

## IT DISASTER RECOVERY PLAN DALAM MENDUKUNG BUSINESS CONTINUITY PLAN SAAT TERJADI FORCE MAJEURE

Nora Fitriawati<sup>1</sup>, Arief Herdiansah<sup>2</sup>, Rohmat Taufiq<sup>3</sup>, Rachmat Destriana<sup>4</sup>

<sup>1</sup>Universitas Bina Nusantara / Fakultas Teknik, Teknik Informatika

Jl. Kyai H. Syahdan No.9, Kemanggisan, DKI Jakarta 11480, TLP 5345830

<sup>2,3,4</sup>Universitas Muhammadiyah Tangerang / Fakultas Teknik, Teknik Informatika

Jl. Perintis Kemerdekaan 1/33 Cikokol Kota Tangerang TLP. 55793251

Co Responden Email: arief\_herdiansah@umt.ac.id

### Abstract

#### Article history

Received 27 May 2022

Revised 20 Sep 2022

Accepted 3 Oct 2022

Available 27 Oct 2022

#### Keywords

DRP,

BCP,

IT,

Force Majeure,

Customer

*The geographical Republic of Indonesia which are on 3 large plates of the world: the Eurasian plate, the Indo-Australian plate and the Pacific plate, the location of offices, the high rate of labor errors in Indonesia makes a company needs to prepare a Disaster Recovery Plan (DRP) to support the implementation of a Business Continuity Plan (BCP) that is fast, accurate and efficient in the event of force majeure. The method of building a Disaster Recovery Plan (DRP) is carried out by making a risk assessment by making a list of causes of risk, what risks will arise, estimating the impact caused and making a Management Plan for the risks posed. By implementing a Disaster Recovery Plan (DRP), the Company will be able to have more competitiveness, because the company can also implement a Business Continue Plan (BCP) on all IT infrastructure and databases owned so that if Force Majeure occurs, the services provided by the company to customers can still be maintained properly.*

### Abstrak

#### Riwayat

Diterima 17 Mei 2022

Revisi 20 Sep 2022

Disetujui 3 Okt 2022

Terbit 27 Okt 2022

#### Kata Kunci

DRP,

BCP,

IT,

Force Majeure,

Pelanggan

Kondisi geografis negara Republik Indonesia yang berada pada 3 lempengan besar dunia yaitu: lempeng Eurasia, lempeng Indo-Australia dan lempeng Pasifik, lokasi kantor, tingginya tingkat kelalaian tenaga kerja di Indonesia membuat sebuah perusahaan perlu menyusun sebuah Disaster Recovery Plan (DRP) untuk mendukung terimplementasinya Business Continuity Plan (BCP) yang cepat, akurat dan efisien apabila terjadi force majeure. Metode membangun sebuah Disaster Recovery Plan (DRP) dilakukan dengan membuat sebuah asesmen risiko dengan membuat daftar penyebab risiko, risiko apa saja yang akan timbul, perkiraan dampak yang ditimbulkan serta membuat Management Planing terhadap risiko yang ditimbulkan. Dengan mengimplementasikan Disaster Recovery Plan (DRP), Perusahaan akan dapat lebih memiliki daya saing, karena perusahaan juga dapat mengimplementasikan sebuah Business Continue Plan (BCP) pada semua infrastruktur IT dan database yang dimiliki sehingga jika terjadi Force Majeure, pelayanan akan jasa yang diberikan perusahaan kepada pelanggan tetap dapat dijaga dengan baik.

## PENDAHULUAN

Sebagai negara yang berada di 3 lempengan besar dunia yaitu: lempeng Eurasia, lempeng Indo-Australia dan lempeng Pasifik, Indonesia merupakan negara yang subur tetapi rawan akan bencana alam (Syafitri et al., 2018).

Terjadinya bencana alam dapat dikategorikan sebagai sebuah *force majeure*, dan hal tersebut dapat mengakibatkan terjadinya kerusakan terhadap infrastruktur yang menunjang jalannya aktifitas bisnis sebuah perusahaan, terutama infrastruktur yang gterkait dengan perangkat komputer, sistem dan jaringan komputer pada sebuah

perusahaan. *Force majeure* adalah keadaan memaksa yang tidak terduga, tidak direncanakan yang dapat mempengaruhi situasi normal dan menimbulkan konsekuensi, dan hubungan para pihak ketika peristiwa tersebut terjadi (Erniwati, 2020; Hansen, 2020). *Force majeure* merupakan sebuah kondisi yang tidak terduga datangnya dan seringkali luput dalam pantauan ataupun perkiraan pihak-pihak yang bertanggung jawab pada sebuah perusahaan.

Dalam menjalankan bisnis, hampir semua Perusahaan menggunakan teknologi informasi berbasis komputer yang terintegrasi sebagai alat (*tools*) untuk efektifitas dan efisiensi jalannya proses bisnis perusahaan (McLeod & Schell, 2012; Nurofik et al., 2021). Perangkat teknologi informasi berbasis komputer yang digunakan perusahaan tersebut merupakan salah satu perangkat penting yang sangat rentan terhadap dampak yang terjadi akibat *force majeure*, beberapa contoh *force majeure* yang dapat merusak fisik dan fungsi kerja dari perangkat komputerisasi sebuah perusahaan antara lain: gempa bumi, gunung meletus dan banjir akibat meluapnya air sungai. *force majeure* tidak hanya berupa kejadian karena situasi alam, tetapi ada pula *force majeure* yang terjadi karena kelalaian manusia, antara lain kebakaran, konleting listrik yang menyebabkan kerusakan perangkat berbasis komputer, terserang virus komputer ataupun terjadinya kerusakan sistem informasi yang dimiliki perusahaan karena ada serangan dari pihak-pihak yang tidak bertanggung jawab yang ingin mengacaukan sistem komputerisasi sebuah perusahaan.

Berdasarkan penjelasan diatas diperlukan sebuah perencanaan untuk penanganan penanggulangan risiko terhadap terjadinya *force majeure* yang dapat mengakibatkan terjadinya kerusakan, kekacauan bahkan tidak berfungsinya perangkat teknologi informasi milik perusahaan. Persiapan yang dilakukan perusahaan dalam rangka mencegah terjadi hal yang tidak diinginkan karena adanya *force majeure* dilakukan demi menjaga keberlangsungan jalannya bisnis (*Business Continuity Plan*), segala perencanaan tersebut tertuang dalam sebuah aktifitas penanggulangan dan rencana perbaikan terhadap kerusakan (*Disaster Recovery Plan*) yang disusun perusahaan agar proses

perbaikan terhadap infrastruktur sistem informasi perusahaan yang mengalami kerusakan atau kendala dapat yang dilakukan yang cepat dan tepat sehingga operasional bisnis perusahaan dapat tetap dapat berjalan dengan baik disaat terjadi kendala atau *force majeure*.

DRP adalah sebuah dokumen formal rencana pemulihan bencana yang dibuat organisasi berisi instruksi terperinci tentang cara menanggapi insiden yang tidak direncanakan seperti bencana alam, pemadaman listrik, serangan dunia maya, dan peristiwa mengganggu lainnya (IBM, 2022; Prasetyo et al., 2019). Dokumen *IT Disaster Recovery* berisi strategi yang akan dilakukan perusahaan dalam rangka meminimalisir dampak bencana pada perangkat dan infrastruktur IT milik perusahaan (Meilani et al., 2019; Shopshire, 2009). Dokumen *IT Disaster Recovery* dibuat agar perusahaan dapat tetap beroperasi dan cepat dapat dengan cepat beroperasi sebagaimana kondisi sebelum terjadinya *force majeure*.

BCP adalah metodologi yang digunakan untuk membuat dan memvalidasi rencana untuk mempertahankan operasi bisnis yang berkelanjutan sebelum, selama, dan setelah bencana atau peristiwa yang mengganggu (Fikri et al., 2021; Muflihah & Subriadi, 2021).

Penerapan sebuah *Disaster Recovery Plan* (DRP) juga dapat meningkatkan *brand-image* perusahaan, karena pelanggan ataupun rekan bisnis perusahaan akan merasa memperoleh jaminan keamanan layanan barang dan jasa serta keberlanjutan kerjasama dengan perusahaan tersebut. Dengan meningkatkan kepercayaan pelanggan dan rekan bisnis perusahaan maka secara langsung dapat meningkatkan nilai jual Perusahaan, sehingga dapat menambah jumlah pelanggan dari produk barang dan jasa yang dipasarkan perusahaan tersebut, karena calon pelanggan akan merasa dapat tetap terlayani dengan baik pada saat terjadi sebuah kendala atau *force majeure*.

Persaingan antar perusahaan terutama dibidang jasa saat ini semakin ketat, bisa dikatakan istilah pelanggan adalah raja memang benar adanya, karena saat ini pelanggan bukan hanya mencari barang yang berkualitas tetapi saat ini pelanggan juga mencari perusahaan yang dapat memberikan

pelayanan terbaik dalam kondisi apapun, termasuk jika pelanggan atau Perusahaan tersebut sedang mendapat hambatan, kendala dan musibah dari sebuah *force majeure*.

Teknologi informasi memainkan peran utama dalam proses rekayasa ulang proses bisnis. Kecepatan, kemampuan pengolahan informasi, konektivitas komputer dan teknologi internet secara substansial dapat meningkatkan efisiensi proses bisnis, serta komunikasi dan kolaborasi di antara orang-orang yang memiliki tanggung jawab untuk operasi dan manajemen<sup>[4]</sup>. Melihat dari perannya yang sangat penting, keberadaan dan kesiapan peralatan yang mendukung teknologi informasi harus kita jaga, baik dalam kondisi normal maupun jika terjadi hambatan, bencana atau *force majeure*, agar aktifitas/kinerja bisnis tidak terganggu.

Ancaman keamanan informasi adalah orang, organisasi, mekanisme atau peristiwa yang memiliki potensi membahayakan sumber daya informasi Perusahaan (McLeod & Schell, 2012). Ancaman keamanan informasi perlu diwaspadai, dan perusahaan perlu mengambil langkah-langkah pencegahan agar keamanan informasi yang dimiliki perusahaan dapat terjaga dengan sebaik-baiknya.

Untuk melindungi semua peralatan IT yang mendukung teknologi informasi dari ancaman keamanan informasi termasuk risiko dari dampak terjadinya sebuah hambatan, bencana atau *force majeure*, Perusahaan perlu menyiapkan DRC yang dapat mendukung BCP.

Rencana Pemulihan dari Bencana / DRP adalah metode perbaikan operasi pemrosesan informasi yang terhambat karena kerusakan atau kecelakaan. Penyusunan sebuah DRP adalah untuk menyediakan kemampuan atau sumber daya dalam menjalankan sebuah proses yang sangat penting di sebuah tempat tertentu untuk sementara waktu dan memperbaiki, mengembalikan fungsi tempat utama menjadi berfungsi normal kembali dalam suatu batasan waktu tertentu, dengan menjalankan prosedur pemulihan kerusakan yang cepat, untuk meminimalisir kerugian organisasi yang timbul akibat bencana/*force majeure*.

Beberapa penelitian sebelumnya berkaitan dengan DRP dan BCP yang membahas tentang Perusahaan yang bergerak dibidang *food industry* yang dalam

menjalankan proses bisnisnya menggunakan *software*, *hardware* dan jaringan komputer yang belum terintegrasi. Untuk mengatasi permasalahan diatas peneliti melakukan penelitian analisa risiko terhadap seluruh area IT dan proses bisnis yang ada di PT. X. Area-area yang akan dianalisa didapat dengan cara memetakan COBIT 4.1 ke dalam IT *domain*. Analisa risiko dilakukan dengan menerapkan tiga langkah dalam metode *Global Technology Audit Guide*. Hasil penelitian berupa analisa risiko yang membantu Perusahaan menyadari risiko-risiko apa yang mungkin terjadi dan dapat membahayakan kelangsungan bisnis sehingga Perusahaan dapat mengambil tindakan untuk mencegah atau menanganinya (Wanarta et al., 2013).

Penelitian lain dengan BCP membahas tentang bagaimana BAKA Universitas Kristen Petra yang mempunyai tugas membantu mahasiswa dalam bidang kesejahteraan dan pembinaan softskill mahasiswa, menjalin relasi dengan para alumni, ternyata BAKA tidak pernah dilakukan penilaian terhadap risiko dari sisi IT. Penelitian ini membantu BAKA Universitas Kristen Petra melakukan penilaian risiko terhadap infrastruktur IT-nya menggunakan metode *GTAG*, *OWASP Testing Guide*, dan *A Guide to the PM of Body Knowledge*. Hasil penelitian berupa analisa risiko yang membantu BAKA membuat daftar risiko-risiko apa yang mungkin terjadi, dapat membahayakan kelangsungan layanan di BAKA sehingga BAKA Universitas Kristen Petra dapat mengambil tindakan untuk mencegah atau menangani risiko tersebut (Puspa et al., 2013).

Penelitian berkaitan DRP yang membahas Kerangka kerja bagi end-to-end DRP. Penelitian ini mendesain dan mengimplementasikan dengan kesungguhan dan penelitian ini tidak seperti penelitian yang ada, yang menyiapkan DRP dalam satu lapisan stack IT. Penelitian ini menggunakan model *canonical* dari teknologi replikasi yang sudah tersedia di semua lapisan, dan melakukan sebuah tulisan untuk memetakan-mencari-mengurangi heuristik untuk mengidentifikasi DRP yang terbaik sebagai kebutuhan seorang administrator sistem informasi. Penelitian ini menyajikan analisis rinci dari kegiatan untuk mendapatkan sesuatu termasuk karakteristik empiris dari berbagai teknologi DRP (Nayak et

al., 2010), memberikan komposisi dan studi kasus end-to-end

#### METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode observasi ke staf yang menjadi penanggungjawab proses implementasi DRP di sebuah perusahaan swasta. Peneliti juga mencari informasi tambahan melalui pustaka baik jurnal ilmiah maupun buku berkaitan dengan perencanaan dan implementasi DRP dan bagaimana melakukan proses *recovery* yang cepat pada saat terjadi bencana alam ataupun *force majeure* agar perusahaan dapat melakukan BCP dengan tepat dan cepat.

Peneliti juga telah mempelajari referensi dari pedoman perencanaan dan implementasi DRP dan sistem operasi kerja proses *recovery* yang cepat pada saat terjadi bencana alam ataupun *force majeure* yang digunakan perusahaan dimana penelitian dilakukan.

Dari sumber-sumber penelitian yang dilakukan peneliti dapat menggarisbawahi bahwa ada beberapa hal yang perlu menjadi perhatian perusahaan dalam menyusun DRP untuk keberlangsungan jalannya roda bisnis perusahaan (BCP), dan perencanaan tersebut dapat mengacu pada National Institute of Standards and Technology (NIST) edisi 800-34 tentang -panduan dalam perencanaan sistem informasi, berikut poin-poin yang dibutuhkan dalam membangun sebuah DRP:

1. Membuat dan menetapkan kebijakan perencanaan. Kebijakan hukum yang sah dan mengikat dalam perencanaan DRP di perusahaan / di lembaga.
2. Membuat analisis dampak bisnis. Pada masa serba komputerisasi saat ini perangkat IT harus menjadi prioritas dalam penyusunan kebijakan DRP.
3. Membuat panduan pencegahan dini terhadap kemungkinan terjadinya bencana dan *force majeure*.
4. Membuat aturan batas usia perangkat keras computer untuk menghindari kerusakan mendadak dikarerenakan usia perangkat yang sudah seharusnya diganti.
5. Membuat perencanaan dan upaya penanganan perbaikan dan *recovery* jika terjadi bencana atau *force majeure*.

6. Membuat jadwal perencanaan uji coba jika terjadi bencana alam ataupun *force majeure* agar dapat mengukur kesiapan tim yang menjadi PIC dalam proses menjalani DRP untuk menunjang BCP.

#### HASIL DAN PEMBAHASAN

Dalam membuat sebuah DRP perlu dilakukan asesmen untuk menentukan faktor-faktor apa saja yang menjadi prioritas dan membuat tabel hasil asesmen dalam sebuah table yang berisi:

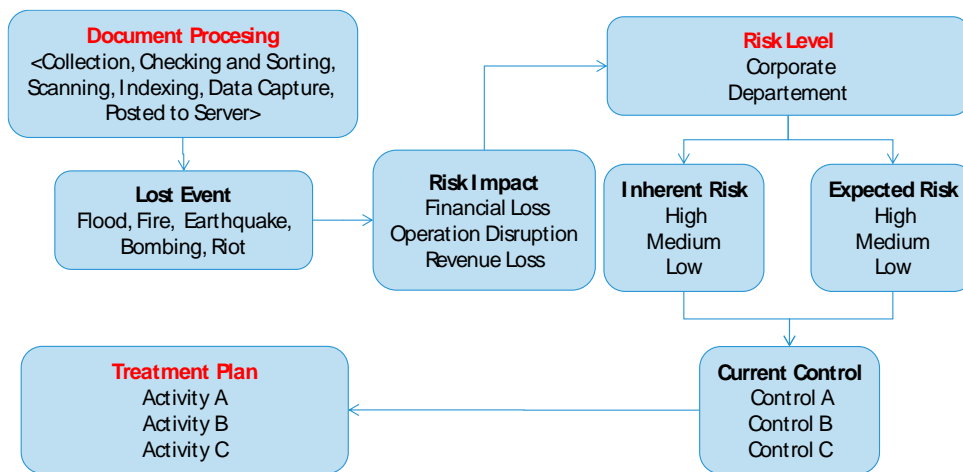
- 1) Bagian/*department* dimana proses asesmen dilakukan.
- 2) Daftar bisnis proses di bagian/*department* yang dilakukan proses asesmen.
- 3) Daftar aktifitas dari bisnis proses yang dilakukan proses asesmen. Kemudian dibuat laporan asesmen risiko yang memuat
- 4) Daftar penyebab terjadinya gangguan / bencana.
- 5) Risiko apa saja yang mungkin timbul sebagai akibat dari gangguan.
- 6) Tingkat risiko yang timbul berdampak bagi bagian atau perusahaan.
- 7) Dibuat analisa besarnya risiko yang melekat sebagai akibat risiko.
- 8) Dibuat analisa besarnya risiko yang diharapkan bagi Perusahaan. Dari masing-masing data diatas disusunlah sebuah perencanaan manajemen yang memuat informasi aktifitas yang telah dilakukan saat ini serta proses kontrol yang dilakukan untuk mengelola risiko tersebut, aktifitas tersebut meliputi :
- 9) Proses kontrol apa yang akan/telah dilakukan.
- 10) Kelayakan proses kontrol.
- 11) Proses kontrol secara keseluruhan.
- 12) Langkah perbaikan/pencegahan yang telah/akan dilakukan.

Gambar 1 merupakan tabel laporan pembuatan *Disaster Recovery Plan* (DRP).

Department Objective / KPI	Business Process (Owner/Department)	Activity	RISK ASSESSMENT				MANAGEMENT PLANNING						
			Risks Description		Level	Inherent Risk		Expected Risk	Current Actions/ Controls to Manage The Risk				
			Loss Events / Cause	Risk - Impact		Impact	Overall - Inherent		Controls	Appropriateness	Operation	Overall - Control	Treatment Plan
Increasing customer satisfaction & speed of Policy handling	Service Delivery Operation	Document Collection, Document Checked & Sorted, Document Scanning, Indexing & Data Capture	Flood	1. Financial loss 2. Operation disturbing 3. Revenue Loss	1 - Corporate	Major	High	Medium	Keep document in safe place	Marginal	Always	Moderate	Save the document and Move production room to backup 1
			Fire	1. Financial loss 2. Operation disturbing 3. Revenue Loss	3 - Departement	Major	High	Low	Check the availability of Fire Extinguisher, Smoke Al	Marginal	Always	Moderate	Move production room to backup 1
			Earthquake	1. Financial loss 2. Operation disturbing 3. Revenue Loss	1 - Corporate	Minor	Medium	Low	Check availability of emergency card	Marginal	Always	Moderate	Stop Production temporary together with checking production availability (machine, resource)
			Bombing	1. Financial loss 2. Operation disturbing 3. Revenue Loss	3 - Departement	Minor	High	Low	Check the availability of CCTV & Security.	Marginal	Always	Moderate	Move production room to backup 1
			Riot	1. Financial loss 2. Operation disturbing 3. Revenue Loss	1 - Corporate	Major	Medium	Medium	Check availabilit' of emergency card, security & CCTV.	Marginal	Always	Moderate	Move production room to backup 1

Gambar 1. Laporan metode pembuatan Disaster Recovery Plan (DRP)

Dari masing-masing aktifitas dalam gambar 1 diatasn dibuatkan alur proses aktifitas penanganan jika terjadi kendala dilapangan atau *force majeure*, gambar 2 merupakan *template* ilustrasi alur proses aktifitas DRP sebagaimana gambar 2.



Gambar 2. Gambar alur proses aktifitas DRP

Dari table hasil asesmen dan diagram alur yang dibuat, manajemen Perusahaan dapat membuat kebijakan dan pengambilan keputusan untuk membuat suatu DRP sebagai bentuk penangan dan menjaga keberlangsungan bisnis Perusahaan (BCP) apabila terjadi bencana atau *force majeure*.

Berikut ini beberapa contoh implementasi DRP yang dilakukan oleh salah satu perusahaan penyedia jasa outsourcing pencetakan dokumen tagihan karti kredit:

- a) DRP untuk skala Lokal  
Perusahaan mengimplementasi-kan sistem komputerisasi terdistribusi untuk memperingan kerja server pusat dan sebagai metode untuk mengurangi dampak yang ditimbulkan jika disuatu kantor cabang mengalami bencana skala lokal.
- b) DRP untuk skala Regional  
Salah satu unit bisnis Perusahaan tersebut adalah jasa pencetakan dokumen (billing statement), dimana saat ini di kantor pusat Perusahaan terssebut (Jakarta) memiliki pusat produksi pencetakan yang mampu melakukan proses pencetakan sampai 5

juta lembar/bulan. Untuk mengantisipasi terjadinya force majeure, Perusahaan tersebut telah membangun pusat produksi di Surabaya yang berfungsi sebagai sistem backup proses produksi jika terjadi hambatan atau force majeure di kantor pusat

## KESIMPULAN

- 1) DRP merupakan salah satu bentuk implementasi dari sebuah *IT Risk Management* dan merupakan salah satu hal yang harus diperhatikan terutama untuk mengurangi dampak kerugian dari risiko IT sebagai akibat terjadinya *force majeure*. Aktifitas penting yang harus diperhatikan antara lain kegiatan mengelola penyimpanan, database, server dan mesin virtual. Pengaktifan dari suatu DRP sebaiknya otomatis dengan proses yang terkoordinasi, agar sedikit mungkin melibatkan manusia secara manual yang dapat menimbulkan *human error*.
- 2) DRP merupakan sebuah aktifitas penting yang harus menjadi perhatian pembuat kebijakan Perusahaan terutama yang berhubungan dengan *Business*.
- 3) Dilihat dari peran penting perangkat TI dalam menjalankan roda bisnis perusahaan, sudah sewajarnya DRP terhadap perangkat TI harus menjadi prioritas utama apabila sebuah perusahaan menyusun BCP.
- 4) Peralatan teknologi informasi yang harus dijadikan prioritas utama dalam sebuah DRP adalah :
  - a) Jaringan Komputer (LAN, WAN, *Internet Connection*)
  - b) Server yang menyimpan semua data pelanggan, data transaksi dan aplikasi. Perangkat keras lainnya (PC, monitor, Telephone) yang berkaitan dengan aktifitas menjalankan bisnis Perusahaan.

## REFERENSI

- Erniwati, E. (2020). Konsepsi Force majeure dalam Kontrak/Perjanjian di Masa Pandemi. *Jurnal Ilmiah Magister Ilmu Hukum SOL JUSTICA*, 3(2), 189–198.
- Fikri, A. M., Fachrurza, F., Octaraisya, N., Agustyana, N. A., Putra, M. G. L., & Amalia, D. N. (2021). Implementation of Business Continuity Planning

Methodology in Making Business Continuity Planning Documents at PT. XYZ. *JBTI Jurnal Bisnis Teori Dan Implementasi*, 12(1), 51–62.

- Hansen, S. (2020). Does the COVID - 19 Outbreak Constitute a Force Majeure Event? A Pandemic Impact on Construction Contracts. *Journal of Civil Engineering FORUM*, 6(2), 201–214.
- IBM, S. & C. (2022). *What is a disaster recovery (DR) plan?* <https://www.ibm.com/uk-en/services/business-continuity/disaster-recovery-plan>.
- McLeod, R. J., & Schell, P. G. (2012). *Sistem Informasi Manajemen* (N. Setyaningsih, Ed.; 10th ed.). Salemba Empat.
- Meilani, D., Ikhwan, A., & Habitullah, M. (2019). Designing Disaster Recovery Plan of Data System for University. *IOP Conference Series: Materials Science and Engineering*, 1–11.
- Muflihah, Y., & Subriadi, A. P. (2018). A basic element of it business continuity plan: systematic review. *Jurnal Informatika Universitas Ahmad Dahlan*, 12(1), 17–23.
- Nayak, T., Routray, R., Singh, A., Uttamchandani, S., & Verma, A. (2010). End-to-end disaster recovery planning: From art to science. *IEEE Journal*.
- Nurofik, A., Rahajeng, E., Munti, N. Y. S., Sutisna, Firmansyah, H., Sani, A., Hendarsyah, D., Adrianto, S., Darma, W. A., Herdiansah, A., Ariestiandy, D., Nurnaningsih, D., Setiawan, I., Wiyono, A. S., & Zaharah. (2021). *Pengantar Teknologi Informasi* (I. Kusumawati & M. Sari, Eds.; Ed.1). Insania.
- Prasetyo, H. N., Supriatna, N., Raharjo, A. P., & Wikusna, W. (2019). Information Technology Disaster Recovery Plan (IT-DRP) Model-Based on NIST Framework in Indonesia. *International Journal of Applied Information Technology*, 3(1), 34–45.
- Puspa, R. H., Wibowo, A., & Gunawan, I. (2013). IT risk assessment di biro administrasi kemahasiswaan dan alumni

- (BAKA) Universitas Kristen Petra .  
*Jurnal Infra* , 1(2), 1–6.
- Shopshire, J. (2009). Developing the IT  
Distater Recovery Planng Construct.  
*Journal of Information Technology  
Management*, XX(4), 37–57.
- Syafitri, Y., Bahtiar, & Didik, Lalu. A. (2018).  
Analisis Pergeseran Lempang Bumi yang  
Meningkatkan Potensi Terjadinya Gema  
Bumi di Pulau Lombok. *KONSTAN  
Jurnal Fisika Dan Pendidikan Fisika*,  
3(2), 139–146.
- Wanarta, C., Wibowo, A., & Gunawan, I.  
(2013). IT Risk Assessment di PT. X.  
*Jurnal Infra*, 1(2), 1–7.