 adalah kondisi darurat. Hal ini dapat terjadi karena BCP yang tidak tepat dapat mengakibatkan kesalahan dalam identifikasi risiko dan pemetaan proses bisnis kritis, sehingga rencana pemulihan yang dikembangkan tidak efektif dan tidak dapat meminimalkan dampak yang mungkin terjadi pada bisnis dan pelanggan. Bank sendiri telah memiliki pusat pemulihan bencana yang dilengkapi dengan fasilitas pendukung seperti generator listrik cadangan, sistem pendingin udara, dan sistem komunikasi yang memadai. Manajemen Risiko bencana menjadi tanggung jawab berbagai unit dan fungsi yang bekerja sama untuk mengidentifikasi, mengelola, dan memitigasi risiko terkait bencana.

DAFTAR REFERENSI

Abrams, J. (Consultive G. to A. the P. (2021). *Crisis Roadmap for Microfinance*. *February*.

Amanda, A. A., & Subriadi, A. P. (2014). Konsep Penyusunan Kerangka Kerja Business Continuity Plan Teknologi Dan Sistem Informasi. *Seminar Nasional Sistem Informasi Indonesia*, *22*(September), 1–6.

Chandra, K. D. (2017). Penerapan Business Continuity pada Bank Central Asia. *Bina Ekonomi: Majalah Ilmiah Fakultas Ekonomi Universitas Katolik Parahyangan*, *21*(1), 13–24.

Dewi, Y. W. D. M. D., Mulyana, R., & Santoso, A. F. (2023). Penggunaan COBIT 2019 I&T Risk Management untuk Pengelolaan Risiko Transformasi Digital BankCo. *Jutisi : Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *12*(3), 1366–1380.

Dianta, I. A., & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan Pada Nasabah Pengguna Internet Banking. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *3*(1), 1. https://doi.org/10.29407/intensif.v3i1.12125

Hermawan, A., Hartati, T., & Wijaya, Y. A. (2022). Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad. *Jurnal Informatika: Jurnal Pengembangan IT*, *7*(3), 125–130. https://doi.org/10.30591/jpit.v7i3.3428

Mudholkar, P. K. (2013). Protecting E-Business by implementing Business Continuity and Disaster Recovery Planning in the Banking Industry. *International Journal of Innovations in Engineering and Technology*, *2*(1), 145–155.

Muparadzi, T., & Rodze, L. (2021). Business Continuity Management in a Time of Crisis: Emerging Trends for Commercial Banks in Zimbabwe during and Post the Covid-19 Global Crisis. *Open Journal of Business and Management*, *09*(03), 1169–1197. https://doi.org/10.4236/ojbm.2021.93063

Muslih, M., & Marbun, S. O. (2020). The Effect of Risk Management, Firm Age, and Firm Size on the Performance of Banking Companies Registered in Indonesia Stock Exchange Moderated By Corporate Governance and Budget as Control Variable. *International Journal of Science and Society*, *2*(4), 274–290. https://doi.org/10.54783/ijsoc.v2i4.211

Otero González, L., Durán Santomil, P., & Tamayo Herrera, A. (2020). The effect of Enterprise Risk Management on the risk and the performance of Spanish listed companies. *European Research on Management and Business Economics*, *26*(3), 111–120. https://doi.org/10.1016/j.iedeen.2020.08.002

Pratama, R. (2018). Penerapan Manajemen Risiko Pada Perbankan Syariah (Studi Kasus Pada Bank Muamalat & Bank Syariah Mandiri Cabang Kota Ternate). *Jurnal Mitra Manajemen*, *2*(6), 597–609. https://doi.org/10.52160/ejmm.v2i6.162

Sawalha, I. H. S., Anchor, J. R., & Meaton, J. (2012). Business continuity management in Jordanian banks: Some cultural considerations. *Risk Management*, *14*(4), 301–324. https://doi.org/10.1057/rm.2012.10

Steen, R., Haug, O. J., & Patriarca, R. (2023). Business continuity and resilience management: A conceptual framework. *Journal of Contingencies and Crisis Management*, *32*(1). https://doi.org/10.1111/1468-5973.12501

Tutuhatunewa, K. A., & Purwaningsih, M. (2013). *Disaster Recovery Planning Procedure for BPR Lokadana Disaster Recovery Planning Procedure for BPR Lokadana*. *May*.