Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.2023106507
Vol. 10, No. 2, April 2023, hlm. 329-338 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

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)

Hafizh Ghozie Afiansyah*[1], Septia Ulfa Sunaringtyas[2], Amiruddin Amiruddin[3]

[1,2,3]Politeknik Siber dan Sandi Negara, Kabupaten Bogor
Email: [1]hafizh.ghozie@student.poltekssn.ac.id, [2]septia.ulfa@poltekssn.ac.id, [3]amir@poltekssn.ac.id
*Penulis Korespondensi

(Naskah masuk: 01 September 2022, diterima untuk diterbitkan: 11 April 2023)

Abstrak

Pada Institut XYZ, unit kerja yang memiliki tanggung jawab untuk mengelola layanan teknologi informasi dan pusat data adalah Unit TI. Berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019, untuk menanggulangi dampak kehilangan layanan pada pusat data yang disebabkan oleh bencana dan ancaman, diperlukan adanya rencana yang bertujuan untuk mencegah kehilangan dan kerusakan, yaitu rencana pemulihan bencana atau DRP. Hal tersebut didukung dengan kuesioner dan wawancara yang dilakukan kepada jajaran pejabat struktural, kepala unit dan mahasiswa Institut XYZ yang menyatakan bahwa layanan yang dikelola oleh Unit TI XYZ bersifat vital bagi proses bisnis perkuliahan, administrasi umum dan kemahasiswaan. Pada tahun 2021, terjadi kegagalan pada pusat data Unit TI XYZ yang menyebabkan proses perkuliahan daring dan administrasi terhenti karena portal daring yang tidak dapat diakses dan hilangnya data yang disimpan pada penyimpanan awan. Berdasarkan hal tersebut, dilakukan perancangan rencana pemulihan bencana menggunakan NIST SP 800-34 Rev 1 sebagai kerangka kerja penyusunan DRP, NIST SP 800-53 Rev 5 sebagai kendali pencegahan, dan SNI 8799 sebagai acuan persyaratan pusat data. Sebagai hasilnya, disusun enam rencana pemulihan untuk sistem dengan prioritas tinggi, tiga rencana pemulihan untuk sistem dengan prioritas sedang, dan dua rencana pemulihan untuk sistem dengan prioritas rendah.

Kata kunci: *pemulihan bencana, NIST SP 800-34 Rev 1, NIST SP 800-53 Rev 5, SNI 8799-1, teknologi informasi.*

DESIGNING A DISASTER RECOVERY PLAN USING NIST SP 800-34 REV 1, NIST SP 800-53 REV 5, AND SNI 8799 (CASE STUDY: IT UNIT OF XYZ)

Abstract

At the XYZ Institute, the work unit responsible for managing information technology and data center services is the IT Unit. According to Government Regulation Number 71 of 2019, to overcome the impact of service loss in data centers caused by disasters and threats, it is necessary to have a plan that aims to prevent loss and damage, namely a disaster recovery plan or DRP. This is supported by questionnaires and interviews with structural officials, unit heads, and students of the XYZ Institute, which state that services managed by the IT Unit XYZ are vital for the business processes of lectures, general administration, and student affairs. In 2021, there was a failure in the IT Unit XYZ data center, which caused the online lecture and administration process to stop due to an inaccessible online portal and loss of data stored in cloud storage. Based on the regulation requirement, interviews, and questionnaires, a disaster recovery plan was designed using NIST SP 800-34 Rev 1 as a framework for preparing the DRP, NIST SP 800-53 Rev 5 as a preventive control, and SNI 8799 as a reference for data center requirements. As a result, six recovery plans were developed for high-priority systems, three recovery plans for medium-priority systems, and two recovery plans for low-priority systems.

Keywords: *disaster recovery, information technology, NIST 800-34, NIST 800-53, SNI 8799.*

1. PENDAHULUAN

Institut XYZ merupakan institusi perguruan tinggi dibawah naungan Badan ABC yang dibentuk berdasarkan Peraturan Badan ABC Tahun 2019. Pada institut XYZ, layanan dan data administratif disimpan pada pusat data (Badan ABC, 2019). Unit TI memiliki peran vital dalam mengelola layanan TI yang mendukung proses bisnis untuk unit kerja lain di lingkungan Institut XYZ yang meliputi kegiatan perkuliahan, administrasi umum serta kemahasiswaan. Keberlangsungan kegiatan-kegiatan tersebut bergantung pada ketersediaan layanan TI

dimana semua kegiatan dilakukan via portal daring. Berdasarkan kuisioner yang dibagikan kepada sivitas akademika Institut XYZ yaitu pejabat struktural, kepala unit dan mahasiswa Institut XYZ, diketahui bahwa layanan yang dikelola oleh Unit IT XYZ, seperti LMS, Zimbra Mail, dan Drive, merupakan layanan esensial untuk proses bisnis, dimana layanan LMS digunakan untuk kegiatan perkuliahan, Zimbra Mail untuk sarana komunikasi internal maupun eksternal sivitas akademika, dan Drive sebagai media penyimpanan data akademik dan kemahasiswaan.

Dari kuisioner dan wawancara yang dilakukan kepada Kepala Unit TI beserta pejabat struktural dan dosen serta mahasiswa, juga diketahui bahwa sivitas akademika Institut XYZ sangat terpengaruh jika terjadi gangguan terhadap layanan yang dikelola oleh Unit IT. Hal tersebut didasarkan pada laporan tahunan kinerja Unit TI XYZ yang merekam adanya kegagalan pada pusat data Unit TI XYZ secara keseluruhan sehingga seluruh layanan tidak dapat diakses selama 48 jam. Kegagalan tersebut menyebabkan kegiatan perkuliahan yang dilakukan secara daring menjadi terganggu karena modul-modul pembelajaran yang tidak dapat diakses, kegiatan administrasi yang terhenti karena portal untuk mengakses dan mengetahui progres persuratan tidak dapat diakses, dan hilangnya seluruh data yang tersimpan di Drive.

Untuk menghindari dampak hilangnya layanan pada pusat data Unit TI XYZ yang disebabkan oleh bencana dan ancaman, maka diperlukan suatu perencanaan terkait keamanan data dan layanan dalam organisasi untuk menghindari kerugian dan kerusakan yaitu *disaster recovery plan* atau DRP. Di Indonesia, beberapa peraturan menjelaskan bahwa Penyelenggara Sistem Elektronik atau PSE yang dimaksudkan untuk memberikan pelayanan kepada masyarakat (PSE Lingkup Publik) wajib memiliki rencana untuk menghadapi gangguan atau bencana berikut risiko dampak yang ditimbulkannya (Presiden RI).

Dalam studi yang dilakukan oleh Sativa dan Akhmadi (Akhmadi and Agustika Sativa, 2019), dilakukan perbandingan antara kerangka kerja pemulihan bencana, termasuk standar, yaitu NIST SP 800-34, ISO 24762, Webtrust, dan kerangka kerja lainnya. Perbandingan dilakukan dengan menggunakan 18 parameter perbandingan yang diajukan oleh Gupta et al. (Gupta, Kapur and Kumar, 2016). Parameter ini mencakup aspek hak pemangku kepentingan untuk menyelesaikan analisis dampak bisnis dari arsitektur situs cadangan. Dari hasil perbandingan diketahui bahwa NIST SP 800-34 memenuhi parameter paling banyak dibandingkan dengan kerangka kerja lainnya, yaitu 17 dari 18 parameter.

Penelitian lainnya yang berkaitan dengan penelitian ini dilakukan oleh Nurhanudin (Nurhanudin, 2021) dan Setyawan et al. (Setyawan, Giri Sucahyo and Gandhi, 2020), dimana dilakukan perancangan rencana pemulihan bencana menggunakan NIST SP 800-34, namun rekomendasi yang diberikan untuk meningkatkan kapabilitas pusat data pada penelitian tersebut diperbaharui pada penelitian ini dengan menggunakan SNI 8799 yang merupakan standar pusat data untuk Indonesia (Badan Standarisasi Negara, 2019). Penelitian Hamadah (Hamadah, 2019) menjelaskan tentang benefit masing-masing model rencana pemulihan berbasis *cloud*, baik menggunakan *private cloud* maupun *public cloud*. Penelitian tersebut menjadi dasar pertimbangan pemilihan model pemulihan pada penelitian ini berdasarkan aspek *applicability* dan *cost*.

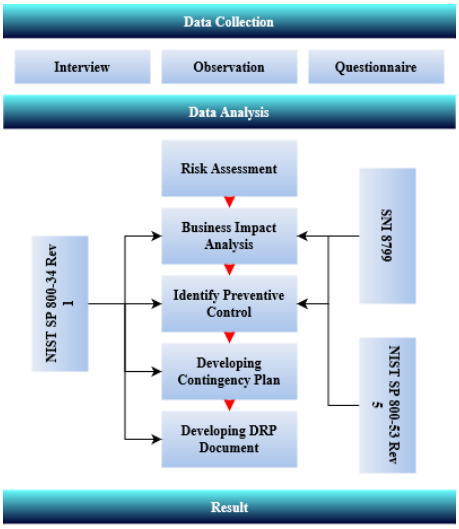
Berdasarkan penjelasan diatas maka pada penelitian ini akan dirancang DRP sebagai pedoman pemulihan data pada Institut XYZ berdasarkan kerangka kerja NIST SP 800-34 Rev 1 untuk penyusunan DRP, kendali keamanan dari NIST SP 800-53 Rev 5 dan SNI 8799 sebagai acuan kebutuhan pusat data. Hasil yang diharapkan adalah dokumen yang berisi prosedur, kebijakan, dan langkah-langkah yang diambil oleh Unit TI XYZ jika terjadi bencana atau gangguan pada layanan.

2. METODE PENELITIAN

Penelitian ini tergolong penelitian kualitatif. Penelitian kualitatif digunakan untuk penelitian yang melakukan pengamatan terhadap suatu objek sebagai kasus (Hardani et al., 2020). Metode ini memahami dan menjelaskan makna dan makna suatu fenomena menurut sudut pandang peneliti. Penelitian ini menggunakan pendekatan studi kasus. Penelitian ini menggunakan teknik pengumpulan data berupa wawancara, angket, observasi, dan teknik validasi data berupa triangulasi sumber dan member check. Teknik pengumpulan data yang digunakan adalah dengan melakukan wawancara, kuesioner, dan observasi.

Pengembangan DRP dilakukan dengan menggunakan proses penilaian risiko yang dijelaskan dalam dokumen NIST SP 800-30 Rev 1, tiga dari tujuh tahap perencanaan kontinjensi yang dijelaskan dalam dokumen NIST SP 800-34, dan kendali yang dijelaskan dalam NIST SP 800-53 Rev 5 dan persyaratan pusat data SNI 8799. Alur penelitian ditunjukkan pada Gambar 1.

Pengujian validitas untuk penelitian ini dilakukan dengan menggunakan triangulasi, member check dan validitas isi dengan *expert judgement*. Triangulasi dalam penelitian adalah validasi silang untuk menilai kecukupan data menurut konvergensi berbagai penggunaan sumber data (Sugiyono, 2013). Validitas isi adalah validitas dengan menguji kelayakan isi penelitian kepada ahli atau *expert judgement* (Azwar, 2012).



Gambar 1. Alur penelitian

3. LANDASAN TEORI

3.1. Pemulihan Bencana

Pemulihan bencana merupakan bagian dari keberlanjutan yang berhubungan dengan dampak langsung dari suatu bencana (Snedaker, 2013).Secara umum, pemulihan bencana merupakan bagian dari kelangsungan bisnis yang berfokus pada sistem dan data TI (Winkler, 2011). Sebagai langkah untuk mempersiapkan kondisi sistem dan data TI saat terjadi bencana atau gangguan perusahaan, dibutuhkan perencanaan yang dapat menghindari kerusakan atau kehilangan data. Ini dapat dilakukan dengan mengembangkan rencana pemulihan bencana atau DRP. DRP mencakup prosedur untuk menanggapi keadaan darurat, menyediakan cadangan untuk operasi selama bencana, dan mengelola proses pemulihan dan penyimpanan.

3.2. SNI 8799

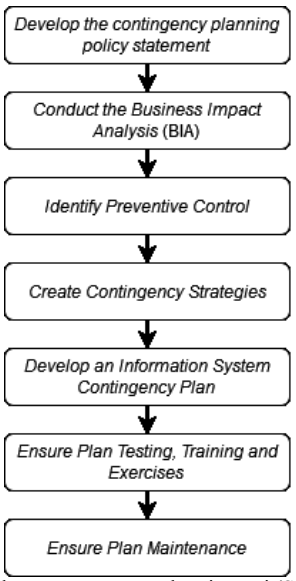
Standar Nasional Indonesia (SNI) 8799 adalah dokumen standar yang dikeluarkan oleh Badan Standardisasi Nasional (BSN), yang menguraikan tentang pedoman spesifikasi teknis pusat data, yang dimaksudkan untuk memberikan standarisasi pusat data di wilayah Indonesia (Badan Standarisasi Negara, 2019). Dalam dokumen ini diuraikan 7 (tujuh) aspek persyaratan teknis pusat data, yaitu spesifikasi bangunan, sistem kelistrikan, sistem pendingin, sistem jaringan data, sistem pemadam kebakaran, pemantauan, keamanan akses fisik.

3.3. Penilaian Risiko

Penilaian risiko adalah kegiatan yang dilakukan untuk mengidentifikasi, memperkirakan, dan memprioritaskan risiko terhadap operasi organisasi (mis., misi, fungsi, citra, dan reputasi), aset organisasi, organisasi lain, dan negara, yang berasal dari pengoperasian dan penggunaan informasi. sistem (Rebecca M. Blank. Patrick D. Gallagher, 2012).

3.4. NIST SP 800-34 Rev 1

Penyusunan rencana pemulihan bencana dapat dilakukan dengan mengacu pada suatu standar, salah satunya NIST SP 800-34 Rev 1. NIST SP 800-34 Rev 1 merupakan dokumen yang dikeluarkan oleh National Institute of Standards and Technology. Dokumen tersebut memberikan informasi tentang keterkaitan perencanaan kontinjensi untuk sistem informasi (ISCP) dengan rencana kontinjensi lain yang terkait dengan manajemen darurat, ketahanan organisasi, dan siklus pengembangan perangkat lunak (SDLC). Ini memandu personel dalam mengevaluasi sistem informasi. Selanjutnya, operasi menentukan persyaratan dan prioritas untuk perencanaan kontingensi (Swanson et al., 2010). Ada tujuh tahap yang dilakukan dalam proses perencanaan kontinjensi yang dapat diterapkan organisasi untuk memelihara program perencanaan kontingensi yang sesuai untuk sistem informasi organisasi. Tahapan tersebut ditunjukkan pada Gambar 2.



Gambar 2. Tahapan perencanaan kontingensi (Swanson et al., 2010)

2.5. Perbandingan Kerangka Kerja Penyusunan DRP

Dalam penyusunan DRP, beberapa kerangka kerja dapat digunakan sebagai panduan, seperti NIST SP 800-34 Rev 1, ISO/IEC 24762, dan NFPA 1600, serta kerangka kerja dari penelitian atau jurnal lain. Untuk memilih kerangka kerja yang tepat untuk proses desain DRP, dilakukan perbandingan antar kerangka kerja untuk mengetahui kerangka kerja yang tepat digunakan sebagai panduan desain DRP di Unit IT XYZ. Perbandingan yang dilakukan Sativa dan Akhmadi (Akhmadi and Agustika Sativa, 2019) meliputi beberapa kerangka kerja yaitu NIST SP 800-34 Rev 1, ISO/IEC 24762, NFPA 1600,

Webtrust, dan empat kerangka kerja lainnya dari jurnal penelitian. Perbandingan dilakukan dengan menggunakan parameter dari Gupta et al., dimana 18 kriteria dapat digunakan untuk membandingkan kerangka kerja DRP (Gupta, Kapur and Kumar, 2016), Hasil perbandingan ditunjukkan pada Tabel I.

Tabel 1. Perbandingan kerangka kerja untuk DRP

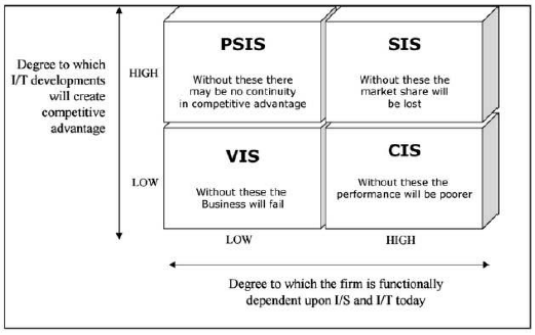
Parameter	Kerangka Kerja							
	(Swanson et al., 2010)	(ISO/IEC, 2008)	(National Fire Protection [illegible])	(CPA Canada, 2017)	(Gupta, Kapur and Kumar, 2016)	(Leong and Marthandan, 2014)	(Hawkins, Yen and Chan, 2000)	(Mudholkar, 2013)
1	✓	✓	✓	-	✓	✓	-	-
2	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	-	✓	✓	✓	✓	✓	-
4	✓	-	✓	✓	✓	-	-	-
5	✓	-	✓	✓	✓	-	-	-
6	✓	✓	✓	✓	✓	✓	✓	✓
7	✓	✓	✓	-	✓	✓	✓	-
8	✓	✓	✓	✓	-	✓	✓	✓
9	✓	-	✓	-	✓	-	-	-
10	-	-	-	-	-	-	-	-
11	✓	✓	✓	✓	✓	✓	✓	✓
12	✓	✓	✓	✓	✓	✓	✓	✓
13	✓	-	-	-	✓	✓	-	-
14	✓	✓	✓	✓	-	✓	✓	-
15	✓	-	-	✓	-	-	-	-
16	✓	-	-	-	-	-	-	-
17	✓	-	-	-	-	-	-	-
18	✓	✓	✓	-	✓	-	✓	✓
Total	17 /18	9 /18	13 /18	10 /18	12 /18	9 /18	10 /18	6 /18

2.5. NIST SP 800-53 Rev 5

NIST SP 800-53 Rev 5 adalah dokumen yang menjelaskan kendali keamanan yang dapat diterapkan oleh organisasi yang memproses, menyimpan, dan mengirimkan informasi.(National Institute of Standards and Technology, 2020). Kendali keamanan adalah tindakan pengamanan atau pencegahan yang digunakan dalam sistem atau organisasi untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem dan informasinya serta mengelola risiko keamanan informasi. Dalam dokumen ini, ada 20 kategori kendali keamanan yang dapat diterapkan oleh organisasi.

2.7. Matriks Warren McFarlan

Matriks Warren McFarlan merupakan kerangka kerja yang dapat menentukan skala prioritas dalam sistem informasi (Lestari, 2017). Matriks ini dibagi menjadi empat kategori berdasarkan kepentingan peran sebagai berikut: (1) Sistem Informasi Strategis (SIS); (2) Sistem Informasi Berpotensi Strategis (PSIS); (3) Sistem Informasi Kritikal (CIS); dan (4) Sistem Informasi Vital (VIS). Matriks Warren McFarlan ditunjukkan pada Gambar 3.



Gambar 3. Matriks Warren McFarlan (Lestari, 2017)

4. HASIL PENELITIAN

4.1. Penilaian Risiko

Penilaian risiko dilakukan untuk mengetahui skenario, kemungkinan, dan dampak risiko terhadap aset yang dikelola oleh Unit TI XYZ. Dalam penilaian ini, beberapa aspek ditentukan; yaitu, aset yang dikelola, ancaman, kerentanan, relevansi, jangkauan efek, kecenderungan untuk terjadi, kerentanan dan kondisi predisposisi, keparahan, kemungkinan kerugian, tren keseluruhan, dan tingkat dampak ancaman pada Unit TI XYZ. untuk kemudian menentukan nilai risiko guna menentukan prioritas penanganan dan pengendalian yang diterapkan terhadap ancaman tersebut.

terdapat sembilan risiko dengan kategori rendah, tiga risiko dengan kategori sedang, dan dua risiko dengan kategori tinggi. Matriks nilai risiko ditampilkan pada Tabel 2, dengan hasil penilaian risiko ditunjukkan pada Tabel 3 (Dimana **H=Tinggi, M=Sedang, L=Rendah, VL=Sangat Rendah, P=Mungkin, C=Terkonfirmasi**, dan **N/A=Tidak Tersedia**).

Tabel 2. Matriks nilai risiko (Rebecca M. Blank. Patrick D. Gallagher, 2012)

Likeli -hood	***Impact***				
	VL	**L**	**M**	**H**	**VH**
VH	VL	L	M	H	VH
H	VL	L	M	H	VH
M	VL	L	M	M	H
L	VL	L	L	L	M
VL	VL	VL	VL	L	L

4.1. Analisis Dampak Bisnis

Analisis dampak bisnis dilakukan untuk menentukan prioritas pemulihan apabila terjadi bencana dengan kategori risiko tinggi, dalam hal ini mengikuti hasil penilaian risiko yaitu penipisan sumber daya dan pemadaman. Pada tahap ini dilakukan pendataan kekritisan proses bisnis dan

tingkat layanan yang ditargetkan untuk dicapai dari setiap sistem yang dikelola oleh Unit TI XYZ.

Hasil analisis dampak bisnis berdasarkan MTD, RTO, RPO, dampak kegagalan aplikasi atau sistem, tingkat ketersediaan, dan waktu henti maksimum digunakan untuk menentukan urutan prioritas pemulihan dari aplikasi atau sistem yang dikelola oleh Unit TI XYZ. Hasilnya, ada enam aplikasi/sistem dengan prioritas tinggi, tiga aplikasi/sistem dengan prioritas sedang, dan dua aplikasi/sistem dengan prioritas rendah. Hasil analisis dampak bisnis ditunjukkan pada Tabel 4 (Dimana **H=Tinggi, M=Sedang, L=Rendah**).

4.3. Identifikasi Kendali Pencegahan

Tahap identifikasi kendali pencegahan bertujuan untuk mendeskripsikan pengendalian yang diterapkan oleh Unit TI XYZ untuk melindungi aset yang dikelola dari eksploitasi ancaman terhadap kerentanan yang ada. Tahapan ini bertujuan untuk mengetahui langkah-langkah preventif yang telah dilakukan oleh Unit IT XYZ untuk mendeteksi dan mengurangi dampak dari ancaman yang ada pada sistem. Oleh karena itu, rekomendasi kendali didasarkan pada standar NIST SP 800-53 Rev 5 dan SNI 8799 untuk memastikan pengendalian diterapkan.

Dari hasil penilaian pusat data Unit TI menggunakan parameter pusat data SNI 8799 Strata 2 diketahui bahwa Unit TI tidak memenuhi 12 parameter. Untuk memenuhi kebutuhan pusat data Strata 2, terdapat rekomendasi tindakan yang dapat diterapkan oleh Unit TI yang terangkum dalam Tabel 5.

Tabel 3. Hasil penilaian risiko

No	Ancaman	Jangkauan Efek	Relevansi	Dampak	Kecenderungan	Risiko
1.	Kebocoran informasi sensitif	M	C	H	L	L
2.	Kesalahan penanganan informasi kritikal oleh *privileged user*	M	N/A	M	VL	VL
3.	Kesalahan pengaturan *privilege*	M	N/A	M	VL	VL
4.	Kontensi komunikasi	L	N/A	L	VL	VL
5.	Perangkat penampil tidak terbaca	L	N/A	L	VL	VL
6.	Gempa bumi pada situs utama	L	C	M	L	L
7.	Kebakaran pada situs utama	M	P	M	L	L
8.	Kebakaran pada situs cadangan	M	N/A	M	VL	VL
9.	Banjir pada situs utama	M	N/A	M	VL	VL
10.	Banjir pada situs cadangan	VL	N/A	M	VL	VL
11.	Badai pada situs utama	M	N/A	M	VL	VL
12.	Badai pada situs cadangan	VL	N/A	VL	VL	VL
13.	Kerusakan perangkat karena usia	VH	C	VH	M	H
14.	*Blackout*	VH	C	VH	M	H

Tabel 4. Hasil analisis dampak bisnis

#	*Identifier*	Dampak	Kategori	MTD	RTO	RPO	Target Max. Downtime	Prioritas
1.	IS.01	H	VIS	3	1-3	24	21h 54m	H
2.	IS.02	H	VIS	3	1-3	24	21h 54m	H
3.	IS.03	M	PSIS	12	1-6	24	21h 54m	M
4.	IS.04	M	CIS	12	1-6	168	21h 54m	M
5.	IS.05	M	SIS	12	1-6	168	21h 54m	M
6.	IS.06	H	CIS	3	1-3	24	21h 54m	H
7.	IS.07	H	CIS	3	1-3	24	21h 54m	H
8.	IS.08	L	PSIS	24	1-12	168	21h 54m	L
9.	IS.09	L	CIS	24	1-12	168	21h 54m	L
10.	IS.10	M	VIS	3	1-3	24	21h 54m	H
12.	IS.11	H	VIS	3	1-3	24	21h 54m	H

Tabel 5. Analisis kesenjangan dan rekomendasi berdasarkan SNI 8799

#	Kendali SNI 8799	Kondisi saat ini	Rekomendasi
1.	Dinding partisi area server	Ruang pusat data Unit TI tidak memiliki partisi untuk area server.	Menerapkan pemisah antara area server dengan area telekomunikasi yang terbuat dari material tahan api
2.	Pompa tangki penyimpanan	Pompa tangki bahan bakar untuk genset pusat data Unit TI berjumlah 1 unit	Menambah pompa tangki bahan bakar menjadi berjumlah 2 unit.
3.	Kapasitas bahan bakar yang tersedia di lokasi	Kapasitas bahan bakar untuk genset maksimal dapat digunakan untuk 12 jam	Menambah jumlah bahan bakar untuk genset sehingga dapat digunakan selama minimal 24 jam.
4.	Titik pantau	Pusat data Unit TI belum memiliki titik pantau untuk UPS dan genset.	Membangun/membuat ruang kendali untuk menjadi titik pantau pusat data dan menjadi
5.	Metoda pemberitahuan	Pusat data Unit TI belum memiliki	metoda pemberitahuan
6.	Ruang kendali	ruang kendali.	apabila terjadi anomali dalam operasional pusat data
7.	Pintu menuju area ruang server	Pengamanan pada ruang pusat data Unit TI menggunakan kunci pengaman gembok dengan Standar Nasional Indonesia (SNI)	Pengamanan pintu ruang server diganti menggunakan kartu akses elektronik.
8.	Pintu utama menuju area server	Pusat data Unit TI tidak memiliki pintu pemisah menuju area server selain pintu menuju area ruang server	Menambahkan pengamanan terhadap ruang server dengan menambahkan pintu sebelum memasuki area server dengan pengamanan kartu akses dan biometric.
9.	Membangun pintu masuk dengan pos pemeriksaan keamanan	Pintu masuk dengan pos pemeriksaan keamanan dibangun di area server	Menambahkan pos keamanan atau penjagaan sebelum memasuki ruang server.
10.	Pencatatan tamu atau pengunjung	Unit TI tidak melakukan pencatatan tamu atau pengunjung pusat data	Melakukan pencatatan untuk mengetahui riwayat pihak-pihak yang mengunjungi atau berkeperluan mengakses pusat data Unit TI.
11.	Jumlah pelaksana operasional per sif	Staf TI memiliki jam operasional sesuai dengan jam dinas yaitu pada pukul 08.00-16.00 lima hari dalam satu minggu	Menambah ketersediaan jumlah Staf Unit TI sehingga dapat dilakukan piket sif untuk 1x24 jam dalam lima hari kerja.

Selanjutnya, dilakukan identifikasi kendali pencegahan terhadap ancaman yang telah diidentifikasi pada penilaian risiko. Ancaman yang diidentifikasi untuk pengendalian pencegahan adalah ancaman yang dikonfirmasi dan mungkin. Ada lima ancaman yang diidentifikasi sebagai kendali pencegahan, dirangkum dalam Tabel 6. Rekomendasi kendali diambil dari NIST SP 800-53 Rev 5.

Tabel 6. Rekomendasi kendali

#	Ancaman	Kerentanan	Rekomendasi
1.	Kebocoran informasi sensitif	Pengembangan, penerapan, dan operasional teknis aplikasi atau sistem masih dilakukan oleh anggota unit kerja selain Unit TI. Dimana aspek keamanan aplikasi atau sistem. Komunikasi diabaikan.	Memantau aplikasi atau sistem untuk mendeteksi kebocoran informasi sensitif dan memberikan pemberitahuan kepada pihak yang proses bisnisnya terkait dengan aplikasi atau sistem dan menggunakan alat otomatis untuk memantaunya. Memberikan pelatihan dan bimbingan dalam mengembangkan aplikasi atau sistem yang memiliki keamanan yang baik. Memantau komunikasi pada antarmuka jaringan eksternal dan antarmuka jaringan internal dengan sistem, mengimplementasikan sub-jaringan untuk akses eksternal, dan menghubungkan ke jaringan atau sistem eksternal hanya melalui antarmuka terkendali yang terdiri dari perangkat perlindungan batas yang diatur mengikuti arsitektur keamanan Unit TI.
2.	Gempa bumi pada situs utama	Pusat data Unit IT belum memiliki situs cadangan untuk memindahkan pengoperasian layanan atau sistem aplikasi terkelola pada saat gempa yang merusak	Menempatkan perangkat yang terkait dengan pengoperasian data center Unit IT pada lokasi di gedung-gedung yang kuat dan dapat menahan dampak guncangan gempa, dan menerapkan *recovery site* atau situs pemulihan sehingga jika terjadi

#	Ancaman	Kerentanan	Rekomendasi
		bangunan dan perangkat terkelola.	kerusakan signifikan pada situs utama , masih ada situs cadangan untuk aplikasi atau layanan agar dapat beroperasi.
3.	Kebakaran pada situs utama	Pusat data Unit TI bersifat tunggal dan belum memiliki situs cadangan untuk memindahkan pengoperasian layanan atau sistem aplikasi terkelola jika terjadi kebakaran.	Menempatkan perangkat yang terkait dengan pengoperasian pusat data Unit TI di lokasi di gedung yang cukup kuat untuk menahan dampak kebakaran (tidak runtuh). Menerapkan sistem deteksi dan pemadam kebakaran dengan metode cairan (penyemprot) dan pemadam api berbahan dasar bubuk/bubuk, di mana sumber daya independen mendukung sistem tersebut. Sistem deteksi dan pemadaman kebakaran dapat diaktifkan secara otomatis dan diaudit setiap periode untuk memastikan kondisi dan kelayakan sistem deteksi dan pemadaman kebakaran. Menerapkan situs pemulihan sehingga masih ada situs cadangan untuk aplikasi atau layanan untuk beroperasi jika terjadi kerusakan signifikan pada situs utama.
4.	Kerusakan perangkat karena usia	Usia peralatan yang digunakan oleh Unit IT sudah cukup tua, sehingga jika terjadi sedikit gangguan dapat memicu kerusakan permanen dan tidak dapat diperbaiki.	Membentuk siklus pembaharuan perangkat yang diawali dengan analisis rata-rata usia perangkat, dimana hasil analisis tersebut kemudian dijadikan bahan pertimbangan batas usia rata-rata perangkat. Ketika usia rata-rata peralatan melebihi batas yang telah ditentukan, dilakukan penilaian untuk menentukan prioritas peralatan yang perlu diganti atau diperbaharui sesegera mungkin.
5.	*Blackout*	Saluran listrik untuk catu daya pusat data adalah tunggal tanpa saluran listrik cadangan, intensitas pemadaman listrik di lingkungan lembaga XYZ tinggi, dan Unit TI belum memiliki situs cadangan untuk operasi	Menambahkan saluran listrik cadangan untuk pusat data Unit TI dan saluran utama dan menyediakan bahan bakar yang cukup untuk generator dalam pemadaman yang berkepanjangan. Unit-unit TI juga direkomendasikan untuk memiliki situs cadangan untuk kelangsungan proses bisnis aplikasi yang dikelola dalam pemadaman yang melebihi waktu henti maksimum aplikasi atau sistem.

Hasil penilaian, analisis kesenjangan beserta rekomendasi yang diberikan kemudian diterima oleh Kepala Unit TI XYZ dan akan diolah kembali serta dibahas pada rapat rencana kerja tahunan Institusi XYZ, dengan harapan bahwa rekomendasi yang diberikan dapat diterapkan paling cepat pada tahun anggaran baru.

4.4. Pengembangan Rencana Kontingensi

Setelah mengetahui risiko dan dampak yang ditimbulkan jika Unit TI XYZ mengelola aplikasi atau sistem dan menjelaskan pengendalian yang diterapkan, untuk melindungi aplikasi atau sistem yang dikelola, maka langkah selanjutnya adalah menyusun rencana kontingensi *atau contingency plan* untuk setiap aplikasi. atau sistem berdasarkan klasifikasi dampak yang ditimbulkan. Rencana kontijensi untuk Unit TI XYZ ditunjukkan pada Tabel 7 (Dimana **H=Tinggi, M=Sedang, L=Rendah**).

.

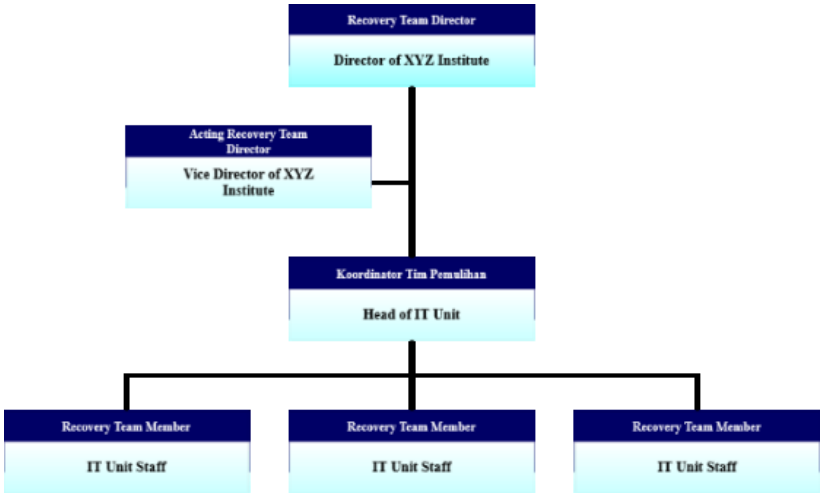
Tabel 7. Strategi pemulihan

Dampak	Prioritas	Penjelasan	Aplikasi /Sistem	Strategi Pencadangan	Strategi Pemulihan
L	L	Mencakup aplikasi atau sistem dengan efek mengganggu yang memengaruhi komputer dan akun pengguna di lingkungan Institut XYZ atau memiliki sedikit efek pada proses belajar-mengajar atau proses administrasi	IS.08 IS.09	Aplikasi atau sistem dicadangkan seminggu sekali (7 hari kalender) dengan cadangan di situs utama.	Menggunakan *cold site* dengan situs cadangan yang terletak di Pusat Data Badan ABC.
M	M	Mencakup aplikasi atau sistem dengan efek mengganggu yang mempengaruhi infrastruktur jaringan, server, atau akun administrator di Unit TI XYZ atau memiliki efek sedang pada proses belajar mengajar dan proses administrasi.	IS.03 IS.04 IS.05	Aplikasi atau sistem dicadangkan setiap tiga hari dengan cadangan di situs utama.	Menggunakan *warm site* dengan situs cadangan yang terletak di Pusat Data Badan ABC.

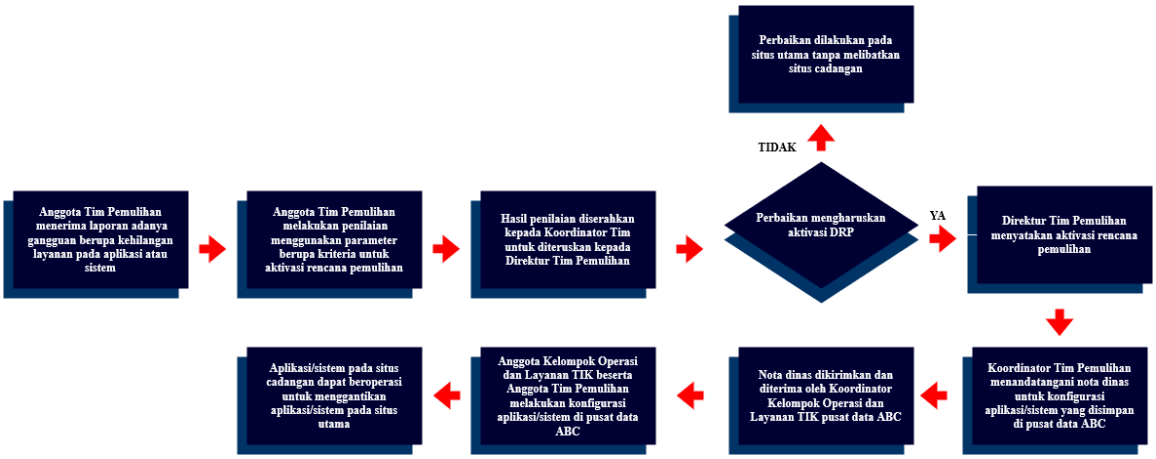
Dampak	Prioritas	Penjelasan	Aplikasi /Sistem	Strategi Pencadangan	Strategi Pemulihan
H	H	Mencakup aplikasi atau sistem dengan dampak disruptif yang berdampak signifikan terhadap proses bisnis utama unit kerja di lingkungan XYZ Institute atau berdampak signifikan terhadap proses belajar mengajar serta proses administrasi	IS.01 IS.02 IS.06 IS.07 IS.10 IS.11	Aplikasi atau sistem dicadangkan sekali sehari dengan pencadangan di situs cadangan	Menggunakan *Hot Site* dengan situs cadangan yang terletak di Pusat Data Badan ABC.

Menurut NIST SP 800-34, rencana pemulihan bencana harus memiliki deskripsi tim pelaksana pemulihan (Swanson et al., 2010). Struktur tim terdiri dari Direktur Tim Pemulihan, Plt. Direktur Tim Pemulihan, Koordinator Tim Pemulihan, dan Anggota Tim Pemulihan, seperti terlihat pada Gambar 4.

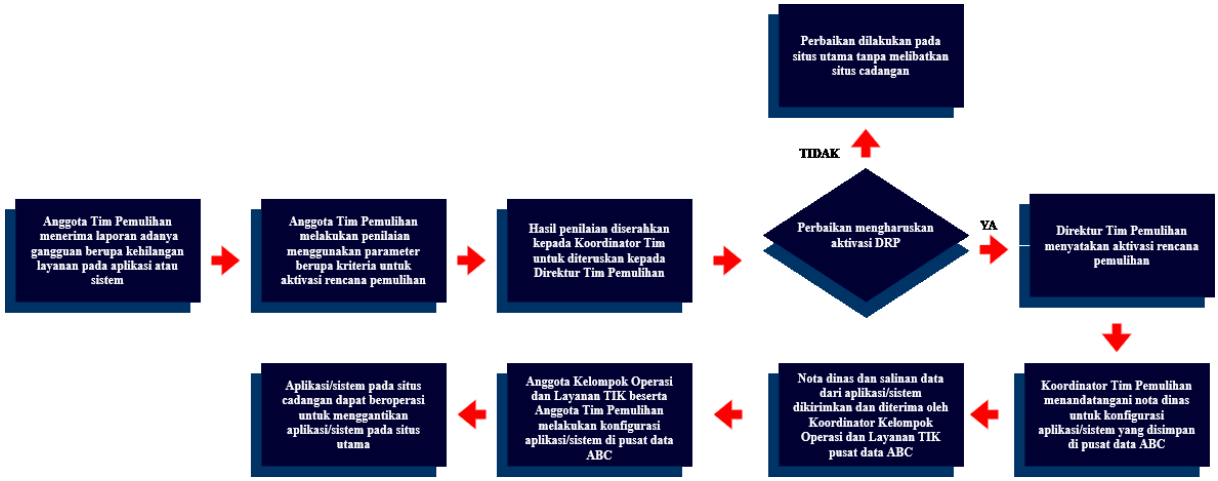
Berikutnya, setelah menentukan strategi dan menyusun tim pemulihan, dilakukan penyusunan dari DRP berdasarkan masing-masing strategi pemulihan. Untuk aplikasi/sistem dengan metode pemulihan hot site, warm site, dan cold site ditampilkan masing-masing pada Gambar 5, Gambar 6, dan Gambar 7.



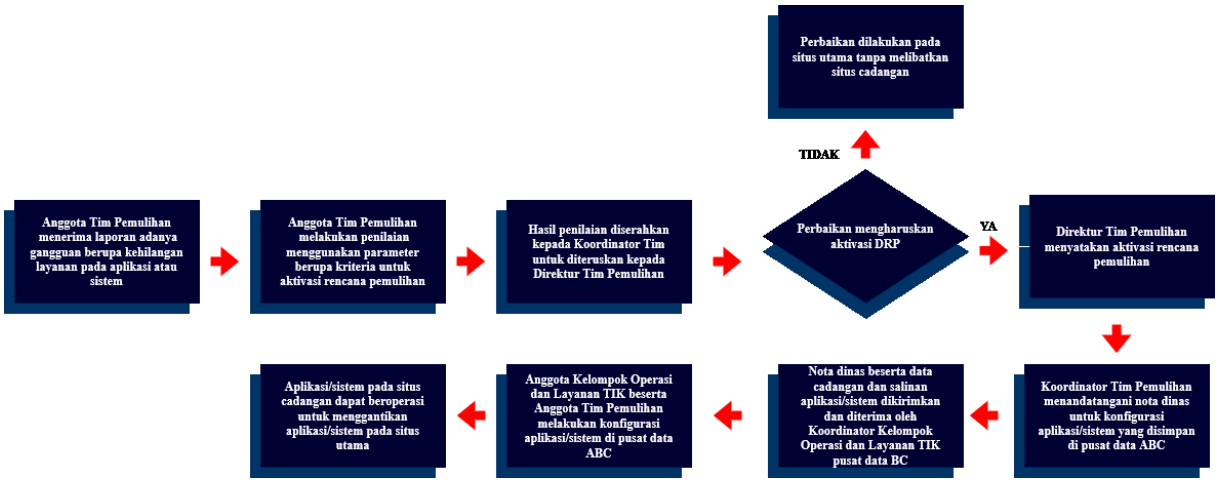
Gambar 1. Struktur tim pemulihan



Gambar 5. Rencana pemulihan bencana dengan strategi *hot site*



Gambar 6. Rencana pemulihan bencana dengan strategi *warm site*



Gambar 6. Rencana pemulihan bencana dengan strategi *cold site*

5. KESIMPULAN

Berdasarkan hasil analisis data pada rancangan rencana pemulihan bencana untuk Unit TI XYZ, dapat disimpulkan bahwa rencana pemulihan bencana telah disusun menggunakan dasar acuan NIST SP 800-34 Rev 1 sebagai kerangka kerja penyusunan, NIST SP 800-53 Rev 5 sebagai kendali pencegahan dan SNI 8799-1 sebagai persyaratan pusat data. Rencana pemulihan ini disusun berdasarkan hasil dari tahap penilaian risiko yang diketahui terdapat sembilan (9) risiko dengan kategori *very low*, tiga (3) risiko dengan kategori *low*, dan dua (2) risiko dengan kategori *high*, kemudian tahap analisis dampak bisnis dimana diketahui bahwa terdapat 6 (enam) aplikasi dengan prioritas *high*, 3 (tiga) aplikasi dengan prioritas *moderate*, dan 2 (dua) aplikasi dengan prioritas *low*.

Setelah itu, dilakukan penilaian terhadap pusat data Unit TI menggunakan parameter strata 2 SNI 8799-1, terdapat terdapat 12 parameter yang belum sesuai sehingga diiberikan rekomendasi untuk memperbaiki dan memenuhi parameter tersebut. Berikutnya, berdasarkan identifikasi kendali berdasarkan NIST SP 800-53 Rev 5, terdapat 9 rekomendasi kendali yang dapat diterapkan untuk memitigasi dampak dari ancaman. Hasil rencana pemulihan melibatkan situs pusat data ABC sebagai situs cadangan dengan pengaturan yaitu aplikasi prioritas *high* menggunakan metode *hot site*, aplikasi prioritas *moderate* menggunakan metode *warm site*, dan aplikasi prioritas *low* menggunakan *cold site*.

DAFTAR PUSTAKA

AKHMADI, A.A. and AGUSTIKA SATIVA, I.G.R., 2019. *Penyusunan Disaster Recovery Plan (DRP) pada Otoritas Sertifikat Digital Layanan Universal (OSD LU) Kelas 2 Balai Sertifikasi Elektronik (BSrE) Berdasarkan NIST SP 800-34 Rev 1 dan Webtrust Principle and Criteria for Certification Authority Version 2.1*. Bogor: Sekolah Tinggi Sandi Negara.

AZWAR, S., 2012. *Reliabilitas dan validitas*. Yogyakarta: pustaka pelajar.

BADAN ABC, 2019. *Peraturan Badan ABC No. 12 Tahun 2019*.

BADAN STANDARISASI NEGARA, 2019. SNI-8799.

CPA CANADA, 2017. *WEBTRUST® FOR CERTIFICATION AUTHORITIES WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES-SSL BASELINE WITH NETWORK SECURITY*.

GUPTA, V., KAPUR, P.K. and KUMAR, D., 2016. Exploring disaster recovery parameters in an enterprise application. *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, pp.294–299.

HAMADAH, S., 2019. Cloud-based disaster recovery and planning models: An overview. *ICIC Express Letters*, 13(7), pp.593–599. https://doi.org/10.24507/icicel.13.07.593.

HARDANI, H., ANDRIANI, H., FARDANI, R.A., USTIAWATY, J., UTAMI, E.F., SUKMANA, D.J. and ISTIQOMAH, R.R., 2020. Metode penelitian kualitatif & kuantitatif. *Yogyakarta: Pustaka Ilmu*.

HAWKINS, S.M., YEN, D.C.-C. and CHOU, D.C., 2000. Disaster recovery planning: a strategy for data security. *Inf. Manag. Comput. Secur.*, 8, pp.222–230.

ISO/IEC, 2008. *Information technology-Security techniques-Guidelines for information and communications technology disaster recovery services*. [online] Available at: <www.iso.org>.

LEONG, L.H. and MARTHANDAN, G., 2014. Critical Dimensions of Disaster Recovery Planning. *International Journal of Business and Management*, 9(12). https://doi.org/10.5539/ijbm.v9n12p145.

LESTARI, A.D., 2017. Menentukan Skala Prioritas Sistem Informasi Layanan Opac Studi Kasus Di Badan Perpustakaan Umum Dan Arsip Daerah Kabupaten Tulungagung. Jurnal Kajian Perpustakaan dan Informasi.

MUDHOLKAR, P.K., 2013. Protecting E-Business by implementing Business Continuity and Disaster Recovery Planning in the Banking Industry.

NATIONAL FIRE PROTECTION ASSOCIATION, 2019. NFPA 1600.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2020. Security and privacy controls for federal information systems and organizations. *NIST Special Publication 800-53*.

NURHANUDIN, 2021. *Designing a Disaster Recovery Plan Using NIST 800-34 Framework on the Information System of The Directorate General of Hajj and Umrah*. [online] *ISSN*, Available at: <http://journal.stmikglobal.ac.id/index.php/sisfotek>.

REBECCA M. BLANK. PATRICK D. GALAGHER, 2012. NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Special Publication*, (September), p.95.

SETYAWAN, A., GIRI SUCAHYO, Y. and GANDHI, A., 2020. Design of disaster recovery plan: State university in indonesia. In: *2020 5th International Conference on Informatics and Computing, ICIC 2020*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICIC50835.2020.9288543.

SNEDAKER, S., 2013. *Business continuity and disaster recovery planning for IT professionals*. Newnes.

SUGIYONO, D., 2013. Metode penelitian pendidikan pendekatan kuantitatif, kualitatif dan R&D.

SWANSON, M., BOWEN, P., PHILLIPS, A.W., GALLUP, D. and LYNES, D., 2010. Contingency Planning Guide for Federal Information Systems. *NIST Special Publication 800-34 Rev. 1*, (May), p.150.

WINKLER, V.J.R., 2011. *Securing the Cloud: Cloud computer Security techniques and tactics*. Elsevier.