Perancangan Dokumentasi Disaster Recovery Plan Terhadap Data APBD Berdasarkan Iso 24762:2008 Studi Kasus : Dewan Perwakilan Rakyat Daerah Kota Bandung

Indra Yudha Pratama[1], Rita Rijayanti[2], MT, Doddy Ferdiansyah[3]

[1,2,3] Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pasundan
Jln. Dr. Setiabudhi no. 193 Bandung, Jawa Barat

Abstrak- Kebutuhan terhadap data yang terus meningkat menjadikan data sebagai aset penting bagi seperti instansi pemerintah. Hal inipun tidak lepas dari risiko kehilangan akses data akibat bencana yang mungkin terjadi setiap saat. Dewan perwakilan rakyat (DPRD) Kota Bandung Dewan Perwakilan Rakyat Daerah (DPRD) Kota Bandung yang memiliki tugas Pokok melaksanakan Pengawasaan terhadap Pelaksanaan Peraturan Daerah dan APBD Kota Bandung nomor 58 Tahun 2005 tentang Pengelolaan Keuangan Daerah, Anggaran Pendapatan Daerah (APBD) diatur dengan peraturan daerah. Saat ini Dewan Perwakilan Rakyat Daerah Kota Bandung masih belum memiliki dokumen terkait dengan disaster recovery plan, karena tidak lepas dari kemungkinan terjadinya bencana seperti; bencana alam, kebakaran, kesalahan manusia, data corrupt, maupun serangan kepada sistem seperti virus. Mengingat data yang tersimpan di DEWAN PERWAKILAN RAKYAT DAERAH Kota Bandung sangatlah penting yang memiliki dasar hukum dan dilindungi Undang-Undang, maka penelitian ini bertujuan untuk merancang dokumen Disaster recovery plan yang difokuskan pada penggunaan teknologi informasi (TI) untuk pemulihan kinerja sistem, aplikasi atau sebuah fasilitas komputer yang dijalankan dari suatu tempat yang berbeda (off-site) ketika terjadi situasi darurat di DRPD Kota Bandung. Metode yang digunakan dalam penelitian ini adalah Risk Assessment.

Kata Kunci- Rencana Pemulihan Bencana, Penilaian Risiko, Analisis Dampak Bisnis, Mitigasi Risiko, ISO 24762:2008.

I. PENDAHULUAN

Bencana merupakan suatu kejadian yang waktunya tidak bisa di prediksi yang berisfat merusak. Dampak yang di akibatkan oleh bencana itu sendiri adalah kerugian baik materil maupun non materil. Hal ini dapat mengganggu kegiatan operasional suatu instansi yang sedang berlangsung dan akan berakibat fatal. Jika hal tersebut dibiarkan , dan telebih lagi jika tidak ada tempat recovery site yang sesuai dengan standar yang tersedia setelah terjadi nya bencana (disaster) akan megganggu keberlangsungan suatu instansi.

Dewan Perwakilan Rakyat Daerah (DPRD) Kota Bandung yang memiliki tugas Pokok melaksanakan Pengawasaan terhadap Pelaksanaan Peraturan Daerah dan APBD Kota Bandung nomor 58 Tahun 2005 tentang Pengelolaan Keuangan Daerah, Anggaran Pendapatan Daerah (APBD) diatur dengan peraturan daerah. Terhitung jumlah APBD Kota Bandung Tahun 2018 adalah 6.672.618.474.393 untuk Pendapatan dan untuk Belanja Daerah Sebesar 7.239.813.537.305 ada juga Pembiayaan Daerah Sebesar 1.022.342.672.866 Saat ini Dewan Perwakilan Rakyat Daerah Kota Bandung. Masih adanya data APBD yang berupa fisik belum terdigitalisasi bisa menjadi salah satu faktor bencana. dan di DPRD sendiri belum memiliki dokumen terkait dengan disaster recovery plan, karena tidak lepas dari kemungkinan terjadinya bencana seperti; bencana alam, kebakaran, kesalahan manusia, data corrupt, maupun serangan kepada sistem seperti virus. Mengingat data yang tersimpan di DEWAN PERWAKILAN RAKYAT DAERAH Kota Bandung sangatlah penting yang memiliki dasar hukum dan dilindungi Undang-Undang.

Rencana penanggulangan bencana (Disaster Recovery Plan) adalah salah rencana darurat dibidang teknologi informasi yang ditujukan untuk memulihkan layanan setelah terjadinya suatu gangguan besar/bencana, namun pada instansi tersebut belum terdapat dokumen mengenai pemulihan dampak bencana yang akan memengaruhi keberlangsungan instansi dimasa pemulihan, sementara kecepatan pemulihan setelah terjadi bencana sangat lah penting bagi instansi tersebut. Salah satu upaya untuk mengantisipasi hal-hal tersebut adalah dengan menyusun rencana pemulihan bencana melaluli pendekatan ilmu teknologi informasi yaitu Disaster recovery plan.

II. LANDASAN TEORI

A. APBD

Anggaran pendapatan dan belanja daerah (APBD) adalah rencana keuangan tahunan daerah yang dibahas dan disetujui bersama oleh pemerintah daerah dengan dewan perwakilan rakyat daerah (DPRD), dan ditetapkan melalui peraturan daerah (PEMENDAGRI NO.13 TAHUN 2006) APBD merupakan instrument yang digunakan sebagi alat dengan tujuan untuk meningkat kan peayanan umum

dan masyarakat di daerah. Dalam penerapan APBD dapat menggambarkan kebutuhan dan kemampuan setiap daerah sesuai dengan keunikan dan potensinya tersendiri,Data APBD itu sendiri di bagi menjadi 3 bagian yaitu:

Pendapatan asli daerah: pendapatan yang diperoleh daerah yang dipungut berdasarkan peratuan daerah sesuai peratuan perundang-undagan UUD tentang perimbangan keuangan antara pemerintah pusat dan pemerintah daerah no.33 tahun 2004.

Belanja daerah : Anggaran Pendapatan dan Belanja Daerah (APBD) merupakan rencana keuangan pemerintah daerah selama satu tahun yang ditetapkan oleh peraturan daerah. APBD dapat dijadikan sebagai sarana komunikasi pemerintah daerah kepada masyarakatnya mengenai prioritas pengalokasian yang dilakukan oleh pemerintah daerah setelah berkoordinasi dengan pihak legislatif, DPRD.

Pembiayaan daerah :Pembiayaan daerah sebagaimana tercantum dalam peraturan menteri dalam negri nomor 13 tahun 2006 merupakan setiap penerimaan yang perlu dibayar dan pengeluaran yang akan diterima kembali,baik pada tahun anggaran yang bersangkutan maupun tahun-tahun berikutnya .

B. Bencana dan Disaster Recovery Plan

Berdasarkan perararaturan Undang-undang Nomor 24 Tahun 2007 [2] menyebutkan bahwa bencana adalah peristiwa peristiwa atau rangkaian peristiwa yang mengancam dan mengganggu kehidupan dan penghidupan masyarakat yang disebabkan, baik oleh faktor alam dan/atau faktor non-alam maupun faktor manusia, sehingga mengakibatkan timbulnya korban jiwa manusia, kerusakan lingkungan, kerugian harta benda dan dampak psikologis. Bencana sendiri terbagi kedalam beberapa bagian sebagai berikut :

Bencana alam adalah bencana yang diakibatkan oleh peristiwa atau serangkaian peristiwa yang disebabkan oleh alam antara lain, berupa gempa bumi, tsunami, gunung meletus, banjir, kekeringan, angin topan, dan tanah longsor.

Bencana non-alam adalah bencana yang diakibatkan oleh peristiwa atau serangkaian peristiwa yang antara lain berupa gagal teknologi, gagal modernisasi, dan wabah penyakit. Bencana sosial adalah bencana yang diakibatkan oleh peristiwa atau serangkaian peristiwa yang diakibatkan oleh manusia yang meliputi konflik sosial antar kelompok atau antar komunitas masyarakat, dan terror.

Suatu perusahaan atau instansi pemerintah dituntut untuk menjalankan bisnis agar terus berjalan meskipun, terjadi suatu bencana yang tak terduga. Oleh karena itu untuk mencegah dan mengurangi dampak bencana yang terjadi pada bisnis maka, perlu dilakukannya disaster recovery plan. Menurut buku “Disaster Recovery Strategies with Tivoli Storage Management”, dengan pengarang Charlotte Brooks, Matthew Bedernjak, Igor Juran, dan John Merryman, tahun 2002, menyatakan bahwa Disaster recovery plan merupakan rencana yang difokuskan pada penggunaan teknologi informasi (TI) untuk pemulihan kinerja sistem, aplikasi atau sebuah fasilitas komputer yang dijalankan dari suatu lokasi yang berbeda (offsite) ketika terjadi situasi darurat” [4].

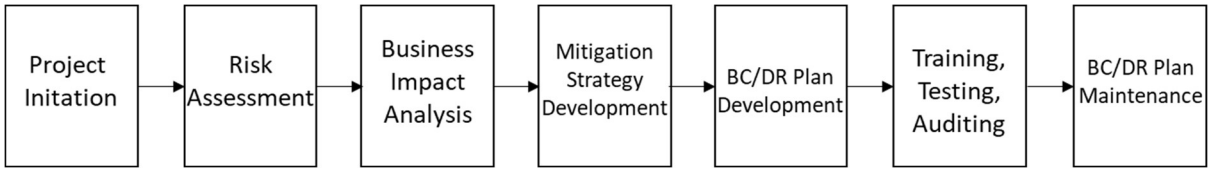
Sedangkan menurut artikel yang berjudul “10 Steps to Implement a Disaster Recovery Plan” dengan penulis Neil A. Rosenberg, 2006, menyatakan bahwa disaster recovery plan adalah mendefinisikan tentang konsisten, tindakan sebelum perencanaan yang akan bereaksi terhadap berbagai skenario bencana. Dengan kata lain, adalah tentang reaksi terhadap skenario setelah terjadinya bencana [9].

Menurut buku “Business Continuity & Disaster Recovery For IT Professionals”, dengan penulis Susan Sneadaker, tahun 2007 menyatakan bahwa terdapat komponen bisnis dalam disaster recovery plan, yaitu orang (people), proses (process), dan teknologi (technology). Orang (people) merupakan sumber daya manusia (SDM) yang bertanggung jawab dalam merancang, menerapkan, dan memantau proses. Proses (process) merupakan suatu rangkaian atau tindakan (prosedur) yang harus dilakukan ketika terjadi bencana. Sedangkan teknologi (technology) merupakan pemahaman terhadap berbagai komponen teknologi infrasruktur ketika terjadi berbagai bencana [11].

Menurut artikel yang berjudul “Business Continuity Plan and Disaster Recovey Plan”, dengan penulis Usep Solehudin menyatakan bahwa tujuan utama dari Disaster Recovery Plan adalah untuk menyediakan kemampuan atau sumber daya untuk menjalankan proses vital pada lokasi cadangan sementara waktu dan mengembalikan fungsi lokasi utama menjadi normal dalam batasan waktu tertentu, dengan menjalankan prosedur pemulihan cepat, untuk meminimalisir kerugian organisasi [12].

B.1 Tahapan Pembangunan Disaster Recovery Plan

Menurut buku “Business Continuity & Disaster Recovery For IT Professionals”, dengan penulis Susan Sneadaker, tahun 2007 menyatakan bahwa disaster recovery plan merupakan proses bertahap yang tersusun secara metodikal (peran-peran yang mengacu pada cara melakukan tindakan). Tahapan pembangunan sebuah disaster recovery plan tidak selalu sama, karena bergantung pada kebutuhan dan tujuan pembuatannya. Berikut pada gambar 1 merupakan langkah-langkah business continuity dan disaster recovery plan yang digunakan dari dasar-dasar perencanan kontigensi yang memiliki kesamaan dengan metodologi proyek, sebagai berikut [11]:



Gambar 1. Tahapan BC/DR Plan

C. Risk Assessment

Dalam melakukan penilaian risiko ini penulis menggunakan metode Failure-Mode and Effects Analysis (FMEA). Failure Mode and Effects Analysis (FMEA) dapat digambarkan sebagai cara sistematis mengidentifikasi risiko atau mode kegagalan sistem, fungsi, dan mengevaluasi efek dari mode kegagalan pada tingkat yang lebih tinggi (prioritas). Tujuannya adalah untuk menentukan penyebab terjadinya mode kegagalan dan apa yang bisa dilakukan untuk menghilangkan atau mengurangi kemungkinan kegagalan. Sebuah teknik bottom-up seperti FMEA adalah cara yang paling efektik untuk mengindentifikasi kegagalan komponen atau kerusakan sistem, dan mendokumentasikan sistem di bawah pertimbangan [7].

a. Menentukan nilai dampak (severity), merupakan untuk mengetahui skenario buruk efek akhir yang merugikan dari suatu kejadian atau gangguan yang memengaruhi kegiatan di organisasi. Berikut pada tabel 1 merupakan definisi dari nilai dampak (severity).

Tabel 1 Definisi dari nilai dampak (Severity)

Efek	Dampak dari Efek	Peringkat
Catasptrophic	Gangguan menyebabkan kerugian secara finansial dan seluruh proses bisnis terhenti.	10
Extreme	Gangguan menyebabkan kerugian secara finansial, proses bisnis sangat terganggu,	9
Very High	Gangguan menyebabkan kerugian secara finansial, sangat menghambat proses bisnis, dan penurunan kinerja.	8
High	Gangguan menyebabkan kerugian secara finansial, menghambat proses bisnis, dan penurunan kinerja	7
Moderate	Gangguan menyebabkan penurunan kinerja dan proses bisnis terhambat.	6
Low	Gangguan menyebabkan kerugian secara finansial.	5
Very Low	Gangguan menyebabkan sedikit gangguan.	4
Minor	Gangguan menyebabkan gangguan dengan skala kecil.	3
Very Minor	Tanpa disadari atau memberikan dampak kecil pada proses bisnis.	2
None	Tanpa disadari atau tidak memengaruhi proses bisnis sama sekali.	1

b. Menentukan nilai probabilitas (probability), merupakan tingkat frekuensi atau kemungkinan terjadinya suatu kejadian atau gangguan tersebut, yang dapat menyebabkan terjadinya kegagalan. Berikut pada tabel 2 merupakan definisi dari nilai probabilitas (probability).

Tabel 2 Definisi dari nilai probabilitas (Probability)

Probabilitas Kegagalan	Kegagalan Probabilitias	Peringkat
Very High : Kegagalan hampir tak terelakkan	Lebih dari 1 kali dalam 1 hari	10
	Satu kali dalam 3 hari.	9
High : Kegagalan berulang	Satu kali dalam 1 minggu.	8
	Satu kali dalam 1 bulan.	7
Moderate : Kegagalan kadang-kadang	Satu kali dalam 3 bulan.	6
	Satu kali dalam 6 bulan.	5
	Satu kali dalam 1 tahun.	4
Low : Kegagalan relatif sedikit	Satu kali dalam 1 sampai 5 tahun	3
	Satu kali dalam 5 sampai 10 tahun	2

c. Menentukan nilai deteksi (detectability), merupakan penilaian terhadap kemampuan pengelola di organisasi dalam melakukan kontrol dan kendali terhadap skenario kegagalan dari suatu kejadian atau kegagalan yang terjadi. Berikut pada tabel 3 merupakan definisi dari nilai deteksi (detectability).

Tabel 3 Definisi dari nilai deteksi (Detectability)

Deteksi	Kemungkinan Deteksi	Peringkat
Absolute Uncertainty	Tidak ada metode deteksi	10
Very Remote	Metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi	9
Remote	Motede deteksi tidak terbukti untuk mendeteksi tepat waktu	8
Very Low	Metode deteksi tidak andal dalam mendeteksi tepat waktu	7
Low	Metode deteksi memiliki tingkat efektifitas yang rendah	6
Moderate	Metode deteksi memiliki tingkat efektifitas yang rata-rata	5
Moderately High	Metode deteksi memiliki kemungkinan cukup tinggi untuk dapat mendeteksi risiko	4
High	Metode deteksi memiliki kemungkinan tinggi untuk dapat mendeteksi risiko	3
Very High	Metode deteksi sangat efektid untuk dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	2
Almost Certain	Metode deteksi hampir pasti dapat mendeteksi dengan waktu yang cukup	1

d. Menghitung Kalkulasi Nilai

Setelah mendapatkan nilai dari nilai dampak (severity), nilai probabilitas (probability), dan nilai detektsi (detectability). Selanjutnya adalah melakukan kalkukalasi nilai dari nilai yang sudah didapatkan dengan menggunakan rumus, yaitu :

RPN = S x P x D.

Keterangan :

RPN : Risk Priority Number, perhitungan nilai prioritas risiko.

S : Severity, nilai dampak.

P : Probability, nilai probabilitas.

D : Detectability, nilai deteksi.

Tabel 4 Skala nilai RPN dengan level risiko

Level Risiko	Skala Nilai RPN
Very High	> 200
High	< 200
Medium	< 120
Low	< 80
Very Low	< 20

D. BC/DR Plan Development

Tahap selanjutnya adalah menyusun bagaimana caranya untuk merencanakan pemulihan bencana yang terdapat di perusahaan maupun instansi pemerintah. Bencana yang telah di prediksi dengan melakukan identifikasi risiko dan penilaian risiko selanjutnya akan dibuat perencanaan untuk pemulihan bencana tersebut, sehingga dari daftar risiko tersebut dapat di deteksi ketika terjadi bencana lalu direspon dan di tangani pemulihannya segera untuk keberlangsungan bisnis perusahaan maupun instansi pemerintah. Dalam penyusunan dokumen disaster recovery plan, membutuhkan sebuah acuan atau standar yang baku internasional. Berikut pada tabel 5 merupakan struktur dokumen yang digunakan dalam penelitian ini berdasarkan ISO 24762:2008 [10]

Tabel 5 Struktur dokumen berdasarkan ISO 24762:2008

Template Dokumen		Klausa ISO 24762:2008
Latar Belakang	Tujuan	General
	Ruang Lingkup	
	Pernyataan Kebijakan	Kebijakan dan prosedur
Strategi Disaster Recovery Plan	Identifikasi Data APBD	5.3 Asset management
	Kontak dengan Third Party	5.5 Vendor management
	Manajemen Risiko	9.5 Risk management
Fasilitas Disaster Recovery Plan	Lokasi tempat Disaster Recovery	6.2 Location of DR Sites
	Telekomunikasi	6.7 Telecommunications
	Power Supply	6.8 Power Supply
Disaster Recovery Plan	Prosedur backup dan penyimpanan offsite dan onsite	Kebijakan dan prosedur
	Layanan penyimpanan offsite dan onsite	5.4 Proximity of site
	Respon bencana	7.15 Emergency response plan
	Aktivitas Disaster Recovery Plan	5.8 Activation and deactivation of DRP
Fungsional tim dan tanggung jawab (meliputi kontak personil dan notifikasi calling tree)	Tim Eksekutif	8.3 Skilled manpower and support
	Tim penilaian kerugian	
	Tim pemulihan	
	Tim operasional	
	Tim costumer support	
	Tim penyelamatan	
	Tim administration support	

III. HASIL PENELITIAN

A. Identifikasi Data APBD Pendapatan Daerah

DPRD Kota Bandung memiliki 3 data APBD Pendapatan daerah yang penting dari setiap layanan sistem informasi dan digunakan setiap harinya. Data-data tersebut akan tersimpan di pusat data yang berada di ruang server DPRD Kota Bandung. Berikut pada tabel 6 merupakan penjelasan mengenai data-data yang terdapat di DPRD Kota Bandung.

Tabel 6 Data yang terdapat di DPRD Kota Bandung

Data ABPD	Jenis Data	Jenis Pendapatan	Sistem Informasi	Detail Data
• Data pendapatan asli daerah	1.Data hasil Pajak daerah	Pajak hotel Pajak restoran Pajak reklame Pajak penerangan jalan Pajak parkir Pajak air tanah Pajak mineral bukan logam dan batuan Pajak bumi dan bangunan pedesaan dan perkotaan	SIKD	Sebagian fisik\sebagian digital
	2.Data Retribusi Daerah	Retrebusi jasa umum Retrebusi jasa usaha Retrebusi perizinan tertentu	SIKD	Data sudah digital
	3.Data Hasil pengelolaan daerah yang di pisahkan	Bagian Laba atas penyertaan modal pada perusahaan milik daerah/BUMN	SIKD	Sebagian fisik\sebagian digital
	4.Data Lain-lain pendapatan asli daerah yang sah	Jasa giro Pendapatan dari pengembalian Fasilitas social dan fasilitas umum Hasil pengelolaan dana bergulir	SIKD	Sebagian fisik\sebagian digital
Data perimbangan	1. Data bagi hasil pajak/Bagi hasil bukan pajak	Dana Jenis pendapatan Bagi hasil pajak Bagi hasil bukan pajak/sumber daya alam	SIKD	Data sudah digital
	2.Data alokasi umum	Dana hasil alokasi umum	SIKD	Sebagian fisik\sebagian digital
	3.Data alokasi khusus	Dana hasil alokasi khusus	SIKD	Sebagian fisik\sebagian digital
Lain-lain pendapatan yang sah	1.Data Pendapatan hibah	Dana pendapatan hibah dari pemerintah	SIKD	Sebagian fisik\sebagian digital
	2.Data bagi hasil pajak provinsi dan pemerintahan daerah	Dana bagi hasil pajak dari provinsi	SIKD	Data sudah digital

B. Identifikasi Dampak

Identifikasi dampak dilakukan untuk menentukan nilai dari dampak terjadinya risiko.

Tabel 7 Nilai Identifikasi Dampak

No	Risiko	Dampak Terjadinya Risiko	*Severity*
1	Gunung meletus	Gangguan menyebabkan kerugian secara finansial, sangat menghambat proses bisnis, dan penurunan kinerja.	8
2	Gempa bumi	Gangguan menyebabkan kerugian secara finansial dan seluruh proses bisnis terhenti.	10
3	Badai	Gangguan menyebabkan kerugian secara finansial, sangat menghambat proses bisnis, dan penurunan kinerja.	8
4	Banjir	Gangguan menyebabkan kerugian secara finansial, menghambat proses bisnis, dan penurunan kinerja	7
5	Kebakaran	Gangguan menyebabkan kerugian secara finansial dan seluruh proses bisnis terhenti.	10
6	Kegagalan *server* dan *storage*	Gangguan menyebabkan kerugian finansial dan proses bisnis terhambat.	6
7	Kerusakan perangkat jaringan	Gangguan menyebabkan penurunan kinerja dan proses bisnis terhambat.	6
8	Ketiadaan daya listrik	Gangguan menyebabkan kerugian secara finansial, sangat menghambat proses bisnis, dan penurunan kinerja.	8
9	Jaringan komputer mati	Gangguan menyebabkan penurunan kinerja dan proses bisnis terhambat.	6
10	Serangan cyber	Gangguan menyebabkan penurunan kinerja dan proses bisnis terhambat.	6
11	*Human error*	Tanpa disadari atau memberikan dampak kecil pada proses bisnis.	6
12	Pemogokan pegawai	Gangguan menyebabkan penurunan kinerja dan proses bisnis terhambat.	6
13	Unjuk rasa masyarakat	Gangguan menyebabkan kerugian secara finansial, menghambat proses bisnis, dan penurunan kinerja	7
14	Pencurian perangkat	Gangguan menyebabkan kerugian secara finansial, menghambat proses bisnis, dan penurunan kinerja	7

C. Identifikasi Probabilitas

Identifikasi probabilitas dilakukan untuk menentukan nilai frekuensi atau kemungkinan terjadinya risiko.

Tabel 8 Nilai Probabilitas

No	Risiko	Penyebab Terjadinya Risiko	*Probability*
1	Gunung meletus	Disebabkan oleh alam	1
2	Gempa bumi	Disebabkan oleh alam	1
3	Badai	Disebabkan oleh alam	2
4	Banjir	Disebabkan oleh alam	1
5	Kebakaran	Ruang *server* dapat saja terbakar atau menjadi bagian dari sumber kebakaran gedung	2
		Tidak adanya manajemen kabel untuk memisahkan kabel listrik dan kabel komunikasi.	2
6	Kegagalan *server* dan *storage*	Beban kinerja *server* dan *storage* telah mendekati atau melebihi kemampuan *server* dan *storage*.	8
		Server mengalami *overheat*	7
		Terdapat *bad sector* pada *harddisk* yang digunakan pada *storage*.	5
7	Kerusakan perangkat jaringan	Beban kinerja perangkat jaringan yang sudah usang	8
		Memaksakan perangkat jaringan yang terus menyala	8
8	Ketiadaan daya listrik	Aliran listrik dari PLN terputus	3
		Kesalahan operasional pegawai	3
9	Jaringan komputer mati	Terdapat perangkat jaringan yang rusak	8
		Kabel jaringan terputus	8
10	Serangan cyber	Terdapat celah keamanan di jaringan komputer yang dieksploitasi oleh orang yang tidak bertanggung jawab.	4
11	*Human error*	Kesalahan dalam melakukan manipulasi secara sengaja maupun tidak sengaja	5
12	Pemogokan pegawai	Menunggaknya gaji pegawai	3
13	Unjuk rasa masyarakat	Protes terhadap layanan yang tidak memuaskan	7
14	Pencurian perangkat	Akses terhadap perangkat keras sangat terbuka.	4

D. Identifikasi Deteksi

Identifikasi deteksi dilakukan untuk menentukan nilai proses kontrol saat ini atau pemahaman organisasi dalam menangani risiko.

Tabel 9 Nilai Deteksi

No	Risiko	Proses Kontrol Saat Ini	*Detectability*
1	Gunung meletus	Belum memiliki kontrol secara tertulis.	10
2	Gempa bumi	Belum memiliki kontrol secara tertulis.	10
3	Badai	Belum memiliki kontrol secara tertulis.	10
4	Banjir	Belum memiliki kontrol secara tertulis	10
5	Kebakaran	Belum memiliki kontrol secara tertulis	10
		Terdapat tabung pemadam kebakaran di beberapa titik di DPRDKota Bandung.	8
6	Kegagalan *server* dan *storage*	Pemeliharan jarang dilakukan dan mengandalkan prediksi yaitu melakukan perawatan 1 kali dalam 3 bulan	7
7	Kerusakan perangkat jaringan	Pemeliharan jarang dilakukan dan mengandalkan prediksi yaitu melakukan perawatan 1 kali dalam 3 bulan	7
8	Ketiadaan daya listrik	Terdapat UPS dan Generator sebagai *backup* listrik, namun tidak berjalan dengan optimal.	4
9	Jaringan komputer mati	Pemeliharan jarang dilakukan dan mengandalkan prediksi yaitu melakukan perawatan 1 kali dalam 3 bulan	7
10	Serangan cyber	Melakukan *update antivirus* dan sistem operasi secara *default*.	8
		Terdapat cadangan *backup* data APBD saja di JATEL	5
11	*Human error*	Melakukan teguran kepada pegawai	5
12	Pemogokan pegawai	Melakukan musyawarah kepada pegawai terkait permasalahan yang terjadi	7
13	Unjuk rasa masyarakat	Melakukan musyawarah dengan masyarakat terkait permasalahan yang terjadi	5
14	Pencurian perangkat	Terdapat Kebijakan terhadap aset yang dimiliki DPRD Kota Bandung	6

E. Penilaian Resiko

Setelah mendapatkan nilai dari nilai dampak (severity), nilai probabilitas (probability), dan nilai deteksi (detectability). Selanjutnya adalah melakukan kalkulasi nilai risiko, dari nilai yang sudah didapatkan dengan menggunakan rumus RPN.

Tabel 10 Nilai dan Level Risiko

No	Risiko	*Severity*	*Probability*	*Detectability*	RPN	Level
1	Gunung meletus	8	1	10	80	*Low*
2	Gempa bumi	10	1	10	100	*Medium*
3	Badai	8	2	10	160	*High*
4	Banjir	7	1	10	70	*Low*
5	Kebakaran	10	2	10	200	*High*
			2	8	160	*High*
6	Kegagalan *server* dan *storage*	6	8	7	336	*Very high*
			7		294	*Very high*
			5		210	*Very high*
7	Kerusakan perangkat jaringan	6	8	7	336	*Very high*
			8		336	*Very high*
8	Ketiadaan daya listrik	8	3	4	96	*Medium*
			3		96	*Medium*
9	Jaringan komputer mati	6	8	7	336	*Very high*
			8		336	*Very high*
10	Serangan cyber	6	4	8	192	*High*
				5	120	*Medium*
11	*Human error*	6	5	5	150	*High*
12	Pemogokan pegawai	6	3	7	126	*High*
13	Unjuk rasa masyarakat	6	7	5	210	*Very high*
14	Pencurian perangkat	8	4	6	192	*High*

F. Evaluasi Resiko

Setelah melakukan penilaian risiko, selanjutnya adalah melakukan evaluasi risiko yang didapat dari hasil penilaian risiko. Hasil penilaian risiko tersebut dikelompokan dari nilai yang tertinggi sampai ke nilai yang terendah, sehingga menghasilkan prioritas risiko.

Tabel 11 Pengelompokan berdasarkan Level Risiko

No	Risiko	RPN	Level
1	Kegagalan *server* dan *storage*	336	*Very High*
		294	
		210	
2	Kerusakan perangkat jaringan	336	
		336	
3	Jaringan komputer mati	336	
		336	
4	Unjuk rasa masyarakat	210	
5	Badai	160	*High*
6	Kebakaran	200	
		160	
7	*Human error*	150	
8	Pemogokan pegawai	126	
9	Pencurian perangkat	192	
10	Serangan cyber	192	
		120	*Medium*
11	Gempa bumi	100	
12	Ketiadaan daya listrik	96	
		96	
13	Gunung meletus	80	*Low*
14	Banjir	70	

G. Analisis Dampak Bisnis

Sebelum melakukan analisis dampak bisnis, hal yang perlu diperhatikan adalah mengindentifikasikan sistem informasi yang terdapat di DPRD Kota Bandung hal ini bertujuan untuk mengetahui proses bisnis kritis dari sistem informasi yang dimiliki oleh DPRD Kota Bandung.

Tabel 12 Level Dampak Bisnis

No	Sistem Informasi	Dampak yang dialami jika Sistem Informasi Terhenti	Tingkat Dampak
1	Sistem Informasi Keuangan Daerah	• Pegawai DPRD tidak dapat melakukan input data APBD. • Pegawai DPRD tidak dapat mengakses sistem informasi keuangan daerah • Tidak adanya pengambilan keputusan/kebijakan baru di karenakan sistem informasi keuangan tidak dapat di aksess • Pegawai tidak dapat menyajikan Keuangan daerah secara berkala • Kegiatan Operasional tidak dapat berjalan sebagaimana mestinya.	*High*
2	Situs web DPRD Kota Bandung	Pengguna (masyarakat) tidak dapat mengakses informasi mengenai DPRD Kota Bandung.	*Medium*

H. Pengembangan Strategi Mitigasi

Pengembangan strategi mitigasi dilakukan setelah melakukan analisis penilaiaan risiko dan analisis dampak bisnis. Pengembangan strategi mitigasi dilakukan untuk mengurangi dampak dari suatu kejadian yang diakibatkan oleh risiko. Pada tahap ini, strategi mitigasi risiko dikembangkan untuk penerapan kontrol, dan menentukan lokasi pemulihan.

Tabel 13 Kontrol terhadap Risiko

No	Risiko	Kontrol yang dimiliki	Penerapan Kontrol
1	Kegagalan Server dan Storage	Melakukan perawatan 1 kali dalam 3 bulan	• Menghubungi supplier/vendor terkait • Melakukan perawatan rutin 1 bulan sekali • Melakukan pengembangan strategi backup • Menerapkan asuransi terhadap perangkat keras server dan storage
2	kerusakan perangkat jaringan	pemeliharaan jaringan dilakukan dan mengandalkan prediksi yaitu melakukan perawatan 1 kali dalam 3 bulan	• Menghubungi supplier/vendor terkait • Melakukan perawatan dan pengecekan secara rutin minimal 1 bulan sekali • Melakukan pengembangan strategi backup • Menerapkan asuransi terhadap perangkat keras jaringan
3	jaringan komputer mati	melakukan perawatan 1 kali dalam 3 bulan	• Menerapkan network monitoring • Memperbaruhi kontrak dengan third party dengan mempertimbangkan SLA • Melakukan perawatan minimal 1 bulan sekali • Melakukan manajemen kabel
4	unjuk rasa masyarakat	melakukan musyawarah dengan masyarakat terkait permasalahaan yang terjadi	• Menerima kritik dan saran dari masyarakat
5	badai	belum memiliki control secara tertulis	• Menerapkan asuransi terhadap perangkat keras • Menerapkan rencana pemulihan terhadap bencana

6	kebakaran	belum memiliki control secara tertulis tetapi sudah memiliki tabung pemadam kebakaran di beberapa titik	• Menerapkan asuransi terhadap perangkat keras
7	human error	melakukan teguran kepada pegawai	• Melakukan control administrative • Melakukan pelatihan dan pembinaan pegawai
8	pemogokan pegawai	melakukan musyawarah kepada pegawai yang bermasalah	• Melakukan control administrative
9	pencurian perangkat	membuat kebijakan terhadap asset yang dimiliki	• Melakukan penyimpanan perangkat dengan tata cara yang sesuai
10	serangan siber	melakukan update antivirus dan sistem operasi, serta memiliki cadangan backup di JATEL	• Menggunakan kombinasi password yang kuat • Menerapkan prosedur penggantian password secara berkala • Melakukan control preventif, detektif, dan korektif
11	gempa bumi	belum memiliki control secara tertulis	• Menerapkan asuransi terhadap perangkat keras • Menerapkan rencana pemulihan terhadap bencana
12	ketiadaan daya listrik	terdapat UPS dan Generator sebagai backup daya listrik	• Menerapkan asuransi terhadap perangkat keras • Melakukan perawatan terhadap peralatan UPS dan Generator yang ada
13	gunung Meletus	belum memiliki control secara tertulis	• Menerapkan asuransi terhadap perangkat keras • Menerapkan rencana pemulihan terhadap bencana
14	banjir	belum memiliki control secara tertulis	• Menerapkan asuransi terhadap perangkat keras • Menerapkan rencana pemulihan terhadap bencana

IV. KESIMPULAN

Berdasarkan hasil analisis dan perancangan pada penelitian di Dewan Perwakilan Rakyat Daerah Kota Bandung dapat diambil beberapa kesimpulan yaitu DPRD Kota Bandung belum memiliki rencana pemulihan bencana yang terdokumentasi terhadap bencana. Kurangnya sumber daya manusia di bidang teknologi informasi, sehingga DPRD Kota Bandung hanya mengandalkan 1 orang dalam mengelola sistem. Di DPRD Kota Bandung memiliki waktu restorasi 1 hari. DPRD Kota Bandung memiliki cadangan backup data APBD di JATEL yang berada di Kota Bandung, dan belum memiliki lokasi cadangan DRP. Dari hasil temuan pada penelitian ini terdapat waktu restorasi selama 1 hari, oleh itu penulis menyarankan kepada DPRD Kota Bandung untuk melakukan restorasi selama 1 hari di perkecil menjadi 1-4 jam, karena untuk mendapatkan nilai RTO dan RPO yang sesuai dalam pemulihan agar lebih cepat serta tidak ada waktu yang terbuang. Sehigga disarankan kepada DPRD Kota Bandung dalam memilih lokasi cadangan yang berada di luar kawasan jawa barat dari lokasi utama dengan potensi risiko yang terbilang sedikit dari lokasi utama.

DAFTAR PUSTAKA

[1] Al-Bahra Bin Ladjamudin, “Analisis dan Desain Sistem Informasi”. Yogyakarta:Graha Ilmu. 2005

[2] Badan Nasional Penanggulangan Bencana, “Definisi dan Jenis Bencana”, tersedia : https://www.bnpb.go.id/home/definisi (diakses 28 Oktober 2016)

[3] Budianto SPd, 9 april 2015. “Pengertian Aset dan Macam-macamnya”, tersedia : http://www.budhii.web.id/2015/09/pengertian-aset-dan-macam-macamnya.html (diakses 30 Oktober 2016)

[4] Charlotte Brooks, Matthew Bedernjak, Igor Juran, dan John Merryman, “Disaster Recovery Strategies with Tivoli Storage Management”, IBM Redbooks, 2002

[5] Ina Jainab, 27 November 2013. “Pengertian Dokumen dan dokumentasi”, tersedia : http://inamayladin.blogspot.co.id/2013/11/pengertian-dokumen-dokumentasi.html (diakses 30 Oktober 2016)

[6] ISO 24762. “Information techonology – Security techniques – Guidelines for information and communications technology disaster recovery serveices”. 2008

[7] Haapenen Pentti, Helminen Atte. “Failure Mode and Effects Analysis of Software-Based Automation Systems”. Stuk-yto-tr 190. 2002.

[8] Kevin Kelleher, Casey G., Lois D., “Cause and Effect Diagram : Plain & Simple”. Joiner Associates Inc, USA, 1995.

[9] Neil A. Rosenberg. “10 Steps to Implement a Disaster Recovery Plan”. Quality Technology Solutions, Inc, 2006

[10] Rima, Panduan Disaster Recovery Plan, Standar, template, dan panduan DRP. 13 Januari 2014, tersedia : https://panduandrp.wordpress.com/ (diakses 25 Desember 2017)

[11] Susan Snedaker. “Business Continuity & Disaster Recovery For IT Professionals”. Syngres, 2007.

[12] Usep Solehudin. “Business Continuity Plan and Disaster Recovey Plan”. Magister Universitas Indonesia, 2005.