EVALUASI EFEKTIVITAS DISASTER RECOVERY PLAN DALAM PEMULIHAN LAYANAN TEKNOLOGI INFORMASI PASCA BENCANA BERBASIS ISO 22301 (STUDI KASUS PT. JASA RAHARJA)

Setiawan, Abdul Azis dan Eko Wahyudi

Sekolah Tinggi Manajemen Informatika dan Komputer Jakarta STI&K
Jalan BRI No. 17, Radio Dalam, Kebayoran Baru, Jakarta Selatan 12140
setiawan.st@outlook.com, abdul5905@gmail.com, ekobkrt@gmail.com

ABSTRAK

Peraturan pemerintah semakin menekankan pentingnya memiliki rencana pemulihan bencana bagi organisasi, terutama BUMN. Penelitian ini dilakukan sebagai tindak lanjut dari regulasi tersebut, dengan mengevaluasi implementasi penggunaan layanan perusahaan mengenai keharusan memiliki Business Continuity Management Systems (BCMS) dalam penyediaan layanan maupun ketersediaan serta kesiapan Disaster Recovery Plan (DRP) pada PT. Jasa Raharja khususnya dalam bidang manajemen risiko dan teknologi informasi. Selain itu, hasil penelitian ini juga diharapkan dapat menjadi referensi bagi organisasi lain dalam menyusun dan mengimplementasikan DRP yang efektif. Pengujian Disaster Recovery Plan (DRP) yang dilakukan pada PT. Jasa Raharja bertujuan untuk memastikan kesiapan sistem dan prosedur dalam menghadapi bencana serta optimalisasi proses penanganan insiden. Implementasi DRP pada PT. Jasa Raharja telah memenuhi sebagian besar persyaratan regulasi, namun masih terdapat ruang untuk perbaikan guna meningkatkan ketahanan bisnis terhadap bencana serta mengidentifikasi area yang perlu perbaikan dan menunjukkan bahwa meskipun telah ada upaya untuk membangun kesiapan menghadapi bencana, masih terdapat beberapa area yang perlu ditingkatkan. Selain itu, identifikasi beberapa kelemahan dalam konfigurasi sistem juga menjadi temuan penting. Berdasarkan hasil pengujian, beberapa rekomendasi perbaikan diajukan, antara lain peningkatan efisiensi proses pemulihan, perluasan lingkup pengujian, waktu respons terhadap insiden dan kesiapan teknis tim dan pemeliharaan sistem secara berkala.

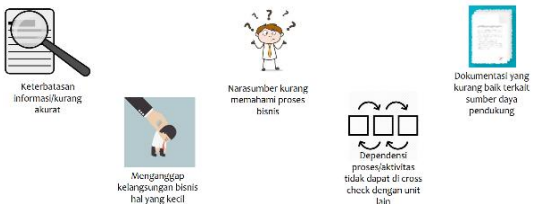
Kata Kunci: *Disaster Recovery Plan, PT. Jasa Raharja, Business Continuity Management Systems, BUMN, Infrastruktur Teknologi Informasi.*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mengubah cara organisasi menjalankan bisnis. Karena teknologi informasi dapat memperbaiki pelaksanaan proses bisnis suatu perusahaan dengan cara mengotomatisasi langkah-langkah yang tadinya dilakukan secara manual [1]. Ketergantungan yang tinggi terhadap teknologi informasi membuat organisasi rentan terhadap berbagai ancaman, termasuk bencana alam, serangan siber, dan kegagalan sistem. Bencana dapat menyebabkan gangguan yang signifikan terhadap operasional bisnis, hilangnya data penting, dan kerugian finansial yang besar.

Menurut standart internasional ISO 22301:2012 memiliki tujuan strategis organisasi, produk dan layanan, toleransi risiko, peraturan, kontrak dan mendukung keselarasan dengan para pihak pemangku kepentingan [2]. BCMS adalah proses manajemen secara menyeluruh yang mengidentifikasi potensi ancaman terhadap organisasi dan dampak pada operasi bisnis yang terancam. BCMS menyediakan kerangka kerja untuk membangun ketahanan organisasi dengan kemampuan untuk melakukan aksi tanggap yang efektif yang melindungi stakeholder, reputasi, merk, dan kegiatan penciptaan nilai [3]. Dalam perkembangannya untuk mempertahankan agar implementasinya selalu berjalan konsisten diperlukan reviu dan evaluasi terhadap dokumen – dokumen eksisting yang berhubungan dengan Business Continuity Management – Business Continuity Plan dan Disaster Recovery Plan. Strategi pemulihan bencana yang efektif akan membantu organisasi untuk

memulihkan kembali operasional bisnis dengan cepat dan efisien setelah terjadi bencana diperlukan juga Analisis Kebutuhan Kontinuitas (Continuity Requirement Analysis) yang merupakan langkah awal yang dalam merumuskan strategi Manajemen Kontinuitas Bisnis (BCM) dan Rencana Pemulihan Bencana (DRP) oleh karena itu organisasi perlu melakukan pendekatan proactive dilengkapi dengan kerangka pendukung keputusan untuk melindungi terhadap gangguan [4].



Gambar 1. *Kendala dalam Analisis Kebutuhan Kontinuitas*

Pengujian Disaster Recovery Plan diharapkan meningkatkan kesiapan (readiness) dari tim tanggap darurat dan pemulihan teknologi serta mengidentifikasi kesesuaian konfigurasi sistem/perangkat, perubahan dan penambahan perangkat, maupun potensi update patch sehingga proses penanganan dalam kondisi gangguan/bencana/darurat dapat dijalankan secara efektif. Penelitian pada Kajian Kesiapan Implementasi Bisnis Continuity Management System (BCMS) Berbasis ISO 22301 (Studi Kasus: PT. XYZ) oleh Whildan Zainudin dan Febriliyan Samopa [5]. dilakukan pada perusahaan yang menyediakan jasa IT, penelitian tersebut menggunakan metode Triangulasi untuk keabsahan data, melakukan wawancara dan ceklis berdasarkan kontrol dari ISO 22301:2012, menentukan gap antara kondisi sekarang terhadap ISO 22301:2012 dan menentukan solusi guna memenuhi syarat BCMS berdasarkan ISO 22301:2012 [6]. ISO 22301: 2012 (BCMS) Business Continuity Management System merupakan persyaratan dalam merencanakan, menetapkan, mengoperasikan, memantau, menerapkan, mereview, mempertahankan dan terus meningkatkan sistem manajemen yang terdokumentasi untuk mempersiapkan, menanggapi dan memulihkan diri dari kejadian yang mengganggu (disruptive) ketika gangguan itu terjadi [7]. Dengan demikian, organisasi dapat meminimalkan dampak negatif dari bencana dan menjaga kelangsungan bisnis.

Dengan memahami dan menerapkan siklus BCM sebagai proses berkelanjutan (continuous improvement), maka strategi dan rencana BCM akan terus menerus mengalami penyempurnaan sesuai dengan kebutuhan dan perubahan karakteristik organisasi dan layanan Perusahaan.

Gambar 2. *Siklus Business Continuity Management*

Pengembangan dan penyusunan dokumen DRP merupakan bagian yang tidak dapat terpisahkan dari strategi Business Continuity Management (BCM) Perusahaan dengan mempertimbangkan:

1. Kebutuhan tingkat ketersediaan informasi dan sistem informasi;
2. Toleransi downtime sistem informasi;
3. Hasil kajian Business Impact Analysis (BIA) dan IT risk assessment;
4. Persyaratan peraturan perundang-undangan yang berlaku

Dasar pelaksanaan implementasi berdasarkan:

1. Pertimbangan Kepatuhan Regulasi Eksternal sesuai dengan Ketentuan dalam Peraturan Menteri Badan Usaha Milik Negara No PER-2/MBU/03 Tahun 2023 – Tentang Pedoman Tata Kelola Dan Kegiatan Korporasi Signifikan – Bab VII Penyelenggaraan TI BUMN Bagian Keempat - Keberlangsungan Layanan Teknologi Informasi [8];

Pasal 207:

a. BUMN wajib memiliki rencana keberlangsungan layanan TI;
b. BUMN wajib memastikan rencana keberlangsungan layanan TI sebagaimana dimaksud pada ayat (1) dapat dilaksanakan, sehingga keberlangsungan operasional BUMN tetap berjalan saat terjadi bencana dan/atau gangguan pada sarana TI yang digunakan BUMN;
c. BUMN wajib melakukan uji coba dan evaluasi atas rencana keberlangsungan layanan TI terhadap sumber daya TI yang kritikal sesuai hasil analisis dampak bisnis dengan melibatkan pengguna TI paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

2. Pertimbangan Kepatuhan Regulasi Internal:
   Keputusan Direksi Nomor Kep/ 213 /2021 Tentang Pedoman Business Continuity Management sudah didefinisikan Uji Coba Business Continuity Management wajib dilakukan minimal 1 kali setiap tahunnya, dimana Divisi Manajemen Risiko bertanggung jawab untuk menetapkan jadwal pelaksanaan uji coba Business Continuity Management.
3. Pertimbangan Kesesuaian dengan ISO/IEC 27001:2022 [9] Annex A.5.30 ICT Readiness For Business Continuity Pernyataan Kontrol: Kesiapan TIK harus direncanakan, dilaksanakan, dipelihara dan diuji berdasarkan tujuan kelangsungan bisnis dan persyaratan kelangsungan TIK. ISO 22301 dapat dengan mudah dihubungkan dengan standar Business Continuity dan Keamanan Informasi yang lain (ISO 9001,ISO 27001) [10].

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kuantitatif. Peneliti dapat mengukur secara objektif efektivitas DRP, mengidentifikasi area yang perlu ditingkatkan, dan memberikan rekomendasi yang lebih terukur dan data yang dihasilkan dari pengujian DRP, seperti waktu pemulihan sistem, waktu penanganan insiden, dan persentase keberhasilan pengujian, bersifat numerik. Hasil penelitian kuantitatif dapat digunakan ke dalam populasi yang lebih luas, dalam hal ini dapat diimplementasikan ke BUMN lain atau perusahaan yang memiliki karakteristik serupa dengan PT. Jasa Raharja sehingga dapat menunjukkan bahwa DRP yang efektif sangat penting untuk memastikan kelangsungan operasional sistem informasi.

HASIL DAN PEMBAHASAN

Dalam pengujian ini melibatkan 2 (dua) kantor cabang yaitu: Kantor Cabang Maluku dan Kantor Cabang Sumatera Utara untuk uji fungsionalitas difokuskan pada layanan aplikasi kritikal yaitu Aplikasi DASI (DAta KoorperaSI) Pelayanan dan DASI Asuransi.

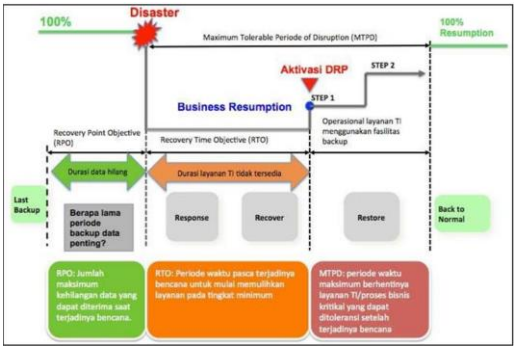
Keadaan darurat bagi Layanan TI meliputi skenario sebagai berikut:

1. Skenario 1 - Kebakaran Data Center Perusahaan dengan tingkat kerusakan > 50% ruang atau perangkat;
2. Skenario 2 - Kerusakan struktur bangunan/ruang Data Center dengan tingkat kerusakan > 50% (misalnya disebabkan oleh usia bangunan, gempa bumi, bencana alam lainnya dan sebagainya);
3. Skenario 3 - Gangguan teknis > 50% perangkat pendukung Layanan TIK utama (misal: server, core switch, perangkat jaringan komunikasi, A/C dan sebagainya) selama lebih dari 2 jam.

Tahapan kegiatan pengujian menggunakan skenario 2, yang bersifat non teknis terpisah (tidak sekuensial) dengan kegiatan pengujian yang bersifat teknis (pengalihan DC – DRC). Target dalam pengujian adalah untuk mendapatkan estimasi waktu dalam menjalankan tahapan kegiatan non teknis dan teknis sebagai dasar penentuan Recovery Time Objective (RTO).

Tabel 1. *Tabel tugas dan tanggung jawab personil DRP PT Jasa Raharja*

BAGIAN	SUB BAGIAN	TANGGUNG JAWAB
Ketua Satuan Tugas Pemulihan Teknologi (Divisi TIK)	Kepala Divisi Teknologi Informasi	1. Mendeklarasikan kondisi darurat 2. Mendeklarasikan aktivasi DRC 3. Mendeklarasikan kembali ke DC
Tim Manajemen Krisis (Divisi Manajemen Risiko)	Tim Manajemen Risiko	Koordinasi internal dan pemantauan kegiatan pengujian
Tim Pemulihan Teknologi (Divisi TIK)	Tim Asesmen Bencana (Damage Assessment) / Tim Perbaikan Fasilitas	1. Melakukan penilaian tingkat kerusakan dan estimasi penanganannya 2. Eskalasi kondisi kerusakan kepada Koordinator Manajemen Krisis
	Tim Pendukung Aplikasi & Sistem	1. Melakukan konfigurasi terhadap aplikasi 2. Melakukan konfigurasi terhadap database (replikasi, status database, dll) 3. Melakukan uji umum fungsionalitas aplikasi
	Tim Pendukung Infrastruktur	Melakukan konfigurasi terhadap perangkat jaringan dan security
	Tim Koordinasi Internal	Melakukan komunikasi dan koordinasi internal
Pengguna Aplikasi Dasi Pelayanan dan Dasi Asuransi	Pengguna Kantor Cabang Sumut dan Cabang Maluku	1. Mengganti DNS pengguna dari DC Ke DRC. 2. Pengecekan kelengkapan fitur aplikasi 3. Pengecekan pembuatan Laporan oleh Pengguna



Gambar 3. *MTPD, RTO, RPO* [6]

Tabel 2. *Tabel pengukuran DRP PT Jasa Raharja*

Nama Layanan/Aplikasi Kritikal	PLANNED TIME		
	MTPD	RTO	RPO
Layanan Aplikasi DASI-JR Modul IW	6 Jam	4 Jam	Near Real Time
Layanan Aplikasi DASI-JR Modul Pelayanan	6 Jam	4 Jam	Near Real Time
Layanan Aplikasi DASI-JR Modul SW	6 Jam	4 Jam	Near Real Time

Hasil dari pengujian sistem DRP:

1. Estimasi waktu pengalihan operasional DASI Pelayanan dan Asuransi dari DC ke DRC adalah 2 jam 57 menit;
2. Estimasi waktu tiketing pelaporan dan penanganan insiden (pelaporan insiden, eskalasi insiden, penanganan insiden, ticketing problem, penilaian kerusakan dan problem root cause, rekomendasi deklarasi kondisi darurat & aktivasi DRC, dan deklarasi kondisi darurat & aktivasi DRC) dengan normal flow adalah sekitar 4 jam;
3. Total estimasi waktu pengujian adalah 6 jam 57 menit;
4. Tiketing pelaporan dan penanganan insiden dengan normal flow, respon dan resolution time membutuhkan waktu yang lama (sekitar 4 jam) sehingga menjadi catatan serius dalam menangani insiden maupun problem;
5. Fungsional testing dilakukan melalui pengecekan akses (login & password),
6. pengecekan fitur, dan pengecekan pelaporan dengan membandingkan antara data di DC dengan di DRC.

Tabel 3. *Tabel Hasil Pengujian DRP PT Jasa Raharja*

Nama Layanan/Aplikasi Kritikal	Hasil Pengujian		
	RTO	Pengujian	Keterangan
Layanan Aplikasi DASI-JR Modul IW	4 Jam	2 Jam 57 Menit	Tercapai
Layanan Aplikasi DASI-JR Modul Pelayanan	4 Jam	2 Jam 57 Menit	Tercapai
Layanan Aplikasi DASI-JR Modul SW	4 Jam	2 Jam 57 Menit	Tercapai

Rekomendasi berdasarkan pengujian DRP, diantaranya:

1. Pengujian terhadap tahapan aktivitas yang bersifat non teknis dan teknis dapat dilakukan secara sekuensial;
2. Pengujian dapat melibatkan lebih dari 2 (dua) kantor cabang, dan jika dimungkinkan melibatkan semua kantor cabang, dan secara fungsional dapat menambahkan pengujian yaitu pengecekan terhadap entry data;
3. Merencanakan update patch pada kondisi operasional terhadap software database yang sekarang digunakan untuk mengantisipasi terjadinya bug error dimasa mendatang.

PENUTUP

Implementasi DRP pada PT. Jasa Raharja merupakan langkah yang positif dalam meningkatkan ketahanan bisnis terhadap bencana dan PT. Jasa Raharja telah berhasil mengimplementasikan DRP dan melakukan pengujian secara berkala dan konsisten. Pentingnya kepatuhan regulasi dalam melaksanakan implementasi DRP pada PT. Jasa Raharja juga menunjukkan pentingnya kepatuhan terhadap regulasi yang berlaku, baik dari pemerintah maupun internal perusahaan. DRP berkontribusi pada keberlangsungan bisnis di perusahaan serta DRP telah memberikan kontribusi positif dalam menjaga keberlangsungan bisnis PT. Jasa Raharja, terutama dalam menghadapi gangguan atau bencana yang berpotensi mengganggu operasional. Terdapat area yang perlu ditingkatkan meskipun telah berjalan, masih terdapat beberapa area yang perlu ditingkatkan, seperti waktu respons terhadap insiden, kesiapan teknis tim, dan cakupan pengujian.

Pengembangan simulasi bencana yaitu dengan melakukan simulasi bencana secara berkala dapat membantu mengidentifikasi kelemahan dalam DRP dan meningkatkan kesiapan tim tanggap darurat. Peningkatan frekuensi pengujian dalam pengujian DRP sebaiknya dilakukan secara lebih sering, misalnya setiap enam bulan sekali, untuk memastikan kesiapan sistem selalu terjaga. Peningkatan pelatihan bagi tim IT dan tim bisnis perlu dilakukan secara rutin untuk meningkatkan pengetahuan dan keterampilan dalam menjalankan DRP serta Pertimbangan penggunaan teknologi baru: seperti cloud computing dan automation, dapat membantu meningkatkan fleksibilitas dan efisiensi DRP.

DAFTAR PUSTAKA

[1] Laudon, K. C., & Jane, P. L. (2012). Management System: Managing the Digital Firm Twelfth Edition. New Jersey: Prentice Hall

[2] Avaluation Consulting and BSI Management System America., 2010. How to Deploy BS 25999 2nd Edition.

[3] St-Germain, Aliu, R., Lachapelle, E., & Dewez, E. (2012). Whitepaper – ISO 22301 Societal Security Business Continuity Management Systems. Professional Evaluation and Certification Board (PECB).

[4] Boehmer, W., 2009. Survivability and Business Continuity Management System According BS 25999. IEEE. Hochschlulstr, Germany: IEEE.

[5] Zainuddin, W., & Samopa, F. (2017). Kajian Kesiapan Implementasi Bisnis Continuity Management System (BCMS) Berbasis ISO 22301 (Studi Kasus: PT. XYZ). Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer1, 12(2), 82–87.

[6] Standard, I. (2012). Organization for Standardization (ISO/FDIS) 22301:2012 Societal Security – Business Continuity Management Systems – Requirements. Geneva

[7] BSI, 2010. Bisnis Continuity Management System: Requirement

with Guidance For use, American Nasional Standart, ASIS International.

[8] Kementerian BUMN Republik Indonesia, "Peraturan Menteri BUMN Nomor PER-2/MBU/03/2023 Tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara," Jakarta, Pasal 207, Jakarta, Indonesia, 2023.

[9] International Organization for Standardization (ISO), "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," ISO/IEC 27001:2022, 2022.

[10] Andrew Hiles, 2007. The Definitive Handbook of Business Continuity Management Second Edition, England, Kingswell International Limited