CESS (Journal of Computer Engineering System and Science) **p-ISSN :2502-7131**
Vol. 3 No. 2 Juli 2018 **e-ISSN :2502-714x**

RANCANGAN DOKUMEN *DISASTER RECOVER* PLAN PADA IS/ITDI DINAS XYZ

Zanuar Rifai[1], Andini Maydina[2], Arief Adhy Kurniawan[3]
[1,2]Sistem Informasi STMIK AMIKOM Purwokerto
Jl. Letjen Pol Sumarto Watumas Purwanegara Purwokerto, 53123Indonesia
[3]Teknik InformatikaSTMIK AMIKOM Purwokerto
Jl. Letjen Pol Sumarto Watumas Purwanegara Purwokerto, 53123Indonesia
zanuar.rifai@amikompurwokerto.ac.id[1], amaydinaa@gmail.com[2], ariefadhykurniawan@gmail.com[3]

Abstrak—**Tidak beroperasinya sistem informasi akibat kerusakan dan bencana sangat mempengaruhi proses bisnis dari sebuah Instansi. Tidak terkecuali instansi pemerintah Dinas XYZ Kabupaten Banyumas. Sehingga, Tindakan untuk memulihkan kembali sistem informasi yang tidak dapat beroperasi akibat kerusakan, dan kegagalan akibat bencana sangat diperlukan. Di sisi lain instansi Dinas XYZ Kabupaten Banyumas belum memiliki sebuah dokumen perencanaan pemulihan akibat bencana. Dokumen perencanaan pemulihan bencana adalah sebuah dokumen yang menjelaskan setiap prosedur yang harus dilakukan oleh sebuah institusi ketika menghadapi bencana sehingga dapat menyelamatkan aset pada sektor yang dimiliki sistem informasi pada Dinas XYZ Kabupaten Banyumas. Pada penelitian ini kami mengusulkan perancangan dokumen pemulihan akibat bencana yang disesuaikan dengan karakteristik Dinas XYZ Kabupaten Banyumas. Untuk mengetahui tingkat keberhasilan perancangan dokumen pemulihan akibat bencana kami melakukan pengujian dokumen tersebut dengan standar NIST SP 800-34. Berdasarkan hasil pengujian yang telah dilakukan, tindakan pemulihan terhadap masalah yang terjadi bisa dilakukan dengan yang lebih cepat.**

Kata Kunci: ***Disaster Recovery Plan, NIST SP 800-34 Rev.1, Sistem Informasi.***

Abstract—**The malfunction of the information system due to damage and disaster greatly affect the business process of an agency. No exception government agencies XYZ Banyumas District. Thus, Actions to restore information systems that can not operate due to damage, and catastrophic failure are necessary. On the other hand, the Banyumas District Office of XYZ does not have a disaster recovery planning document. Disaster recovery planning document is a document that explains every procedure that an institution must take when facing a disaster so as to save assets in the sector owned by the information system at Banyumas District XYZ Office. In this study we propose the design of disaster recovery documents that are tailored to the characteristics of Banyumas District XYZ Office. To determine the success rate of disaster recovery document design we have tested the document with NIST SP 800-34 standard. Based on the results of tests that have been done, the recovery action to the problems that occur can be done with a faster.**

Keywords: ***Disaster Recovery Plan, NIST SP 800-34 Rev.1, Information System***

I. PENDAHULUAN

Dalam meningkatkan nilai usaha, sebuah Instansi harus mempunyai sumber daya yang strategis salah satu sumber daya yang strategis adalah informasi, karena informasi adalah aset yang sangat krusial berharga bagi sebuah Instansi. Maka dari itu segenap jajaran, pemilik, manajemen dan karyawan wajib untuk melindungi *Information System/Information Technology* (IS/IT) secara sunggung-sungguh karena merupakan syarat mutlak perusahaan atau instansi yang bersangkutan[1][2][3]. Banyak Instansi atau perusahaan yang bergantung pada IS/IT untuk mendukung operasi bisnisnya sehari-hari termasuk didalam sektor pemerintahan. Dinas XYZ Kabupaten Banyumas merupakan instansi milik pemerintah yang dalam pelaksanaan tugas dan pekerjaannya tidak dapat lepas dari penggunaan IS/IT.

Perlindungan dilakukan padaIS/IT yang ada didalam perusahaan atau Instansi dari kejadian yang tak terduga seperti bencana baik bencana alam maupun non-alam yang dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup Instansi[3].

Bencana yang terjadi dapat berdampak langsung maupun tidak langsung terhadap operasional sebuah organisasi atau instansi. Organisasi atau instansi harus siap menghadapi dampak yang terjadi akibat bencana tersebut, dampak bencana tersebut sangat bervariasi seperti terhentinya jaringan komputer, terhentinya layanan IS/IT, terhentinya aliran listrik, supplier yang menghentikan supply produknya, ketidakhadiran pegawai, rusaknya fasilitas umum, keterlambatan pembayaran gaji dan lain sebagainya[4].

Indonesia merupakan kategori negara dengan risiko terjadinya bencana alam sangat besar, indonesia

dalam posisi paling tinggi dalam peta rawan bencana. Bencana tersebut adalah gempa bumi, tsunami, tanah longsor dan letusan gunung berapi(BNPB, 2012). Selain bencana alam serangan hacker (DDoS, Web Deface, Virus, SQL Injection), Power Loss,Bandwidth Loss, Kehilangan Data, Human error juga berpotensi pada rusaknya peralatan yang dapat menimbulkan terhentinya suatu layanan IS/IT sehingga berdampak pada kerugian terhadap suatu institusi/perusahaan[5].

Perlu dibuatkan sebuah mekanisme penangan bencana yang mampu mengatasi dampak dari kerusakan bencana baik itu bencana alam dan kerusakan akibat perbuatan manusia. Karena itu perlu dibuatkan sebuah mekanisme untuk meminimalisir kerugian akibat bencana tersebut[6].

Adalah perencanaan pemulihan bencana yang merupakan dokumen yang memuat proses, kebijakan dan mekanisme yang berhubungan dengan persiapan pemulihan atau keberlangsungan infrastruktur teknologi yang kritis bagi Instansi atau perusahaan setelah terjadinya bencana, baik bencana yang disebabkan oleh tindakan manusia ataupun bencana alam[7][8]. Selain itu *Disaster Recovery Plan* merupakan bagian perencanaan dari sebuah institusi untuk melakukan tahapan tertentu yang nantinya akan menjamin kelangsungan pelayanan (khususnya dari segi IS/IT) yang diberikan tanpa mengurangi kapabilitas serta kinerja dari sebuah sistem jika terjadi sebuah bencana didalamnya. Faktor yang terpenting dalam sebuah *Disaster Recovery Plan* (DRP) adalah dari sisi corporate office. Karakteristik tiap orang, budaya Instansi serta tipe kepemimpinan dari sebuah Instansi sangatlah berpengaruh terhadap penyusunan serta implementasi dari *Disaster Recovery Plan*[9][10].

Pada paper ini kami membahas tentang perancangan *Disaster Recovery Plan*pada Dinas XYZ Kabupaten Banyumas. Dalam pembahasannya, paper ini dibagi menjadi beberapa bagian. Bagian 1 adalah pendahuluan. Metode penelitian akan dibahas pada bab 2. Bab 3 menjelaskan hasil dan pembahasan, sedangkan kesimpulan akan disajikan pada bab 4.

II. METODE PENELITIAN

A. Observasi.

Didalam pembuatan prosedur *Disaster Recovery Plan* diperlukan data-data pendukung untuk prosedur *Disaster Recovery Plan* tersebut sehingga sesuai dengan IS/IT di Dinas XYZ Kabupaten Banyumas. Metode Observasi merupakan suatu metode untuk pengumpulan data dengan cara melakukan pengamatan secara langsung terhadap kondisi IS/IT di Dinas XYZ Kabupaten Banyumas[11]. Dari hasil pengamatan secara langsung tersebut, nantinya didapatkan suatu data yang digunakan sebagai acuan untuk pembuatan prosedur *Disaster Recovery Plan*.

Adapun data yang diperoleh dari hasil observasi IS/IT adalah sebagai berikut data bencana yang pernah terjadi terhadap IS/IT, data perangkat IS/IT baik perangkat keras maupun perangkat lunak. Dari data hasil observasi tersebut digunakan sebagai pembobotan untuk mendapatkan nilai yang digunakan sebagai atribut didalam menentukan potensi yang ditimbulkan dari suatu bencana.

B. Studi dokumentasi

Pada tahap studi dokumen ini, melakukan pengumpulan data melalui pencarian dan penemuan bukti-bukti yang tidak langsung ditujukan pada subjek penelitian, namun melalui dokumen. Pada penelitian tentang *Disaster Recovery Plan*dokumen yang digunakan adalah dokumen tentang IS/ITdan topologi jaringan komputer di Dinas XYZ Kabupaten Banyumas. Didalam penelitian ini, data dari hasil dokumentasi sangat penting untuk analisa dan pembahasan lebih lanjut tentang prosedur *Disaster Recovery Plan*[11].

C. Wawancara

Wawancara merupakan suatu teknik pengumpulan data dengan mengajukan pertanyaan secara langsung oleh pewawancara (pengumpuldata) kepada responden dengan dicatat, ditulis atau diketik untuk jawaban responden[11]. Pada tahap teknik wawancara ini, dilakukan secara langsung di kampus Dinas XYZ Kabupaten Banyumas pada bagian IT khususnya yang menangani IS/IT. Pada bagian yang berwenang mengelola IS/IT akan diajukan beberapa pertanyaan untuk proses wawancara terkait dengan pengumpulan data untuk pembangunan Prosedur *Disaster Recovery Plan* terhadap IS/IT di Dinas XYZ Kabupaten Banyumas.

D. Framework & Metode Analisa Data

Dalam membuat rancangan dokumen perancangan *Disaster Recovery Plan* ini, kerangka kerja yang digunakan adalah NIST SP 800-34 memuat prosedur-prosedur antara lain kontrol pencegahan, strategi dan rencana kontigensi. Faktor utama yang dibutuhkan dalam perancangan *Disaster Recovery Plan* yaitu strategi yang digunakan untuk pemulihan aset IS/IT, penentuan teknologi pada masing-masing IS/IT, dan sumber daya manusia yang melaksanakan kegiatan [12].

Untuk memastikan rancangan dokumenRecovery Plan dapat diimplementasikan dengan baik, perlu tim *Disaster Recovery Plan* yang memiliki tugas yang sesuai dengan kemampuan yang dimiliki oleh masing-masing anggota. Perlu juga diperhatikan kondisi dan karakteristik yang dimiliki oleh oleh instansi yaitu instansi Dinas XYZ Kabupaten Banyumas ketika membentuk tim tersebut.

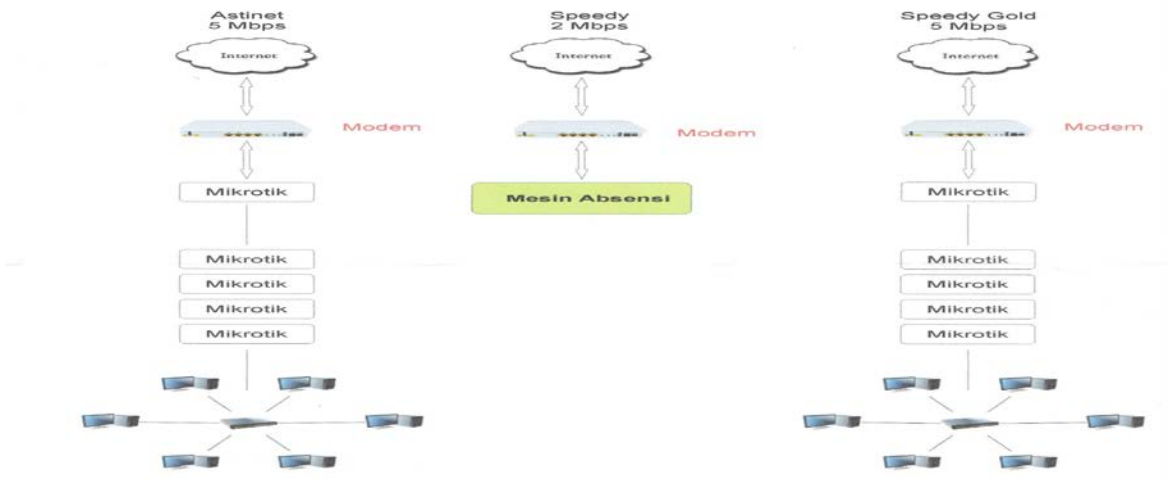
III. HASIL DAN PEMBAHASAN

A. Skema Jaringan IS/IT

Dinas XYZ Kabupaten Banyumas merupakan instansi pemerintah yang memanfaatkan IS/IT selama menjalankan kegiatan operasionalnya sehari-hari. Dengan mengimplementasikan IS/IT pada Dinas XYZ

Kabupaten Banyumas maka diperlukan infrastruktur jaringan komputer untuk mengintegrasikan IS/IT yang digunakan. Pada tahun 2012 server pada Dinas XYZ Kabupaten Banyumas terkena petir yang mengakibatkan rusaknya 36 Komputer pada Dinas XYZ Kabupaten Banyumas[13]. kerusakan yang diakibatkan oleh suatu bencana baik itu bencana alam maupun akibat dari manusia perlu dibuat sebuah prosedur manajemen resiko yang mampu memitigasi resiko tersebut[14]. Oleh karena itu *Disaster Recovery Plan* (DRP) merupakan dokumen yang wajib dimiliki oleh instansi salah satunya adalah inas XYZ Kabupaten Banyumas untuk meminimalisir kerugian dan kerusakan akibat bencana tersebut.

Berikut skema dari jaringan komputer pada Dinas XYZ Kabupaten Banyumas:



Gbr. 1 Skema Jaringan Komputer pada Dinas XYZ Kabupaten Banyumas[15]

B. Sistem Informasi XYZ

Dalam menjalankan kegiatan operasionalnya sehari-hari, Dinas XYZ Kabupaten Banyumas menggunakan beberapa sistem informasi antara lain:

1) Sistem Informasi Manajemen Absensi Pegawai (SIMAP)
2) Sistem Informasi Pengelolaan Website dan Sub-Domain (SIWEDO).
3) Sistem Informasi Analisis Jabatan dan Evaluasi Jabatan (Si ANA)
4) Banyumas Mail (Email) merupakan akun surel Instansi Perangkat Desa (OPD)
5) PPDB Online.
6) Pengelolaan Calon Peserta Ujian Sekolah Madrasah (USM) atau UN.
7) Satria Keuangan
8) Simbada Mas

C. Risk Assesment

Risk Assesment pada tahan ini berfokus pada ancaman yang dapat mempengaruhi aset-aset instansi yang ada hubungannya dengan pelaksanaan pelayanan publik[16]oleh Dinas XYZ Kabupaten Banyumas. Risk Assessment diperlukan untuk dapat menentukan klasifikasi dampak dan penyebab terjadinya gangguan atau bencana yang mungkin terjadi dan berguna dalam penentuan langkah-langkah yang optimaluntuk memitigasi risiko yang terjadi.

Risiko yang terjadi pada gedung baik secara menyeluruh atau hanya sebagian dapat merusak dan menghancurkan aset-aset tersebut, misalnya pemadaman listrik berkepanjangan, gempa bumi, banjir, kebakaran, gunung meletus, kerusakan server, serangan virus, dan lain-lain. Menurut data yang diperoleh dari wawancara dengan Kasubbag Umum dan Kepegawaian Dinas XYZ Kabupaten Banyumas, pernah terjadi sambaran petir pada server Dinas XYZ Kabupaten Banyumas yang mengakibatkan rusaknya 36 komputer pada Dinas XYZ Kabupaten Banyumas.

Tahap Risk Assessment ini merupakan tahap pertama dari prosedur *Disaster Recovery Plan*. Risk Assessment digunakan untuk menentukan ancaman apa saja yang berpotensi menimbulkan risiko terhadap aset-aset yang ada di Dinas XYZ Kabupaten Banyumas. Berikut penjabaran mengenai ancaman yang dapat menimbulkan risiko beserta data mengenai kerentanan, aset penting serta konsekuensi dari ancaman yang terjadi:

TABEL I
RISK ASSESSMENT[13]

No.	Ancaman	Ancaman yang terjadi	Kerentanan	Aset Kritis	Konsekuensi
1	Petir	Sambaran petir dapat	Petir dapat mengenai	Aset-aset	a. Berhentinya

No.	Ancaman	Ancaman yang terjadi	Kerentanan	Aset Kritis	Konsekuensi
		menyebabkan rusaknya jaringan listrik atau LAN serta alat-alat elektronik	*server* yang menyebabkan kerusakan pada aset Instansi	perkantoran dan Gedung	kegiatan operasional b. Rusaknya jaringan listrik atau LAN serta alat-alat elektronik
2	Banjir	Banjir dapat menimbulkan kerusakan sarana dan prasarana kantor	Kerusakan yang terjadi pada sarana dan prasarana akibat banjir	Aset-aset perkantoran, Gedung dan karyawan	a. Ketidakhadiran pegawai b. Sistem komputer dan komunikasi terpaksa dihentikan
3	Gempa bumi	Gempa bumi dapat merusak infrastruktur yang ada pada gedung jika melebihi kekuatan 5 dalam skala richter	Infrastruktur terletak pada gedung yang hanya tahan gempa sampai 5 skala richter	Aset-aset perkantoran dan Gedung	Terhentinya kegiatan operasional instansi
4	Gunung meletus	Lava dan abu dari gunung meletus dapat mengganggu dan bahkan menghentikan kegiatan operasional	Lava dan abu dari gunung berapi menyebabkan seluruh pegawai harus dievakuasi dan kegiatan operasional terhenti	Aset-aset perkantoran, Gedung dan karyawan	a. Ketidakhadiran pegawai b. Terhentinya kegiatan operasional instansi
5	Kebakaran	a. Timbulnya api b. Akibat dari hubungan arus pendek aliran listrik atau yang lainnya	a. Gedung dapat terbakar atau menjadi bagian dari kebakaran b. Adanya material yang mudah terbakar pada setiap ruangan dan gedung	Gedung dan aset kantor	Terhentinya kegiatan operasional instansi
6	Listrik mengalami gangguan	a. Kehilangan daya sehingga menyebabkan beberapa perangkat tidak bisa diakses b. Tegangan tidak stabil menyebabkan kerusakan pada perangkat keras	Peralatan yang membutuhkan aliran listrik tidak berfungsi sebagaimana mestinya	Komputer, aset kantor dan peralatan kantor	Kerusakan alat-alat listrik dan jaringan
7	*Serverdown*	*Server* mengalami kerusakan dan mengakibatkan *down*	*Server* mengalami kerusakan dan mengakibatkan *down* sehingga tidak bisa diakses oleh pengguna	Informasi, komputer	Kerusakan *server*
8	Serangan *worm, malware, virus* dan sejenisnya	a. Serangan *worm, malware, virus* dan sejenisnya yang mencoba mencari *bugs* pada *operating system* dan atau aplikasi b. *Worm, malware, virus* dan sejenisnya melalui proses mengirim dan menerima surel	a. aplikasi dan system operasi memiliki celah keamanan. b. lampiran pada surel dapat disisipi oleh virus	Informasi	Kehilangan data
9	*Cyber threat*	Adanya lubang keamanan pada system jaringan komputer oleh *cracker* untuk masuk	Penyalahgunaan akun karena penggunaan *password* yang lemah	Informasi, reputasi	a. Bocornya informasi rahasia b. Rusaknya reputasi

Dari jenis ancaman yang terdapat pada tabel 1, ancaman seperti server down, virus, dan cyber threat dapat mengancam IS/IT yang ada pada Dinas XYZ Kabupaten Banyumas. Setelah didapatkan data mengenai ancaman yang dapat terjadi, selanjutnya data

tersebut digunakan sebagai acuan untuk tahap analisa dampak Business Impact Analysis (BIA).

D. Business Impact Analysis (BIA)

Business Impact Analysis atau analisis dampak bisnis merupakan tahapan dalam pembuatan *Disaster Recovery Plan* (DRP) yang dilakukan untuk mengetahui proses bisnis mana yang merupakan proses bisnis yang vital dalam Instansi dan juga untuk mengetahui dampak yang akan dialami oleh Instansi jika terjadi gangguan atau bencana pada IS/IT yang menunjang proses bisnis tersebut[16]. Selain itu BIA juga digunakan untuk mengambil suatu keputusan manajemen atas Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) untuk masing-masing fungsi bisnis atau proses layanan.

Business Impact Analysis (BIA) bertujuan untuk membantu suatu Instansi didalam memahami dampak yang diakibatkan dari suatu bencana yang tidak diharapkan, misalnya infrastruktur jaringan komputer down sehingga layanan tidak bisa digunakan baik untuk akses informasi maupun layanan email, IS/IT dan lain sebagainya. Sehingga diperlukan periode waktu yang bisa ditoleransi jika suatu layanan sistem lumpuh.

Maping layanan IS/IT dapat dilakukan untuk mengetahui layanan apa saja yang diberikan oleh sebuah IS/IT dalam melakukan pelayanan baik kepada internal instansi ataupun kepada masyarakat. Maping layanan sistem informasi ini dapat dilihat pada tabel 2.

TABEL II
MAPING LAYANAN SISTEM INFORMASI

No.	Sistem Informasi	Layanan
1	SIMAP	Manajemen absensi pegawai
2	SIWEDO	a. Media informasi b. Pengaduan masyarakat
3	Banyumas Mail	Manajemen email Instansi Perangkat Daerah (OPD)
4	Si ANA	Analisis dan evaluasi jabatan
5	PPDB Online	Pendaftaran peserta didik baru online
6	Pengelolaan Capes USM/UN	Pendataan peserta Ujian Sekolah Madrasah atau Ujian Nasional
7	Satria Keuangan	Pengelolaan transaksi keuangan Dinas XYZ Kabupaten Banyumas, UPK, SKB dan sekolah
8	Simbada Mas	Pengelolaan aset Dinas XYZ Kabupaten Banyumas, UPK, SKB dan sekolah

Dinas XYZ Kabupaten Banyumas merupakan instansi pemerintahan yang mempunyai tugas melaksanakan operasional pemerintahan daerah secara teknis yang bergerak dalam bidang XYZ, tahapan berikutnya adalah menentukan IS/IT yang mempunyai tingkat kritis tinggi, sedang dan rendah berdasarkan peraturan dan tingkat reputasi instansi tersebut.

Berdasarkan wawancara yang telah dilakukan mengenai penentuan tingkat kritis suatu sistem informasi atau layanan yang ada pada Dinas XYZ Kabupaten Banyumas berdasarkan pada banyaknya masyarakat yang merasakan dampak dari sistem informasi atau layanantersebut. Berikut merupakan kategori tingkat dampak gangguan atau bencana terhadap bisnis, yaitu:

a. Tinggi

Sistem informasi mempunyai dampak dan efek samping yang signifikanterhadap instansi dan keberlangsungan sebuah organisasi selain itu berdampak juga pada pihak luar atau pengguna system yang ada hubungannya dengan masyarakat luas.

b. Sedang

IS/IT mempengaruhi aktivitas utama setiap unit kerja pada sebuah instansi dan juga mempunyai dampak serius terhadap instansi. selain itu berdampak pada hubungan dengan pihak luar instansi dalam lingkup kecil seperti instansi pemerintah diluar Instansi.

c. Rendah

Sistem informasi hanya berdampak pada kegiatan penunjang instansi atau hanya digunakan dalam lingkup internal dalam skala kecil instansi.

Selanjutnya, hasil analisis dampak bisnis dapat dilihat pada Tabel 3 Analisis dampak bisnis menggunakan Tabel 1 sebagai acuan. Pada Tabel 3 ini dijelaskan dampak seperti apa yang akan didapat apabila IS/IT yang ada pada Dinas XYZ Kabupaten Banyumas mengalami gangguan atau down. Juga dijelaskan mengenai tingkat dampak yang ditimbulkan terhadap bisnis.

TABEL III
PEMETAAN LAYANAN IS/IT

No.	Sistem Informasi (SI)	Dampak yang dialami jika SI down	Tingkat dampak
1	SIMAP	Informasi absensi pegawai tidak dapat diketahui	Sedang
2	SIWEDO	Pengguna tidak bisa mengakses informasi mengenai Dinas XYZ Kabupaten Banyumas, dan reputasi Dinas XYZ Kabupaten Banyumas akan dipertanyakan	Sedang
3	Banyumas Mail	Layanan email tidak bisa digunakan, sehingga para pegawai tidak dapat mengirim email menggunakan email dinas	Rendah
4	Si ANA	Tidak dapat melihat dan merubah data pegawai sehingga tidak bisa melakukan analisis dan evaluasi	Sedang
5	PPDB Online	Pelayanan kepada calon peserta didik baru tertunda	Tinggi
6	Pengelola	Pengguna tidak bisa	Tinggi

	an Capes USM/UN	melihat data dan melakukan pendataan peserta USM atau UN	
7	Satria Keuangan	Tidak bisa menginput laporan pelaksanaan transaksi keuangan	Sedang
8	Simbada Mas	Kegiatan pengelolaan aset tidak dapat dilakukan	Sedang

Menentukan Recovery Point Objective (RPO) dan Recovery Time Objective (RTO) dari setiap layanan IS/IT adalah tahapan selanjutnya untuk menganalisa dampak bisnis. Recovery Time Objective (RTO) merupakan waktu yang tersedia untuk memulihkan sistem dan sumber daya yang terganggu, sedangkan Recovery Point Objective (RPO) adalah banyaknya jumlah kehilangan data yang dapat ditoleransi oleh sistem bisnis kritis Instansi[16]. Untuk menentukan Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) pengambilan datanya melalui wawancara langsung dengan penanggung jawabIS/IT pada instansi tersebut, hasil dari data tersebut ditampilkan ada pada Tabel 4

TABEL IV
IDENTIFIKASI RECOVERY TIME OBJECTIVE DAN RECOVERY POINT OBJECTIVE

No.	Sistem Informasi	Recovery Time Objective	Recovery Point Objective	Tingkat Dampak
1	SIMAP	1-7 jam	1-7 jam	Sedang
2	SIWEDO	1-7 jam	1-7 jam	Sedang
3	Banyumas Mail	1-7 jam	1-7 jam	Rendah
4	Si ANA	1-7 jam	1-7 jam	Sedang
5	PPDB Online	14-24 jam	14-24 jam	Tinggi
6	Pengelolaan Capes USM/UN	12-24 jam	14-24 jam	Tinggi
7	Satria Keuangan	14-24 jam	14-24 jam	Sedang
8	Simbada Mas	14-24 jam	14-24 jam	Sedang

Tahapan terakhir dalam proses analisa ini adalah menentukan IS/IT yang prioritas pada Dinas XYZ Kabupaten Banyumas. Dalam menentukan prioritas IS/IT dilakukan dengan cara mengolah hasil dari analisis dampak risiko terhadap bisnis Instansi dan penentuan nilai Recovery Time Objective dan Recovery Point Objective dari masing-masing IS/IT.

IS/IT yang mempunyai prioritas tertinggi Dinas XYZ Kabupaten Banyumas adalah pengelolaan Capes USM/UN karena sebagai sistem tersebut merupakan sistem penunjang pelayanan ke sekolah atau madrasah. Selain itu sistem ini juga menyimpan data mengenai calon peserta ujian. Setelah itu PPDB Online yang dimiliki oleh Dinas XYZ Kabupaten Banyumas, karena juga berhubungan dengan pelayanan kepada sekolah atau madrasah. Kedua IS/IT ini juga dipegang dan dijalankan oleh pihak ketiga yaitu dari Dinas XYZ Provinsi Jawa Tengah.

Selanjutnya Satria Keuangan menjadi prioritas berikutnya karena sistem ini merupakan sistem pengelolaan transaksi keuangan pada Dinas XYZ Kabupaten Banyumas, UPK, SKB dan sekolah. Simbada Mas menjadi prioritas selanjutnya karena berhubungan dengan pengelolaan aset-aset yang ada pada Dinas XYZ Kabupaten Banyumas. SIMAP menjadi prioritas selanjutnya karena berhubungan dengan manajemen absensi pegawai. Jika terjadi gangguan pada sistem ini maka informasi mengenai absensi pegawai tidak akan diketahui.

SIWEDO menjadi prioritas IS/IT berikutnya, karena sistem ini adalah media informasi kepada masyarakat. Si ANA menjadi prioritas IS/IT selanjutnya karena sistem ini menyediakan data pegawai beserta jabatannya. Kalau sistem ini terganggu, maka kegiatan analisis dan evaluasi tidak dapat dilakukan. Lalu urutan prioritas terakhir adalah Banyumas Mail. Banyumas Mail ini digunakan sebagai manajemen email OPD. Apabila sistem ini terganggu maka para pegawai tidak bisa mengirimkan email melalui email dinas dan para pegawai masih bisa menggunakan layanan email selain email dinas seperti layanan email dari google dan yahoo yang keamanannya masih rentan. Selanjutnya penentuan prioritas IS/IT mengikuti hasil penilaian risiko dan penentuan dampak terhadap Instansi disajikan pada Tabel 5

TABEL V
PRIORITAS PEMULIHAN SISTEM INFORMASI

Prioritas	Sistem Informasi	Urutan Prioritas
Tinggi	Pengelolaan Capes USM/UN	1
Tinggi	PPDB Online	2
Sedang	Satria Keuangan	3
Sedang	Simbada Mas	4
Sedang	SIMAP	5
Sedang	SIWEDO	6
Sedang	Si ANA	7
Rendah	Banyumas Mail	8

E. Startegy Recovery

Strategy Recovery merupakan proses untuk melakukan pemulihan ketika terjadi suatu kegagalan pada sistem. Didalam melakukan proses Recovery terdapat beberapa hal yang perlu diketahui seperti penyediaan fasilitas baik perangkat keras maupun perangkat lunak yang berguna untuk pemulihan layanan. Dari hasil Risk Assessment dan Business Impact Analysis dapat diambil jenis-jenis ancaman yang mampu menjadi acuan untuk melakukan proses recovery. Untuk menentukan proses strategi pemulihan (strategy recovery) perlu

mempertimbangkan lingkup kerusakan yang disebabkan oleh gangguan atau bencana.

Ancaman terhadap IS/IT dapat dilihat dari atribut-atribut ancaman pada Risk Assessment yang memerlukan suatu strategi pemulihan. Berikut ini tabel proses pemulihan terhadap sistem informasi pada Dinas XYZ Kabupaten Banyumas.

TABEL VI
PROSES PEMULIHAN SISTEM INFORMASI

No.	Gangguan	Kendala	Proses *Recovery*
1	*Server down*	*Server* mengalami kerusakan dan mengakibatkan *down*, sehingga tidak bisa diakses oleh pengguna	Diganti dengan menggunakan *server* cadangan
2	Listrik mengalami gangguan	a. Kehilangan daya menyebabkan beberapa perangkat tidak bisa diakses b. Tegangan tidak stabil menyebabkan kerusakan pada perangkat keras	Menambah perangkat UPS untuk mencegah perangkat mati secara tiba-tiba dan menyebabkan kerusakan parah
3	Sistem terinfeksi virus	a. Sistem operasi menjadi lambat b. Beberapa file hilang karena diduplikat oleh virus	a. Menggunakan anti virus dan melakukan *scanning* secara rutin b. Melakukan *repair* terhadap sistem informasi
4	*Cyber threat*	a. Terdapat celah keamanan pada jaringan komputer b. Bocornya informasi rahasia yang diambil oleh *hacker*	a. Penggunaan *password* yang kuat dengan kombinasi huruf dan angka b. Pergantian *password* secara rutin
5	SIMAP	a. Sistem informasi mengalami error dan informasi absensi pegawai tidak bisa diakses b. Database mengalami error sehingga tidak bisa diakses	a. Melakukan pengecekan didalam *coding* dan koneksi ke database b. Melakukan *backup* sistem informasi
6	SIWEDO	Informasi mengenai Dinas XYZ Kabupaten Banyumas tidak bisa diakses dan reputasi Dinas XYZ Kabupaten Banyumas akan dipertanyakan	Melakukan pengecekan didalam *coding* dan koneksi ke database
7	Banyumas Mail	Layanan email tidak bisa digunakan sehingga para pegawai tidak dapat mengirim email menggunakan email dinas	Menggunakan email lain seperti gmail, yahoo dan lain-lain
8	Si ANA	a. Sistem informasi mengalami error dan data pegawai tidak bisa diakses sehingga tidak dapat melakukan analisis dan evaluasi b. Database mengalami error sehingga tidak bisa diakses	a. Melakukan pengecekan didalam *coding* dan koneksi ke database b. Melakukan *backup* sistem informasi
9	PPDB Online	a. Sistem informasi mengalami error dan tidak bisa diakses b. Pelayanan kepada calon peserta didik baru menjadi tertunda	a. Melakukan pengecekan didalam *coding* dan koneksi ke database b. Melakukan *backup* sistem informasi
10	Pengelolaan Capes USM/UN	a. Sistem informasi mengalami error dan data mengenai calon peserta USM/UN tidak bisa diakses b. Database mengalami error sehingga tidak bisa diakses	a. Melakukan pengecekan didalam *coding* dan koneksi ke database b. Melakukan *backup* sistem informasi
11	Satria Keuangan	a. Sistem informasi mengalami error dan laporan pelaksanaan transaksi keuangan tidak bisa diinput	a. Melakukan pengecekan didalam *coding* dan koneksi ke database b. Melakukan *backup* sistem informasi

No.	Gangguan	Kendala	Proses *Recovery*
		b. Database mengalami error sehingga tidak bisa diakses	
12	Simbada Mas	a. Sistem informasi mengalami error dan kegiatan pengelolaan aset tidak dapat dilakukan b. Database mengalami error sehingga tidak bisa diakses	a. Melakukan pengecekan didalam *coding* dan koneksi ke database b. Melakukan *backup* sistem informasi

F. Dokumentasi

Dokumentasi *Disaster Recovery Plan* merupakan tahap mendokumentasikan prosedur *Disaster Recovery Plan* (DRP). Langkah-langkah penyusunan dokumentasi DRP menggunakan standar framework NIST SP 800-34 Rev.1 dan nantinya dokumen ini akan diterapkan di Dinas XYZ Kabupaten Banyumas untuk mendukung proses penanggulangan jika terjadi gangguan atau bencana pada Dinas XYZ Kabupaten Banyumas.

IV. PENUTUP

Berdasarkan penelitian yang telah dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Hasil akhir berupa dokumen *Disaster Recovery Plan* yang didalamnya berisi prosedur-prosedur *Disaster Recovery Plan* yang dapat dijadikan sebagai masukan dalam pembuatan dan penerapan rencana pemulihan setelah terjadinya bencana pada Dinas XYZ Kabupaten Banyumas.
2. *Disaster Recovery Plan*IS/IT pada Dinas XYZ Kabupaten Banyumas dirumuskan melalui tahapan Risk Assessment, Business Impact Analysis (BIA), Strategy Recovery, Dokumentasi *Disaster Recovery Plan*, sampai dengan Testing.
3. Pembuatan *Disaster Recovery Plan* disesuaikan dengan situasi dan kondisi yang ada pada Dinas XYZ Kabupaten Banyumas agar perencanaan dan penanganannya dapat dilakukan secara tepat.

UCAPAN TERIMAKASIH

Terima kasih penulis sampaikan kepada STMIK AMIKOM Purwokerto, yang telah mendukung penelitian ini.

REFERENSI

[1] P. R. E. Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*. Yogyakarta: Graha Ilmu, 2014.
[2] R. Budiarto, "Manajemen Risiko Keamanan Sistem Informasi," vol. 2, no. 2, pp. 48–58, 2017.
[3] Yakub, *Pengantar Sistem Informasi*. Yogyakarta: Graha Ilmu, 2012.
[4] P. P. Ardhiatno, "Perancangan business ...., Prabowo Priyo Ardhiatno, Fasilkom UI, 2013," 2013.
[5] Pemerintah Republik Indonesia, *Undang-Undang Republik Indonesia Nomor 24 Tahun 2007 tentang Penanggulangan Bencana*. Indonesia, 2007.
[6] J. C. Daud, "Pembuatan Disaster Recovery Plan (DRP) Berdasarkan ISO / IEC 24762 : 2008 Di ITS Surabaya (Studi Kasus di Pusat Data dan Jaringan BTSI ITS)," *J. Tek. Pomits*, 2008.
[7] N. Rachmaningrum, "Studi Kelayakan Disaster Recovery Plan pada Infrastruktur Jaringan Komputer (Studi kasus Jaringan Komputer Universitas Widyatama)," in *semnasIF 2011 UPN Veteran Yogyakarta*, 2011, vol. 2011, no. semnasIF, pp. 30–36.
[8] A. F. U. Fahmawati, "Faktor-Faktor yang Mempengaruhi Disaster Recovery Plan dan Business Continuity Planning," Universitas Lampung, 2016.
[9] I WAYAN ARDI YASA, "Perumusan Disaster Recovery Plan Pada Infrastruktut Jaringan Komputer(Studi Kasus STMIK STIKOM Bali)," 2016.
[10] R. Soetam, *Disaster Recovery Plan*. Jakarta: Prestasi Pustaka, 2008.
[11] Jogiyanto, *Sistem Teknologi Informasi*. Yogyakarta: Andi, 2005.
[12] NIST, *Contingency Planning Guide for Federal Information Systems, National Institute of Standards and Technology*. U.S. Department of Commerce, 2010.
[13] Dinas Pendidikan Kabupaten Banyumas, "Wawancara Bencana Yang Pernah Terjadi," 2017.
[14] H. faqih Zanuar Rifai, "Perancangan Business Continuty Plan (Bcp) Layanan Sistem Informasi Stmik Amikom Purwokerto (Studi Kasus : Stmik Amikom Purwokerto)," *Probisnis*, vol. 10, no. 2, 2017.
[15] Dinas Pendidikan Kabupaten Banyumas, "Topologi Jaringan Sistem Informasi," Banyumas, 2017.
[16] R. L. Tammineedi, "Business continuity management: A standards-based approach," *Inf. Secur. J.*, vol. 19, no. 1, pp. 36–50, 2010.