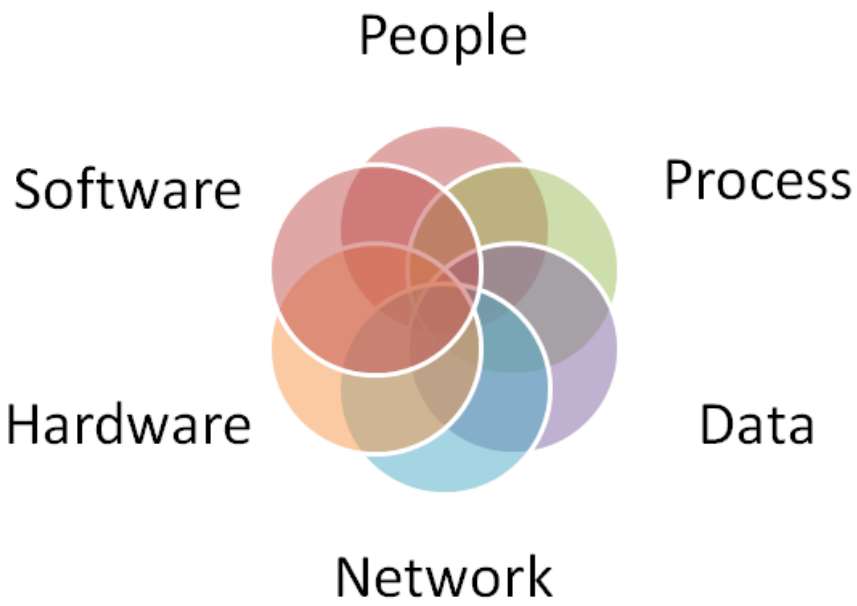
OAJIS
Open Access
Journal of
Information
Systems
is.its.ac.id/pubs/oajis/

ISSN 1979-3979

jurnal sisfo

Inspirasi Profesional Sistem Informasi

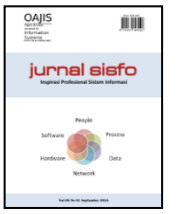


Vol. 12 No. 01 Mei 2025

OAJIS
Open Access
Journal of
Information
Systems
is.its.ac.id/pubs/oajis/

jurnal sisfo

Jurnal Sisfo Vol. 12 No. 01 (2025) i–ii



Sekretariat

Departemen Sistem Informasi – Fakultas Teknologi Elektro dan Informatika Cerdas
Institut Teknologi Sepuluh Nopember (ITS) – Surabaya
Telp. 031-5999944 Fax. 031-5964965
Email: editor@jurnalsisfo.org
Website: http://jurnalsisfo.org

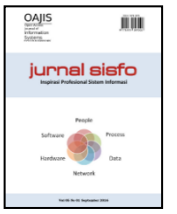
Jurnal SISFO juga dipublikasikan di *Open Access Journal of Information Systems* (OAJIS)

Website: http://is.its.ac.id/pubs/oajis/index.php

OAJIS
Open Access
Journal of
Information
Systems
is.its.ac.id/pubs/oajis/

jurnal sisfo

Jurnal Sisfo Vol. 12 No. 01 (2025) i–ii



Mitra Bestari

Prof. Nur Aini Rakhmawati, S.Kom., M.Sc.Eng., Ph.D
(Institut Teknologi Sepuluh Nopember)

Dr. Jusak (James Cook University, Singapore)

Dr. Muhammad Ainul Yaqin, S.Si., M.Kom. (UIN Maulana Malik Ibrahim)

Dr. Bambang Setiawan, S.Kom., M.T. (Institut Teknologi Sepuluh Nopember)

Dr. Feby Artwodini, S.Kom., M.T. (Institut Teknologi Sepuluh Nopember)

Arif Wibisono, S.Kom., M.Sc., Ph.D. (Institut Teknologi Sepuluh Nopember)

Dr. Agus Subhan Akbar, S.Kom, M.Kom. (Universitas Islam Nahdlatul Ulama Jepara)

Ir. Nunik Endah Sulistiyawati, M.T. (TNI AL, Indonesia)

Dhiani Tresna Absari, S.T. M.Kom. (Universitas Surabaya)

Muhamad Amirul Haq, S.T., M.Sc. (Universitas Muhammadiyah Surabaya)

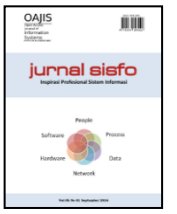
Ronny Trian Surbakti S.IP., M.M. (Universitas Katolik Parahyangan)

Agus Dwi Purwolastono, SE, M.Acc, Ak. (Institut Teknologi Sepuluh Nopember)

OAJIS
Open Access
Journal of
Information
Systems
is.its.ac.id/pubs/oajis/

jurnal sisfo

Jurnal Sisfo Vol. 12 No. 01 (2025) iii



Daftar Isi

OAJIS
Open Access
Journal of
Information
Systems
is.its.ac.id/pubs/oajis/

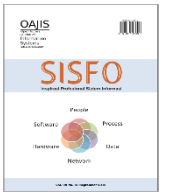
jurnal sisfo

Jurnal Sisfo Vol. 12 No. 01 (2025) iv

Halaman ini sengaja dikosongkan

OAJIS
Open Access Journal of Information Systems
is.its.ac.id/pubs/oajis/

SISFO
Inspirasi Profesional Sistem Informasi
Jurnal SISFO Vol.12 No.01 (2025) 81–96



Penyusunan Disaster Recovery Planning (DRP) Pada Data Center Unusa Menggunakan NIST 800-34

Riko Adi Kurniawan*, Endang Sulistiyani

Sistem Informasi, Fakultas Ekonomi Bisnis dan Teknologi Digital, Universitas Nahdlatul Ulama Surabaya

Abstract

The data center at Universitas Nahdlatul Ulama Surabaya (Unusa) has an important role in campus operational. However, its management depends on staff member from the Directorate of Information Systems, which increases risks if disasters or threats happen. This study develops a Disaster Recovery Plan (DRP) using the NIST 800-34 approach. The research consists of three main stages: (1) Reviewing the existing conditions and data center management, (2) Assessing the risks of Information Technology (IT) assets, and (3) Formulating the DRP based on NIST 800-34. The study results a DRP document that includes the DRP organizational structure, effective recovery strategies based on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), and procedures for ensuring the continuity of data center operations. The integration of these standards aims to balance technical aspects and risk management to enhance the resilience of Unusa's data center services.

Keywords: Data Center, DRP, NIST 800-34, Risk

Abstrak

Data center di Universitas Nahdlatul Ulama Surabaya (Unusa) memiliki peran vital dalam operasional kampus, tetapi pengelolaannya sangat bergantung pada staf dari Direktorat Sistem Informasi (Dir.SI), yang meningkatkan risiko jika terjadi bencana atau ancaman. Penelitian ini menyusun *Disaster Recovery Plan* (DRP) dengan pendekatan NIST 800-34. Terdapat tiga tahapan utama dalam penelitian ini: (1) Kajian kondisi eksisting dan manajemen *data center*, (2) penilaian risiko aset Teknologi Informasi (TI), dan (3) penyusunan DRP berdasarkan NIST 800-34. Penelitian ini menghasilkan dokumen DRP yang mencakup struktur organisasi DRP, strategi pemulihan efektif berdasarkan *Recovery Time Objectives* (RTO) dan *Recovery Point Objectives* (RPO), serta prosedur keberlanjutan operasional data center. Integrasi kedua standar ini bertujuan untuk menyeimbangkan aspek teknis dan manajemen risiko dalam meningkatkan ketahanan layanan *data center* Unusa.

Kata kunci: *Data center, DRP, NIST 800-34,* Risiko

Histori Artikel: Disubmit 17-02-2025; Direvisi 27-03-2025; Diterima 08-04-2025; Tersedia online 31-05-2025

*Corresponding Author
Email address: rikoadik@unusa.ac.id (Riko Adi Kurniawan)
https://doi.org/10.24089/j.sisfo.2025.07.006

1. Pendahuluan

Data center merupakan salah satu komponen vital dalam operasional sebuah perguruan tinggi di era digital saat ini. *Data center* berfungsi sebagai tempat penyimpanan dan pengolahan data perguruan tinggi [1]. Tidak hanya sebagai infrastruktur fisik, data center juga berfungsi menjaga layanan dan aplikasi secara berkelanjutan [2].

Universitas Nahdlatul Ulama Surabaya (Unusa) merupakan salah satu institusi perguruan tinggi yang memanfaatkan *data center* sebagai infrastruktur teknologi informasinya. *Data center* Unusa dikelola oleh Direktorat Sistem Informasi (Dir.SI), dengan lokasinya terpusat di lantai 2 dan 7 Unusa tower kampus B. Namun, pengelolaan *data center* Unusa ini menghadapi masalah besar. Hanya ada satu staf Dir.SI yang ditunjuk untuk menjaga keberlanjutan dan keberfungsian *data center*. Pengelolaanya dilakukan dengan tanpa adanya dokumentasi prosedur penanganan bencana. Sedangkan berbagai risiko mengancam keberlangsungan operasional *data center*. Mulai dari *human error*, kegagalan sistem, kerusakan *hardware*. Di sisi lain, keberlangsungan operasional *data center* menjadi sebuah kebutuhan dan keharusan agar keberlangsungan layanan Unusa tetap terjaga. Sebagaimana disimpulkan oleh peneliti lain [1] dalam penelitiannya tentang sistem *Disaster Recovery Plan* dengan metode *failover* berbasis Linux di Politeknik Negeri Malang menyimpulkan bahwa perguruan tinggi adalah entitas dengan layanan informasi yang kompleks. Layanan informasi ini tidak hanya ditujukan untuk civitas akademika di lingkungan internal, tetapi juga untuk alumni dan masyarakat umum, sehingga mendorong Perguruan Tinggi untuk memiliki sistem informasi yang berkualitas tinggi [1].

Terkait dengan keberlanjutan operasional *data center*, terdapat beberapa penelitian yang relevan. Pertama, penelitian [1] tentang Implementasi DRP *Server System* dengan metode *failover* berbasis Linux di Politeknik Negeri Malang menyebutkan bahwa implementasi DRP merupakan solusi dalam memastikan keberlanjutan operasional layanan teknologi informasi [1]. Namun, dalam penelitian [1] hanya berfokus kepada implementasi DRP berbasis Linux saja, dan belum menerapkan standar DRP. Kedua, penelitian [3] menggunakan pendekatan kerangka NIST 800-34 dan menyimpulkan bahwa DRP adalah langkah preventif dalam menjaga keberlangsungan suatu sistem terutama saat terjadi ancaman [3]. Namun, meskipun penelitian [3] menggunakan kerangka NIST 800-34, studi ini kurang memperhitungkan variabel eksternal seperti faktor manusia dan infrastruktur yang dapat mempengaruhi keberhasilan DRP. Ketiga, penelitian [4] terkait perancangan DRP menggunakan kerangka NIST 800-34 menyimpulkan bahwa penyusunan DRP memerlukan penentuan skala prioritas tinggi dan rendah pada masing-masing layanan atau aplikasi [4]. Namun, penelitian [4] menekankan pentingnya skala prioritas dalam penyusunan DRP, tetapi tidak menjelaskan metode yang digunakan untuk menentukan prioritas tersebut secara detail dan kurang mengevaluasi hasil implementasi skala prioritas dalam berbagai skenario bencana.

Berbagai penelitian sebelumnya sudah menunjukkan penyusunan DRP menggunakan standar. Akan tetapi belum dikaitkan dengan kondisi aset Teknologi Informasi (TI) yang terkait. Padahal, aset TI menjadi elemen utama pengelolaan layanan TI yang rentan dengan risiko. Tidak hanya itu, *data center* juga perlu didefinisikan berdasarkan kriteria dan protokol yang sesuai dengan standar industri yang berlaku.

Berdasarkan kondisi pengelolaan *data center* di Unusa saat dimana hanya ada satu staff pengelola data center, dimana hal tersebut menyebabkan ketergantungan kepada staf tertentu, maka penelitian ini mengusulkan penyusunan DRP sebagai solusinya. Penyusunan didasarkan pada kerangka NIST 800-34. Hal ini dipilih karena lebih fokus terhadap aspek teknis di lingkungan data center Unusa. Harapannya, penelitian ini akan menghasilkan dokumen DRP yang dapat menjadi acuan dalam pengelolaan *data center* kaitannya dengan penanganan bencana. Berbagai prosedur akan didokumentasikan dan dapat menjadi acuan semua pihak. Hasilnya pengelolaan *data center* tidak hanya bergantung pada satu staf tanpa adanya prosedur standar yang terdokumentasi.

2. Tinjauan Pustaka

Tinjauan pustaka adalah komponen esensial dalam setiap karya akademik, yang berfungsi untuk mengkaji dan menganalisis literatur yang relevan dengan topik penelitian. Melalui tinjauan pustaka, peneliti dapat memetakan pengetahuan yang sudah ada, mengidentifikasi kesenjangan penelitian, serta menilai validitas dan relevansi berbagai teori dan metode yang telah digunakan sebelumnya. Tinjauan pustaka yang digunakan untuk mendukung penyusunan penelitian ini diantaranya:

2.1 Data Center

Menurut standar SNI 8799, *data center* adalah gedung, ruangan khusus dalam gedung, atau sekumpulan gedung yang digunakan untuk penempatan sistem elektronik serta komponen terkait antara lain sistem penyimpanan data, sistem komunikasi data, dan didukung oleh infrastruktur untuk menjamin keberlangsungan operasional [5].

Standar SNI 8799-1:2023 mengatur tentang tata cara perancangan dan pembangunan *data center*. Standar inilah yang akan penulis gunakan sebagai acuan untuk melakukan observasi pada *data center* Unusa. Berikut adalah beberapa komponen utama yang biasanya diatur dalam standar ini [5]:

1) Ruangan *Data Center*
2) Sistem Pendingin
3) Sistem Kelistrikan
4) Sistem Keamanan Fisik
5) Sistem Pemadam Kebakaran
6) Sistem *Monitoring* Lingkungan
7) Sistem Manajemen Infrastruktur
8) Sistem Proteksi Terhadap Gangguan
9) Ruang Cadangan
10) Sistem Pemantauan Keamanan Informasi.

2.2 Disaster Recovery Plan (DRP)

DRP menurut NIST 800-34 adalah dokumen prosedural yang sangat penting untuk membantu organisasi merespons dan memulihkan layanan IT mereka dengan efektif setelah mengalami bencana atau gangguan serius lainnya [6].

DRP biasanya berfokus pada teknologi informasi (TI) dan dirancang untuk memulihkan operasi sistem, aplikasi, atau fasilitas komputer di lokasi alternatif setelah keadaan darurat. Cakupan DRP mungkin tumpang tindih dengan rencana darurat TI, namun cakupan DRP lebih sempit dan tidak mencakup gangguan minor yang tidak memerlukan relokasi. Tergantung pada kebutuhan organisasi, beberapa DRP dapat diintegrasikan ke dalam Rencana Keberlanjutan Bisnis (*Business Continuity Plan*/BCP) [6].

2.3 NIST 800-34

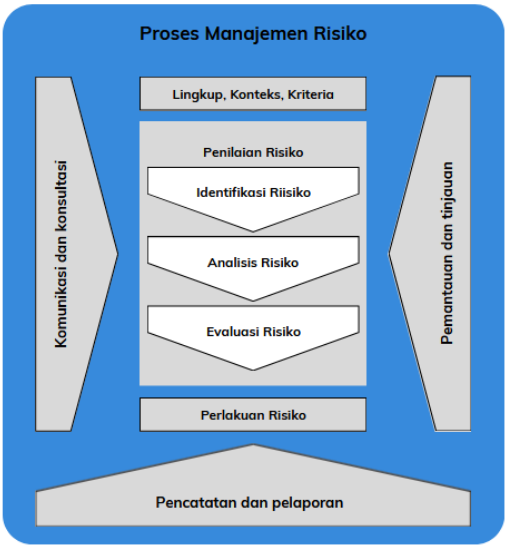
NIST 800-34 adalah dokumen yang diterbitkan oleh *National Institute of Standards and Technology* (NIST) yang berjudul "*Contingency Planning Guide for Information Technology Systems*." Dokumen ini memberikan panduan untuk pengembangan, implementasi, dan pemeliharaan rencana kontingensi yang efektif untuk sistem teknologi informasi (TI) dalam organisasi. Standar ini dirancang untuk membantu organisasi dalam mempersiapkan, merespon, dan memulihkan operasi setelah terjadi gangguan atau bencana yang dapat mempengaruhi operasional TI [6].

Tahapan-tahapan dalam menyusun DRP menurut standar NIST 800-34 adalah sebagai berikut:

1) Mengembangkan Pernyataan Kebijakan Perencanaan Kontingensi
2) Melakukan Analisis Dampak Bisnis
3) Mengidentifikasi Kontrol Pencegahan
4) Membuat Strategi Cadangan
5) Pengembangan Rencana Kontingensi Sistem Informasi
6) Memastikan Pengujian, Pelatihan, dan Latihan Rencana
7) Memastikan Pemeliharaan Rencana

2.4 Manajemen Risiko

Pada penelitian ini, akan memfokuskan pada 3 proses manajemen risiko seperti yang ada pada Gambar 1 yaitu, Identifikasi risiko, Analisis risiko, dan Evaluasi risiko pada ISO 31000.



Gambar 1. Proses manajemen risiko ISO 31000:2018

2.5 Failure Mode and Effect Analysis (FMEA)

FMEA adalah sebuah metode yang digunakan untuk meningkatkan keandalan dan keamanan suatu proses dengan mengidentifikasi potensi kegagalan, yang disebut sebagai modus kegagalan. Setiap modus kegagalan dievaluasi menggunakan tiga parameter: keparahan (*severity* - S), kemungkinan terjadinya (*occurrence* - O), dan kemungkinan kegagalan deteksi (*detectability* - D). Ketiga parameter ini kemudian digabungkan untuk menentukan signifikansi kekritisan dari setiap modus kegagalan. Gabungan dari ketiga parameter ini dikenal sebagai Angka Prioritas Risiko (*Risk Priority Number* - RPN).

2.6 Business Impact Analysis (BIA)

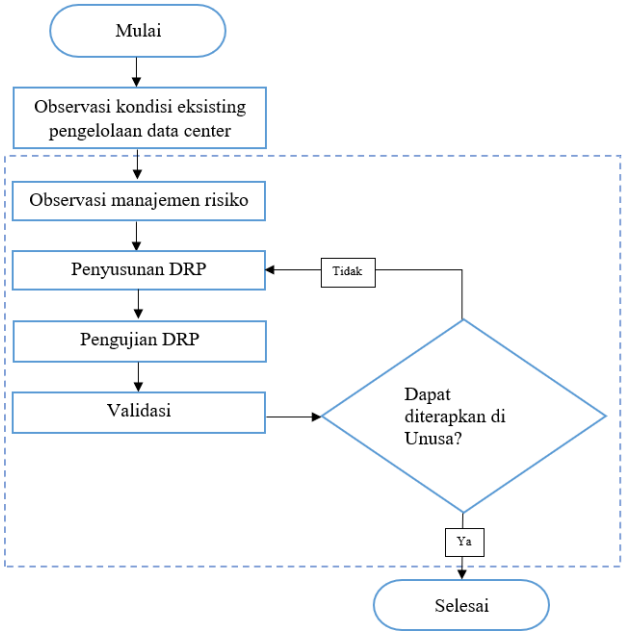
Business Impact Analysist (BIA) atau Analisis Dampak Bisnis adalah proses yang digunakan untuk menilai konsekuensi dari gangguan operasional terhadap operasi bisnis suatu organisasi. Menurut NIST 800-34, BIA didefinisikan sebagai: "BIA adalah proses untuk mengevaluasi dampak dari kehilangan layanan kritis terhadap kegiatan bisnis." Dalam konteks NIST 800-34, BIA dilakukan untuk mengidentifikasi dan menilai dampak potensial dari gangguan terhadap layanan kritis organisasi [6].

3. Metodologi

Metodologi merupakan pendekatan sistematis yang digunakan dalam proses penelitian untuk mencapai tujuan penelitian secara efektif, efisien dan terarah. Bagian ini menyajikan Gambaran mengenai tahapan-tahapan pelaksanaan proses penelitian serta penjelasan mendetail tentang skema metodologi yang diterapkan dalam penelitian ini.

3.1 Tahapan Pelaksanaan Penelitian

Berikut Gambar 2 yang menampilkan tahapan pelaksaan dalam penelitian ini.



Gambar 2. Tahapan Pelaksanaan Penelitian

3.2 Uraian Tahapan Pelaksanaan

Terdapat 3 tahapan besar dalam penelitian ini yaitu:

1) Oberservasi Kondisi Eksisting
2) Penilaian Risiko
3) Penyusunan DRP

3.2.1 Observasi Kondisi Eksisting

Tahapan pertama adalah melakukan observasi terhadap kondisi eksisting pengelolaan *data center*. Observasi diawali dengan melakukan identifikasi aset TI berkenaan dengan *data center* Unusa. Observasi dilakukan secara langsung di area *data center* Unusa untuk pengumpulan informasi kondisi eksisting. Penyusunannya didasarkan pada kondisi ideal standar acuan terkait *data center*, yakni SNI 8799:2023.

3.2.2 Penilaian Risiko

Tahapan ini bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko. Ketiga proses tersebut didasarkan dan dilakukan menggunakan standar ISO 31000. Detail masing-masing proses pada tahapan ini dijelaskan pada bagian selanjutnya. Detail pembagian kategori disajikan pada Tabel 1. Hasilnya adalah RPN dan kategorinya untuk setiap risiko.

Tabel 1. Skala penilaian RPN [8]

RPN	Kategori
0-20	Sangat Rendah
21-80	Rendah
81-120	Sedang
121-200	Tinggi
>200	Sangat Tinggi

Penggunaan ISO 31000 memberikan pendekatan yang lebih luas dan fleksibel dalam manajemen risiko diberbagai sektor yang tidak hanya dilingkup teknis *data center* saja namun lebih luas terhadap sektor non teknis seperti kebijakan manajerial.

3.3 Penyusunan Dokumen DRP

DRP diterapkan saat terjadi gangguan besar, biasanya gangguan fisik yang menghalangi akses ke infrastruktur fasilitas utama dalam jangka waktu yang lama. DRP adalah rencana yang berfokus pada sistem informasi yang dirancang untuk memulihkan operabilitas sistem target, aplikasi, atau infrastruktur komputer di lokasi alternatif setelah terjadi keadaan darurat. DRP dapat didukung oleh beberapa rencana kontingensi sistem informasi untuk menangani pemulihan sistem individu yang terdampak setelah fasilitas alternatif didirikan. DRP dapat mendukung *Business Continuity Plan* (BCP) atau *Continuity Operation Plan* (COOP) dengan memulihkan sistem pendukung untuk proses atau fungsi esensial bisnis di lokasi alternatif. DRP hanya menangani gangguan sistem informasi yang memerlukan relokasi [6].

1) Proses Perencanaan Kontingensi TI
2) Menyusun Pernyataan Kebijakan Perencanaan Kontingensi
3) Melakukan Analisis Dampak Bisnis
4) Mengidentifikasi Kontrol Pencegahan
5) Membuat Strategi Kotingensi
6) Pengembangan Rencana Kontingensi Sistem Informasi

3.4 Pengujian

Berikut Tabel 2 yang merupakan proses pengujian DRP

Tabel 2. Proses Pengujian DRP

Tahapan	*Input*	Proses	*Output*
Pengujian DRP	Dokumen DRP	1. Menyusun skenario pengujian 2. Melaksanakan skenario pengujian 3. Evaluasi hasil pengujian	Hasil pengujian

4. Hasil dan Pembahasan

4.1 Kondisi Eksisting Data Center Unusa

Berdasarkan obervasi lapangan, *data center* Unusa berada di Gedung dengan berbagi fungsi dengan kegiatan administrasi kampus, dan memiliki sistem atau komponen pencadangan seperti perangkat cadangan yang tersedia secara *standby* sampai perangkat yang meimplementasikan sistem redudansi. Sehingga dalam SNI 8799 untuk spesifikasi teknis *data center* Unusa telah memenuhi nilai Strata 2.

Nilai Strata 2 akan menjadi acuan dalam menentukan tingkat kesesuaian kondisi eksisting dengan SNI 8799. Hasil dari penilaian tersebut disajikan pada Tabel 3 yang merupakan hasil observasi kondisi eksisting pada aset data center berdasarkan SNI 8799.

Tabel 3. Kondisi Eksisting Aset Data Center Berdasarkan SNI 8799

Spesifikasi Teknis	Memenuhi Minimal Strata 2	Sub Persyaratan yang Tidak Sesuai	Saran
Spesifikasi Teknis data center secara umum	Ya	-	-
Spesifikasi gedung data center	Ya	-	-
Spesifikasi sistem kelistrikan	Ya	-	-
Spesifikasi sistem jaringan data	Tidak	Tidak memenuhi pada sub persyaratan. Memiliki label kabel yang terdiri dari nomor rak dan nomor baris pada rak	Penulis menyarankan kepada pihak Dir.SI untuk menggunakan print label khusus untuk melakukan *labeling* kabel dan juga perangkat yang ada pada *data center* guna memudahkan dalam melakukan perbaikan dan identifikasi saat terjadi kerusakan.
Spesifikasi keamanan akses fisik	Ya	-	-

4.2 Penialaian Risiko

Pada Tabel 4 merupakan hasil evaluasi risiko pada *data center* Unusa yang diperoleh berdasarkan hasil observasi dan dilakukan analisa sesuai kondisi lapangan untuk menemukan potensi risiko-risiko apa saja yang dapat muncul didalam operasional *data center* Unusa dan dihitung nilai risiko untuk mengetahui RPN.

Tabel 4. Evaluasi Risiko

ID Risiko	Risiko	*Severity*	*Occurance*	*Detection*	RPN	Kategori
DC-HW01	Gangguan *Server Down*	9	6	7	378	Risiko Sangat Tinggi
DC-HW02	Kegagalan sistem kritis	9	5	7	315	Risiko Sangat Tinggi
DC-SEC01	Kerusakan data dan kebocoran data	9	5	6	270	Risiko Sangat Tinggi
DC-WEB01	Gangguan *website*	8	4	7	224	Risiko Sangat Tinggi
DC-APP01	Gangguan aplikasi	5	7	4	140	Risiko Tinggi
DC-NET02	Kegagalan *provider* internet	7	3	5	105	Risiko Sedang
DC-NET01	Gangguan koneksi *provider*	5	2	4	40	Risiko Rendah
DC-POW01	Kegagalan Sumber daya energi	8	2	2	32	Risiko Rendah

4.3 Penyusunan DRP

4.3.1 Penyusunan Kebutuhan Sumber Daya

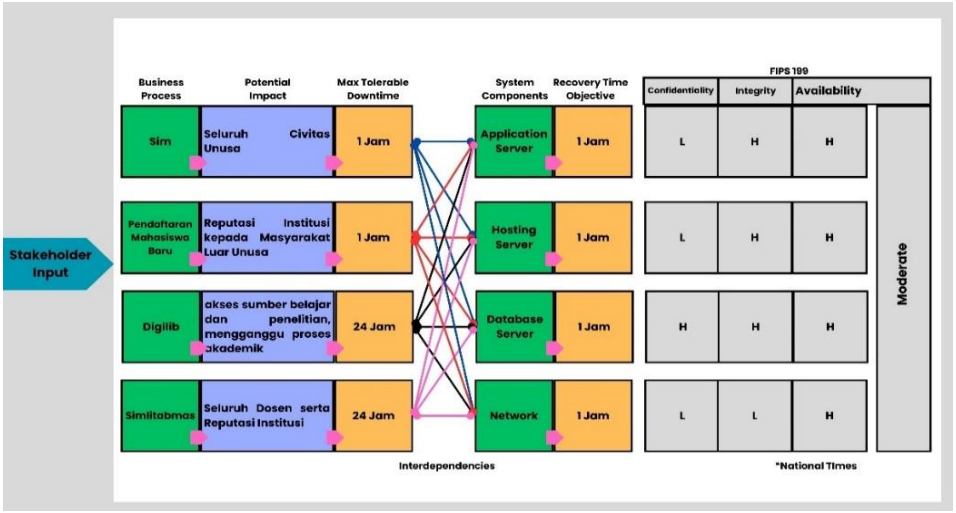
Pada Gambar 4 merupakan hasil penyusunan sumber daya manusia yang ideal dalam struktur organisasi DRP Unusa. Dalam penyusunan tersebut ada 1 bagian yang belum dapat terpenuhi oleh kondisi eksisting saat ini yaitu bagian *Administrator Database*.

Gambar 3. Struktur Organisasi DRP Unusa

4.3.2 Analisis Dampak Bisnis

Pada Gambar 5 merupakan hasil analisa dampak bisnis (BIA), dimana pada tahap ini penulis melakukan identifikasi dampak yang ditimbulkan pada bisnis jika terjadi gangguan pada layanan *data center*.

Selanjutnya penulis melakukan penyusunan MTD, RTO, RPO terhadap sistem *data center* apa saja yang mendukung proses bisnis. Hasil dari penyusunan tersebut disajikan pada Tabel 5.



Gambar 4. Analisa Proses Bisnis Unusa terhadap Layanan *Data Center*

Tabel 5. Penyusunan MTD, RTO, RPO terhadap *System Component* Proses Bisnis

Nama Layanan	Potensial Dampak	*System Component*		MTD (Jam)	RTO (Jam)	RPO (Jam)
Sim	Seluruh Civitas Unusa	*Application Server*	VPS *Server* Sim	1	1	24
		Hosting Server	*Hosting domain* Unusa	1	1	24
		Database Server	VPS *Server Database* Utama Unusa	1	1	1
		Network	- Internet - *Core Router* - *Core Switch* - *Firewall* - *Wireguard*	1	1	24
PMB	Reputasi Institusi kepada masyarakat	*Application Server*	VPS Server PMB	1	1	24
		Hosting Server	*Hosting domain* Unusa	1	1	24
		Database Server	VPS *Server Database* Utama Unusa	1	1	1
		Network	- Internet - *Core Router* - *Core Switch* - *Firewall* - *Wireguard*	1	1	24
Digilib	Akses sumber belajar dan penelitian, mengganggu proses akademik	*Application Server*	VPS *Server* Digilib	24	1	24
		Hosting Server	*Hosting domain* Unusa	24	1	24
		Database Server	VPS *Server Database* Perpustakaan	24	1	1
		Network	- *Internet* - *Core Router* - *Core Switch* - *Firewall* - *Wireguard*	24	24	24
Simlitabmas	Seluruh dosen Unusa dan reputasi institusi	*Application Server*	VPS *Server* Simlitabmas	24	1	24
		Hosting Server	*Hosting domain* Unusa	24	1	24
		Database Server	VPS *Server Database* Simlitabmas	24	1	1
		Network	- Internet - *Core Router* - *Core Switch* - *Firewall* - *Wireguard*	24	24	24

Tabel 6. Manajemen Aset *Data Center*

Jenis Aset Hardware	Detail Aset	Deskripsi	Poin pada NIST 800-53	Aktivitas Manajemen Aset
Server	*Server* fisik dan virtual	Perangkat utama untuk menjalankan layanan seperti *database*, aplikasi, dan *server* web.	*CM-8 Iventory of System Components* (Inventarisasi Komponen Sistem)	Melakukan audit berkala untuk memastikan semua server tercatat dengan benar dalam inventaris.
			MP-3 Media Marking (Pelabelan)	Memberikan label fisik dan digital pada *server* untuk identifikasi yang jelas.
			MA-2 Controlled Maintenance (Pemeliharaan)	Jadwalkan pemeliharaan rutin termasuk update firmware dan pengecekan hardware.
			CM-4 Impact Analyses (Analisis Dampak)	Melakukan analisis dampak jika ada perubahan konfigurasi pada server.
Jaringan	*Router*, *Switch*, *Firewall*	Perangkat untuk konektivitas jaringan internal dan eksternal, termasuk pengamanan data komunikasi.	*CM-8 Iventory of System Components* (Inventarisasi Komponen Sistem)	Mencatat perangkat jaringan dalam inventaris aset.
			MP-3 Media Marking (Pelabelan)	Menandai perangkat dengan label unik untuk identifikasi.
			MA-2 Controlled Maintenance (Pemeliharaan)	Melakukan inspeksi dan pemeliharaan berkala pada perangkat jaringan.
			CM-4 Impact Analyses (Analisis Dampak)	Melakukan analisis dampak perubahan konfigurasi pada jaringan terhadap layanan.
Security Fisik	CCTV, *Smart door lock*	Sistem keamanan untuk memantau akses fisik ke *data center* dan mencegah akses tidak sah.	*PE-3 Physical Access Control* (Pengendalian Akses Fisik)	Memastikan perangkat keamanan fisik berfungsi optimal melalui pengujian berkala.
			CM-4 Impact Analyses (Analisis Dampak)	Menganalisis dampak penambahan atau pengurangan perangkat keamanan fisik.
Pendingin Ruangan	AC	Perangkat untuk menjaga suhu optimal dan mencegah kerusakan perangkat akibat *overheating*.	*MA-2 Controlled Maintenance* (Pemeliharaan)	Melakukan pengecekan dan pembersihan filter AC secara rutin untuk menjaga efisiensi.
			CM-4 Impact Analyses (Analisis Dampak)	Melakukan analisis dampak jika terjadi kegagalan sistem pendingin pada operasional *data center*.
Apar	Pemadam Api Ringan	Peralatan untuk menangani kebakaran kecil yang dapat mengancam perangkat keras atau *data center*.	*PE-13 Fire Protection* (Perlindungan kebakaran)	Melakukan inspeksi rutin dan memastikan alat pemadam api dalam kondisi siap digunakan.
			CM-4 Impact Analyses (Analisis Dampak)	Menganalisis dampak potensial kebakaran terhadap perangkat keras dan operasional *data center*.
Electrical	*Genset*, UPS, Listrik Premium	Perangkat penyedia daya cadangan untuk memastikan operasional tetap berjalan meskipun listrik padam.	*PE-11 Emergency Power* (Daya Darurat)	Melakukan pengujian berkala terhadap genset dan UPS untuk memastikan ketersediaan daya cadangan.

4.3.3 Mengidentifikasi Kontrol Pencegahan

Pada Tabel 6 merupakan hasil penyusunan manajemen aset berdasarkan pada NIST 800-53. Hasil dari penyusunan ini digunakan sebagai prosedur dalam melakukan aktivitas manajemen aset sebagai pedoman untuk aktivitas perawatan pada aset *data center*.

4.3.4 Penyusunan Strategi Kontingensi

Setelah dilakukan observasi kondisi eksisting *data center* serta dilakukan analisis risikonya, maka tahap selanjutnya adalah menyusun strategi untuk tindakan pencegahan sebelum dan sesudah terjadinya bencana.

Pada Tabel 7 merupakan hasil penyusunan strategi kontingensi untuk menanggulangi jika terjadi bencana pada *data center* Unusa.

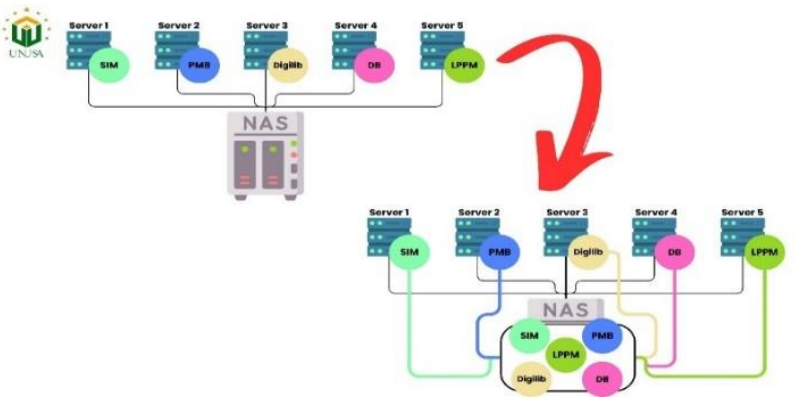
Tabel 7. Daftar Strategi Kontingensi

Kode Strategi	Nama Strategi
ST-01	Strategi *Backup Virtual Private Server*
ST-02	Strategi *Recovery Virtual Private Server*
ST-03	Strategi Duplikasi *Virtual Private Server*
ST-04	Strategi *Backup* Konfigurasi Perangkat Jaringan
ST-05	Strategi *Recovery* Konfigurasi Perangkat Jaringan

Uraian strategi kontingensi:

1) Strategi *Backup Virtual Private Server*

Pada Gambar 6 merupakan skema dari strategi *backup Virtual Private Server*. Strategi ini digunakan untuk mengamankan data dan konfigurasi dari *Virtual Private Server* Nas *Storage* terpisah, agar jika sewaktu waktu terjadi bencana, maka layanan dari *data center* tersebut dapat dupulihkan dengan cepat.

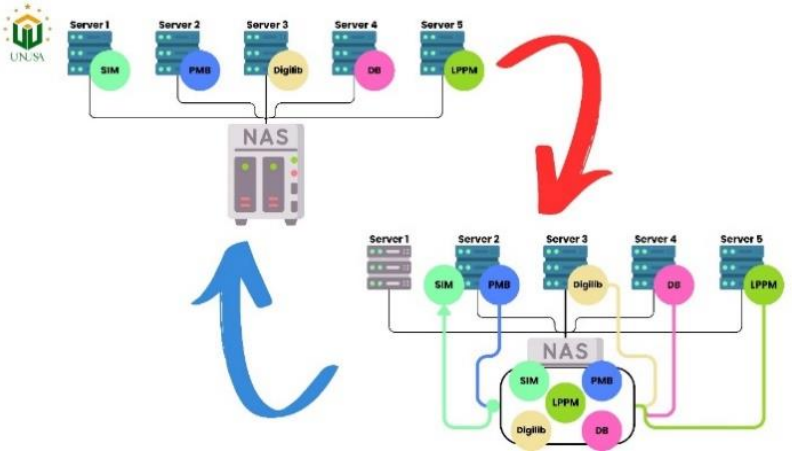


Gambar 5. Strategi *Backup Virtual Private Server*

2) Strategi *Recovery Virtual Private Server*

Pada Gambar 7 merupakan skema dari strategi *recovery Virtual Private Server*. Strategi ini digunakan untuk mengeksekusi saat terjadi bencana, dengan menggunakan hasil dari *backup* yang sudah dilakukan di Nas

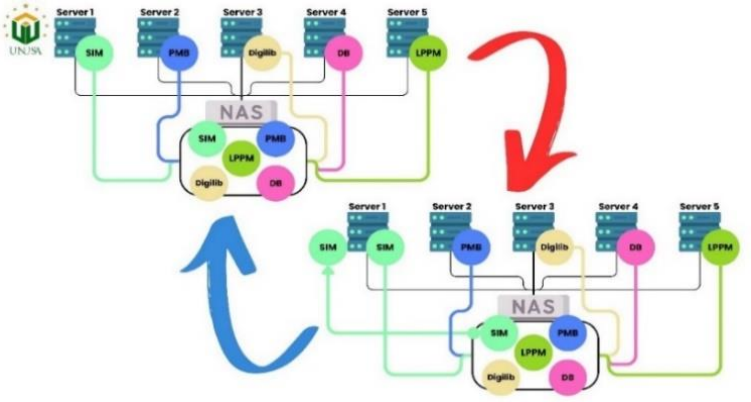
storage khusus *backup*. Yang kemudian hasil *image* tersebut dapat di*restore* kedalam server yang dibutuhkan.



Gambar 6. Strategi *Recovery Virtual Private Server*

3) Strategi Duplikasi *Virtual Private Server*

Pada Gambar 8 merupakan skema dari strategi duplikasi *Virtual Private Server*. Strategi ini digunakan untuk mengambil konfigurasi dari Nas *Storage* yang dibutuhkan saat sebelum terjadinya kesalahan. Selain itu, strategi ini juga bisa digunakan untuk mereplikasi konten yang ada.

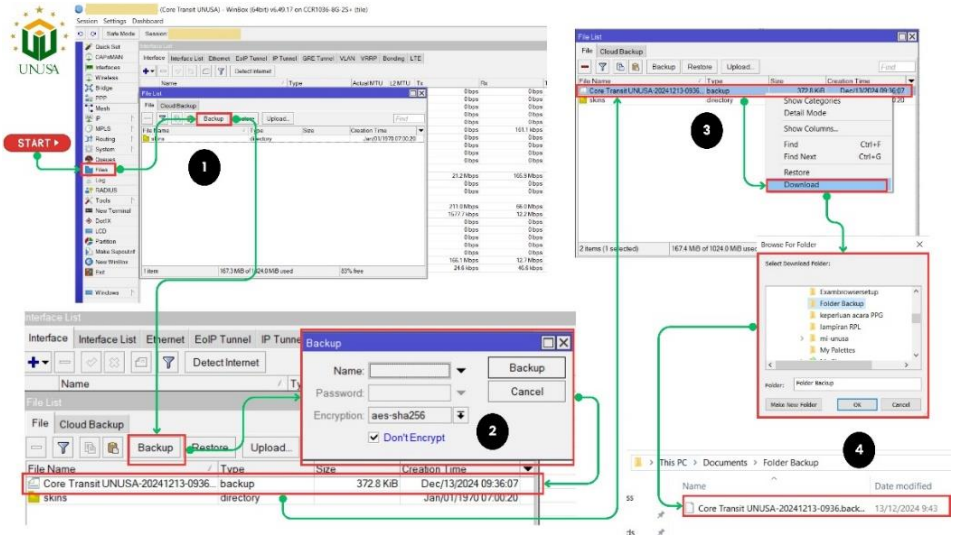


Gambar 7. Strategi Duplikasi *Virtual Private Server*

4) Strategi *Backup* Konfigurasi Perangkat Jaringan

Pada Gambar 9 merupakan skema dari strategi *backup* perangkat mikrotik untuk mengamankan konfigurasi yang sudah berjalan, agar sewaktu waktu jika terjadi bencana kerusakan pada perangkat mikrotik, maka bisa langsung dipulihkan dengan cepat. Strategi ini terdiri dari beberapa langkah yaitu:

a. Proses *backup* dilakukan melalui menu *Files – Backup*.
b. Maka akan muncul *pop up encrypt*, sehingga hasil *backup* konfigurasi akan ter*generate*.
c. Hasil *backup* yang telah ter*generate* dapat di*download*.
d. Hasil *download* tersebut disimpan kedalam komputer/laptop.

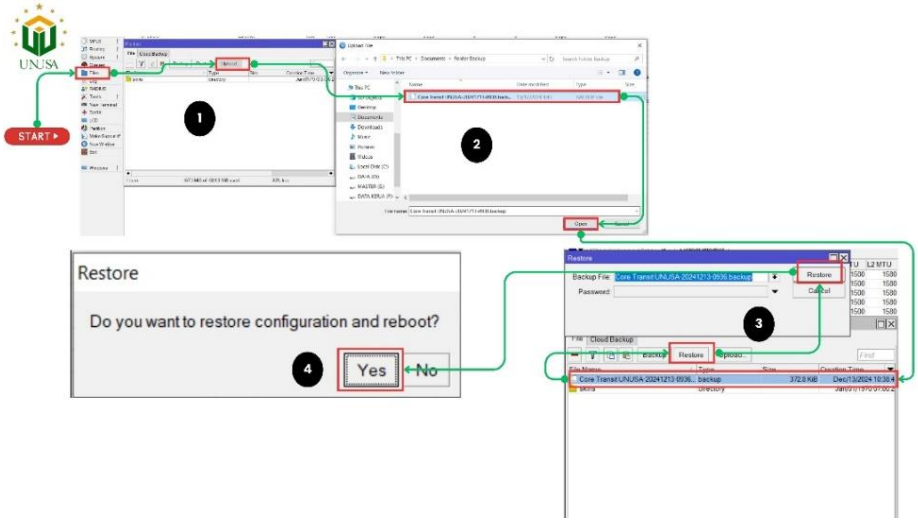


Gambar 8. Strategi *Backup* Perangkat Mikrotik

5) Strategi *Recovery* Konfigurasi Perangkat Jaringan

Pada Gambar 10 merupakan skema dari strategi *recovery* perangkat mirotik. Strategi ini digunakan untuk mengembalikan konfigurasi dari mikrotik yang rusak dengan menggantinya dengan perangkat mikrotik yang baru dengan memanfaatkan hasil backup yang telah dilakukan sebelumnya. Strategi ini terdiri dari beberapa langkah yaitu:

a. Proses upload konfigurasi dari *backup* Mikrotik sebelumnya dilakukan melalui menu *Files – Upload*.
b. Maka akan muncul *pop up directory* komputer, cari lokasi penyimpanan backup konfigurasi sebelumnya.
c. Hasil *backup* bisa dilakukan *restore*.
d. *Router* akan melakukan *restart* untuk memuat konfigurasi.



Gambar 9. Strategi *Recovery* Konfigurasi Mikrotik

4.4 Pengujian DRP

Pada Tabel 8 merupakan hasil dari pengujian yang sudah divalidasi oleh Pimpinan Direktorat Sistem Informasi Unusa. Hasil pengujian ini bertujuan untuk mengetahui apakah strategi yang telah dibuat dapat diterapkan di *data center* Unusa atau tidak, serta dilakukan analisa berupa saran apabila strategi tersebut tidak dapat diterapkan. Proses pengujian dilakukan dengan RTO dan RPO pada Tabel 5 sebagai acuan keberhasilan pengujian. Berikut merupakan hasil pengujian dari skenario saat terjadi risiko:

1) Gangguan *server down* dan kegagalan sistem kritis dapat dipulihkan dalam waktu 30 menit.
2) Kerusakan data dan kebocoran data dengan melakukan tes *inject script* SQL Injection dapat terdeteksi oleh *firewall data center* secara *real time*.
3) Gangguan *website* dan aplikasi dapat dipulihkan dengan melakukan duplikasi VPS untuk memulihkan file konfigurasi sebelumnya secara cepat kurang dari 30 menit.
4) Kerusakan perangkat jaringan dengan melakukan reset konfigurasi dan melakukan *restore backup* konfigurasi yang ada dapat dilakukan dalam waktu 10 menit.
5) Gangguan *provider* internet tidak berhasil disimulasikan karena *data center* Unusa hanya memiliki 1 *provider* aktif.
6) Kegagalan sumber energi dengan melakukan pemadaman listrik di dalam *data center*, dan hasilnya UPS berhasil mem*backup* power listrik serta genset berhasil dinyalakan sehingga listrik di dalam *data center* kembali normal dalam waktu 10 menit.

5. Kesimpulan

5.1 Simpulan

Secara keseluruhan hasil dari Penyusunan *Disaster Recovery Plan* (DRP) untuk *data center* Unusa yang dilakukan dengan pendekatan berbasis standar NIST 800-34, analisis risiko sesuai ISO 31000:2018 serta kondisi ideal *data center* berdasarkan SNI 8799, telah menghasilkan hal-hal sebagai berikut:

1) Kondisi ideal infrastruktur *data center* Unusa berdasarkan nilai strata 2 SNI 8799
2) Daftar potensi risiko yang dapat muncul pada operasional *data center* Unusa
3) Susunan organisasi DRP untuk Direktorat Sistem Informasi Unusa
4) Penentuan prioritas layanan kampus berdasarkan analisis dampak bisnis
5) Standar operasional dalam manajemen aset *data center*
6) Strategi pemulihan dan pencegahan gangguan pada layanan *data center* Unusa

Dari hasil penyusunan dokumen DRP pada penelitian ini, telah dilakukan pengujian dengan skenario yang telah dibuat, dan hasilnya telah divalidasi dan diketahui oleh Direktur Sistem Informasi Unusa. Hasil dari pengujian dan validasi tersebut diketahui bahwa penyusunan DRP pada penelitian ini dapat diterima dan diterapkan di *data center* Unusa.

5.2 Saran

Berdasarkan hasil penelitian, penulis memberikan beberapa saran untuk optimalisasi lebih lanjut dan pengembangan penelitian di masa yang akan datang. Penelitian dapat dikembangkan dengan mengikuti perkembangan teknologi infrastruktur di masa depan. Selain kerangka kerja NIST 800-34, penelitian selanjutnya dapat menggunakan kerangka kerja yang lain seperti ISO/IEC 27031:2011, ISO/IEC 22301:2019, ITIL, COBIT, TOGAF.

Tabel 8. Validasi Hasil Pengujian DRP

Risiko	Skenario	Spesifikasi Aset Yang Dibutuhkan dalam Menjalankan DRP	Dapat diterapkan di *Data Center*	Sesuai Standar DRP	Saran
Gangguan *Server Down* Kegagalan Sistem Kritis	Simulasi server utama mengalami kerusakan total sehingga layanan tidak dapat diakses.	*Hardware*: Server Nas *Storage* *Software*: Proxmox TrueNas *Network*: *Router* Mikrotik *Switch* Mikrotik *Provider*	Ya	Sesuai	Beberapa konten Unusa masih menggunakan konsep server konvensional seperti (*website* fakultas dan *website* unit lembaga). Meskipun tidak berdampak secara signifikan, namun perlu dipertimbangkan untuk penerapan server secara keseluruhan dengan konsep virtualisasi.
Kerusakan data dan kebocoran data	*Testing injects script* SQL Injection	*Network*: *Router* Mikrotik *Switch* Mikrotik *Provider* *Firewall*	Ya	Sesuai	-
Gangguan *website* Gangguan aplikasi	Simulasi pemblokiran file asing di server *website*, seperti yang pernah terjadi (slot gacor). Pemulihan kembali file kebentuk semula sebelum adanya penyusupan. Simulasi gangguan pada aplikasi akibat perubahan fitur atau kode.	*Hardware:* Server Nas *Storage* *Software*: Proxmox TrueNas *Network*: *Router* Mikrotik *Switch* Mikrotik *Provider*	Ya	Sesuai	-
Kerusakan perangkat jaringan	Simulasi *Router* transit mengalami kerusakan	*Network*: *Router* *Switch*	Ya	Sesuai	-
Gangguan Koneksi *Provider*	Simulasi kegagalan total pada layanan *provider*	*Network*: *Router* Mikrotik *Switch* Mikrotik *Provider*	Tidak	Tidak	*Data Center* Unusa perlu menambahkan *upstream provider* cadangan sebagai *backup* jika terjadi *down* pada *provider* yang ada saat ini.
Kegagalan Sumber daya energi	Simulasi pemadaman listrik di area *data center* berada.	*Hardware*: UPS Genset	Ya	Sesuai	-

6. Daftar Rujukan

[1] F. Abroni, A. Prasetyo, and S. N. Arief, "IMPLEMENTASI DISASTER RECOVERY PLAN SERVER SYSTEM DENGAN METODE FAILOVER BERBASIS LINUX DI POLITEKNIK NEGERI MALANG," 2019.

[2] Zulkarnain, "Computer Based Information System Journal," *Computer Based Information System Journal*, vol. 10, pp. 1–6, Sep. 2022, [Online]. Available: http://ejournal.upbatam.ac.id/index.php/cbishttp://ejournal.upbatam.ac.id/index.php/cbis

[3] I. G. T. Isa, "Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi," *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, vol. 15, no. 2, p. 103, Sep. 2020, doi: 10.30872/jim.v15i2.3724.

[4] S. U. S. A. A. Hafizh Ghozie Afiansyah, "PERANCANGAN RENCANA PEMULIHAN BENCANA MENGGUNAKAN NIST SP 800-34 REV 1, NIST SP 800-53 REV 5 DAN SNI 8799 (STUDI KASUS: UNIT TI XYZ)," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 10, pp. 1–10, 2022.

[5] "SNI 8799-1:2023," 2023.

[6] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, "Contingency planning guide for federal information systems," Gaithersburg, MD, 2010. doi: 10.6028/NIST.SP.800-34r1.

[7] W. Adi Prabowo and R. Dias Ramadhani, "Perancangan Contingency Planning Disaster Recovery Unit Teknologi Informasi Perguruan Tinggi menggunakan NIST SP800-34 Design of Contingency Planning Disaster Recovery for Higher Education Information Technology Units using NIST SP800-34."

[8] H. I. Pribadi and E. Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)," *JURNAL SISTEM INFORMASI BISNIS*, vol. 10, no. 1, pp. 28–35, May 2020, doi: 10.21456/vol10iss1pp28-35.

[9] E. D. Pamungkas, N. S. Fatonah, G. Firmansyah, and H. Akbar, "Disaster Recovery Plan Analysis Based on the NIST SP 800-34 Framework (Case Study: PT Wijaya Karya (Persero) Tbk.)," *Jurnal Indonesia Sosial Sains*, vol. 4, no. 09, 2023, [Online]. Available: http://jiss.publikasiindonesia.id/

[10] A. B. Dammara, F. Adam, M. Pranata, T. Purwokero, and J. Di Panjaitan, "ANALISIS PERBANDINGAN KINERJA VIRTUALISASI SERVER MENGGUNAKAN PROXMOX DAN VMWARE ESXI (STUDI KASUS : VIRTUALISASI SERVER UNTUK PENGGUNAAN MOODLE)," 2023. [Online]. Available: https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

[11] M. H. Alifian and D. Priharsari, "Penyusunan Disaster Recovery Plan (DRP) menggunakan framework NIST SP 800-34 (Studi Kasus pada Perusahaan IT Nasional)," 2021. [Online]. Available: http://j-ptiik.ub.ac.id

[12] M. S. A. Setiawan, E. M. Safitri, M. A. T. Taufiqurahman, and M. A. Pratama, "Analisis Manajemen Risiko Keamanan Sistem Informasi Rocketic.id menggunakan Metode OCTAVE dan FMEA," *Jurnal Sistem dan Teknologi Informasi (JustIN)*, vol. 11, no. 3, p. 504, Jul. 2023, doi: 10.26418/justin.v11i3.66628.