Journal of Information System, Informatics and Computing

Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)

JISICOM (Journal of Information System, Informatics and Computing)

PENGEMBANGAN APLIKASI PEMULIHAN LAYANAN BENCANA SISTEM INFORMASI PENERIMAN NEGARA BUKAN PAJAK ONLINE DI LINGKUNGAN KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Verdi Yasin*[1], Azhar Ahmad Riza*[2], Rumadi Hartawan*[3]
*[1]Program Studi Teknik Informatika, STMIK Jayakarta, *[2]Program Studi Teknik Informatika STMIK Jayakarta, *[3]Program Studi Teknik Informatika STMIK Jayakarta, Jakarta Indonesia.
Jln. Salemba I No.10 Jakarta Pusat 10430 Indonesia.
Email: verdiyasin@jayakarta.ac.id , azharthenarsis@gmail.com , rumadi@gmail.com

ABSTRAK

Disaster Recovery Plan (DRP) merupakan perincian dari prosedur-prosedur *emergency* secara detil untuk memudahkan melakukan *recovery* saat terjadi bencana (*disaster*) yang mempengaruhi sistem komputer organisasi. Dokumen DRP diperlukan oleh Kementerian Keuangan (Kemenkeu) sebagai dokumentasi terstruktur yang dapat digunakan oleh tim pemulihan untuk menjaga kelangsungan bisnis proses Kementerian Keuangan, manakala terjadi bencana di *Data Center* (DC) Kemenkeu. Dengan adanya Rancangan Pemulihan Bencana, maka layanan SIMPONI yang ada DC Kemenkeu tetap dapat berjalan manakala terjadi bencana di DC Kemenkeu, yaitu dengan menjalankan sistem/aplikasi dari *Data Recovery Center* (DRC) Kemenkeu. Dalam mengembangkan sistem ini, menggunakan Metode *Business Impact Analysis* (BIA) dan Metodologi Pengembangan *Disaster Recovery Plan* (DRP) sedangkan Metode Proses Pelaksanaan ialah *Business Continuity Plan Life Cycle* (BCPLC) Tujuan dari pelaksanaan penelitian ini adalah menghasilkan Rancangan Pemulihan Bencana khususnya untuk aplikasi Sistem Informasi Penerimaan Negara Bukan Pajak Online (SIMPONI). Sehingga apabila terjadi bencana pada DC Kemenkeu, tim pemulihan dapat memahami peran dan tanggung jawabnya untuk menjamin keamanan dan kelangsungan Aplikasi SIMPONI yang berjalan di DC dan di DRC.

Kata Kunci: *Business Impact Analysis* (BIA), *Disaster Recovery Plan* (DRP), *Data Recovery Center* (DRC), Sistem Informasi Penerimaan Negara Bukan Pajak Online (SIMPONI),

A. PENDAHULUAN

Dalam rangka mewujudkan *Integrated Financial Management Information System* (IFMIS) yang akurat, handal, terkini, dan mampu menyajikan informasi keuangan negara yang dibutuhkan dalam pengambilan keputusan, maka menjaga kelangsungan layanan TIK

menjadi hal yang penting bagi unit TIK Kementerian Keuangan (Kemenkeu).

Kemenkeu telah membangun dan menyediakan *Disaster Recovery Center* (DRC) sebagai backup layanan dari *Data Center* (DC) Kemenkeu. Sehingga, manakala terjadi bencana di DC Kemenkeu, kelangsungan layanan TIK diharapkan tetap dapat berjalan dari DRC Kemenkeu.
Pusat Sistem Informasi dan Teknologi Keuangan (Pusintek) selaku Unit TIK Pusat Kementerian Keuangan berkoordinasi dengan Unit TIK di semua Eselon 1 Kemenkeu selaku pemilik layanan sehingga memperoleh suatu sinergi kompetensi dan pembagian tugas yang efektif dalam penanganan bencana terhadap layanan TIK di lingkungan Kemenkeu.

Salah Satu Unit Eselon 1 yang mempunyai layanan sistim online dengan tingkat kritikalitas tinggi adalah Direktorat Jenderal Anggaran (DJA). DJA memiliki aplikasi Sistem Informasi Penerimaan Negara Bukan Pajak Online (Simponi) yang merupakan sebuah aplikasi berbasis web, Simponi sebagai billing sistem dalam Penerimaan Negara Bukan Pajak, Semua jenis penyetoran PNBP dilakukan secara elektronis, sehingga dapat terjaga transparasi dan akuntabilitasnya, seluruh Wajib Bayar diwajibkan membuat billing di Simponi, dan billing tersebut dapat disetorkan di seluruh Bank/Pos yang telah bergabung dengan Modul Penerimaan Negara Generasi kedua (MPN G2), tanpa batas waktu dan tempat. Pengguna simponi adalah seluruh wajib bayar pada satuan kerja Kementerian/Lembaga (K/L) yang memiliki PNBP Fungsional, Wajib Bayar SDA Migas dan Non Migas, BUMN Perbankan dan Non Perbankan.

Apabila aplikasi SIMPONI terhenti, maka akan terhentinya proses pembuatan billing untuk pembayaran PNBP baik oleh K/L maupun oleh pengguna layanan PNBP K/L (masyarakat). Dampaknya adalah terhentinya layanan oleh K/L kepada Masyarakat, wajib bayar dan pihak lain, potensi kerugian negara dengan tertundanya realisasi penerimaan negara, citra kemenkeu dan potensi tuntutan hukum dari wajib bayar.

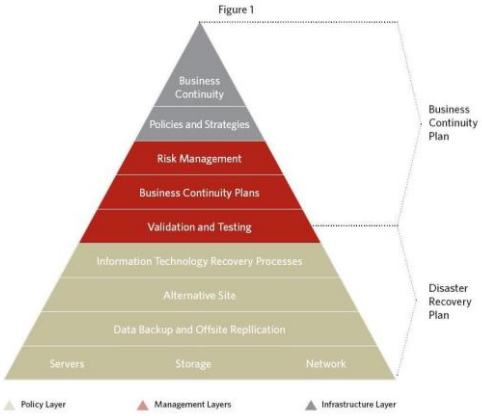
B. KONSEP DASAR DAN METODOLOGI PENGEMBANGAN *DISASTER RECOVER PLAN (DRP)* DAN *BUSINESS CONTINUITY PLAN*

Setiap hari, selalu ada kemungkinan terhadap terjadinya gangguan pada bisnis, krisis, bencana, atau keadaan darurat lainya. Apa pun yang dapat menggangu proses dan

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

aktivitas bisnis dapat didefinisikan sebagai bencana. Perusahaan dapat mengalami banyak ancaman gangguan yang berbeda terhadap aktivitas perusahaan, seperti untuk dipersiapkan ketika terjadi. Pemulihan bencana *(Disaster recovery)* menjadi masalah antara tahun 1960 ke tahun 1980 dan mensyaratkan untuk melakukan *backup* pada komputer *mainframe*. Saat ini pemulihan bencana telah dilakukan dengan menggabungkan semua skenario diperlukan untuk menjamin kesuksesan menjalankan sistem penting selama keadaan darurat terjadi dan termasuk saat pemulihan dari aktivitas bisnis (EKAM Solutions :1).

Dalam suatu jaringan komputer berskala bisnis dan enterprise, perencanaan suatu pemulihan adanya bencana dan kesinambungan bisnis (*Business continuity*) adalah suatu keharusan. Disaster *recovery* dan *business continuity* adalah dua proses yang berbeda akan tetapi keduanya biasanya digabungkan kedalam suatu kerangka kerja tunggal yaitu suatu perencanaan pemulihan bencana dan kesinambungan bisnis atau biasa disebut ***Business Continuity and Disaster Recovery Planning***.

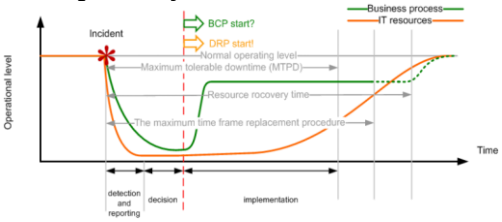


Gambar 2. Hubungan antara BCP dan DRP

kebakaran, banjir, badai petir, *hacker*, kesalahan manusia, listrik padam dan *virus* yang merusak sistem. Sebuah bencana dapat terjadi kapan saja dan itu adalah hal penting

Gambar 1. Perbedaan BCP dan DRP

Business continuity dan *disaster recovery planning* memberikan suatu kerangka kerja untuk membuat suatu penyelamatan /*recovery* infrastruktur IT dari segala macam bencana baik yang berskala kecil maupun besar. Suatu *disaster recovery* dan *business continuity* memberikan daftar yang sudah dibuat dan koordinasi dari langkah-langkah yang perlu dilakukan untuk meminimalkan efek-efek secara kesuluruhan dari suatu bencana. Sepanjang atau kelanjutan dari suatu bencana, dokumen *disaster recovery planning* membantu anda agar tidak sampai mengalami kebingungan apa yang mesti anda lakukan terlebih dahulu. Jadi ada kerangka kerja yang sudah di dokumentasikan sebelumnya, langkah-langkah yang harus di lakukan. Hal ini membantu dalam mempercepat pemulihan sistem kedalam level yang stabil untuk bisa beroperasinya bisnis anda kembali.



Business Continuity Plan (BCP)

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

a. Pengertian *Business Continuity Plan*. Usep (2005: 4) menyebutkan bahwa BCP adalah proses otomatis atau pun manual yang dirancang untuk mengurangi ancaman terhadap fungsi-fungsi penting organisasi, sehingga menjamin keberlangsungan layanan bagi operasi yang penting. Perencanaan keberlangsungan bisnis dibuat untuk mencegah tertundanya aktivitas bisnis normal. BCP didisain untuk melindungi proses bisnis vital dari kerusakan atau bencana yang terjadi secara alamiah atau perbuatan manusia, dan kerugian yang ditimbulkan dari tidak tersedianya proses bisnis normal (rutin, seperti biasa). BCP merupakan strategi untuk meminimalisir efek dari ganguan dan mengupayakan berjalannya kembali proses bisnis suatu organisasi atau perusahaan.

b. Manfaat dan Tujuan BCP. Kejadian atau hal-hal yang menahan proses bisnis adalah segala sesuatu gangguan keamanan yang terduga dan tak terduga yang bisa mematikan operasi normal bisnis dalam kurun waktu tertentu. Tujuan dari BCP adalah untuk meminimalisir efek dari kejadian atau bencana tersebut dalam sebuah perusahaan atau organisasi. Manfaat utama dari BCP adalah untuk mereduksi risiko kerugiaan keuangan dan meningkatkan kemampuan perusahaan untuk memulihkan diri dari bencana atau gangguan sesegera mungkin. Perencanaan keberlangsungan bisnis juga harus dapat membantu meminimalisir biaya dan mengurangi risiko sehubungan dengan kejadian bencana tersebut.

c. Fase – Fase Proses BCP

Gambar 3. *Business Continuity Plan Lifecycle*

Menurut standar *Certified Information System Security Proffesional* (CISSP), proses BCP meliputi 4 fase, yaitu :

d. Penetapan Ruang Lingkup dan Perencanaan. Pada fase ini kebutuhan akan ruang lingkup dari kondisi BCP direncanakan dimana semua elemen-elemen yang diperlukan seperti penanggung jawab pelaksana tindak saat bencana terjadi, area kritis yang perlu dilindungi dan perlu tetap berjalan setelah keadaan bencana terjadi didefnisikan. Pada fase ini, selain hal tersebut dana yang

dibutuhkan pada saat bencana dan pasca bencana perlu direncanakan dan di definisikan. Beberapa area kritis yang perlu di definisikan pada tahap ini meliputi :

1) Kebutuhan jaringan LAN, WAN dan komputer server;
2) Kebutuhan komunikasi data dan telekomunikasi;
3) Kebutuhan *workstation* dan ruang kerja sementara pasca bencana;
4) Kebutuhan aplikasi, perangkat lunak dan data (*backup*);
5) Kebutuhan akan media dan record penyimpanan data;
6) Kebutuhan sumber daya yang akan bertugas pasca bencana serta proses produksi dari organisasi.

e. Penetapan Business Impact Assessment (BIA)

Fase ini merupakan fase untuk membuat suatu dokumentasi yang digunakan untuk membantu *staf task force* saat bencana berlangsung. Dampak atas bencana pada dasarnya dikategorikan dalam 2 bentuk yaitu dampak yang berhubungan dengan nilai uang (bersifat kuantitatif) serta dampak yang berhubungan dengan operasional (kualitatif), analisa dampak tersebut di definisikan dan di buat panduannya, dimana penaksiran atas kelemahan yang muncul saat terjadinya bencana merupakan bagian dari BIA itu sendiri.

BIA memiliki 3 tujuan utama, yaitu :

1) *Criticality Prioritized*

Setiap proses bisnis yang bersifat kritis perlu di identifikasikan dan di klasifikasikan berdasarkan skala prioritas tertentu, dampak yang terjadi saat kegiatan bisnis berhentipun perlu di evaluasi. Proses bisnis yang bersifat *non time critical* di definisikan dalam skala prioritas yang lebih kecil saat proses *recovery* dari kegiatan di skalanya dengan jelas.

2) *Downtime Estimation*

Pada prinsipnya BIA dibuat untuk membantu memperkirakan Toleransi Maksimum Terhentinya Kegiatan (*Maximum Tolerable Downtime*/MTD), yaitu kondisi dimana berapa lama maksimum yang dibutuhkan oleh organisasi dalam proses pemulihan dirinya. Semakin lama periode terhentinya kegiatan bisnis maka semakin kritis organisasi tersebut dalam memulihkan diri. Tahapan ini perlu di rencanakan lama waktu *downtime* kegiatan bisnis dari suatu organisasi sehingga waktu pulih dari keadaan bencana dapat diperkirakan dan analisa atas kerugian kesempatan (*opportunity loss profit*) dapat dikurangi.

3) Kebutuhan Sumber Daya

Kebutuhan sumber daya saat proses bencana berlangsung

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

perlu di definisikan pada tahap ini, dimana kondisi yang cukup rumit akan terjadi sehingga alokasi sumber daya yang tepat merupakan hal yang perlu di perhatikan.

f. ***Pembuatan BCP***
Tahapan ini menggunakan informasi yang didapat pada proses BIA untuk mengembangkan *business continuity plan* yang sebenarnya. Proses pengembangannya adalah meliputi rencana implementasi, rencana pengujian, dan pemeliharaan rencana yang dijalankan. Tahapan ini juga menentukan strategi pengoperasian *business recovery* alternatif untuk pemulihan bisnis dan kapabilitas TI di dalam periode *recovery time* yang sudah ditentukan.

g. ***Persetujuan Rencana dan Implementasi***
Proses ini terdiri dari mendapatkan persetujuan akhir dari manajemen senior, penyiapan sebuah program *awareness korporat* dan menerapkan prosedur pemeliharaan untuk menyempurnakan rencana sesuai dengan kebutuhan.

Disaster Recovery Plan

a. Pengertian *Disaster Recovery Plan*. *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*. DRP menurut Nilla Racmaningrum dan Falahah (2011:2) pada seminar *Nasional Informatika 2011* DRP adalah proses, kebijakan dan prosedur yang berkaitan dengan persiapan pemulihan atau keberlangsungan infrastruktur teknologi yang kritis bagi organisasi setelah terjadinya bencana, baik bencana yang disebabkan oleh tindakan manusia ataupun bencana alam. *Disaster recovery* merupakan bagian dari *business continuity*. Dr. Jan Hoesad (2013) menyebutkan bahwa 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.

b. Tujuan dan Manfaat DRP. Perencanaan *disaster recovery* mengacu pada persiapan untuk menghadapi bencana dan respon yang harus diberikan ketika bencana terjadi. Tujuan DRP adalah meminimumkan risiko dan optimalisasi kesinambungan entitas dalam menghadapi risiko bencana. Apabila manajemen tak

mampu/tidak tahu merumuskan manfaat DRP, atau menyimpulkan bahwa manfaat DRP lebih kecil dari biaya DRP, maka program DRP tak akan dilaksanakan. 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.

c. Pedoman Standar Penyusunan DRP. Seiring dengan meningkatnya kebergantungan bisnis terhadap teknologi informasi maka meningkat juga risiko 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*) maupun eksternal (*outsourced*), dan meliputi fasilitas fisik dan layanan.

Spesifikasi ISO/IEC 24762 (2008) meliputi:

1) ***Kebutuhan untuk menerapkan, mengoperasikan, memonitor dan memelihara fasilitas dan layanan* disaster recovery *untuk Teknologi Informasi dan Komunikasi (TIK).***
2) ***Kemampuan yang harus dimiliki oleh layanan* disaster recovery *TIK eksternal dan pedoman praktis yang harus dijalankan untuk menyediakan lingkungan operasional minimal yang aman dan memfasilitasi usaha organisasi untuk melakukan pemulihan.***
3) ***Pedoman memilih situs* recovery *dan pedoman untuk peningkatan layanan* disaster recovery *TIK.***

d. Langkah-langkah pengelolaan DRP. Keberlangsungan (*continuity*) atau kemampuan organisasi untuk bertahan dalam menghadapi bencana. Proses penyusunan DRP meliputi analisis, perencanaan, pembuatan DRP, pengujian dan revisi periodik berdasarkan kondisi bisnis terkini. Penyusunan DRP untuk teknologi informasi di suatu organisasi, secara umum mengacu pada langkah-langkah pengelolaan proyek pada umumnya, yaitu : inisialisasi, eksekusi dan evaluasi. Pada tahap inisialisasi, diperlukan

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

dukungan manajemen dan kontrak proyek yang jelas antara manajemen yang berwenang dengan pihak yang akan menyusun DRP. Kontrak proyek ini diperlukan untuk menjaga konsistensi komitmen semua pihak yang terlibat. Pada tahap eksekusi, dilakukan sekumpulan aktivitas yang keluaran akhirnya diharapkan dapat menghasilkan dokumen DRP yang sesuai dengan kondisi dan kebutuhan organisasi. Menurut Peter Gregory (2007) Aktivitas tersebut antara lain:

1) ***Melakukan* Business Impact Analysis, *yang meliputi penentuan* maximum tolerable downtime *(MTD), penentuan* recovery objective *yang meliputi* recovery time objective *(RTO), dan* recovery point objective *(RPO), membuat analisis risik0, menyajikan semua hasil analisis dalam satu laporan terintegrasi.***
2) ***Mendefinisikan prosedur* recovery, *yaitu membuat DRP untuk setiap proses dengan cara memetakan proses dengan infrastruktur, membuat DRP dalam bentuk tertulis, dan menguji DRP tersebut.***
3) ***Evaluasi dan monitoring meliputi proses pengujian dan kaji ulang secara periodik misalnya setiap bulan, setiap 4 bulan atau tahunan. Tahap lainnya yaitu memberikan pelatihan yang memadai bagi semua tim DRP yang terlibat, khususnya tim* recovery.**

Gambar .4. Metodologi DRP

Business Impact Analysis

a. **Pengertian *Business Impact Analysis. Business Impact Analysis* (BIA) merupakan salah satu bagian dari rencana kelanjutan bisnis/*business continuity planning* (BCP) organisasi yang menggambarkan potensi risiko organisasi. Menurut Kusuma Wardani (2007) BIA adalah proses mengidentikasi, menganalisa, dan menentukan dampak yang terjadi pada kelangsungan bisnis proses di organisasi seandainya terjadi gangguan/bencana yang menimbulkan terhentinya operasional dari bisnis proses tersebut.**

b. **Tujuan BIA. BIA digunakan untuk mengukur tingkat kritikalitas layanan TIK dengan menentukan prioritas layanan TIK yang paling kritis ketika terjadi gangguan/bencana. Laporan hasil analisa dampak bisnis (BIA) dapat mengidentifikasikan biaya yang dikeluarkan jika layanan TIK tidak**

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

berfungsi kembali saat terjadi bencana, contohnya antara lain kehilangan daftar gaji pegawai yang seharusnya dilakukan tanggal 25 setiap bulan, kehilangan arus kas/*cash flow* keuangan organisasi, dan perbaikan/penggantian peralatan dan sebagainya. Selain dampak keuangan, laporan hasil BIA sebaiknya juga menilai dampak keamanan, pemasaran, kepatuhan hukum, dan jaminan kualitas setelah terjadinya bencana karena perlu strategi untuk membangun kepercayaan pelanggan.

c. **Implementasi BIA. Sebelum melakukan BIA, perlu disiapkan daftar layanan yang akan dilakukan *assessment*, nama serta kontak informasi dari pengguna yang akan dilakukan *assessment*, dan daftar pertanyaan yang nantinya digunakan untuk *assessment.* Sebaiknya *assessment* dilakukan kepada pengguna layanan TIK yang terkait karena pengguna lebih mengetahui sejauh mana kepentingan layanan TIK digunakan.**

Adapun daftar pertanyaan sebaiknya ada di dalam analisa dampak BIA antara lain:

1) ***Deskripsi organisasi (visi, misi dan strategis organisasi);***
2) ***Daftar jumlah pegawai mulai pegawai tetap, pegawai tidak tetap, pegawai magang, dan vendor/pihak ketiga;***
3) ***Penentuan bisnis proses utama organisasi;***
4) ***Urutan proses bisnis dari yang paling penting;***
5) ***Penentuan* Recovery Time Objective *(RTO)/Batas waktu pemulihan pada bisnis proses utama;***
6) ***Penentuan* Recovery point objective *(RPO)/Toleransi jumlah data yang hilang pada bisnis proses utama;***
7) ***Ketergantungan bisnis proses utama;***
8) ***Spesifikasi untuk mengoperasikan bisnis proses utama;***
9) ***Penentuan sub bisnis proses (Opsional);***
10) ***Penentuan peringkat prioritas sub bisnis proses (Opsional);***
11) ***Penentuan* Recovery time objective *(RTO)/Batas waktu pemulihan pada sub bisnis proses (Opsional);***
12) ***Penentuan* Recovery point objective *(RPO)/Batas waktu pemulihan pada sub bisnis proses (Opsional);***
13) ***Ketergantungan sub bisnis proses(Opsional);***
14) ***Spesifikasi untuk mengoperasikan sub bisnis proses (Opsional);***
15) ***Dampak finansial jika terjadi gangguan/bencana;***
16) ***Dampak non finansial jika terjadi gangguan/bencana;***
17) ***Waktu untuk memulihkan staff;***
18) ***Strategi pemulihan;***

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

19) Teknologi/jasa yang diperlukan untuk pemulihan.

Setelah di *assessment* dengan menggunakan BIA, setiap bagian di dalam organisasi perlu mengadakan diskusi agar semua bagian yang memiliki layanan TIK kritis dapat tersedia saat terjadi bencana. Kemudian, hasil *assessment* dibuat ke dalam bentuk daftar dengan mengelompokkan layanan TIK menjadi satu. Adapun penentuan tingkat kritikalitas layanan TIK dibagi menjadi 3, yaitu :

1) ***Tingkat kritikalitas* high*/tinggi. Layanan TIK yang memiliki tingkat kritikalitas tinggi akan di*-backup *dengan baik dan disimpan di DRC.***
2) ***Tingkat kritikalitas* medium*/sedang. Layanan TIK yang memiliki tingkat kritikalitas sedang mempunyai perlakuan yang sama dengan tingkat kritikalitas tinggi yaitu akan di*-backup *di DRC***
3) ***Tingkat kritikalitas* low*/rendah. Untuk layanan TIK yang memiliki tingkat kritikalitas rendah akan di*-backup *dan tidak disimpan di DRC tetapi bisa disesuaikan dengan kebijakan manajemen di organisasi tersebut.***

Untuk menentukan prioritas tingkat kritikalitas layanan BIA dapat dilihat dari jumlah pengguna yang terkena dampak akibat gangguan/bencana yang terjadi dan biaya yang dikeluarkan untuk pemulihan. Jumlah pengguna yang terkena dampak disesuaikan dengan jumlah data pengguna yang selama ini menggunakan layanan tersebut kemudian dibagi menjadi tiga bagian, yaitu tinggi, sedang, dan rendah. Sedangkan, biaya yang dikeluarkan diurutkan berdasarkan layanan TIK yang mengeluarkan biaya terbanyak diprioritaskan menjadi tinggi, selanjutnya sedang, dan rendah jika biaya yang dikeluarkan sedikit.

C. MANFAAT APLIKASI SIMPONI DAN PROSEDUR PEMULIHAN SISTEM

1. ***Standarisasi dan Penyederhanaan proses pengisian data dalam rangka pembayaran dan penyetoran PNBP;***
2. ***Menghindari atau meminimalisir kemungkinan terjadinya* human error *dalam perekaman data pembayaran dan penyetoran PNBP;***
3. ***Memberikan kemudahan dan fleksibilitas melalui beberapa alternatif saluran pembayaran dan penyetoran PNBP;***
4. ***Memberikan akses kepada Wajib Bayar dan Wajib Setor PNBP untuk memonitor status atau***

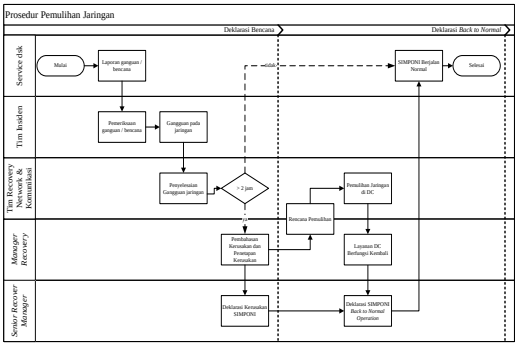
Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

realisasi pembayaran dan penyetoran PNBP.

1. Mekanisme Pembayaran/Penyetoran PNBP Menggunakan Simponi

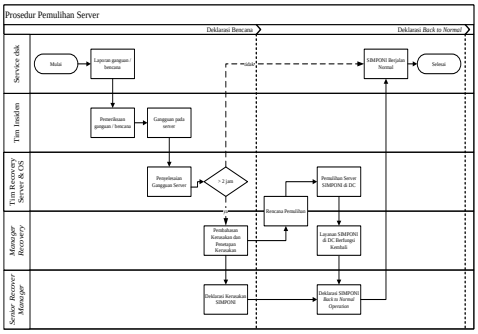
Gambar 5. Mekanisme Pembayaran/Penyetoran

2. Prosedur Pemulihan Gangguan Jaringan Layanan SIMPONI



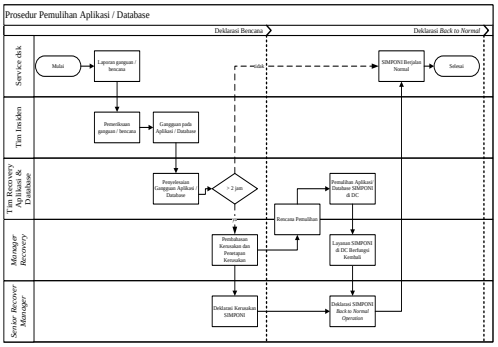
Gambar 6. Flowchart Pemulihan Layanan Jaringan SIMPONI

3. Prosedur Pemulihan Gangguan Server Layanan SIMPONI



Gambar 7. Flowchart Pemulihan Server Layanan SIMPONI

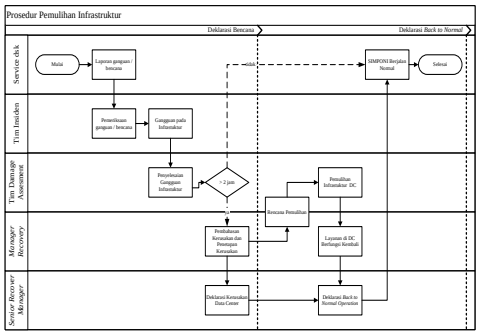
4. Prosedur Pemulihan Gangguan Aplikasi/Database Layanan SIMPONI



Gambar 8. Flowchart Pemulihan Aplikasi/Database Layanan SIMPONI

5. Prosedur Pemulihan Gangguan Infrastuktur *Data Center*

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)



Gambar 9. Flowchart Pemulihan Infrastuktur *Data Center*

D. PENGEMBANGAN DAN IMPLEMENTASI SISTEM

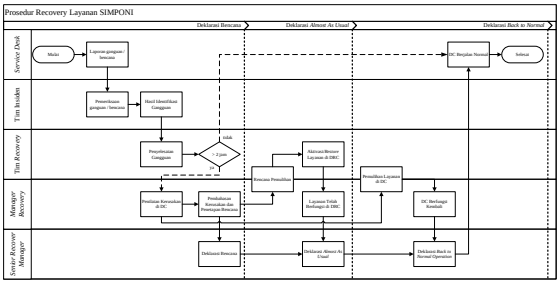
1. **Perancangan Prosedur. Perancangan prosedur pemulihan layanan SIMPONI yang diusulkan :**
   a. ***Apabila Tim* Recovery *tidak dapat memulihkan layanan SIMPONI dalam waktu kurang dari 2(dua) jam, maka kerusakan yang menyebabkan layanan terhenti akan dilaporkan ke* Manager Recovery.**

Manager Recovery *berkoordinasi dengan Tim* Recovery *melakukan penilaian terhadap kerusakan di DC Kemenkeu, mengaktivasi layanan SIMPONI di DRC Kemenkeu dan melakukan pemulihan layanan di DC Kemenkeu.*

Senior Recovery Manager *menerima hasil laporan penilaian kerusakan, memerintahkan aktivasi layanan di DRC Kemenkeu dan menerima hasil laporan pemulihan layanan.*

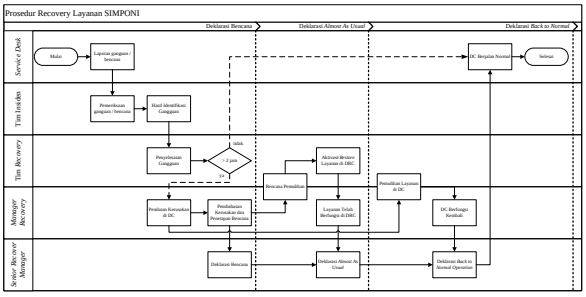
Adapun pemodelan rancangan yang diusulkan akan berorientasi objek dengan menggunakan *flowchart* dan notasi UML yang berfungsi sebagai perancangan, dokumentasi dan visualisasi :

2. ***Flowchart Prosedur Pemulihan Layanan SIMPONI Usulan***



Gambar 10. *Flowchart* Prosedur Pemulihan layanan SIMPONI

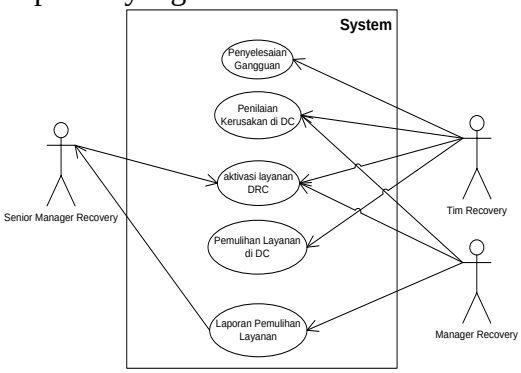
3. ***Flowchart Prosedur Pemulihan Layanan SIMPONI***



Gambar 11. *Flowchart* Prosedur Pemulihan layanan SIMPONI Usulan*Use Case Diagram*

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

Berikut ini *use case* yang menggambarkan tambahan proses yang diusulkan.



Gambar 12. *Use Case Diagram*

Skenario *Use Case* Penyelesaian Gangguan Layanan SIMPONI

Aktor : Tim *Recovery*

Skenario : Penyelesaian Gangguan Layanan SIMPONI

Aktor	Sistem
1. Melakukan penilaian kerusakan di DC Kemenkeu yang menyebabkan layanan SIMPONI terhenti.	
	2. Membuat laporan hasil penilaian kerusakan dan rekomendasi untuk aktivasi layanan SIMPONI di DRC Kemenkeu.
	3. Laporan akan diteruskan ke *Manager Recovery*.

Tabel 1. Skenario Penyelesaian Gangguan Layanan SIMPONI

Aktor	Sistem
4. Melakukan penyelesaian terhadap gangguan yang menyebabkan layanan SIMPONI terhenti.	
	5. Jika gangguan diselesaikan kurang dari 2

	jam, maka sistem akan meneruskan ke *Service Desk*, jika gangguan tidak dapat diselesaikan dalam waktu 2 jam, maka sistem akan meneruskan ke *Manager Recovery*.

Skenario *Use Case* Penilaian Kerusakan di DC Kemenkeu

Aktor : Tim *Recovery* dan *Manager Recovery*
Skenario : Penilaian Kerusakan di DC Kemenkeu

Tabel 2. Skenario Penilaian Kerusakan di DC Kemenkeu

Skenario *Use Case* Aktivasi Layanan di DRC Kemenkeu

Aktor : Tim *Recovery*, *Senior Recovery Manager* dan *Manager Recovery*
Skenario : Aktivasi Layanan di DRC Kemenkeu

Tabel 3. Skenario Aktivasi Layanan di DRC Kemenkeu

Aktor	Sistem
6. Deklarasi Bencana dan penetapan untuk melakukan aktivasi layanan SIMPONI di DRC Kemenkeu.	
7. Melakukan aktivasi layanan SIMPONI di DRC Kemenkeu.	
8. Layanan SIMPONI berjalan di	

DRC.	
	9. Membuat laporan layanan SIMPONI berjalan di DRC Kemenkeu.
	10. Laporan akan diteruskan ke *Service Desk.*

Skenario *Use Case* Pemulihan Layanan di DC Kemenkeu

Aktor : Tim *Recovery*

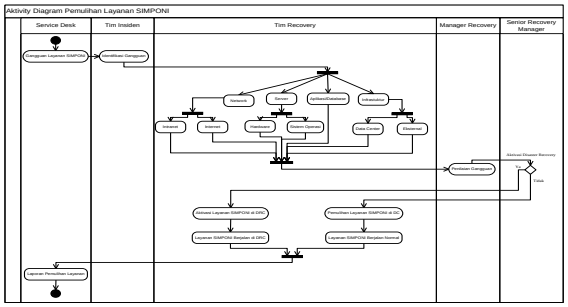
Skenario : Pemulihan Layanan di DC Kemenkeu

Tabel 4 Skenario Pemulihan Layanan di DC Kemenkeu

Aktor	Sistem
11. Melakukan Pemulihan Layanan SIMPONI di DC Kemenkeu.	
12. Layanan di DC Kemenkeu dapat berjalan normal kembali	
	13. Membuat laporan layanan SIMPONI berjalan di DC.
	14. Laporan akan diteruskan ke *Manager Recovery* dan *Senior Manager Recovery*..

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

4. Activity Diagram *Prosedur Pemulihan Layanan SIMPONI*

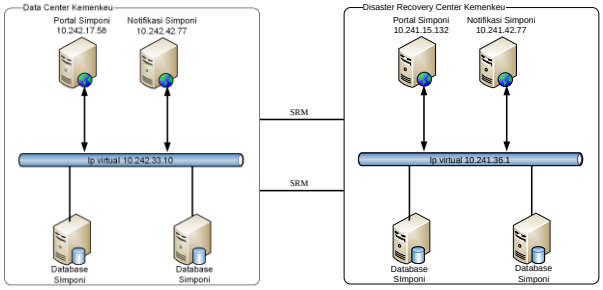


Gambar 13. *Activity Diagram* Prosedur Pemulihan layanan SIMPONI

5. Deployment Diagram *Pemulihan Layanan SIMPONI*

Diagram ini memperlihatkan pemetaan perangkat server, jaringan dan aplikasi/database. Diagram ini menggambarkan detail bagaimana komponen deployment dalam infrastruktur system yang di kembangkan.

4) *Deployment Diagram* Perangkat Server di DRC



Gambar 14. Topologi Server SIMPONI

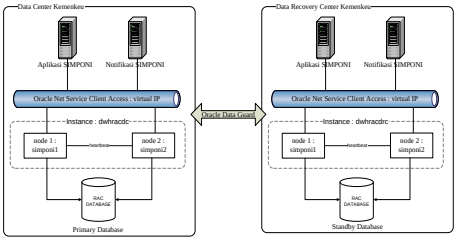
Penjelasan :

a) Replikasi seluruh perangkat server di DRC menggunakan *tools VMware vSphere*;

b) *IP Address* pada perangkat server disesuaikan dengan *segmentasi* jaringan yang ada di DRC Kemenkeu;

c) Aktivasi teknologi SRM pada seluruh perangkat Server SIMPONI.

5) *Deployment Diagram* Perangkat Database di DRC



Gambar 15. Topologi Database SIMPONI

Penjelasan :

a) Aktifkan fitur *Oracle Data Guard* (ODG) pada database SIMPONI dengan cara membuat *primary* database di DC Kemenkeu dan *standby* database di DRC Kemenkeu menggunakan *tools Oracle 11.2g R2*;

b) Mekanisme *update standby* database menggunakan mekanisme *apply archived log* dengan tipe *physical standby* database.

c)

6. Implementasi Sistem

a. Spesifikasi Sistem.

Dalam pengaplikasian sistem pemulihan layanan SIMPONI ini, ada

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

Perangkat Lunak	Keterangan
Linux Ubuntu versi 16.04	Sebagai OS server Aplikasi
SunOS 5.10	Sebagai OS server Database
*Cent*OS 7	Sebagai OS server Notifikasi
Windows Server 2008	Sebagai OS server Active Direktory
Apache versi 2.4	Sebagai *Web Service* Aplikasi
PHP versi 5.6.3	Pemograman web aplikasi
mutt	Untuk *email-gateway*
VMware vSphere Client	Untuk mengelola server VM
Oracle versi *11.2g*	Sebagai DBMS SIMPONI
Oracle Enterprise Manager Cloud Control 12c	Untuk mengelola RAC database SIMPONI
winsCP	Untuk mengakses server
toad	Untuk mengakses remote database
putty	Untuk mengakses dan mengelola jaringan

beberapa hal yang harus disiapkan antara lain perangkat keras (*Hardware*), perangkat lunak (*Software),* hak akses (*Brainware*) dan perangkat jaringan yang dibutuhkan dalam

menjalankan sistem ini. Diantaranya :

***b. Spesifikasi* Hardware**

Perangkat server* virtual machine, *dengan spesifikasi minimum sebagai berikut :

Tabel 5. Spesifikasi Server Aplikasi SIMPONI di DC

Spesifikasi Server Aplikasi SIMPONI	
CPU	3,2 GHz
CPU Core	8 Core
RAM	32 Gb
Harddisk	138 Gb

Tabel 6. Spesifikasi Server Database SIMPONI di DC

Spesifikasi	Server DB 1	Server DB 2 SIMPONI

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

	SIMPONI	
CPU	2,8 GHz	2,8 GHz
CPU *Core*	16 *Core*	16 *Core*
RAM	64 Gb	64 Gb
Harddisk	200 Gb	200 Gb

Tabel 7. Spesifikasi Server Notifikasi SIMPONI di DC

Spesifikasi Server Notifikasi SIMPONI	
CPU	1,2 GHz
CPU *Core*	4 *Core*
RAM	16 Gb
Harddisk	120 Gb

7. *Spesifikasi* Software

Perangkat Lunak yang diperlukan untuk sistem pemulihan layanan ini adalah :

Tabel 8. Spesifikasi *Software*

8. *Spesifikasi Perangkat Jaringan*

Perangkat jaringan yang diperlukan untuk sistem pemulihan layanan ini adalah *link* yang menghubungan jaringan di DC Kemenkeu dan DRC Kemenkeu.

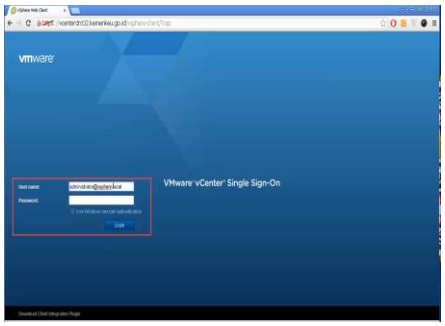
9. *Spesifikasi* Brainware

Adapun kebutuhan hak akses yang dibutuhkan dalam mengoperasikan sistem pemulihan ini yaitu Tim Operasional DRC, Admin Server, Admin Jaringan, Admin Database dan Admin Aplikasi. Tahap implementasi merupakan tahap kelanjutan dari kegiatan perancangan sistem. Wujud dari hasil implementasi ini nantinya adalah sebuah sistem yang siap untuk diuji dan digunakan.

10. *Implementasi* Hardware

Mengaktifkan *Recovery Plan* Aplikasi SIMPONI dan Notifikasi SIMPONI di DRC dengan langkah sebagai berikut :

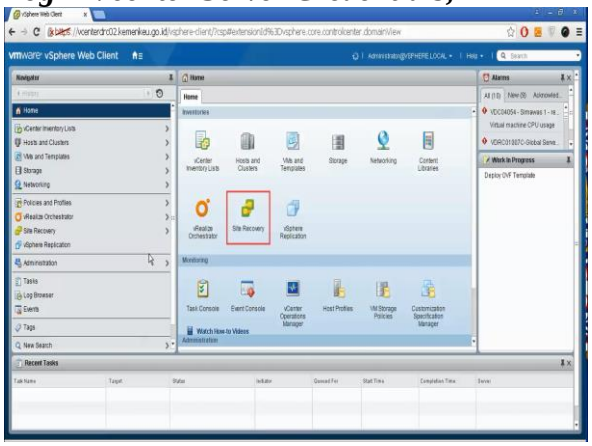
Login ke dalam* Vcenter *menggunakan* tools VMware vSphere Client *Sebagai Administrator;



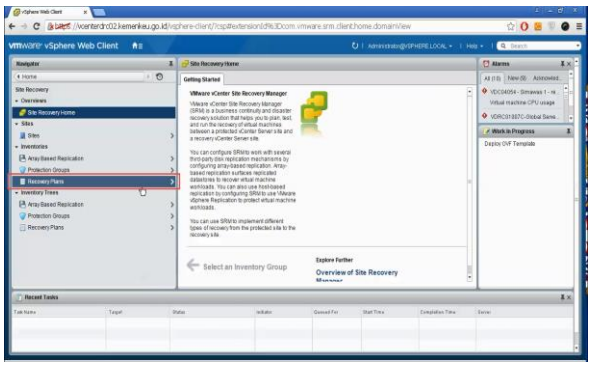
Gambar 16. Halaman *Login Vcenter*

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

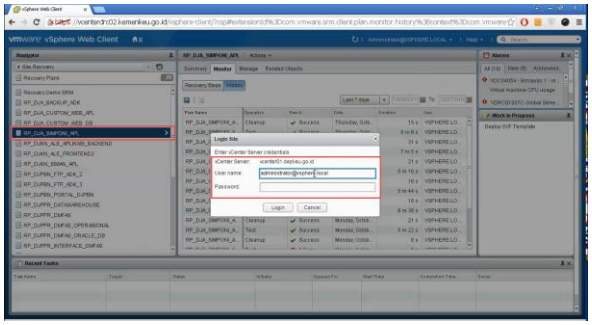
Pilih Site Recovery → Recovery Plan → Login Vcenter Server Credentials;



Gambar 17. Halaman *Home Vcenter*

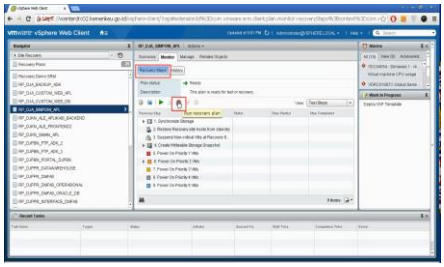


Gambar 18. Halaman *Site Recovery Vcenter*



Gambar 19. Halaman *Recovery Plan Vcenter*

Pilih RP_DJA_SIMPONI_APL → Run Recovery;



Gambar 20. Halaman *Recovery Plan* Aplikasi SIMPONI

Pilih Recovery Confirmation, pilih Disaster Recovery;

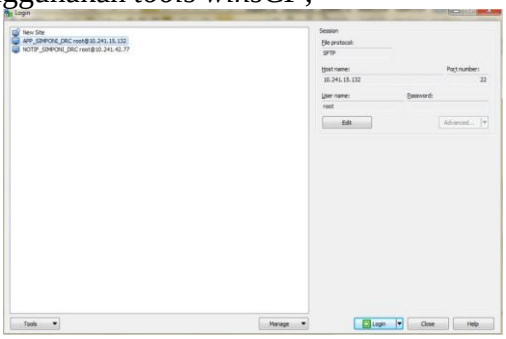
Pilih* Finish,*tunggu hingga proses* recovery *selesai;

Jalankan* reprotect recovery *plan RP_DJA_SIMPONI_ APL;

Lakukan tahap yang sama seperti poin c, d dan e, pada RP_DJA_SIMPONI_NOTIF.

Implementasi* Software, *Mengaktifkan Aplikasi dengan cara melakukan perubahan koneksi DNS ke Server Aplikasi SIMPONI di DRC Kemenkeu, dengan langkah sebagai berikut :

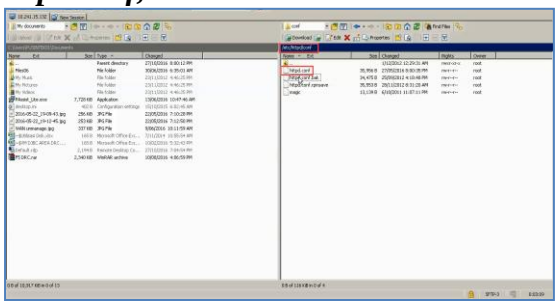
Login ke server Aplikasi menggunakan *tools winsCP*;



Gambar 21. *Login* WinSCP Aplikasi SIMPONI

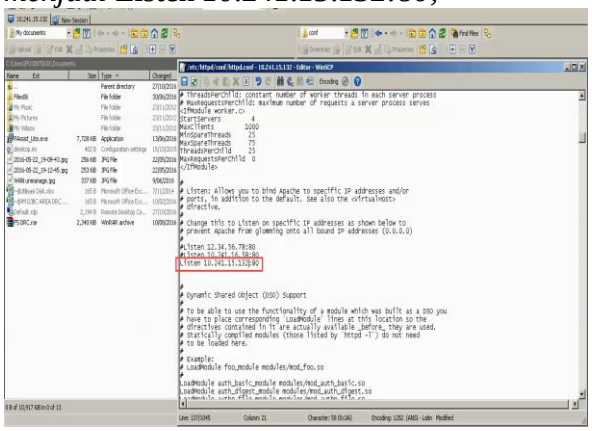
Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

Masuk* direktori */etc/httpd/conf* → *edit file httpd.conf;



Gambar 22. *Direktori*: etc/httpd/config

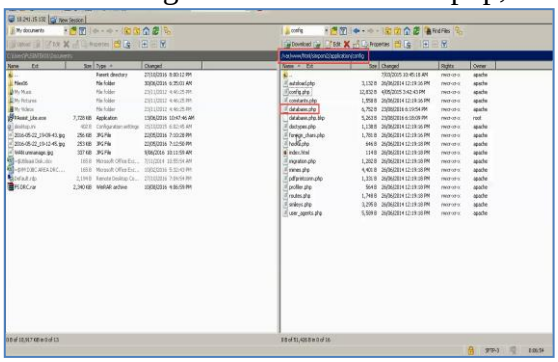
Cek/Ubah syntax Listen *10.242.17.58:80 menjadi* Listen *10.241.15.132:80;*



Gambar 23. *File* httpd.conf

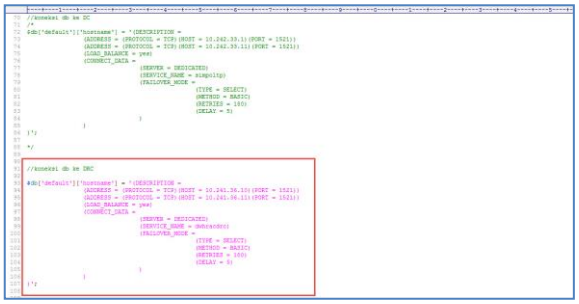
Restart service *httpd Aplikasi SIMPONI* →login telnet *10.241.15.132 menggunakan user* root →*service httpd restart; Melakukan perubahan koneksi database di server Aplikasi ke Server database di DRC Kemenkeu, dengan cara sebagai berikut :*

Masuk,*direktori*/var/www/html/simponi2/application/ config → edit file database.php;



Gambar 24. *Direktori*:/var/www/html/simponi2/application/config

Merubah konfigurasi koneksi database di Aplikasi SIMPONI di DRC Kemenkeu dari IP 10.242.33.1, 10.242.33.11 menjadi 10.241.36.10, 10.242.36.11;

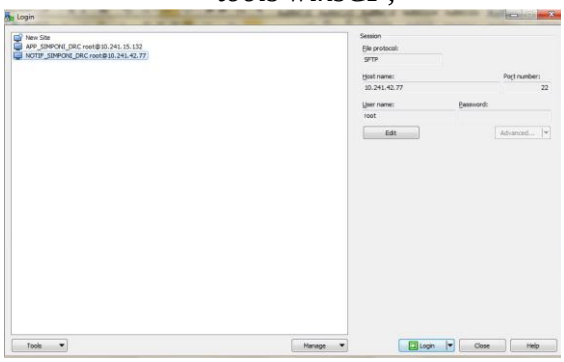


Gambar 25. *Konfigurasi* Koneksi Aplikasi ke Database

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

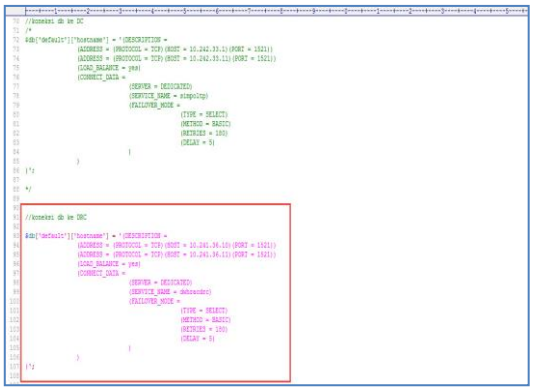
Melakukan perubahan koneksi database Server Notifikasi ke server database di DRC Kemenkeu, dengan cara sebagai berikut :

Login ke server Notifikasi menggunakan *tools winsCP*;



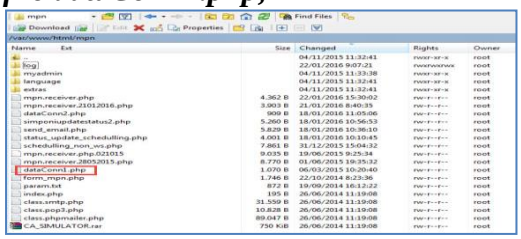
Gambar 26. *Login* WinSCP Notifikasi SIMPONI

Merubah konfigurasi koneksi database di Notifikasi SIMPONI di DRC dari IP 10.242.33.1, 10.242.33.11 menjadi 10.241.36.10, 10.242.36.11;



Gambar 28. *Konfigurasi* Koneksi Notifikasi ke Database

Masuk* direktori */var/www/html/mpn* → *edit file dataConn1.php;



Gambar 27. *Direktori*: /var/www/html/mpn

Restart service *httpd Notifikasi SIMPONI* →login telnet *10.241.42.77 menggunakan user* root→*service httpd restart.* Restart *database SIMPONI pada Server Database dengan nama* service dwhracdrc *menggunakan* tools toad, *dengan cara sebagai berikut :*

Login *user sebagai* sysdba → *Cek role pada standby database apakah dalam keadaan s*tandby →*SQL*>select name,open_mode,database_role from v$database*; Lakukan* convert *dari* standby *database menjadi* primary *database* → *SQL>alter database recover managed standby database finish;* → *SQL>alter database activate standby database;*

Matikan database→SQL> shutdown immediate;

Hidupkan kembali database→SQL> startup;

Cek Status database apakah suda menjadi primary→ SQL>select name,open_mode,database_role from v$database.

11. *Implementasi Jaringan*

Merubah jalur *routing IP Public* SIMPONI sehingga akses layanan SIMPONI berada di DRC Kemenkeu, dengan langkah sebagai berikut :

ke *router* MPN yang ada di DC Kemenkeu, menggunakan *tools putty* → hapus IP NAT 10.242.17.52*;*

Masuk ke router *MPN yang ada di DRC Kemenkeu, menggunakan* tools putty → *tambahkan NAT* IP Publik *dari 10.241.15.132 ke 202.137.xxx.xxx;*

Melakukan Advertise *IP 202.137.xxx.xxx/32 di router MPN DRC Kemenkeu.*

Merubah DNS www.simponi.kemenkeu.go.id sehingga akses layanan SIMPONI berada di DRC Kemenkeu, dengan langkah sebagai berikut :

Remote desktop server *active direktory* Kemenkeu dengan *IP address* 10.242.xxx.xxx;

Masuk DNS *Management* → ganti alias DNS www.simponi.kemenkeu.go.id dari 10.242.17.58 ke 10.241.15.132.

E. KESIMPULAN

Setelah di analisa dan melakukan proses pengembangan suatu aplikasi simponi maka dapat di simpulkan : Deklarasi bencana dan pengaktifan layanan di DRC dilakukan apabila terjadi bencana yang menyebabkan kerusakan katastropik dan kerusakan mayor yang menyebabkan layanan di DC terhenti dan tidak bisa dipulihkan dalam waktu kurang dari 2 (dua) jam (*downtime system* > RTO). Strategi *backup offline* harian dilakukan secara *incremental* setiap hari Senin hingga Kamis, dan secara *full backup* setiap hari Jumat dan di simpan di TIK Pusat. Strategi *Redundancy* sudah ada di seluruh aspek penting di infrastruktur DC antara lain jaringan, suplai listrik, sistem pendingan ruangan DC, *hardware* server, dan komponen *software.* Pemanfaatan layanan *hosting* di DRC kemenkeu dapat di implementasikan untuk layanan SIMPONI. pemulihan layanan usulan penulis dapat digunakan sebagai *backup* sistem SIMPONI dengan meminimalisir *downtime* sistem. Pemutakhiran BIA harus dilakukan guna mengetahui tingkat kritikalitas layanan SIMPONI.

F. REFERENSI

[1] Alih. 2010. *Disaster Recovery Planning.* Diambil dari http://www.jaringan-komputer.cv-sysneta.com/disaster-recovery-planning. (3 April 2017).

[2] Carolina, Julia. Pembuatan DRP berdasarkan ISO/IEC 24762:2008. Surabaya: ITS.

[3] *Certified Information System Security Proffesional* (CISSP). *Business Continuity Plan.* Diambil dari https://ipqi.org/business-continuity-plan-bcp-2. (3 April 2017).

[4] EKAM Solutions Ltd. *Disaster Recovery.* Waterford : Enterprise House.

[5] Gregory, Peter. 2007. *IT Disaster Recovery Planning for Dummies*. New York :Willey Publishing

[6] Hoesada, Jan, Dr. *Disaster Recovery Planning: Manajemen Bencana Administrasi dan Akuntansi.* Diambil dari http://crmsindonesia.org/knowledge/crms-articles/disaster-recovery-planning-manajemen-bencana-administrasi-dan-akuntansi. (5 April 2017)

[7] International Organization for Standardization. *Managing crises with new ISO/IEC standard for IT disaster recovery*. Diambil dari

https://www.iso.org/standard/41532.html. (5 April 2017)

[8] Mayasari, Winda. 2015. *Business Impact Analysis* (BIA) Tahun 2015, Jakarta: Kementerian Keuangan.

[9] Rachmaningrum, Nilla dan Falahah. 2011. Studi Kelayakan Disaster Recovery Plan pada Infrastruktur Jaringan Komputer. Yograkarta : Seminar Nasional Informatika.

[10] Solehudin, Usep. 2005. *Business Continuity and Disaster Recovery Plan*. Jakarta:Universitas Indonesia.

[11] Wardani, Kusuma. 2007. Pentingnya Analisa Dampak Bisnis/*Business Impact Analysis* (BIA) Bagi Organisasi. Diambil dari https://www.ilmukomputer.com. (5 April 2017)

[12] Keputusan Menteri Keuangan No 64-2012, tentang Kebijakan dan Standard Manajemen Layanan Teknologi Informasi dan Komunikasi Area Service Delivery.

[13] Undang Undang No 24 Tahun 2007, Tentang Penanggulangan Bencana.

.