Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.1148959
Vol. 11, No. 4, Agustus 2024, hlm. 929-938 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

PERANCANGAN *DISASTER RECOVERY PLAN* PADA PUSAT DATA DAN TEKNOLOGI INFORMASI KOMUNIKASI INSTANSI XYZ

Sefiulki Weni Sari[*1], Kalamullah Ramli[2]

[1,2] Universitas Indonesia, Depok
Email: [1]sefiulki.weni@ui.ac.id, [2]kalamullah.ramli@ui.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 28 April 2024, diterima untuk diterbitkan: 19 Agustus 2024)

Abstrak

Pusat Data dan Teknologi Informasi Komunikasi (Pusdatik) adalah bagian penting dari Instansi XYZ yang bertanggung jawab atas manajemen teknologi informasi dan pengoperasian pusat data. Dalam menghadapi tantangan dari era digital dan konektivitas yang cepat, Pusdatik harus memiliki kesiapan untuk mengatasi gangguan layanan dan operasional yang disebabkan oleh bencana dan ancaman. Salah satu langkah untuk meminimalkan dampak dari gangguan tersebut dengan melalui penyusunan *Disaster Recovery Plan* (DRP). Dalam penelitian ini, berdasarkan hasil wawancara dengan pimpinan, ketua tim, dan staf Pusdatik, terungkap bahwa layanan yang dikelola oleh Pusdatik memiliki peran yang krusial dalam mendukung proses bisnis organisasi. Namun, saat ini Pusdatik belum memiliki DRP yang dapat dijalankan dalam situasi bencana. Oleh karena itu, diperlukan perancangan DRP yang akan menjadi panduan dalam menghadapi gangguan dan bencana yang tidak terduga. Metode kualitatif dengan pendekatan studi kasus yang digunakan dalam penelitian ini. Data dikumpulkan dengan proses wawancara, studi pustaka, dan observasi langsung ke pusat data. Perancangan DRP dilakukan dengan merujuk pada NIST SP 800-34 Rev 1. Tahapan penelitian meliputi analisis proses bisnis, identifikasi aset, penilaian risiko, analisis dampak bisnis, evaluasi kontrol pencegahan sesuai dengan standar SNI 8799-1:2023, dan penyusunan dokumen DRP. Hasil penelitian ini merupakan dokumen DRP yang sesuai dengan kondisi Pusdatik saat ini.

Kata kunci: *disaster recovery plan, risk assessment, business impact analysis*, NIST SP 800-34

DESIGN OF DISASTER RECOVERY PLAN FOR THE DATA CENTER AND COMMUNICATION INFORMATION TECHNOLOGY OF XYZ INSTITUTION

Abstract

The Data Center and Communication Technology Information (Pusdatik) is an essential part of Institution XYZ responsible for managing information technology and operating data centers. In facing the challenges of the digital era and rapid connectivity, Pusdatik must be prepared to address disruptions in services and operations caused by disasters and threats. One step to minimize the impact of such disruptions is through the development of a Disaster Recovery Plan (DRP). In this study, based on interviews with leaders, team leaders, and staff of Pusdatik, it was revealed that the services managed by Pusdatik play a crucial role in supporting the organizational business processes. However, currently, Pusdatik does not have a DRP that can be implemented in disaster situations. Therefore, the development of a DRP is needed to serve as a guide in facing unforeseen disruptions and disasters. The research method used is qualitative with a case study approach. Data was collected through interviews, literature review, and direct observation of the data center. DRP development was carried out with reference to NIST SP 800-34 Rev 1. The research stages include business process analysis, asset identification, risk assessment, business impact analysis, preventive control evaluation in accordance with the SNI 8799-1:2023 standard, and DRP document preparation. The result of this study is a DRP document that aligns with the current condition of Pusdatik.

Keywords: *disaster recovery plan, risk assessment, business impact analysis, NIST SP 800-34*

1. PENDAHULUAN

Peningkatan penggunaan internet di Indonesia yang sejalan dengan kemajuan teknologi, mencerminkan transformasi digital yang signifikan di berbagai sektor. Masyarakat Indonesia semakin mengandalkan internet untuk akses informasi, komunikasi, interaksi sosial, dan layanan publik.

Berdasarkan informasi yang didapatkan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia berjumlah 221 juta orang pada tahun 2024, yang setara dengan sekitar 79,5% dari total populasi pada tahun sebelumnya (APJII, 2024). Ketergantungan pada internet telah menjalar ke semua lapisan masyarakat, mulai dari bisnis hingga pendidikan, komunikasi, dan hiburan. Namun, penggunaan internet juga membawa risiko keamanan, dengan serangan siber yang semakin sering terjadi di Indonesia, termasuk serangan malware, ransomware, dan phishing.

Berdasarkan Laporan Monitoring BSSN, terdapat beberapa jenis dugaan insiden keamanan siber yang melibatkan data breach, ransomware, proaktif, kerentanan, profiling, web defacement, DDoS, dan doxing. Data breach menjadi insiden keamanan siber yang paling umum, dengan 422 kasus tercatat (BSSN, 2023). Hal ini menunjukkan bahwa transformasi digital di Indonesia juga membawa tantangan serius terkait dengan keamanan siber, terutama dalam menjaga infrastruktur teknologi informasi dan data sensitif. Sektor administrasi pemerintahan terindikasi paling rentan terhadap serangan siber, dengan 36% dari insiden yang dilaporkan terjadi di sektor tersebut.

Manajemen risiko keamanan informasi menjadi krusial untuk menghadapi tantangan keamanan siber. Pendekatan ini mencakup identifikasi kerentanan dan ancaman serta penilaian dampak buruk pada organisasi (E. Wheeler, 2011). Berbagai ancaman seperti bencana alam dan serangan siber dapat menyebabkan gangguan operasional serta risiko kehilangan data bagi organisasi. Dalam era globalisasi dan konektivitas yang semakin pesat, organisasi harus siap menghadapi berbagai tantangan yang dapat mengganggu jalannya proses bisnis organisasi. Dengan manajemen risiko yang tepat, organisasi dapat mengurangi risiko serangan siber dan merespons dengan cepat jika terjadi insiden. Hal ini penting untuk melindungi aset dan reputasi organisasi dari kerusakan yang disebabkan oleh serangan siber, serta meningkatkan kesiapan dalam menghadapi bencana alam dan mempercepat proses pemulihan pasca-bencana (UNISDR, 2009).

Berdasarkan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), instansi pemerintah diharuskan menerapkan manajemen risiko SPBE yang mencakup manajemen keamanan informasi, data, aset teknologi informasi, sumber daya manusia, pengetahuan, perubahan, serta layanan SPBE (SPBE, 2018). Salah satu aspek penilaian dalam manajemen risiko adalah kesiapan terhadap bencana dengan adanya *Business Continuity Plan* (BCP) dan DRP. Namun, data dari BSSN menunjukkan bahwa masih banyak instansi pemerintah yang belum memiliki dokumen BCP dan DRP, yang dapat menyebabkan kesulitan dan keterlambatan dalam penanganan masalah saat terjadi gangguan atau bencana.

DRP merupakan bentuk rencana kontingensi yang mencakup persiapan dan tanggapan organisasi terhadap bencana, baik yang disebabkan oleh alam maupun oleh manusia dan dibuat dengan mengidentifikasi jenis bencana dan kondisi proses bisnis [Fernandes, Karepowan, Tannady, 2024]. Proses pemulihan bencana akan menangani sistem teknologi informasi suatu organisasi, sementara BCP cenderung melibatkan semua aspek operasional organisasi. Merencanakan pemulihan bencana dapat berkontribusi pada penghematan biaya dan menjaga masa depan sebuah organisasi.

Instansi XYZ merupakan salah satu lembaga pemerintah yang membutuhkan implementasi DRP yang sesuai dengan risiko yang dihadapi. Pusat Data dan Teknologi Informasi Komunikasi (Pusdatik) yang memiliki tugas dan fungsi dalam pengelolaan layanan teknologi informasi komunikasi dan penyelenggaraan pusat data belum memiliki DRP berdasarkan hasil wawancara dengan ketua tim Pusdatik. Sebagai unit kerja yang mengelola pusat data dan teknologi informasi (TI), Pusdatik harus mengelola aset yang dimilikinya. Dengan banyaknya aset yang dikelola oleh Pusdatik, maka diperlukan manajemen risiko dalam menangani, mengendalikan, melindungi aset TI, menangani risiko, dan meminimalkan risiko yang mungkin terjadi [Bisma, 2022].

Pusdatik pernah mengalami insiden keamanan siber yang mengganggu layanan teknologi informasi dan komunikasi. Salah satunya adalah aplikasi email yang tidak dapat diakses oleh pegawai karena terdapat akun pegawai yang melakukan SPAM email, sehingga mengakibatkan IP Publik yang digunakan masuk ke dalam blacklist di beberapa SPAMHAUS. Dampak dari gangguan tersebut adalah email dari domain tersebut tidak dapat diterima oleh instansi lain karena IP publik masuk ke dalam blacklist.

Pada bulan Agustus 2019, terjadi pemadaman listrik di wilayah Banten, DKI Jakarta, dan Jawa Barat. Pemadaman listrik tersebut berdampak pada pusat data Pusdatik. Pemadamam listrik selama belasan jam tersebut menyebabkan hampir tidak beroperasinya layanan pada pusat data karena menipisnya bahan bakar untuk mengoperasikan generator listrik yang merupakan penghasil listrik cadangan atau darurat.

Menurut data dari BMKG mulai dari bulan November 2023 sampai dengan bulan April 2024, gempa yang terjadi di Pulau Jawa adalah sebanyak 433 laporan. Pulau Jawa adalah salah satu wilayah yang rentan terhadap gempa bumi dan memiliki populasi yang padat [Wahyu dan Rushendra, 2022]. Menurut pemetaan wilayah rawan bencana, ada empat provinsi dengan tingkat kerawanan tinggi, yaitu Aceh, Jawa Tengah, Jawa Timur, dan Jawa Barat. Pusat data Pusdatik berada di daerah Jawa Barat dan termasuk ke dalam provinsi rawan bencana dengan tingkat tinggi sehingga hal ini sangat mempengaruhi strategi penempatan dan pengelolaan

pusat data. Untuk mengurangi dampak buruk dan menjaga kontinuitas dari proses bisnis instansi XYZ diperlukan DRP sebagai panduan dalam menghadapi gangguan dan bencana yang tidak terduga.

Penelitian sebelumnya yang membahas terkait DRP adalah penelitian yang dilakukan (Setyawan, dkk, 2020), penelitian ini membahas perancangan DRP pada Universitas X di Indonesia. Pada penelitian tersebut dibahas tahapan yang dilakukan dalam membuat DRP sesuai dengan NIST SP 800-34 Rev.1, namun pada tahapan penilaian risiko tidak disebutkan kerangka kerja yang digunakan. Untuk tahapan analisis kontrol pencegahan menggunakan standar ANSI / TIA 942-A. Hasil penelitian tersebut adalah menghasilkan draf dokumen DRP yang dapat digunakan untuk implementasi manajemen risiko di Universitas X.

Penelitian selanjutnya adalah perancangan DRP di unit IT XYZ (Afiansyah, H., Sunaringtyas, S., Amiruddin, 2023). Penelitian ini membahas perancangan DRP pada unit IT XYZ yang merupakan bagian organisasi yang bertanggung jawab atas pengelolaan layanan oleh Unit IT XYZ yang sangat penting bagi kelancaran perkuliahan, administrasi, dan layanan kepada mahasiswa. Perancangan DRP ini dilakukan pada institusi pendidikan dengan merujuk pada NIST SP 800-34 Rev.1. Namun, pada proses penilaian risiko tidak disebutkan kerangka kerja yang digunakan. Pada tahap kontrol pencegahan, digunakan NIST SP 800-53 Rev 5, dan sebagai panduan untuk memenuhi persyaratan pusat data digunakan SNI 8799:2019. Hasil penelitian berupa dokumen DRP dengan enam strategi pemulihan untuk sistem yang memiliki tingkat prioritas tinggi, tiga strategi pemulihan untuk sistem prioritas sedang, dan dua strategi pemulihan untuk sistem prioritas rendah.

Penelitian berikutnya adalah penyusunan DRP pada perusahaan IT Nasional (Alifian, H., dan Priharsari, D., 2021). Penelitian tersebut melakukan penyusunan DRP dengan menggunakan kerangka kerja NIST SP 800-34 Rev.1. Langkah yang dilakukan setelah merancang strategi kontingensi dalam penelitian ini adalah melakukan pengembangan rencana kontingensi dengan membuat perencanaan pada fase aktivasi, pemulihan, dan rekonstitusi. Dokumen DRP yang dihasilkan dari penelitian ini sesuai dengan kondisi internal PT XYZ.

Dari tiga penelitian tersebut, disusun langkah-langkah untuk merancang DRP yang mengikuti NIST SP 800-34. Proses diawali dengan mengidentifikasi dan mengevaluasi risiko untuk menyusun daftar potensi risiko yang dapat mengancam ketersediaan layanan di Pusdatik, penilaian risiko dilakukan dengan menggunakan NIST SP 800-30 Rev.1 (Rebecca M. Blank. Patrick D. Gallagher, 2012). Langkah berikutnya adalah menentukan prioritas pemulihan layanan Teknologi Informasi (TI) dengan melakukan analisis dampak bisnis. Selanjutnya adalah melakukan kontrol pencegahan dengan melakukan penilaian terhadap persyaratan pusat data yang sesuai dengan strata dan kondisi pusat data Pusdatik dengan menggunakan standar SNI 8799-1:2023 yang merupakan perbaikan dari versi sebelumnya di tahun 2019. Pemahaman terkait risiko dan prioritas dalam pemulihan layanan diperlukan untuk merancang rencana kontingensi.

2. METODE PENELITIAN

Pendekatan kualitatif digunakan pada penelitian ini. Pendekatan kualitatif merupakan suatu metode penelitian yang menekankan pada konteks alami dan proses pengumpulan serta analisis data yang bersifat deskriptif (Sugiyono, 2021). Penelitian ini akan difokuskan pada penyusunan DRP untuk Pusat Data dan Teknologi Informasi Komunikasi di Instansi XYZ. Proses perancangan DRP ini didasarkan pada analisis data sesuai dengan panduan NIST SP 800-34 Rev.1. Studi kasus adalah metode kualitatif yang digunakan dalam penelitian ini, di mana seorang peneliti melakukan penyelidikan yang mendalam terhadap suatu sistem khusus berdasarkan data yang telah dikumpulkan secara menyeluruh (Fitrah dan Luthfiyah, 2017). Penelitian ini menghasilkan dokumen DRP yang ditujukan untuk Pusdatik Instansi XYZ.

Pengumpulan data dengan cara wawancara, tinjauan literatur, dan observasi di pusat data. Langkah pengumpulan data melibatkan dari berbagai sumber, termasuk wawancara dengan pimpinan, ketua tim, dan staf Pusdatik. Penulis juga melakukan studi pustaka, mencari peraturan dan kebijakan serta dokumentasi pendukung untuk penelitian ini dan melakukan obervasi di pusat data.

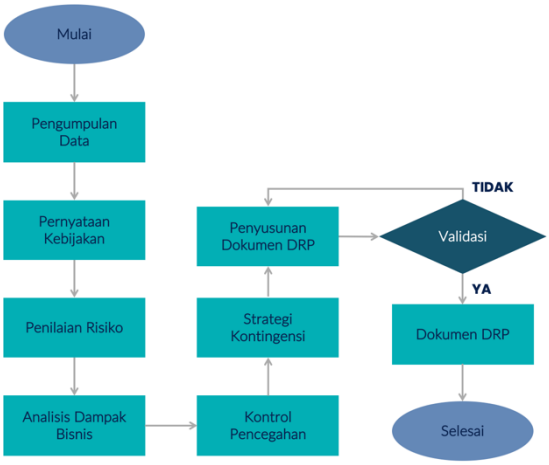
Setelah mengumpulkan data, langkah berikutnya adalah memproses data tersebut. Wawancara akan ditranskripsikan kemudian diproses sehingga menghasilkan informasi yang tepat. Sedangkan untuk hasil observasi, studi literatur, dan dokumentasi, dilakukan proses triangulasi. Setelah itu, analisis kesesuaian dilakukan dengan menggunakan NIST SP 800-34 Rev.1 sebagai panduan untuk menyusun DRP. Validasi dokumen DRP yang telah disusun dilakukan oleh ahli eksternal yang sesuai dengan keahliannya di bidang keamanan informasi dan pengelolaan pusat data.

NIST SP 800-34 Rev.1 menguraikan tujuh langkah proses perencanaan kontingensi yang dapat digunakan dalam membangun dan menjaga program perencanaan kontingensi sistem informasi (Swanson dkk., 2010). Tujuh langkah tersebut dirancang dalam siklus pengembangan sistem, yaitu:

1) Mengembangkan pernyataan kebijakan perencanaan kontingensi
2) Melakukan analisis dampak bisnis
3) Melakukan identifikasi kontrol pencegahan
4) Menyusun strategi kontingensi
5) Mengembangkan rencana kontingensi sistem informasi

6) Memastikan rencana pengujian dan pelatihan
7) Memastikan rencana pemulihan.

Penelitian ini hanya melaksanakan langkah pertama sampai dengan kelima karena keterbatasan waktu. Rangkaian proses ini digambarkan dalam Tahapan Penelitian seperti tergambar pada Gambar 1.



Gambar 1. Tahapan Penelitian

Panduan NIST SP 800-34 Rev.1 menyajikan tiga format contoh untuk menyusun rencana kontinjensi sistem informasi yang berada pada tingkat rendah, sedang, atau tinggi. Penetapan format ini mengacu pada *Federal Information Processing Standard* (FIPS) 199 (FIPS PUB 199, 2004). Setiap format memiliki tiga tahap yang mengatur langkah-langkah yang perlu diambil dalam situasi bencana atau gangguan sistem.

1. Tahap aktivasi/pemberitahuan, tahap awal untuk memulai rencana berdasarkan dampak dan memberitahukan kepada tim pemulihan.
2. Tahap pemulihan, langkah untuk mengevaluasi dampak yang terjadi dan sementara memindahkan sistem ke tempat yang lebih aman.
3. Tahap rekonstitusi, kegiatan untuk menguji dan memvalidasi proses pemulihan tim sehingga sistem dapat beroperasi secara normal.

Penelitian ini menggunakan NIST SP 800-34 Rev. 1 sebagai panduan dalam menyusun DRP Pusdatik Instansi XYZ. Instansi XYZ merupakan salah satu instansi pemerintah di Indonesia. NIST SP 800-34 Rev.1 digunakan dengan mempertimbangkan perbedaan karakteristik antara instansi pemerintah dan swasta. Beberapa pertimbangannya adalah instansi pemerintah memiliki tanggung jawab utama dalam menyediakan layanan publik yang krusial untuk kesejahteraan masyarakat secara keseluruhan. Sedangkan, swasta cenderung lebih terfokus pada keuntungan dan kepuasan pelanggan. NIST SP 800-34 Rev. 1 memastikan kesinambungan layanan penting yang mempengaruhi masyarakat luas, sehingga membantu dalam mengidentifikasi dan mengelola risiko yang dapat mengganggu layanan publik pemerintah. Instansi pemerintah mengelola berbagai jenis layanan dan sistem yang beragam, sedangkan swasta cenderung lebih terfokus pada satu sektor atau industri. NIST SP 800-34 Rev. 1 memberikan kerangka kerja yang dapat disesuaikan dengan berbagai jenis layanan dan sistem, memungkinkan integrasi yang baik antar departemen dan fungsi di dalam instansi pemerintah.

Dengan mempertimbangkan perbedaan karakteristik tersebut, NIST SP 800-34 Rev. 1 memberikan panduan yang sesuai dan komprehensif untuk penyusunan DRP bagi instansi pemerintah di Indonesia. Standar ini dapat membantu memastikan bahwa perencanaan kontingensi tidak hanya fokus pada pemulihan cepat tetapi juga pada keberlanjutan layanan esensial dan kepatuhan terhadap regulasi yang berlaku.

3. HASIL DAN PEMBAHASAN

3.1. Analisis Proses Bisnis

Sesuai dengan proses bisnis di Instansi XYZ, Pusdatik termasuk dalam proses pendukung dengan proses bisnis utamanya adalah Pengelolaan Teknologi Informasi. Proses bisnis utama tersebut terdiri dari empat sub proses bisnis yaitu tata kelola Teknologi Informasi Komunikasi (TIK), pengelolaan infrastruktur TIK dan pusat data, pengelolaan data dan aplikasi dan penyelenggaraan keamanan TIK.

3.2. Identifikasi Aset

Aset yang ada di pusat data mencakup sistem informasi/aplikasi, data dan informasi, perangkat keras, perangkat jaringan, dan tenaga kerja. Pudatik memiliki 7 sistem informasi/aplikasi yang dikelola, 6 server, 6 penyimpanan data, 10 UPS, 49 perangkat jaringan dan 31 perangkat keamanan. Pusdatik memiliki 77 orang personel dengan berbagai jabatan dan tingkat pendidikan.

3.3. Mengembangkan Pernyataan Kebijakan Perencanaan Kontingensi

Kebijakan DRP perlu didefinisikan dengan jelas dan dikomunikasikan kepada semua pegawai, khususnya pegawai yang memiliki akses ke pusat data. Isi dari kebijakan DRP ini meliputi peran serta tanggung jawab tim, ruang lingkup, sumber daya, pelatihan DRP, pengujian, pemeliharaan DRP, pencadangan, dan strategi pemulihan.

3.4. *Risk Assessment* (Penilaian Risiko)

Untuk mengenali kemungkinan risiko yang dapat mengganggu sistem informasi/aplikasi Pusdatik dilakukan penilaian risiko. Dalam proses evaluasi ini, terdapat beberapa faktor yang dipertimbangkan antara lain ancaman, sumber ancaman, kerentanan, kondisi predisposisi, kemungkinan, dampak, dan tingkat risiko. Terdapat empat sumber ancaman yang diidentifikasi yaitu yang berasal dari individu/organisasi, perangkat teknologi

informasi (TI), infrastruktur dan lingkungan. Sumber risiko diperoleh melalui diskusi dengan ketua tim dan staf Pusdatik dan diproses kembali dengan menggunakan kerangka NIST SP 800-30 Rev.1. Hasil penilaian risiko digunakan untuk menetapkan urutan prioritas dalam mengambil langkah-langkah untuk menangani dan mengendalikan ancaman tersebut.. Matriks nilai risiko yang digunakan dalam penelitian ini sesuai dengan NIST SP 800-30 Rev.1 diperlihatkan dalam Tabel 1 (ST=Sangat Tinggi, T=Tinggi, S=Sedang, R= Rendah, SR=Sangat Rendah).

Tabel 1. Matriks Nilai Risiko

Kemungkinan	Dampak				
	SR	**R**	**S**	**T**	**ST**
ST	SR	R	S	T	ST
T	SR	R	S	T	ST
S	SR	R	S	S	T
R	SR	R	R	R	S
SR	SR	SR	SR	R	R

Dari evaluasi risiko pada pusat data Pusdatik, teridentifikasi empat risiko dengan tingkat rendah, tiga risiko dengan tingkat sedang, enam risiko dengan tingkat tinggi, dan enam risiko dengan tingkat sangat tinggi. Beberapa ancaman memiliki tingkat risiko sangat tinggi, antara lain kebocoran data/informasi sensitif, hacking, kegagalan instalasi, gangguan internet, gempa bumi dan petir. Hasil penilaian risiko dapat dilihat pada Tabel 2 (C:Confirmed, A:Anticipated, P:Possible, ST:Sangat Tinggi, T:Tinggi, S:Sedang, R:Rendah, SR:Sangat Rendah).

Tabel 2. Hasil Penilaian Risiko

No.	Ancaman	Relevansi	Kemungkinan	*Impact*	Risiko
1.	Kebocoran data/ informasi sensitif	C	T	ST	ST
2.	*Hacking*	A	ST	ST	ST
3.	*Phising*	C	S	ST	T
4.	Infeksi Virus/ *Malware*	P	S	ST	T
5.	Kesalahan Administrasi	C	R	R	R
6.	Kesalahan Prosedur	P	S	T	S
7.	Perangkat Rusak	A	S	ST	T
8.	Perangkat Dicuri	P	R	S	R
9.	Instalasi Gagal	C	T	ST	ST
10.	Kegagalan backup	C	R	T	R
11.	Data Hilang	C	S	ST	T
12.	Data rusak	C	S	T	S
13.	Sumber Daya Menipis	C	ST	T	T
14.	Internet Terganggu	C	T	ST	ST
15.	Blackout	C	R	T	R
16.	Kebakaran	P	R	ST	T
17.	Gempa Bumi	A	T	ST	ST
18.	Petir	A	ST	ST	ST
19.	Banjir	A	S	T	S

3.5. *Business Impact Analysis* (Analisis Dampak Bisnis)

Bagian ini menguraikan proses analisis dampak bisnis yang dipersiapkan sesuai dengan pedoman dari NIST SP 800-34 Rev.1. Analisis dampak bisnis digunakan untuk menentukan dampak bisnis jika layanan sistem informasi tidak dapat diakses, serta memanfaatkan hasil dari analisis dampak bisnis untuk menetapkan prioritas pemulihan sistem informasi. Analisis dampak bisnis dimaksudkan untuk memahami dampak yang timbul pada proses tertentu saat terjadi bencana di Pusdatik. Tujuan dilakukannya analisis dampak bisnis adalah untuk menghubungkan komponen sistem dan teknologi informasi dengan layanan kritis yang disediakan oleh Pusdatik.

Analisis dampak bisnis terbagi menjadi dua tahap utama, pertama adalah memahami proses bisnis kritis, kemudian mengaitkannya dengan sistem dan teknologi informasi. Proses analisis dampak bisnis melibatkan identifikasi proses bisnis yang penting bagi Pusdatik, melakukan wawancara dengan pengelola sistem informasi/aplikasi dan menghimpun masukan untuk menetapkan estimasi waktu tidak beroperasinya seperti *Recovery Time Objective* (RTO), *Recovery Point Objective* (RPO), dan *Maximum Tolerance Downtime* (MTD). Dalam penelitian ini, perkiraan waktu tidak beroperasinya dibagi menjadi empat tingkat untuk memudahkan pengelompokan. Metrik yang diusulkan dalam RTO, RPO, dan MTD mengacu pada (Setyawan, dkk, 2020) seperti yang diperlihatkan pada Tabel 3.

Tabel 3. Metrik Identifikasi RTO, RPO dan MTD

Metrik	Tingkat 4	Tingkat 3	Tingkat 2	Tingkat 1
RTO	0-2 jam	2-8 jam	8-24 jam	>24 jam
RPO	0-5 menit	15 menit	< 24 jam	24-168 jam
MTD	0-2 jam	2-8 jam	8-24 jam	>24 jam

Dampak dari kegagalan aplikasi/sistem informasi, RTO, RPO, MTD, dan kategori aplikasi/sistem informasi digunakan untuk menghasilkan analisis dampak bisnis dalam penelitian ini, sehingga dapat menentukan urutan prioritas pemulihan pada aplikasi/sistem informasi yang saat ini dikelola oleh Pusdatik. Kategori sistem informasi dibagi menjadi tiga tingkatan yaitu *mission-critical*, *important* dan *low*. Sebagai hasilnya, terdapat satu aplikasi/sistem informasi dengan prioritas tinggi, lima aplikasi/sistem informasi dengan prioritas sedang, dan satu aplikasi/sistem informasi dengan prioritas rendah. Hasil analisis dampak bisnis dapat dilihat pada Tabel 4 (dengan T:Tinggi, S:Sedang, R:Rendah, C:Mission-Critical, I:Important, L:Low).

Tabel 4. Hasil Analisis Dampak Bisnis

No	Sistem Informasi/Aplikasi	Dampak	RTO (Jam)	RPO (Jam)	MTD (Jam)	Kategori	Prioritas
1	A.1	S	4	24	4	I	S
2	A.2	S	4	168	4	I	S
3	A.3	T	2	24	2	C	T
4	A.4	S	6	24	6	I	S
5	A.5	T	8	24	8	L	R
6	A.6	T	4	168	4	I	S
7	A.7	S	6	24	6	I	S

3.6. Analisis Kontrol Pencegahan

Langkah identifikasi kontrol pencegahan memiliki tujuan untuk menjelaskan tindakan pengendalian yang dapat diterapkan oleh Pusdatik agar aset yang dilindungi dapat dikelola sehingga potensi ancaman serta kerentanan yang teridentifikasi dapat dikendalikan. Langkah tersebut bertujuan untuk mengenali tindakan pencegahan yang sudah dilakukan oleh Pusdatik dalam mendeteksi dan meminimalisasi dampak dari potensi ancaman terhadap sistem. Analisis pada kontrol pencegahan di pusat data dilakukan dengan menggunakan standar SNI 8799-1:2023 tentang Spesifikasi Teknis Pusat Data untuk melakukan penilaian terhadap pusat data.

Standard tersebut terdiri dari tujuh aspek utama, mencakup gedung, sistem kelistrikan, sistem pendingin, sistem jaringan data, sistem pemadam kebakaran, sistem pemantauan pusat data, dan keamanan akses fisik., yang dibagi menjadi empat tingkat/strata. Strata pusat data menunjukkan tingkatan atau level ketersediaan atau availabilitas fungsi dan layanan pusat data (Badan Standarisasi Negara, 2023). Pengelompokan strata pusat data adalah sebagai berikut:

a. Strata 1, menggambarkan level pusat data yang berbagi fungsionalitas dengan area lain selain pusat data, dengan hanya memiliki satu sistem atau komponen fungsi utama dan tidak ada sistem atau komponen cadangan.
b. Strata 2, merujuk pada level pusat data yang berbagi fungsi dengan area lain selain pusat data, dimana sistem atau komponen fungsi utama telah memiliki sistem atau komponen cadangan.
c. Strata 3, mencakup level pusat data yang berlokasi di bangunan khusus untuk pusat data, yang memiliki sistem atau komponen fungsi utama cadangan (N+1).
d. Strata 4, mengacu pada level pusat data yang berada di bangunan khusus untuk pusat data, dimana terdapat redundansi sistem atau komponen fungsi utama (2N) yang beroperasi secara otomatis.

Hasil evaluasi pusat data Pusdatik menggunakan standar strata 4 SNI 8799-1:2023 terungkap bahwa Pusdatik tidak memenuhi kebutuhan pada tujuh parameter yang ditetapkan. Hasil observasi di pusat data dievaluasi untuk menyusun rekomendasi guna meningkatkan tingkat pusat data yang ada saat ini agar memenuhi persyaratan menjadi Strata 4. Berikut rekomendasi yang dapat dilakukan Pusdatik, yang diuraikan dalam Tabel 5.

Tabel 5. Kondisi dan Rekomendasi Pusat Data

No.	Spesifikasi Teknis Strata 4	Kondisi Pusat Data Pusdatik	Rekomendasi
1	Tidak berada pada area rentan bencana	Belum ada data peta rawan bencana	Memberikan masukan kepada Pemerintah Daerah setempat untuk segera membuat peta rawan bencana
2	Jarak dengan arteri lalu lintas, jalan raya utama dan jalur kereta api utama lebih dari 800 m	Jarak pusat data ke jalur kereta api utama > 800 m dan jarak dengan jalan raya utama 350 m	Perlu dilakukan pengamanan yang lebih ketat terhadap pusat data karena jarak dengan jalan raya utama kurang dari 800 m
3	Terdapat penghalang uap untuk dinding ruang server	Belum terdapat penghalang uap untuk dinding ruang server	Melakukan pengadaan untuk peralatan penghalang uap untuk dinding ruang server
4	Terdapat penghalang uap untuk langit-langit ruang server	Belum terrdapat penghalang uap untuk langit-langit ruang server	Melakukan pengadaan untuk peralatan penghalang uap untuk langit-langit ruang server
5	Analisis sistem listrik, memiliki studi hubungan singkat dan studi koordinasi	Belum ada dokumen terkait analisis sistem listrik	Membuat analisis sistem listrik yang memuat studi hubungan singkat dan studi koordinasi
6	Sistem pemonitoran perangkat a) Inventarisasi perangkat; b) Pendukung penyelesaian masalah perangkat secara daring; c) Sensor getaran perangkat; d) Sensor	Belum ada sensor getaran perangkat dan sensor pembukaan pintu rak	Melakukan pengadaan peralatan sensor getaran perangkat dan sensor pembukaan pintu rak

No.	Spesifikasi Teknis Strata 4	Kondisi Pusat Data Pusdatik	Rekomendasi
	pembukaan pintu rak (khusus Strata 3 dan 4).		
7	Sistem pemonitoran keadaan darurat a) Pengumuman keadaan darurat, dapat dilakukan secara otomatis oleh sistem otomasi bangunan melalui sms, email, dan alarm; b) Kunci antar ruangan yang otomatis terbuka ketika keadaan darurat (interlock); c) Sistem pengeras suara pengumuman untuk publik.	Belum ada sistem pengeras suara pengumuman untuk publik	Melakukan pengadaan sistem pengeras suara pengumuman untuk publik

Salah satu spesifikasi teknis yang tidak sesuai adalah spesifikasi teknis lokasi pusat data, saat ini belum terdapat data peta rawan bencana sehingga dapat direkomendasikan untuk melakukan koordinasi dengan pemerintah daerah setempat untuk membuat peta rawan bencana agar memastikan lokasi pusat data instansi XYZ aman dari bencana alam.

3.7. Pengembangan Rencana Kontingensi

Setelah mengevaluasi risiko dan potensi dampak yang mungkin timbul dalam pegelolaan aplikasi atau sistem, serta mendeskripsikan langkah-langkah pengendalian yang dapat diterapkan dalam melindungi aplikasi atau sistem tersebut, langkah selanjutnya yang dilakukan adalah merancang rencana kontingensi pada setiap aplikasi atau sistem sesuai denagan tingkat dampak yang dapat terjadi. Rencana strategis kontingensi dibuat agar efek bencana terhadap pusat data dan gangguan terhadap proses bisnis Pusdatik dapat berkurang. Ini mencakup rencana pencadangan dan pemulihan, metode penyimpanan cadangan baik di tempat maupun di luar lokasi, opsi lokasi alternatif, penentuan penggantian perangkat, dan peran serta tanggung jawab tim pemulihan bencana. Strategi cadangan yang diusulkan disesuaikan dengan interval waktu yang dapat ditoleransi untuk kehilangan data (RPO) (Alifian, H., dan Priharsari, D., 2021).

Di Pusdatik, sistem informasi dibagi menjadi tiga tingkat, yaitu *mission-critical*, *important*, dan *low*. Tiap tingkatan memiliki strategi pencadangan yang berbeda. Cadangan disimpan di pusat data maupun di tempat alternatif, dengan mempertimbangkan faktor-faktor seperti jenis media cadangan, metode pencadangan, frekuensi pencadangan, dan lokasi alternatif. Prioritas pemulihan tinggi, sedang dan rendah memiliki strategi *backup* dan *recovery* yang sama dalam hal media yang digunakan yaitu berupa perangkat *storage* dan metode yang digunakan yaitu *data replication* dan *virtual machine backup*. Prioritas pemulihan tinggi melakukan *backup* secara *realtime* dan harian serta lokasi alternatif adalah *hot sites*. Prioritas pemulihan sedang, frekuensi dilakukan *backup* adalah harian dan mingguan dengan lokasi alternatif adalah *warm sites*. Prioritas pemulihan rendah, frekuensi dilakukan *backup* adalah mingguan dengan lokasi alternatif adalah *cold sites*.

Strategi backup dan pemulihan ditampilkan pada Tabel 7.

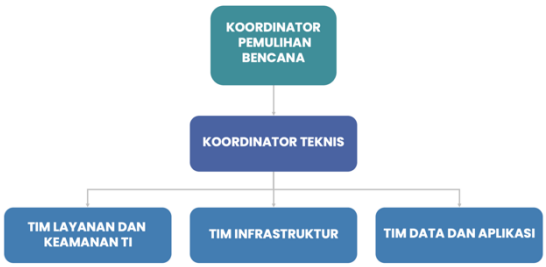
Tabel 7.

Prioritas Pemulihan	Keterangan	Sistem Informasi/ Aplikasi	Strategi backup dan recovery
Tinggi	Gangguan dalam sistem informasi dapat memiliki dampak yang besar pada proses bisnis dan layanan yang diselenggarakan oleh organisasi	A.3	Menggunakan media berupa perangkat storage, metode yang digunakan adalah data replication dan virtual machine backup, frekuensi dilakukan backup adalah realtime dan harian, lokasi alternatif Hot Site
Sedang	Gangguan dalam sistem informasi dapat memiliki dampak yang cukup besar pada proses bisnis dan layanan yang diselenggarakan oleh organisasi	A.1, A.2, A.4, A.6, A.7	Menggunakan media berupa perangkat storage, metode yang digunakan adalah data replication dan virtual machine backup, frekuensi dilakukan backup adalah harian dan mingguan, lokasi alternatif Warm Site
Rendah	Gangguan dalam sistem informasi dapat memiliki dampak yang kecil pada proses bisnis dan layanan yang diselenggarakan oleh organisasi	A.5	Menggunakan media berupa perangkat storage, metode yang digunakan adalah data replication dan virtual machine backup, frekuensi dilakukan backup adalah mingguan, lokasi alternatif Cold Site

Lokasi alternatif yang dimiliki oleh Pusdatik saat ini berada di kantor milik instansi XYZ yang berada di daerah Jakarta Selatan. Strategi kontingensi untuk mengganti perangkat di pusat data Pusdatik

dirancang untuk mengantisipasi kerusakan pada perangkat, termasuk server dan komponen pendukung lainnya. Pusdatik bertanggung jawab atas pengelolaan perangkat di pusat data dan harus memastikan kinerja optimal perangkat tersebut. Penggantian perangkat di pusat data mempertimbangkan beberapa faktor, seperti masa garansi perangkat, ketersediaan stok perangkat dengan redudansi sebagai cadangan dan anggaran.

Dalam NIST SP 800-34, dijelaskan bahwa DRP harus mencakup deskripsi tim yang bertanggung jawab untuk melakukan pemulihan (Swanson dkk., 2010). Setiap anggota tim pemulihan bencana memiliki tanggung jawab dan peran yang ditentukan sebelum, selama, dan setelah terjadinya bencana. Mereka juga harus memiliki kompetensi dan keahlian sesuai dengan tugas dan fungsi masing-masing. Struktur tim tersebut terdiri dari Koordinator Pemulihan Bencana, Koordinator Teknis, Tim Infrastruktur TI, Tim Data dan Aplikasi, dan Tim Keamanan TI, seperti terlihat pada Gambar 2.



Gambar 2. Struktur Tim Pemulihan

Setelah strategi pemulihan telah ditetapkan dan tim pemulihan telah disusun, selanjutnya dilakukan penyusunan dokumen DRP berdasarkan strategi pemulihan yang telah ditentukan.

4. KESIMPULAN

Penelitian ini bertujuan untuk merancang dokumen DRP di Pusdatik. Hasil dari penelitian ini memiliki beberapa kesimpulan diantaranya pada tahap penilaian risiko, beberapa ancaman memiliki risiko sangat tinggi bagi pusat data Pusdatik yaitu kebocoran data/informasi sensitif, *hacking*, kegagalan instalasi, gangguan internet, gempa bumi dan petir. Pada tahap analisis proses bisnis, satu sistem informasi/aplikasi memiliki tingkat prioritas yang tinggi, lima sistem informasi/aplikasi memiliki tingkat prioritas sedang dan satu sistem informasi/aplikasi memiliki tingkat prioritas rendah. Pada tahap analisis kontrol pencegahan, pusat data berada pada strata 4 berdasarkan SNI 8799-1:2023. Terdapat 7 parameter yang perlu diperbaiki agar pusat data Pusdatik sesuai dengan standar SNI 8799-1:2023 strata 4.

Pada tahap strategi kontingensi, strategi pencadangan dan pemulihan dipetakan ke tingkat dampak sistem informasi (*mission-critical*, *important*, dan *low*). Rekomendasi struktur tim pemulihan dirancang berdasarkan kondisi tim yang telah ada di Pusdatik dan perlu ditambahkan koordinator teknis untuk mengordinasikan seluruh tim yang ada di Pusdatik. Data dikumpulkan melalui berbagai metode termasuk wawancara, dokumentasi, penelitian literatur, dan observasi pada tahapan analisis risiko, analisis proses bisnis, dan perumusan strategi kontingensi. Analisis kontrol pencegahan dilakukan dengan menilai pusat data sesuai dengan standar SNI 8799-1:2023, dibantu oleh anggota tim infrastruktur Pusdatik. Pengolahan data dengan melakukan validasi ulang kepada pimpinan, ketua tim dan staf Pusdatik untuk analisis risiko dan analisis kontrol pencegahan.

Dokumen DRP yang dihasilkan dapat menjadi masukan dan pertimbangan untuk Pusdatik, penelitian ini juga memberikan rekomendasi diantaranya penilaian risiko harus dibuat lebih rinci dan dilakukan secara berkala untuk mengidentifikasi ancaman baru. Pimpinan Pusdatik harus mendukung peningkatan kompetensi dan kemampuan anggota Pusdatik. Selain itu, staf Pusdatik harus meningkatkan peran dan tanggung jawab mereka sesuai dengan bidang tugas masing-masing. Pusdatik harus mensimulasikan atau menguji dokumen DRP untuk memastikan kesesuaian dan kecocokannya dengan berbagai keadaan terkait.

5. PENGHARGAAN

Penelitian ini disponsori oleh Badan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika Republik Indonesia.

DAFTAR PUSTAKA

AFIANSYAH, H., SUNARINGTYAS, S., AMIRUDDIN, 2023. 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). In: Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) Vol. 10, No. 2, April 2023, hlm. 329-338.

ALIFIAN, H., dan PRIHARSARI, D., 2021. Penyusunan *Disaster Recovery Plan (DRP)* menggunakan *framework* NIST SP 800-34 (Studi Kasus pada Perusahaan IT Nasional). Surabaya. In: Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-Vol. 5, No. 10, Oktober 2021, hlm. 4673-4679.

APJII, 2024. Survei Penetrasi Internet Indonesia 2024. [Online]. Tersedia melalui: <https://drive.google.com/file/d/1fwybySqrjJaWMg9v6V1LJeGQeOJ4dG6n/view>. [Diakses 1 Februari 2024].

BADAN STANDARISASI NEGARA, 2023. SNI 8799-1.

BISMA, R., 2022. Manajemen Risiko Aset Teknologi Informasi: Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan, Journal Information Engineering and Educational Technology (JIEET), vol. 6, no. 2.

BSSN, 2023. Laporan Bulanan Monitoring Keamanan Siber Tahun 2023. [Online]. Tersedia melalui: <https://www.bssn.go.id/monitoring-keamanan-siber-2023/>. [Diakses 25 Januari 2024].

FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION (FIPS PUB) 199, 2004. Standards for Security Categorization of Federal Information and Information Systems.

FERNANDES, KAREPOWAN, TANNADY, 2024. Disaster Recovery Planning For It/Is Of Hospitality Industry Using NIST SP 800-34 Rev.1 Method, J Theor Appl Inf Technol, vol. 102, no. 8, [Online]. Available: www.jatit.org.

FITRAH, LUTHFIYAH, 2017. Metodologi Penelitian Penelitian Kualitatif, Tindakan Kelas dan Studi Kasus, Sukabumi: CV Jejak.

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

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Jakarta: Kementerian Sekretariat Negara Republik Indonesia.

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/ICIC50835.2020.928 8543.

SUGIYONO, 2021. Metode Penelitian Kuantitatif Kualitatif dan R&D, 3rd ed. Bandung: Alfabeta.

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.

UNISDR, 2009. Terminology on Disaster Risk Reduction. United Nations Office for Disaster Risk Reduction. [Online]. Tersedia melalui: <https://www.undrr.org/publication/2009-unisdr-terminology-disaster-risk-reduction>. [Diakses 9 Februari 2024].

WAHYU, RUSHENDRA, 2022. Klasterisasi Dampak Bencana Gempa Bumi Menggunakan Algoritma KMeans di Pulau Jawa, Jurnal Edukasi dan Penelitian Informatika (JEPIN), vol. 8, no. 1.

WHEELER, E., 2011. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Waltham. USA: Elsevier Inc.

Halaman ini sengaja dikosongkan