INTEGRALISTIK Volume 32 (2) (2020)

INTEGRALISTIK

https://journal.unnes.ac.id/nju/index.php/integralistik/index

Konsep Kebijakan Dis*aster Recovery Plan* (Drp), Dalam Rangka Ketahanan Nasional

Bambang Sutejo

Universitas Singaperbangsa Karawang (UNSIKA)

Informasi Artikel

Hisrtory of Article
Received 2020-07-10
Accepted 2020-07-15
Pusblished 2020-08-18

Keywords:
Kebijakan, Kebencanaan, Disaster Recovery Plan.

Abstrak

Dampak bencana alam yang secara masif dapat merugikan secara ekonomi maupun keselamatan manusia dan merupakan salah satu ancaman nyata terhadap ketahanan nasional suatu bangsa, termasuk Indonesia. Studi ini merupakan sebuah penelitian yang menjelaskan peningkatan kapasitas pengelolaan bencana alam dalam rangka memperkuat ketahanan nasional, salah satunya melalui penerapan konsep *Disaster Recovery Plan (DRP)*. DRP merupakan sebuah konsep yang mendorong pemanfaatan teknologi informasi dalam rangka pemulihan pasca bencana terutama dalam hal pemulihan data dan informasi. Tujuan penelitian ini untuk memberikan gambaran umum tentang bagaimana membangun sistem informasi DRP dan *Disaster Recovery Center* (DRC) agar dapat memperkuat dalam pembuatan kebijakan ketahanan Nasional. Metode penelitian ini menggunakan metode kualitatif, deskriptif terkait dengan pengembangan *frame wor*k untuk konsep kebijakan dengan menggunakan data-data sekunder/studi kepustakaan. Sebagai temuan awal dapat disimpulkan bahwa pengetahuan terkait dengan DRP dalam pengelolaan bencana alam di Indonesia masih relatif terbatas serta ketersediaan sarana dan prasarana teknologi informasi yang belum merata di setiap daerah. Hal ini tentunya dapat berimplikasi terhadap kemampuan Pemerintah dalam membuat kebijakan dan memperkuat ketahanan nasional di bidang

penanggulangan bencana alam. Sebagai saran penelitian ini dapat mendorong Integrasi Data, Pemerintah perlu mempercepat implementasi *e-government* yang dapat mendukung pelaksanaan DRP dan pembangunan DRC di daerah-daerah rawan bencana.

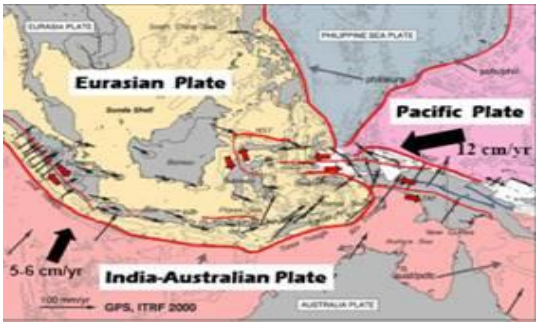
The Impact of natural disasters can massively harm in economic, human safety, and one of the real threats to the national resilience of a nation, including Indonesia. This study is a research that explains the capacity building of natural disaster management in order to strengthen national resilience, one of which is through the application of the concept of the Disaster Recovery Plan (DRP). DRP is a concept that encourages the use of information technology in the context of post-disaster recovery, especially in terms of data and information recovery. The purpose of this study is to provide an overview of how to build a DRP information system and Disaster Recovery Center (DRC) in order to strengthen national policy making resilience. This research method uses qualitative, descriptive related to the development of frame work for policy concepts using secondary data literature studies. As a preliminary finding, it can be concluded that knowledge related to DRP in natural disaster management in Indonesia is still relatively limited and the availability of information technology facilities and infrastructure is not evenly distributed in each region. This certainly can have implications for Goverment's ability to make policies and strengthen national resilience in the field of natural disaster management. As a suggestion this research can encourage Data Integration, the Government needs to accelerate the implementation of e-government which can support the implementation of DRP and DRC development in disaster prone areas.

Corresponding author :
Address: Universits Sebelas Maret Surakarta
E-mail: dewigunawatiuns@gmail.com

ISSN 2549-5011

PENDAHULUAN

Pulau-pulau di Indonesia secara geografis terletak pada pertemuan 3 lempeng tektonik dunia, yaitu lempeng Australasia, lempeng Pasifik, lempeng Eurasia serta Filipina seperti dilihat pada gambar 1. Hal ini menyebabkan Indonesia rentan secara geologis. Di samping itu, kurang lebih 5.590 daerah aliran sungai (DAS) yang terdapat di Indonesia, yang terletak antara Sabang dan Merauke, mengakibatkan Indonesia menjadi salah satu negara yang berisiko tinggi terhadap ancaman bencana gempa bumi, tsunami, deretan erupsi gunung api (129 gunung api aktif), dan gerakan tanah.



Gambar 1. Peta Tektonik Indonesia(http://balai3.denpasar.bmkg.go.id/tentang-gempa)

Selain itu, iklim di Indonesia sangat dipengaruhi oleh lokasi dan karakteristik geografis yang membentang antara Samudra Pasifik dan Samudra Hindia. Indonesia memiliki 3 pola iklim dasar

monsunal, khatulistiwa, dan sistem iklim lokal yang menyebabkan perbedaan pola curah hujan yang dramatis. Kondisi tersebut semakin kompleks lantaran tantangan dampak pemanasan global dan pengaruh perubahan iklim, seperti kenaikan suhu temperatur dan permukaan air laut pada wilayah Indonesia yang berada di garis khatulistiwa. Hal ini cenderung menimbulkan tingginya potensi terjadi berbagai jenis bencana hidrometeorologi, seperti banjir, banjir bandang, kekeringan, cuaca ekstrem, gelombang ekstrem, abrasi, serta kebakaran hutan dan lahan (karhutla).

Berdasarkan hasil kajian risiko bencana tahun 2015 yang disusun oleh BNPB dalam buku Risiko Bencana Indonesia (RBI), potensi jumlah jiwa terpapar risiko bencana, jumlah kerugian fisik, ekonomi, dan lingkungan, berkategori sedang-tinggi yang tersebar di 34 provinsi, per jenis ancaman bencana adalah sebagai berikut [8]:

a. Lima jenis bencana dengan jiwa terpapar tertinggi adalah: cuaca ekstrem (puting beliung) sebanyak 244 juta jiwa, diikuti kekeringan sebesar 228 juta jiwa, dan banjir sebanyak 100 juta jiwa, lalu gempa bumi sebesar 86

juta jiwa, dan bencana tanah longsor sebesar 14 juta jiwa.

b. Sedangkan untuk potensi kerusakan dan kerugian fisik dan ekonomi tertinggi untuk ancaman gempa bumi sebesar 648.874 triliun, potensi kerusakan dan kerugian fisik dan ekonomi banjir serta banjir bandang sebesar 376.886 triliun, dan tanah longsor sebesar 78.279 triliun, sedangkan kekeringan sebesar 192.737 triliun.
c. Selain itu, untuk potensi dampak lingkungan tertinggi adalah ancaman bencana kekeringan 63 juta hektar, diikuti oleh bencana kebakaran hutan dan lahan 42 juta hektar, dan tanah longsor sebesar 41 juta hektar.
d. Diluar kejadian factual tesebut, BNPB telah menyiapkan peta risiko bencana yang dapat menjelaskan jiwa terpapar, kerugian fisik, kerugian ekonomi, dan kerugian lingkungan yang mungkin dapat terjadi.

Bencana (disaster) merupakan suatu risiko yang sangat tidak diharapkan dan diduga untuk dapat terjadi, apalagi bencana yang menimbulkan dampak negatif dan cukup signifikan bagi keberlangsungan suatu perusahaan atau sebuah organisasi pemerintahan. Kemunculan suatu bencana memiliki potensi risiko yang mungkin saja mengakibatkan terganggunya proses dan operasional organisasi terlebih bisnis pemerintahan yang memiliki sifat pelayanan jasa. Dampak terganggunya rutinitas bisnis, memiliki dampak langsung juga pada penigkatan biaya, munculnya permasalahan penyediaan layanan kepada pengguna, terganggunya layanan teknologi informasi kepada pengguna, turunnya produktivitas lingkungan kerja, sampai bisa juga membuat buruk citra perusahaan atau organisasi dimata pelanggan.

Kemunculan suatu bencana memang tidak dapat diperkirakan secara pasti kapan terjadi. Akan tetapi usaha untuk mencegah dan meminimalisasir dampak atas terjadinya bencana bisa dilakukan. Sebuah perusahaan atau organisasi dapat melakukan upaya persiapan yang harus dilakukan untuk dapat memulihkan diri sesegera mungkin jika menghadapi sebuah keadaan darurat atau kejadian musibah yang menderanya.

Semua orang mempunyai risiko terhadap potensi bencana, sehingga penanganan bencana merupakan urusan semua pihak (*everybody's business*). Oleh sebab itu, perlu dilakukan berbagi peran dan tanggung jawab (*shared responsibility*) dalam peningkatan kesiapsiagaan di semua tingkatan, baik anak, remaja, dan dewasa.

Seperti yang telah dilakukan di Jepang, untuk menumbuhkan kesadaran kesiapsiagaan bencana.

Gambaran tren bencana global ke depan juga cenderung akan meningkat karena pengaruh beberapa faktor, seperti 1) Meningkatnya jumlah penduduk, 2) Urbanisasi, 3) Degradasi lingkungan, 4) Kemiskinan, dan 5) Pengaruh perubahan iklim global.

Secara umum, faktor utama banyaknya korban jiwa, kerusakan, dan kerugian yang timbul akibat bencana adalah masih kurangnya pemahaman dan kesadaran masyarakat serta pelaku pengelola sumber daya hayati dan lingkungan terhadap risiko bencana di wilayahnya. Selain itu, dukungan mitigasi struktural yang belum memadai juga menjadi faktor tak terpisahkan. Hal ini mengakibatkan kesadaran, kewaspadaan, dan kesiapsiagaan dalam menghadapi bencana masih sangat kurang.

Belajar dari pengalaman beberapa negara maju yang rawan bencana seperti Jepang, Amerika Serikat, Jerman, Korea Selatan, dan beberapa negara di Eropa, bahwa secara umum, kesadaran, kewaspadaan dan kesiapsiagaan telah tumbuh serta berkembang melalui pelatihan secara teratur.

Hasil survei di Jepang, pada kejadian gempa Great Hanshin Awaji 1995, menunjukkan bahwa presentase korban selamat disebabkan oleh Diri Sendiri sebesar 35%, Anggota Keluarga 31,9 %, Teman/Tetangga 28,1%, Orang Lewat 2,60%, Tim SAR 1,70 %, dan lain-Lain 0,90%. Berdasarkan ilustrasi tersebut, sangat jelas bahwa faktor yang paling menentukan adalah penguasaan pengetahuan yang dimiliki oleh “diri sendiri” untuk menyelamatkan dirinya dari ancaman risiko bencana. Kemudian, diikuti oleh faktor bantuan anggota keluarga, teman, bantuan Tim SAR, dan di sekelilingnya. Maka, edukasi untuk meningkatkan pemahaman risiko berdesain tema Latihan Kesiapsiagaan Bencana Siap, Untuk Selamat! Merupakan pesan utama bersama yang akan didorong dalam proses penyadaran (*awareness*) dalam peningkatan kemampuan diri sendiri [9].

Proses penyadaran tersebut berguna agar setiap orang dapat memahami risiko, mampu mengelola ancaman dan, pada gilirannya, berkontribusi dalam mendorong ketangguhan masyarakat dari ancaman bahaya bencana. Di samping itu, kohesi sosial, gotong royong, dan saling percaya merupakan nilai perekat modal sosial yang telah teruji dan terus dipupuk, baik

kemampuan perorangan dan masyarakat secara kolektif, untuk mempersiapkan, merespon, dan bangkit dari keterpurukan akibat bencana.

Bene, et.al (2012) menyatakan bahwa sebagai suatu proses ketahanan sosial dan budaya sadar bencana dalam jangka panjang, ketangguhan masyarakat menyasar tiga elemen ketangguhan, yaitu: kapasitas meredam ancaman (*absorptive*) yang menghasilkan persistensi, kemampuan beradaptasi (*adoptive*) yang menghasilkan penyesuaian perlahan dan berjangka panjang, dan kapasitas bertransformasi (*transformative*) yang menghasilkan respon-respon transformasional [3].

Salah satu upaya mendasar untuk meningkatkan kewaspadaan dan kesadaran menumbuhkan budaya siaga adalah melalui perencaaan yang matang dalam rangka mengahadapi risiko bencana atau yang sering dikenal sebagai *disaster recovery plan* (DRP).

METODOLOGI

Penelitian ini dengan menggunakan Studi literatur dengan metode kualitatif, deskriptif terkait dengan pengembangan dan pendekatan konseptual melalui perencanaan untuk konsep kebijakan melalui data-data sekunder/studi kepustakaan yang digunakan dalam penulisan karya tulis ilmiah ini, Studi literatur yang dilakukan oleh penulis yaitu dengan melakukan pencarian terhadap berbagai sumber tertulis, baik berupa buku-buku, arsip, majalah, artikel, dan jurnal, atau dokumen-dokumen yang relevan dengan permasalahan yang dikaji dan menganalisis data-data tersebut. Sehingga informasi yang didapat dari studi kepustakaan ini dijadikan rujukan untuk memperkuat argumentasi-argumentasi yang ada untuk menterjemahkan menjadi konsep yang integratif dan akurat menjadi bahan pembuatan kebijakan.

Secara Umum Studi Literatur yang digunakan dalam kegiatan ini digunakan untuk menyelesaikan persoalan dengan menelusuri sumber-sumber tulisan yang pernah dibuat sebelumnya. Dalam sebuah penelitian yang hendak dijalankan, tentu saja seorang peneliti harus memiliki wawasan yang luas terkait objek yang diteliti.

PEMBAHASAN

Dalam beberapa literatur, peningkatan manajemen bencana yang meliputi aspek pencegahan, mitigasi hingga

pemulihan merupakan bagian dari penguatan ketahanan nasional suatu negara. Di Amerika Serikat, misalnya, [6] menjelaskan bagaimana bencana alam telah menyebabkan kerugian ekonomi yang signifikan di negara tersebut. Ditambah lagi, isu degradasi lingkungan semakin intensif seiring dengan kegiatan pembangunan dan praktik pertanian yang cenderung mengabaikan kelestarian lingkungan. Korea adalah gambaran lain dari banyak negara yang sering mengalami bencana alam seperti banjir, angin topan, kekeringan, tanah longsor, badai salju, gempa bumi, dan tsunami. Menurut studi Yoon et al., (2015), berdasarkan data Pusat Informasi Bencana Nasional (NDIC) Korea, peristiwan bencana alam yang terjadi di negara tersebut selama periode 1960-2011 telah menyebabkan kerusakan properti lebih dari $41 milyar dan hampir 10.000 kematian [15].

Ancaman dari bahaya dampak bencana alam terhadap keberlangsungan suatu bangsa tentunya relevan dengan konsep ketahanan nasional yang memfokuskan kepada pembangunan ketahanan dalam seluruh aspek kehidupan suatu bangsa. Hal ini dikemukakan diantaranya dalam Soepandji & Farid, (2018) yang memaknai Ketahanan Nasional sebagai suatu kondisi dinamis bangsa Indonesia mencakup segenap aspek kehidupan nasional secara menyeluruh serta berisi keuletan dan ketangguhan yang mengandung kemampuan mengembangkan kekuatan nasional dalam menghadapi dan mengatasi segala tantangan, ancaman dan hambatan [12] termasuk bencana alam yang sering terjadi di Indonesia. Hal senada juga diungkapkan oleh Agus bahwa ketahanan nasional diperlukan oleh segenap bangsa Indonesia untuk menghadapi ancaman, gangguan, hambatan dan tantangan (AGHI) yang berubah-ubah sesuai dengan situasi atau kondisi eksternal maupun internal yang diantaranya dapat berupa ancaman dari dampak bencana alam [1].

Untuk itu, sebagai salah satu upaya untuk membangun ketahanan nasional di bidang penanggulangan bencana alam diperkenalkan suatu konsep *Disaster recovery planning* (DRP) yaitu perencanaan untuk pengelolaan secara rasional dan cost-effective bencana terhadap sistem informasi yang akan dan telah terjadi. Didalamnya terdapat aspek *catastrophe in information systems* [11]. Seperti halnya polis asuransi, suatu perencanaan preventif terhadap bencana pada sistem informasi dan pemulihan pasca bencana yang efektif harus dirasakan manfaatnya walaupun bencana ”tak pernah akan terjadi” justru karena

efektivitas sistem informasi tersebut. Namun runtuhnya sistem informasi itu sendiri merupakan bencana, terhentinya kegiatan sehari-hari hari karena kehilangan informasi.

Bencana alam yang sifatnya tidak dapat diprediksi dan dapat menyebabkan kerugian baik secara fisik, ekonomi maupun keselamatan manusia merupakan salah satu ancaman terhadap ketahanan nasional suatu bangsa. Kebijakan ketahanan negara terhadap bencana sangat erat dengan kemampuan suatu negara untuk siap menghadapi bencana besar, merespon dan segera memulihkan setiap gangguan yang terjadi agar kembali ke kondisi normal.

Disaster recovery planning (DRP) adalah perencanaan untuk pengelolaan secara rasional dan cost-effective bencana terhadap sistem informasi yang akan dan telah terjadi. Didalamnya terdapat aspek *catastrophe in information systems* [2]. Seperti halnya polis asuransi, suatu perencanaan preventif terhadap bencana pada sistem informasi dan pemulihan pasca bencana yang efektif harus dirasakan manfaatnya walaupun bencana"tak pernah akan terjadi" justru karena efektivitas sistem informasi tersebut. Namun runtuhnya sistem informasi itu sendiri merupakan bencana, terhentinya kegiatan sehari-hari hari karena kehilangan informasi.

Tujuan *disaster recovery planning* (DRP) [4] adalah meminimumkan risiko dan optimalisasi kesinambungan entitas dalam menghadapi risiko bencana. Apabila manajemen tak mampu merumuskan manfaat DRP, atau menyimpulkan bahwa manfaat DRP lebih kecil dari biaya DRP, maka program DRP tak akan dilaksanakan.

Bagi Pemerintah daerah dalam hal ini adalah bagian dari pemerintahan, DRP disusun bersama seluruh masyarakat setempat. DRP merupakan strategi sedia payung sebelum hujan, seringkali upaya dan belanja sumberdaya kecil-kecil berkesinambungan dan tak terasa, dibandingkan besaran bencana. DRP merupakan kesediaan untuk menabung untuk bencana tak terduga.

Diskontinuitas administrasi kepemerintahan menyebabkan diskontinuitas investasi masuk kedalam Pemda tersebut. Arsip hutang-piutang dengan pihak ketiga diluar bencana juga hilang lenyap. Apabila hutang, pihak penagih biasanya mempunyai bukti-legal lengkap untuk menagih pada penderita bencana. Tidak sebaliknya, karena arsip/dokumen piutang lenyap, sangat mungkin pihak ketiga yang berhutang tak mau membayar hutangnya.

Rancangan DRP berguna pula bagi perusahaan komersial atau pemerintahan dengan sistem yang rawan bencana.

Bencana merupakan interupsi signifikan terhadap kesinambungan (*going concern*) kegiatan operasi sehari-hari yang bersifat normal dan berkesinambungan bagi suatu entitas, yang berpengaruh kepada anggota dalam entitas, pemasok entitas, pelanggan entitas dan berbagai stakeholder yang lain. Bencana tetap merugikan mungkin tak mengganggu going concern atau kontinuitas operasi sehari-hari sering disebut musibah atau kecelakaan. Interupsi dapat menyebabkan berbagai proyek, program dan kegiatan Pemda yang hampir selesai, tiba-tiba menjadi sia-sia (nol). Putusnya kontinuitas aktivitas ekonomi menyebabkan GDP dan PAD mengalami penurunan dahsyat, bahkan sebagian kegiatan ekonomi putus.

Bencana dapat berupa (1) fenomena alam seperti banjir, kekeringan, gempa bumi, topan-badai, kebakaran karena alam (gunung meletus, kebakaran hutan musim kemarau, api-gambut abadi, fokus sinar matahari oleh potongan beling disemak belukar); (2)akibat kelalaian manusia seperti kebocoran nuclear plant atau pipa gas,kebakaran karena kelalaian, tumpahan minyak dilaut tak sengaja,arus pendek listrik, penyebaran virus) dan (3) kejahatan seperti sabotase, pembakaran, peledakan, penyebaran virus dan pengrusakan fisik aset. Sebuah bencana banjir dapat menyebabkan kerugian fisik dalam miliar USD [13]. Persentase terbesar bencana mungkin berasal dari api dan air [5]. Bencana air disebabkan hujan, banjir dan angin topan. Administrasi dan akuntansi walaupun misalnya masih terselamatkan, tak mampu mencatat kerugian nonfinansial, seperti kehilangan jiwa dan sanak keluarga, tak mampu mencatat kesedihan, dan tak dapat melaporkan kehilangan sejarah (lokasi restoran, hotel legendaris, dan heritage assets lain).

DRP adalah proses, kebijakan dan prosedur yang berkaitan dengan persiapan pemulihan atau keberlangsungan infrastruktur teknologi yang kritis bagi organisasi setelah terjadinya bencana, baik bencan yang disebabkan oleh tindakan manusia ataupun bencana alam. Disaster recovery merupakan bagian dari business continuity. Sedangkan business continuity sendiri merupakan aktivitas yang dilakukan oleh organisasi untuk menjamin bahwa fungsi bisnis kritis dapat tetap tersedia bagi konsumen, supplier dan pihak-pihak lainnya yang berkepentingan [11].

Wujud DRP sendiri secara sederhana hanya berupa dokumen yang

berisi *response* plan (rencana tanggap) terhadap bencana. Tetapi, proses penyusunan dokumen tersebut tidaklah mudah dan memerlukan pengetahuan yang mendalam mengenai berbagai resiko yang dihadapi perusahaan/organisasi. Ruang lingkup DRP dapat dibuat melebar meliputi infrastruktur, personel dan prosedur. Pada tulisan ini, fokus pembahasan DRP ditekankan pada DRP terkait dengan penyelamatan infrastruktur teknologi informasi dari ancaman bencana [4].

DRP yang baik dapat membantu Pemerintah khususnya Pemerintah daerah yang daerahnya rawan bencana alam agar tidak lumpuh karena terjebak pada posisi buta informasi dan buta posisi pada saat seluruh data dan rencana masa depan pemerintah daerah hilang lenyap ditelan bencana. Hal ini dapat dicapai salah satunya dapat ditempuh adalah dengan menawarkan konsultan sistem informasi, untuk pendampingan pembuatan DRP pihak yang terkait.

Indonesia sendiri, dalam 10 tahun terakhir sudah mengalami beberapa kali bencana besar yang tidak pernah diduga sebelumnya, seperti tsunami di Aceh (2004), gempa di Yogyakarta (2006), letusan gunung berapi dan beberapa kejadian serupa dalam skala yang lebih kecil. Catatan kerugian yang ada saat ini berfokus pada kehilangan nyawa manusia dan kerugian materil berupa kerusakan infrastruktur jalan dan bangunan. Hingga saat ini belum ada data atau penelitian yang dapat memberikan gambaran besarnya kerugian akibat rusak/hilangnya informasi atau infrastruktur teknologi informasi maupun khasanah budaya yang harus dilestarikan. Penangangan bencana tersebut menjadi pengalaman yang sangat berharga dalam kebermanfaatan pengamanan data mengenai artefak dan peninggalan sejarah yang harus didokumentasi dan direkam secara elektronik, disimpan pada arsip pusat. Peninggalan sejarah dan museum sebaiknya direlokasi ke wilayah yang lebih aman, demikian pula rumah tinggal para tokoh budaya dan seniman setempat harus di relokasi ke wilayah lebih aman bencana yang termasuk di dalam penyusunan DRP dan DRC yang terintegrasi dan akurat.

Perencanaan disaster recovery mengacu pada persiapan untuk menghadapi bencana dan respon yang harus diberikan ketika bencana terjadi. tujuan DRP adalah keberlangsungan (continuity) atau kemampuan organisasi untuk bertahan (survival) dalam menghadapi bencana (Proses penyusunan DRP meliputi analisis, perencanaan, pembuatan DRP, pengujian

dan revisi periodik berdasarkan kondisi bisnis terkini.

Domain dari *Busines Continuity Plan* (Perencanaan Keberlangsungan Bisnis atau BCP) dan Disaster Recovery Plan (Perencanaan Pemulihan dari Bencana atau DRP), semuanya adalah mengenai bisnis. Sementara domain- domain yang lainnya concern dengan pencegahan risiko dan melindungi infrastruktur dari serangan, domain ini berasumsi bahwa kejadian terburuk telah terjadi. BCP adalah mengenai pembuatan perencanaan dan frame-work untuk menjamin bahwa proses bisnis dapat terus berlanjut dalam keadaan emergensi. Sedangkan DRP adalah mengenai pemulihan cepat dari keadaan emergensi atau bencana, sehingga hanya mengakibatkan dampak minimum bagi organisasi atau perusahaan [13].

Gambar 2. Siklus Disaster Recovery Plan (DRP)

Disaster manajemen bertujuan mengurangi, atau menghindari, potensi kerugian akibat *hazard*, menjamin dukungan dan bantuan pada korban bencana, serta melakukan pemulihan secara cepat dan efektif. Manajemen bencana dengan model *disaster cycle* (siklus bencana) atau *disaster continuum* menjelaskan proses yang terus menerus di mana pemerintah, bisnis, dan *civil society* menyusun rencana untuk mengurangi dampak bencana, bereaksi saat dan setelah bencana, serta mengambil berbagai langkah untuk pemulihan setelah bencana terjadi [10].

Data dan informasi adalah beberapa hal yang menjadi krusial dalam pemulihan bencana. Sebuah sistem yang berjalan pada suatu instansi akan bergantung pada informasi dan aplikasi yang memproses informasi tersebut. Informasi merupakan salah satu kebutuhan manusia yang paling dasar. Saat ini pengguna informasi bukan saja dari kalangan orang yang mampu. Dengan semakin murahnya sarana dan pendukung informasi, maka alternatif komunikasi saat ini yang dapat mengatasi batasan-batasan seperti jarak adalah penggunaan jaringan komputer internasional atau biasa yang sering disebut dengan

Internet. Sebelum kita bisa menikmati sebuah informasi, maka kita memerlukan data [4]. Di era yang serba digital saat ini, hampir semua data disimpan didalam sebuah media penyimpanan yang selanjutnya diolah menjadi sebuah informasi. Kemajuan teknologi khususnya jaringan komputer mengakibatkan semakin mudahnya dan murahnya perangkat- perangkat pendukung untuk memberikan layanan komunikasi.

Backup data adalah memindahkan atau menyalin kumpulan informasi (data) yang tersimpan di dalam hardisk komputer yang biasanya dilakukan dari satu lokasi/perangkat ke lokasi/perangkat lain. Data atau kumpulan informasi tersebut bisa berupa file dokumen, gambar, video, audio, *system windows*, driver, atau software/program tertentu. Restore data adalah proses penting setelah backup. Backup akan menjadi sia-sia bila proses pengembalian dan perbaikan data sistem sulit dilakukan. Untuk mencapai tujuan ini ada beberapa pendekatan yang harus diperhatikan, yaitu proses backup harus dilakukan dengan aturan yang jelas, hindari membackup dengan sembarangan dengan tidak terstruktur [5].

Salah satu cara untuk meminimalisasi dampak kerusakan tersebut adalah menyiapkan DRP yang paling optimal untuk suatu organisasi. DRP yang pada dekade tahun 90-an tidak terlalu menjadi perhatian di kalangan bisnis, sejak tahun 2000-an mulai banyak diperhatikan oleh berbagai pihak. DRP yang pada awalnya hanya diprioritaskan untuk menyelamatkan nyawa manusia, dikembangkan juga kearah penyelamatan infrastruktur. Seiring dengan meningkatnya kebergantungan bisnis terhadap teknologi informasi maka meningkat juga resiko ancaman akibat bencana terhadap keberlangsungan bisnis. Saat ini bahkan sudah diterbitkan pedoman standar khusus sebagai pedoman penyusunan dan evaluasi DRP, khusus untuk operasional dan manajemen teknologi informasi, yaitu ISO/IEC 24762:2008 yang menyediakan pedoman penyusunan DRP untuk teknologi informasi dan komunikasi. Pedoman ini merupakan bagian dari dari *manajemen business continuity,* dan diterapkan baik bagi penyedia layanan teknologi informasi dan komunikasi internal *(information communication technology*-ICT) maupun eksternal (*outsourced*), dan meliputi fasilitas fisik dan layanan.

Mengapa Disaster Recovery Plan (DRP) ini Penting

Telah banyak kasus *data loss* maupun pencurian data dalam dunia teknologi dewasa ini. Sebuah kesalahan yang

sederhana dapat berujung menjadi sebuah bencana bisnis yang berkaitan dengan keuangan perusahaan. Berdasarkan survey yang dilakukan oleh *National Small Business Poll/* atau *NFIB,* sebesar 10% *disaster* disebabkan oleh faktor *human error* dan bersifat teknis. Sedangkan secara mengejutkan, sebesar 30% disebabkan oleh bencana alam. Hal sederhana seperti hujan dapat menyebabkan listrik padam dan menyebabkan resiko kerugian yang besar. Menurut penelitian yang dilakukan oleh University of Texas, menunjukkan fakta bahwa hanya 6% perusahaan yang mampu bertahan dan mengembalikan data mereka, sebanyak 43% data tidak dapat diakses kembali, dan 51% perusahaan tutup dalam 2 tahun terakhir. Hal ini menunjukkan bahwa *Disaster Recovery Plan* (DRP) sangatlah penting. Berikut beberapa alasan lainnya :

a. **Perangkat keras dan mesin yang rusak.** Meskipun reliabilitas suatu teknologi sudah berada pada level yang terbaru, atau jarang terjadi kegagalan, namun faktanya semua perangkat teknologi akan tetap memiliki kekurangan, kelemahan, serta rentan rusak. Dengan kenyataan demikian, akan menjadi sangat mahal bagi sebuah perusahaan untuk menghapus atau memperbaiki masing-masing kegagalan pada infrastruktur IT. Maka memiliki *Disaster Recovery Plan* merupakan cara yang terbaik untuk mengamankan data-data yang penting akibat kegagalan suatu perangkat keras.

b. **Seperti layaknya mesin, manusia tidaklah sempurna.** Pernahkah Anda mengerjakan suatu pekerjaan dengan sangat sungguh-sungguh namun menyesal karena lupa menyimpan? Ironisnya, hal itu sering sekali terjadi. Sama halnya dengan sistem *firewall,* anti-virus, dan anti-spyware yang merupakan suatu bentuk perlindungan data dari serangan yang tidak diinginkan. Software tersebut hanya memastikan bahwa data akanaman serta dapat diandalkan saat tiba-tiba terjadi downtime. Namun, bagaimana jika ada suatu perusahaan yang melakukan kebijakan tidak boleh ada *data loss saat* saat terjadi downtime? *Disaster Recovery Plan* jawabannya.

c. **Konsumen menuntut kesempurnaan sistem.** Masih ingat sebuah kata-kata lama bahwa konsumen adalah raja? Ya, konsumen selalu menuntut kesempurnaan, apapun hal yang terjadi dibelakang sistem

tersebut, konsumen enggan mencari tahu dan hanya ingin mendapat yang terbaik dalam pelayanannya. Dengan tingkat kompetisi yang semakin tinggi, memaksa perusahaan untuk lebih transparan dan akuntabel. Dengan *Disaster Recovery Plan* Anda tidak akan kesulitan dalam meyakinkan konsumen terkait masalah transparansi dan akuntabilitas data.

d. Bangun Sistem *Disaster Recovery Plan* yang Solid untuk Bangun Kepercayaan Konsumen dan Selamatkan Bisnis

Tidak ada bisnis yang tidak rentan terhadap bencana IT, namun pemulihan cepat dengan adanya *Disaster Recovery Plan* yang baik merupakan tuntutan konsumen. Terlalu banyak bisnis yang gagal karena kurangnya mempersiapkan segala kem ungkinan bencana yang sewaktu-waktu dapat terjadi. Meski solusi sederhana seperti seperti *backup* sangat mudah menyelamatkan hal tersebut, namun jika Anda belum menyiapkan *Disaster Recovery Plan*, maka tentu hal ini harus menjadi prioritas utama bagi perusahaan Anda.

Syarat-Syarat Membuat *Disaster Recovery Plan* (DRP)

Berdasarkan *National Institute of Standards and Technology (NIST)* edisi publikasi 800-34 tentang Panduan Perencanaan sistem informasi, hal-hal yang dibutuhkan dalam membangun *Disaster Recovery Plan* (DRP) adalah sebagai berikut:

a. Mengembangkan kebijakan perencanaan Kebijakan legal yang sifatnya mengikat ini dibuat untuk mendukung dalam peren-canaan dalam mengembangkan *Disaster Recovery Plan (DRP).*
b. Melakukan analisis dampak bisnis. Anda dapat berbicara dengan perusahaan konsultan atau rekanan pihak ketiga yang Anda pilih untuk mengidentifikasi serta memprioritaskan sistem dan komponen IT yang paling kritis.
c. Mengidentifikasi upaya pencegahan. Ini adalah acuan yg dapat dipakai untuk mengurangi efek dari gangguan sistem, dapat juga meningkatkan ketersediaan sistem dan mengurangi biaya-biaya tidak terduga dari segi usia pemakaian hardware.
d. Mengembangkanstrategi *recovery*. Str ategi *recovery* dan *backup* yang cermat akan membuat pemulihan lebih cepat dan efektif akibat gangguan tersebut.

e. Rencanakan untuk uji coba, latihan hingga menjalankan agar *Disaster Recovery Plan* berjalan sesuai dengan skema yang diinginkan.
f. Perencanaan dan perawatan. Semua perencanaan harus ditulis dalam dokumen yang harus diperbarui seiring dengan peningkatan sistem yang baru.

Langkah-Langkah Membuat *Disaster Recovery Plan* (DRP)

Dengan mengetahui struktur sesuai SP 800-34. Anda dapat membuat beberapa langkah dalam penerapan *Disaster Recovery Plan (DRP)* sebagai berikut :

1. Tim perencanaan *Disaster Recovery Plan (DRP)* harus bertemu dengan tim IT, *software developer* dan *network administrator*. Hal-hal yang dperlu dibahas antara lain seperti *internal ele- ment,* aset eksternal, hingga keterlibatan pihak ketiga. Pastikan rencana Anda terkomunikasikan dengan semua senior departemen IT.
2. Kumpulkan semua data yang relevan terkait infrastruktur. Misalnya diagram jaringan, peralatan konfigurasi, dan database.
3. Pastikan Anda mengetahui dokumen-dokumen terkait jaringan yang akan digunakan dalam *Disaster Recovery Plan* (DRP). Jika belum ada, lanjutkan dengan langkah-langkah sebagai berikut :
    a. Identifikasi masalah dengan pihak manajemen terkait ancaman paling serius di lingkungan terhadap Infrastruktur IT, seperti kebakaran, kesalahan manusia, masalah kelistrikan atau kegaga-lan sistem.
    b. Identifikasi masalah dengan pihak manajemen terkait masalah paling rentan dalam Infrastruktur IT seperti tidak adanya listrik cadangan, database yang telah kadaluarsa dan lain-lain.
    c. Ulas kembali riwayat dari gangguan dan bagaimana menangani masalah tersebut.
    d. Identifikasi tentang aset paling penting di perusahaan seperti *call center*, server dan akses internet.

e. Buat peraturan mengenai waktu maksimal yang dibutuhkan manajemen untuk menerima aset IT yang tersedia.
f. Identifikasi prosedur operasional yang saat ini digunakan dalam merespon gangguan kritis.
g. Menentukan kapan prosedur ini terakhir diuji hingga memvalidasi kesesuaiannya.

4. Identifikasi tim respon darurat untuk semua gangguan infrastruktur IT. Tentukan level tim respon darurat tersebut dalam pelatihan suatu sistem kritis, terutama dalam keadaan darurat.
5. Identifikasi vendor atau pihak ketiga yang akan Anda ajak kerja sama, teliti keunggulan dan pengalaman perusahaan tersebut. Pilih perusahaan yang menyediakan garansi dan telah tersertifikasi terutama mengenai keamanan data. Selain data Anda akan ditangani dengan baik, tidak akan ada kebocoran atau serangan terhadap data Anda.
6. Kumpulkan hasil dari segala asesmen yang telah dilakukan dalam bentuk analisa. Identifikasi apa yang telah dilakukan dan yang harus dilakukan, dengan rekomendasi bagaimana cara mencapai, tingkat persiapan serta perkiraan berapa investasi yang dibutuhkan.
7. Minta seluruh manajemen meninjau dan mengulas hasil laporan dan menyetujui tindakan yang direkomendasikan.
8. Persiapkan IT Disaster Recovery Plan yang ditujukan untuk sistem dan jaringan yang paling vital/ kritis.
9. Lakukan uji coba dengan membuat simulasi bencana yang mengharuskan Anda harus memulihkan data.
10. Selalu perbarui dokumen yang Anda gunakan dalam *Disaster Recovery Plan*. Setiap *Disaster Recovery Plan* haruslah memiliki dokumentasi yang kuat dan menyeluruh yang mencakup inventaris terperinci tentang peralatan dalam infrastruktur. Hal ini akan membantu mempertahankan manajemen aset yang baik.
11. jadwalkan secara berkala peninjauan atau audit

terkait *Disaster Recovery Plan (DRP)* yang Anda miliki.

Memiliki *Disaster Recovery Plan (DRP)* merupakan sebuah prioritas utama setiap perusahaan yang sangat menggantungkan datanya pada sistem digital. *Disaster Recovery Plan (DRP)* membuat Anda tidak perlu khawatir akan bencana yang tiba-tiba terjadi pada bisnis, karena tentunya keamanan data konsumen merupakan prioritas yang utama.

Pemulihan Pasca Bencana

Rencana pemulihan harus berkualitas, disusun secara lengkap dan disempurnakan dari tahun ketahun. Makin pendek masa pemulihan, makin kecil kerugian akibat bencana. Sebaliknya, makin panjang masa pemulihan, makin lama mulainya kembali masa produktif. Dengan demikian pendek waktu pemulihan merupakan hal yang terpenting, setiap hari perpanjangan waktu pemulihan mungkin adalah satu hari perpanjangan masa tidak produktif entitas tersebut. Kondisi fisik aset belum pulih mengganggu estetika (rasa keindahan), memelihara rasa gamang, duka-nestapa, yang menyebabkan semangat membangun terganggu bahkan berisiko menyebabkan kerusakan moral.

Strategi pemulihan pasca bencana telah dimulai sebelum [7] bencana terjadi, meng- gunakan rancangan *risk management* untuk; (1) risiko yang tak terduga dan (2) risiko yang diduga pasti akan terjadi dan tak dapat dielakkan. Bila bencana berskala besar, Presiden dapat mengangkat seorang Menteri Khusus untuk pemulihan bencana, untuk mengatasi masalah lintas departemen pemerintah (Jepang, Kobe) dalam kurun waktu cukup lama. Manajemen Pemda bertanggung jawab menyusun DRP paripurna, mengkomunikasikannya kepada DPRD. Semua persiapan DRP dilakukan, dicadangan dan dialokasikan oleh APBD, sekalipun dalam usulan anggaran defisit.

Individu penanggungjawab bencana harus diidentifikasi secara jelas. Bagian peran tanggung jawab tiap individu dan kelembagaan harus jelas, jangan terjadi tumpang tindih. Tumpang tindih tugas kelembagaan antara Departemen Pemerintah Pusat untuk pemulihan bencana harus dibersihkan terus menerus oleh Presiden.

Rencana Pemulihan Bencana atau dikenal pula sebagai D*isaster Recovery Plan (DRP),* hadir sebagai solusi komprehensif untuk membantu perusahaan atau institusi keuangan melakukan antisipasi dan penanggulangan terhadap

bencana yang berpotensi meng-ganggu operasional sistem TI yang merupakan penunjang bisnis penting perusahaan.

Di saat para kompetitor bisnis lain meminta permohonan maaf dan mengajukan *excuse* melalui klausul force majeure, organisasi yang tetap dapat beroperasi pasca bencana akan menikmati *competitive advantage* dari timbulnya risiko bencana, serta meraih peluang-peluang yang ada. Tidakkah kita menghendaki termasuk dalam kategori organisasi seperti ini? Ataukah ketika DRP sudah menjadi standar dalam dunia bisnis, kita tergolong dalam organisasi late followers, yang cukup dengan berharap agar bencana tidak terjadi?.

Bisnis mengadopsi teknologi informasi dengan sangat cepat. Pemrosesan data serta segala aktivitas bisnis tidak hanya menggunakan konsep manual lagi, melainkan telah terdigitalisasi. Aktivitas sehari-hari seperti mengirim email, menelpon menggunakan aplikasi atau platform berbasis internet, hingga pembayaran gaji karyawan atau kebutuhan finansial lainnya dapat dilakukan melalui internet. Untuk melakukan berbagai hal, sekarang Anda tinggal memanfaatkan smartphone maupun gadget dan komputer yang Anda miliki. Perubahan dalam bentuk digitalisasi mengakibatkan sebuah bisnis harus membangun suatu sistem yang efisien serta efektif untuk kebutuhan internal maupun eksternal perusahaan. Digitalisasi bisnis tersebut akhirnya juga dapat membuat suatu perusahaan menerapkan kebijakan baru terkait keamanan data.

Dahulu, penyimpanan data dilaku kan dengan cara tradisional, yaitu dengan cara menyimpan kertas data kedalam brankas maupun lemari arsip, kemudian evolusi digital mulai terjadi dengan metode penyimpanan data pada *hard drive* seperti hard disk, flashdisk, dan lain sebagainya. Namun, saat ini metode serta media penyimpanan data tersebut sudah dianggap tidak aman, hal ini dikarenakan, media penyimpanan tersebut tidak menawarkan sisi fleksibilitas yang saat ini justru sangat dibutuhkan oleh suatu perusahaan dalam menyimpan data maupun informasi yang dimilikinya.

Migrasi data ke sistem cloud juga menjadi penanda bahwa era industri digitalisasi telah dimulai. Data yang disimpan pada sistem cloud lebih mudah diakses serta mudah dalam pengelolaannya. Data cloud juga dapat diakses oleh user yang memiliki akses tersebut dimanapun dan kapanpun asal terkoneksi dengan jaringan internet. Hal-hal konvensional lain seperti tempat dan waktu

sudah bukan penghalang bagi suatu bisnis yang ingin mengakses dan mengolah data-datanya. Namun kemudahan serta fleksibili tas cloud ini sering dianggap lawan dari sisi keamanan itu sendiri. Pada dasarnya sistem cloud didesain tidak hanya meng-unakan satu layer kemanan, melainkan berlapis-lapis mulai dari tier 1 hingga tier 3 bahkan lebih. Kelebihan inilah yang mengakibatkan cloud dipercaya karena fleksibilitas serta keamanannya yang terjaga.

Keamanan yang terjaga dan dapat diandalkan ini merupakan keharusan layanan *cloud* agar mendapat kepercayaan dari konsumen. Garansi *less down time serta lokasi* data center yang aman serta strategis, dan tentunya server yang aman merupakan tanggung jawab yang harus dimiliki oleh perusahan provider cloud, dimana tujuan- nya adalah supaya data-data yang tersimpan pada sistem cloud terhindar dari resiko-resiko yang dapat mengakibatkan data hilang atau rusak. Setelah semua persyaratan terpenuhi, pertanyaan lain yang muncul adalah bagaimana tentang bencana yang tiba-tiba atau tidak dapat diprediksi? Bagaimana cara mengatasi bencana serta merencanakan *Disaster Recovery Plan (DRP) Plan (DRP)* yang baik dan tepat? Apakah setiap perusahaan harus memiliki *Disaster Recovery Plan*? Apakah layanan *Disaster Recovery Plan* termasuk kedalam layanan yang disediakan oleh sebuah perusahaan provider cloud?

Melalui sistem informasi yang telah dibuat dengan berkualitas baik secara tepat, akurat dan cepat atau yang menurut W Kumurotomo dan Agus Margono, harus memenuhi syarat yaitu ketersediaan, mudah dipahami, relevan, bermanfaat, tepat waktu, keandalan, akurat dan konsiten dalam perencanaan DRP dan DRC, maka akan sangat bermanfaat bagi Pemerintah dalam pembuatan konsep kebijakan di bidang pertahanan nasional [14].

KESIMPULAN

Indonesia sebagai negara yang terletak di wilayah rawan bencana perlu memperkuat ketahanan nasional di bidang pencegahan, penanggulangan dan pemulihan bencana diantaranya melalui implementasi konsep *Disaster Recovery Plan (DRP).* Melalui penerapan konsep ini diharapkan semua pihak, termasuk pemerintah daerah yang daerahnya termasuk dalam rawan bencana alam dapat meningkatkan kesiapsiagaan dalam rangka menghadapi potensi bencana alam yang dapat datang secara tiba-tiba.

DRP adalah salah satu upaya untuk memadukan perkembangan teknologi informasi dengan pengelolaan masalah bencana alam. Bencana alam yang berpotensi merusak sarana dan prasarana, termasuk tempat penyimpanan data dan informasi krusial, dapat diantisipasi dengan membuat rencana pemulihan melalui pemanfaatan teknologi informasi.

Prinsipnya, data merupakan hal yang sangat krusial bagi keberlangsungan pemerintahan di dalam pembuatan konsep kebijakan, sehingga sudah sewajarnya pemerintah memberikan perlindungan yang baik serta dapat melakukan pemulihan kembali operasional pengolahan data tanpa kehilangan data berharga jika terjadi suatu bencana (*disaster*). Untuk itulah Pemerintah harus mempersiapkan *Disaster Recovery Center* dan memberikan suatu kerangka kerja yang disebut *Disaster Recovery Plan* untuk membuat suatu skema skenario pelaksanaan penanggulangan bencana.

Meningkatnya bencana alam merupakan bentuk ancaman nyata terhadap ketahanan nasional, selain itu bencana alam juga mempengaruhi kehidupan sosial ekonomi masyarakat, namun dengan tingginya risiko tersebut juga tidak diimbangi dengan kesiapan, termasuk kecepatan dan keakuratan yang mumpuni terhadap suatu sistem informasi yang dapat berpengaruh terhadap pembuatan kebijakan keamanan dan ketahanan nasional.

Dari hasil analisis bagaimana pengaruh kebencanaan dapat berpengaruh terhadap suatu kebijakan ketahanan nasional, Pemerintah dipandang perlu segera melaksanakan penyusunan *Disaster Recovery Plan* (DRP) dan pembangunan *Disaster Recovery Center* (DRC) yang terintegrasi dan akurat dalam *big data*, mengingat Rencana Pemerintah Jangka Panjang Nasional (RPJPN), telah dicanangkan bahwa *e-government* agar dapat terimplementasi dengan baik di Indonesia sesuai dengan perkembangan zaman saat ini. Dari penelitian ini dapat memberikan gambaran umum tentang bagaimana membangun sistem informasi DRP dan DRC agar dapat memperkuat dalam pembuatan kebijakan ketahanan Nasional.

DAFTAR PUSTAKA

[1] Agus, A. A. (2015). Urgensi Ketahanan Nasional Sebagai Geostrategi Indonesia. Jurnal Integrasi PIPS Pascasarjana UNM, 1(2), 247–257.

[2] Badan Nasional Penanggulangan Bencana (2016). *Risiko Bencana Indonesia*. Jakarta: Tim Penyusun.

[3] Béné, C., et al. (2012) Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes. IDS Working Papers, 2012, 1-61

[4] Carlson, S.J., & D.J. Parker. (1998). Disaster Recovery Planning and Accounting Information Systems, *Review of Business.*

[5] Christian, F. (2015). Membangun Data Recovery Center/Disaster Recovery Center. Dokumen tidak dipublikasikan.

[6] Cutter, S. L., Ahearn, J. A., Amadei, B., Crawford, P., Eide, E. A., Galloway, G. E., Goodchild, M. F., Kunreuther, H. C., Li-Vollmer, M., Schoch-Spana, M., Scrimshaw, S. C., Stanley, E. M., Whitney, G., & Zoback, M. L. (2013). Disaster Resilience: A National Imperative. Environment: Science and Policy for Sustainable Development, 55(2), 25–29. https://doi.org/10.1080/00139157.2013.768076

[7] Fadilah, R., & Djumhadi. (2011). *Optimasi Protocol Open Shortest Path First pada Disaster Recovery Data Center*. Seminar Nasional Informatika 2011, 1(7), 37-43.

[8] Jati, R., & Amri, Mohd. R. (Eds.). (2016). Risiko Bencana Indonesia (RBI). Badan Nasional Penanggulangan Bencana (BNPB) RI. http://inarisk.bnpb.go.id/pdf/Buku%20RBI_Final_low.pdf

[9] Prihatin, R. B. (2018). Masyarakat Sadar Bencana: Pembelajaran Dari Karo, Banjarnegara, Dan Jepang. Aspirasi: Jurnal Masalah-Masalah Sosial, 9(2). https://doi.org/10.22212/aspirasi.v7i1.1084

[10] Putri, S.W. (2008). *Pembangunan disaster recoveryplan untuk sistem informasi manajemen terintegrasi*. Bandung: ITB, Tugas Akhir.

[11] Toigo, J.W. (1989). *Disaster Recovery Planning,Managing Risk & Catastrophe in Information Systems*. Yourdon Press Computing Series, Prentice Hall,Inc.

[12] Soepandji, K. W., & Farid, M. (2018). Konsep Bela Negara Dalam Perspektif Ketahanan Nasional. Jurnal Hukum & Pembangunan, 48(3), 436–456. https://doi.org/10.21143/jhp.vol48.no3.1741

[13] Somasundaram, G., & Alok Shrivastava. (2009). *Information Storage and Management: Storing,*

Managing, and Protecting Digital Information. Wiley.

[14] W. Kumurotomo dan Agus S. Margono. (1994). *Sistem Informasi Menejemen dalam Organisasi Publik.* Fisipol UGM. Gadjahmada University Press 1994

[15] Yoon, D. K., Kang, J. E., & Brody, S. D. (2015). A measurement of community disaster resilience in Korea. Journal of Environmental Planning and Management, 436–460. https://doi.org/10.1080/09640568.2015.1016142

.