Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 20, No. 2, Mei 2021, pp. 261~272
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v20i2.1097

Strategi *Recovery Plan* Teknologi Informasi di Perguruan Tinggi Menggunakan Framework NIST SP 800-34

Information Technology Recovery Plan Strategy in Higher Education Using NIST Framework SP 800-34

Didit Suhartono[1], Khairunnisak Nur Isnaini[2]
Universitas Amikom Purwokerto, Indonesia

Article Info

Article history:

Received, 3 Maret 2021
Revised, 27 April 2021
Accepted, 6 Mei 2021

Kata Kunci:

Pemulihan bencana
Disaster recovery plan
Nist sp 800-34
Risk assesment
Recovery strategy

ABSTRAK

Suatu organisasi memerlukan sumber daya yang memadai dan mendukung, seperti informasi yang harus dijaga serta dilindungi dari berbagai macam bencana maupun ancaman. Ancaman yang menyerang suatu sistem pun masih banyak terjadi khususnya pada sistem yang krusial. Risiko-risiko yang dapat terjadi adalah kerusakan fisik dari server maupun gangguan jaringan sehingga membutuhkan rancangan penanganan bencana menggunakan DRP. Perencanaan pemulihan risiko atau disebut sebagai *Disaster Recovery Planning* (DRP) merupakan mekanisme atau sebuah perencanaan yang dilakukan sebagai pemulihan dari bencana yang terjadi. *Strategi Recovery Plan* dibuat berdasarkan kerangka kerja NIST *(National Institute of Standard and Technology)* SP 800-34 terdiri dari *Risk Assesment*, *Business Impact Analysis (BIA)*, *Recovery Strategy*, *Testing*, dan *Plan Documentation*. Hasil yang diperoleh dari penelitian ini menunjukan dokumen *Disaster Recovery Plan* dapat membantu memulihkan sistem informasi apabila terjadi suatu bencana berdasarkan tingkat prioritas risiko dampak yang terjadi. Urutan tingkat prioritasnya antara lain *Website Student* dengan nilai 100% dan masing-masing 67% untuk *E-Learning*; Absensi Perkuliahan; dan *Smart Dosen*.

Keywords:

Disaster recovery
Disaster recovery plan
Nist sp 800-34
Risk assesment
Recovery strategy

ABSTRACT

An organization requires the adequate and supporting resources such as information which must be maintained and protected from any kinds of disaster or threat. The threat attacking the system still exists much especially on the crucial system. The risk that could exist is the physical damage either from server or network disruption so that it requires the program of disaster handling using DRP. The Disaster Recovery Planning (DRP) is a mechanism or a planning which is conducted as the recovery of existed disaster. It is made based on the framework of National Institute of Standard and Technology (NIST) SP 800-34 including Risk Assesment, Business Impact Analysis (BIA), Recovery Strategy, Testing, and Plan Documentation. The finding shows the document of Disaster Recovery Plan can help to recover the information system when the disaster attacks based the rate of existed risk impact. The order of priority rate is Website Student with 100% score and 67% each for E-Learning; Attendance List; and Smart Dosen.

Penulis Korespondensi:

Didit Suhartono,
Program Studi Informatika,
Universitas Amikom Purwokerto,
Email: didit@amikompurwokerto.ac.id

1. PENDAHULUAN

Suatu instansi atau organisasi memerlukan sumber daya yang memadai dan mendukung, seperti informasi yang harus dijaga serta dilindungi dari berbagai macam bencana maupun ancaman. Negara Indonesia, termasuk kategori negara dengan risiko rawan terjadinya bencana alam seperti gempa bumi, tsunami, banjir, dan tanah longsor. Berbagai macam ancaman yang menyerang suatu sistem pun masih banyak terjadi khususnya pada sistem yang krusial dan berhubungan dengan instansi, perusahaan atau banyak orang. Data dan informasi harus dilindungi sebagai sumber daya sensitif yang dimiliki oleh perusahaan maka sebuah keberlanjutan rencana penanganan perlu dibuat[1]. Keberlanjutan proses bisnis pada suatu organisasi dapat dikatakan menjadi komponen utama yang berkaitan dengan tujuan bisnis sehingga apabila terjadi gangguan secara mendadak maka dapat menyebabkan kerugian yang signifikan[2]. Penerapan TI juga dapat menimbulkan risiko yang dapat membahayakan maupun merugikan instansi, maka dari itu sebuah perencanaan penanggulangan atau pemulihan risiko sangat dibutuhkan dalam perusahaan. Perencanaan pemulihan menjadi fondasi sebuah organisasi untuk memelihara prosesnya sehingga dapat berjalan sesuai ditengah-tengah krisis atau bencana [3]. Setiap organisasi yang berjalan tentunya perlu memiliki proses pemulihan bencana yang didokumentasikan dan diuji serta dievaluasi setidaknya setahun dua kali [4].

Perencanaan pemulihan risiko atau bisa disebut sebagai *Disaster Recovery Planning* (DRP) merupakan mekanisme sebuah perencanaan yang dilakukan sebagai pemulihan dari bencana yang dapat terjadi karena bencana alam atau kerusakan yang dilakukan oleh manusia. Perlindungan terhadap berbagai macam aset instansi diperlukan karena infromasi dibutuhkan untuk sebuah organisasi[5]. Bencana yang terjadi bisa berdampak langsung maupun tidak langsung terhadap kegiatan operasional sebuah instansi atau organisasi, dan harus siap menghadapi dampak yang terjadi akibat bencana tersebut**.** Tujuan membangun sebuah *recovery plan* adalah untuk mempertahankan aktivitas proses bisnis yang berjalan dengan meminimaslir kerusakan aset dan biaya yang dikeluarkan[6]. Keuntungan yang dapat diperoleh oleh organisasi dengan menerapkan *recovery plan* di antaranya melindungi aset organisasi, mengruangi dampak kerugian secara finansial, dan meningkatkan stabilitas proses bisnisnya[7]. Rencana pemulihan turut melibatkan semua sumber daya yang ada di dalam sebuah organisasi yang mendukung proses bisnis yang penting[8]. Area utama yang menjadi fokus rencana pemulihan adalah teknologi informasi dan sistem yang mendukung fungsi bisnis yang berbeda-beda[9]. Proses dalam menyusun dokumen *recovery plan* perlu memiliki pengetahuan mendalam mengenai proses bisnis, kebijakan atau prosedur hingga sumber daya manusianya[10].

Kondisi saat ini Universitas Amikom Purwokerto risiko-risiko yang ada meliputi kerusakan fisik dari *server*, gangguan jaringan dari pihak penyedia layanan, dan kendala jaringan di Universitas Amikom Purwokerto, seperti sistem informasi akademik yaitu *web student* yang masih memiliki kendala terkait sistem, diantaranya masalah yang sering terjadi pada saat pengisian KRS kerap terjadi *system error* dan halaman tidak dapat diakses, serta *server down*. Dari permasalahan tersebut risikoya yaitu dapat berpengaruh terhadap kegiatan mahasiswa yang berlangsung pada Universitas Amikom Purwokerto. Pada sistem informasi akademik juga masih rentan keamanannya seperti kejahatan pembobolan sistem, yang membuktikan bahwa sistem tersebut masih rentan keamanannya. Masalah lain ada pada *website* kuliah *online* yaitu sistem belum bisa di-*update* otomatis dan seringkali tidak dapat diakses, terjadinya *server down* dan jawaban atau tanggapan ketika kuliah *online* yang telah di *update* menjadi hilang. Dari beberapa masalah yang ada dapat disimpulkan bahwa sistem kuliah *online* masih memiliki kendala sehingga membuat dosen maupun mahasiswa terganggu dalam kegiatan pembelajaran.

Gangguan arus listrik seperti pemadaman yang dilakukan oleh penyedia layanan secara mendadak juga dapat mengehentikan suatu proses TI/SI seperti pada saat perkuliahan di ruangan kelas seringkali terjadi permasalahan terkait arus listrik, ketika listrik padam genset hanya bisa memberikan tenaga listrik pengganti ke beberapa lantai saja. Hal tersebut berpengaruh pada saat kegiatan belajar mengajar menjadi terganggu dan dapat mengakibatkan data hilang secara tiba-tiba pada saat kegiatan pembelajaran berlangsung. Serta bencana alam yang mungkin terjadi seperti gempa bumi, banjir dan bencana lainnya dengan infrastruktur yang ada saat ini harus memiliki sebuah rencana pemulihan bencana yang baik bagi instansi.

NIST SP 800-34 adalah kerangka kerja yang dirilis oleh *National Institute of Standards and Technology* berisi acuan untuk menyusun sebuah rencana pengananan bencana[11]. Rencana penanganan bencana dapat dimulai dari memetakan aset-aset kritis yang memperngaruhi proses bisnis di suatu organisasi[12]. Kerangka kerja NIST SP 800-34 digunakan untuk merancang *Disaster Recovery Plan* terdiri dari *Risk Assesment, Business Impact Analysis, Recovery Strategy* dan dokumentasinya[13].
Penelitian yang dilakukan oleh [14] menyebutkan bahwa rencana pemulihan bencana seperti bencana alam, pencurian, atau kegagalan server merupakan sebuah cara untuk meminimalisir kerugian dari berbagai macam aspek yang pengelolaannya penting untuk diberikan bobot lebih untuk diberi penanganan yang tepat. Penelitian tersebut lebih mengarah ke faktor-faktor penyebab terjadinya risiko-risiko bencana dan cara penaggulangannya namun tidak secara spesifik mengarah ke acuan atau metode yang diterapkan. Penelitian lain mengungkap NIST 800-34 digunakan untuk mengidentifikasi risiko-risiko yang ada dalam sebuah organisasi hingga mendapat dokumen penyusunan rencana kontingensi dari sistem informasi yang berjalan[15]. Langkah-langkah NIST 800-34 yang diterapkan antara lain Penilaian Risiko, Business Impact Analysis, Identifikasi Pengendalian Pencegahan, Penyusunan Strategi Kontingensi, dan Penyusunan Rencana Kontingensi. Rekomendasi yang diberikan mengarah pada strategi backup khususnya pada saat situasi *RPO (Recovery Point Objective)* dan pembuatan diagram fase pemulihan.

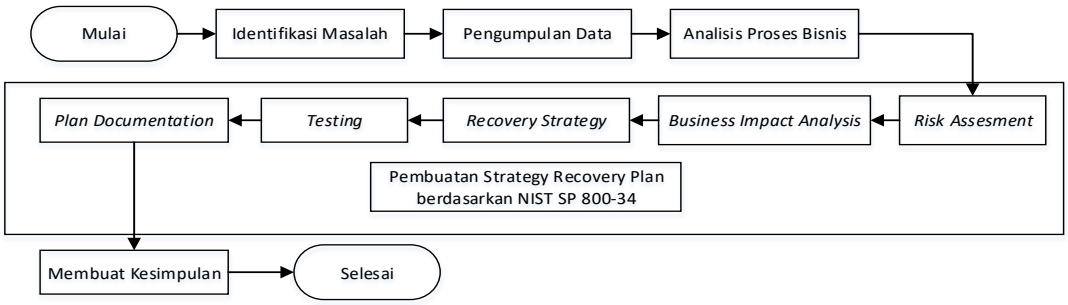
NIST 800-34 juga digunakan oleh [16] untuk memastikan keberlangsungan proses bisnis di Kementerian Pemberdayaan Perempuan dan Perlindungan Anak. Pada penelitian tersebut langkah *recovery strategy* dibuat secara umum tidak spesifik menurut dampak risiko-risiko yang terjadi. Selain itu pada langkah *Business Impact Analysis* hanya berisi layanan-layanan yang berjalan pada instansi tersebut. Salah satu langkah yang diterapkan yaitu strategi pemulihan dengan cara memiliki penyimpanan

cadangan dengan jarak yang jauh dari lokasi utama. NIST 800-34 juga digunakan oleh [17] untuk menyusun penanganan pemulihan bencana khususnya pada inftrastruktur layanan sistem informasi dan membangun langkah-langkah dalam pengamanan data. Penelitian tersebut mengungkap langkah-langkah *framework* NIST 800-34 dengan cara yang berbeda tanpa memberikan *recovery strategy* yang dibutuhkan untuk hasil dokumen DRP.

Penerapan *recovery plan* dengan *framework* NIST SP 800-34 tentu perlu menjadi usulan untuk Universitas Amikom Purwokerto dalam rangka strategi pemulihan layanan, yang dilengkapi dengan prosedur pencegahan. Penelitian yang akan dilakukan berfokus pada objek-objek yang menjadi risiko-risiko serta menjadi alasan dibentuknya dokumen *Disaster Recovery Plan*. Hasil *recovery strategy* diberikan sesuai dengan tingkat prioritas agar dapat spesifik dan sesuai. Hal tersebut juga disesuaikan dengan kondisi organisasi di Universitas Amikom Purwokerto. Hasil penelitian ini diharapkan dapat meningkatkan performa organisasi secara keseluruhan di masa yang akan datang.

2. METODE PENELITIAN

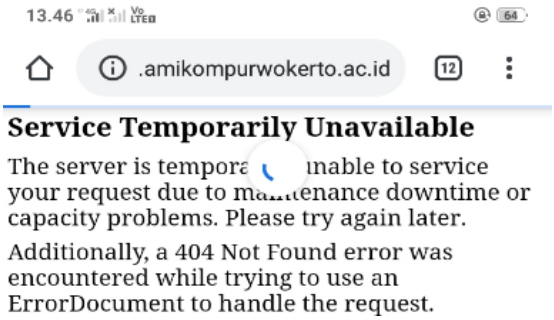
Langkah-langkah pengumpulan data dimulai dari studi pustaka untuk memperlajari hal-hal yang berkaitan dengan penelitian yang sedang berjalan. Wawancara dan observasi dilakukan untuk memperkuat argumen dari masalah-masalah yang diangkat pada penelitian. Langkah-langkah penelitian dapat dilihat pada gambar 1.



Gambar 1 Alur Penelitian

Dilihat dari gambar 1 penelitian dimulai dari mengidentifikasi masalah dengan cara menentukan ruang lingkup penelitian yang berkaitan dengan disaster recovery plan di antaranya acuan atau metode yang digunakan yaitu NIST 800-34, mengkaji daftar masalah yang dihimpun antara lain meliputi kerusakan fisik dari server, gangguan jaringan seperti sistem informasi akademik dan website kuliah online mengalamai system error dan server down sehingga halaman tidak dapat diakses. Khususnya website kuliah online yaitu sistem belum bisa di-update otomatis dan seringkali tidak dapat diakses, terjadinya server down dan jawaban atau tanggapan ketika kuliah online yang telah di update menjadi hilang. Selain itu menyeleraskan dengan teori-teori yang relevan dengan penelitian-penelitian sebelumnya.

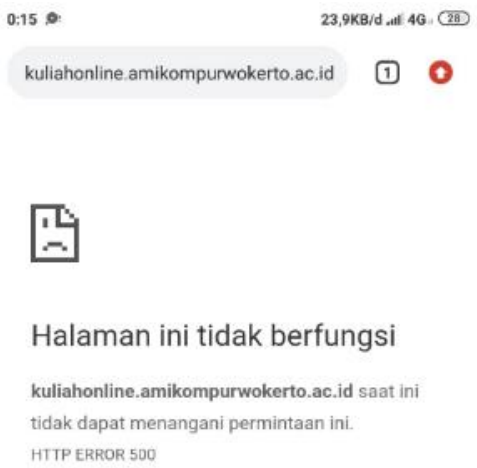
Langkah selanjutnya yaitu mengumpulkan data yang dihimpun melalui observasi maupun wawancara. Observasi yang dilakukan dengan mengamati fasilitas yang dikelola oleh UPT Pengembangan Laboratorium dan Teknologi (PLT) yaitu fasilitas yang dimungkinkan memiliki resiko tinggi terjadinya kerusakann atau hilangnya data penting. Wawancara dilakukan kepada dosen dan mahasiswa untuk mempertegas risiko-risiko yang mungkin terjadi dengan menyelaraskan hasil obervasi yang ada. Hasil observasi dan wawancara menunjukkan bahwa server down yang terjadi pada web student dan kuliah online seperti yang dapat dilihat pada gambar 2 dan gambar 3.



Gambar 2. *Server down* pada *web student*

Gambar 2 memperlihatkan *server down* pada halaman website amikom. *Server down* terjadi karena *server* tidak dapat memberikan *request* halaman yang diminta oleh *user*. Hal ini berdampak pada tidak tersampaikannya informasi untuk *user* baik mahasiswa, dosen, atau masyarakat umum. *Server down* terjadi sering kali terjadi pada saat berlangsungnya kegiatan belajar mengajar sehingga dapat menyulitkan mahasiswa ataupun dosen dalam kegiatan kuliah *online.*

Pada gambar 3 memperlihatkan *website* kuliah *online* yang mengalami *server down*. Peristiwa ini dikarenakan *server* tidak dapat memenuhi permintaan dari pengguna terutama pada jam-jam padat lalu lintas jaringan. Dampak yang terjadi adalah terganggunya proses belajar mengajar mahasiswa dan dosen.



Gambar 3. *Server down* pada saat kuliah *online*

Pada gambar 4 terdapat tampilan *website* yang di *hack* oleh seseorang yang tidak bertanggung jawab. Dimungkinkan akses ilegal ini dapat masuk melalui kerentanan sistem yang ada. Akibatnya terjadi perubahan tampilan halaman *website*, selain itu halaman web juga tidak dapat diakses.

Gambar 4. Pembobolan *web student* oleh *hacker*

Langkah ketiga yang diambil yaitu analisis proses bisnis yang berjalan di di Universitas Amikom Purwokerto. Analisis proses bisnis yang akan dilakukan di antaranya mengetahui sistem-sistem yang berjalan dan topologi jaringan yang digunakan saat ini agar pemetaan ke dalam *framework* menjadi tepat dan sesuai. Hasil proses bisnis yang telah dianalisis kemudian dipetakan pada *framework* NIST SP 800-34 yang terdiri dari *Risk Assesment, Business Impact Analysis (BIA), Recovery Strategy, Testing*, dan *Plan Documentation. Risk assesment* yang dilakukan untuk menilai aset-aset instansi yang ada, menentukan klasifikasi dampak dan penyebab terjadinya gangguan dan penentuan langkah-langkah yang optimal untuk mitigasi risiko.

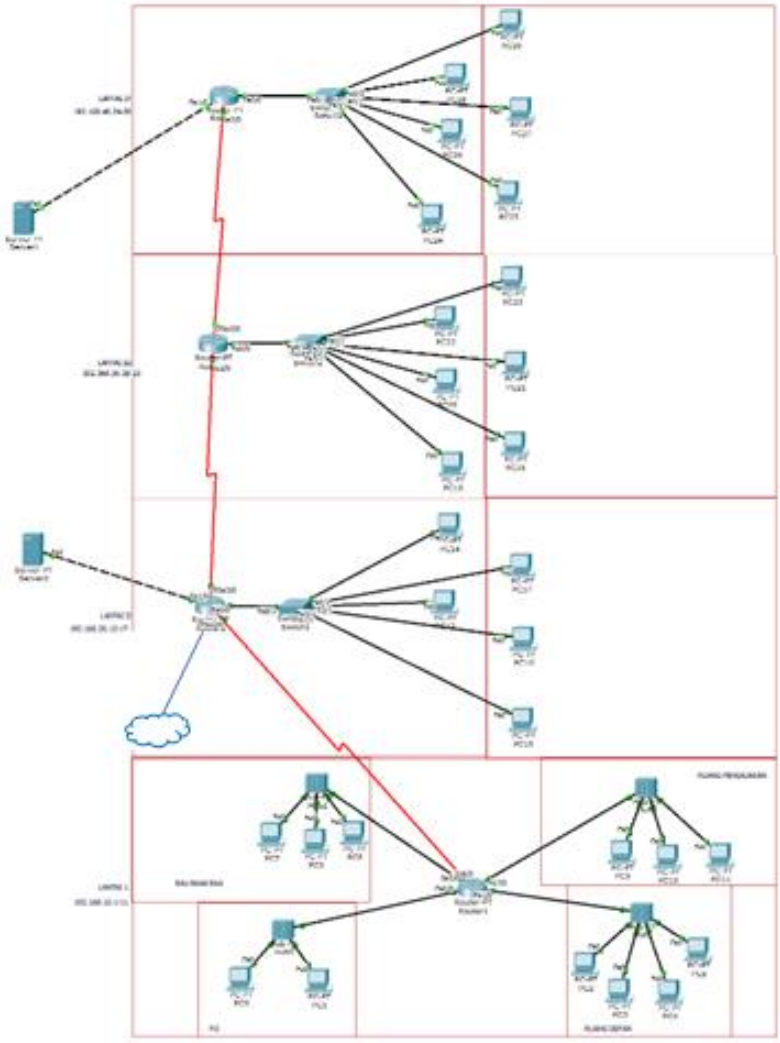
Business Impact Analysis (BIA) dilakukan untuk menentukan layanan yang dianggap tepat dan menjadi prioritas. Recovery Strategy dibuat untuk melakukan pemulihan pada saat terjadinya suatu kegagalan sistem. Testing yang akan dilakukan sesuai dengan rekomendasi *Recovery Strategy. Plan Documentation dibuat berdasarkan framework NIST 800-34* dan rekomendasi *Recovery Strategy* yang berisi *Disaster Recovery Team* beserta dengan tanggung jawabnya. Pemetaan pada *framework* NIST SP 800-34 ditargetkan untuk menghasilkan sebuah strategi *recovery plan.* Langkah terakhir yang dilakukan adalah membuat kesimpulan berdasarkan hasil yang telah dianalisis.

3. HASIL DAN ANALISIS

3.1 Analisis Proses Bisnis

Menurut NIST SP 800-34 dalam merencanakan keberlangsungan bisnis perlu berlandaskan kebijakan yang telah di definisikan sebelumnya pada suatu organisasi maupun peraturan perundang-undangan yang berlaku. Universitas Amikom

Purwokerto menyatakan “Meningkatkan Mutu Prasarana dan Sarana yang dimiliki untuk menyelenggarakan pendidikan terbaik” secara implisit yang dimaksud adalah semua layanan teknologi informasi berfungsi untuk memberikan dukungan agar pendidikan yang diselenggarakan dapat memiliki mutu yang baik dan terjamin. Hal ini diperkuat dengan terbitnya Peraturan Menteri Pendidikan Nasional Republik Indonesia Nomor 38 Tahun 2008 Tentang Pengelolaan Teknologi Informasi Dan Komunikasi Di Lingkungan Departemen Pendidikan Nasional, tertuang pada Pasal 16 tentang pengelolaan TIK dilakukan oleh departemen IT khususnya untuk pengelolaan infrastruktur dan sumber daya komputasi [18]. Berikut ini skema dari jaringan komputer di Universitas Amikom Purwokerto yang terdapat pada gambar 5.



Gambar 5. Skema Jaringan Komputer di Universitas Amikom Purwokerto

Pada gambar 5 di atas, memperlihatkan jaringan di Universitas Amikom Purwokerto dengan tipe LAN. *Server* yang digunakan meliputi dua *server database* backup yang berguna untuk melakukan pencadangan secara berkala dan kontinyu. Jaringan internet dan aliran data dari *server* didistribusikan melalui router kemudan switch di masing-masing bagian hingga masuk ke pengguna akhir. Daftar Sistem Informasi di Universitas Amikom Purwokerto pada tabel 1.

Tabel 1. Daftar Sistem Informasi yang dimiliki Universitas Amikom Purwokerto

No.	Daftar Sistem	No,	Daftar Sistem
1	*Website Student*	11	Absensi Pegawai
2	*Smart* Prodi	12	Absensi Perkuliahan
3	*Smart* Penjadwalan	13	Kesekretariatan
4	KRS *Online*	14	Kroscek Nilai
5	Registrasi PMB	15	*Website Profile* (kampus)
6	*E-Learning*	16	Penggajian dan pembayaran honor dosen
7	*Smart* Perpustakaan	17	PMB *Online*
8	*Smart* Keuangan	18	Pembayaran KRS *Online*
9	Inventori	19	Fedder PDDIKTI
10	OJS	20	E-print
		21	*Smart* Dosen

Tabel 1 menerangkan sistem informasi yang terdapat di Universitas Amikom Purwokerto. Sistem informasi yang ada terbagi dua yaitu sistem untuk pengguna internal dan pengguna umum. Pengguna internal adalah civitas akademika dan karyawan sedangkan pengguna umum misalnya calon mahasiswa barau atau mitra kampus. Daftar sistem informasi yang terdapat di tabel 1 berguna untuk kelancaran jalannya proses bisnis secara umum di Universitas Amikom Purwokerto.

3.2. Pembuatan Recovery Strategy Plan berdasarkan NIST 800-34

Risk Assesment pada tahap ini berfokus pada ancaman yang dapat mempengaruhi aset-aset instansi yang ada hubungannya dengan pelaksanaan pelayanan di Universitas Amikom Purwokerto. Tujuannya untuk menentukan klasifikasi dampak dan penyebab terjadinya gangguan atau bencana yang mungkin terjadi dan berguna dalam penentuan langkah-langkah yang optimal untuk mitigasi risiko yang terjadi, terdapat pada tabel 2.

Tabel 2. *Risk Asessment*

No	Ancaman	Ancaman yang Terjadi	Kerentanan	Aset Kritis	Konsekuensi
1.	Kebakaran	segala jenis aktifitas yang menimbulkan percikan dan korsleting listrik atau kebakaran dari luar gedung	komponen yang dapat terbakar, baik di dalam atau luar gedung.	Area perkantoran dalam gedung dan sarana prasana kantor.	Kegiatan operasional terhenti.
2.	Hujan lebat terus menerus	Berdampak pada area-area didalam gedung menjadi lembab.	Jaringan listrik menjadi lebih rentan terhdap korsleting.	Peralatan kantor yang berhubungan dengan jaringan listrik.	Terjadinya korsleting listrik pada jaringan listrik.
3.	Petir	Jaringan LAN dan alat-alat listrik.	komputer dan jaringan yang saling terhubung.	Sistem dan Jaringan komputer.	Kegiatan operasional menjadi terhambat karena perangkat pendukung rusak.
6.	Gangguan Listrik	Rusaknya hardware.	Semua perangkat kompter harus dimulai dari awal lagi.	Perangkat komputer yang terintegrasi di sistem Universitas Amikom Purwokerto.	Rusaknya komputer, kinerja sistem menjadi lambat hingga terhenti.
7.	*Human Error*	Hilangnya data dan informasi.	Data terhapus, kesalahan input data.	Data informasi pada sistem Universitas Amikom Purwokerto.	Rusaknya komputer, kinerja sistem menjadi lambat hingga terhenti.
8.	*Server down*	Tingginya *traffic* menyebabkan *server* menjadi *down.*	Sistem menjadi lambat atau tidak dapat memperoses permintaan.	Data dan informasi pada sistem Universitas Amikom Purwokerto.	Memperlambat kinerja sistem, menghentikan kinerja sistem.
9.	*Cyber Attack* atau *Hacking*	*Attack dan threat* contohnya *Phising, Sniffing*, SQL *Injection, defacing*, DDoS, atau *Backdoor*.	Celah kerentanan masih dapat ditembus oleh *Hacker*.	Data dan informasi pada sistem Universitas Amikom Purwokerto.	Memperlambat kinerja sistem, menghentikan kinerja sistem.
10.	*Virus, Malware*	terganggunya aktivitas sistem atau jaringan karena telah terinfeksi virus atau *malware* melalui server, router dan end user computer.	Celah kerentanan karena antivirus tidak di*update* atau tidak dihidupkan.	Data dan informasi pada Universitas Amikom Purwokerto.	Memperlambat kinerja sistem, hingga dapat menghentikan sistem serta dapat merusak data dan informasi.

Business Impact Analysis (BIA) adalah tahap-tahap dalam menentukan layanan yang dianggap tepat dan menjadi prioritas bagi Universitas Amikom Purwokerto. Proses tersebut juga di terapkan dalam mengambil keputusan *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO) pada masing-masing fungsi bisnisnya. BIA bertujuan untuk membantu memahami dampak yang diakibatkan dari suatu bencana yang tidak diharapkan, sehingga diperlukan periode waktu yang bisa ditoleransi jika suatu layanan sistem lumpuh. Maka perlu dilakukan pemetaan layanan sistem informasi yang ada di Universitas Amikom Purwokerto, terdapat pada tabel 3.

Tabel 3. Fungsi-fungsi aplikasi layanan informasi

No	Nama Aplikasi	Fungsi
1.	*Website Student*	Aplikasi ini sebagai penunjang kegiatan pelayan akademik untuk mahasiswa.
2.	*Smart* Prodi	Aplikasi penunjang kegiatan prodi.
3.	*Smart* Penjadwalan	Aplikasi pengelolaan penjadwalan perkuliahan.
4.	KRS *Online*	Aplikasi pengelolaan rencana dan hasil studi mahasiswa.
5.	Registrasi PMB	Aplikasi pengelolaan data mahasiswa baru.
6.	*E-Learning*	Aplikasi pengelolaan publikasi karya ilmiah mahasiswa.
7.	*Smart* Perpustakaan	Aplikasi pengelolaan otomatis perpustakaan.
8.	*Smart* Keuangan	Aplikasi pengelolaan registrasi ulang mahasiswa pada setiap semester.
9.	Inventori	Aplikasi pengelolaan inventarisasi barang.
10.	OJS	Aplikasi *online* pengelolaan publikasi hasil penelitian dan pengabdian masyarakat.
11.	Absensi Pegawai	Presensi pegawai
12.	Absensi Perkuliahan	Presensi perkuliahan.
13.	Kesekretariatan	Aplikasi pengelolaan surat masuk dan keluar.
14.	Kroscek Nilai	Apikasi kroscek nilai.
15.	*Website Profile* (kampus)	Sarana publikasi dan informasi terkait aktifitas Universitas Amikom Purwokerto.
16.	Penggajian dan pembayaran honor dosen	Aplikasi penggajian karyawan dan pembayaran honor dosen (menggunakan *MS Excel*).
17.	PMB *Online*	Aplikasi penunjang pendaftaran kuliah *online*.
18.	*E-print*	Aplikasi publikasi karya ilmiah mahasiswa dan dosen.
19.	Pembayaran KRS *Online*	Aplikasi pembayaran KRS *online* dengan menggunakan *virtual account.*
20.	Fedder PDDIKTI	Aplikasi pelaporan data aktivitas mahasiswa ke DIKTI.
21.	*Smart* Dosen	Aplikasi aktivitas dosen dalam hal akademik.

Untuk menentukan tingkat kritis sebuah sistem informasi, maka berdasarkan pada kuantitas pengguna sistem informasi khususnya mahasiswa yang merasakan dari layanan tersebut. Berikut kategori tingkat dampak gangguan atau bencana terhadap proses bisnis yang terdapat pada tabel 4.

Tabel 4. Kategori tingkat dampak risiko sumber [13]

No	Dampak Risiko	Deskripsi
1.	Rendah	Dampak yang dihasilkan tidak begitu signifikan mengganggu jalannya proses aktifitas Sistem Informasi dan *stakeholder* di dalamnya. Dampak masih dapat ditoleransi.
2.	Sedang	Berdampak pada terhambatnya kinerja sebagian sub sistem atau terjadi kelambatan proses data yang dihasilkan dari sistem.
3.	Tinggi	Terjadi penghentian sistem secara signifikan, sistem tidak mampu beroperasi maksimal selama beberapa waktu, mengakibatkan kerugian waktu dan materi di atas rata-rata.

Selanjutnya, menganalisis dampak bisnis dengan acuan dari tabel 4 dari setiap layanan aplikasi atau sistem informasi yang ada di Universitas Amikom Purwokerto yang sering mengalami *server down* dan beberapa kali terjadi peretasan pada *Website Student*, hal tersebut sering dirasakan oleh mahasiswa. Beberapa aplikasi di analisis dampak bisnisnya dijabarkan pada tabel 5 dampak *Human Error*, tabel 6 dampak *Server Down*, dan tabel 7 dampak *Cyber Attack* atau *Hacker*.

Tabel 5. Analisis dampak dari *Human Error*

No	Sistem Informasi	Dampak yang terjadi	Tingkat Dampak
1.	*Website Student*	Kesalahan informasi data, seperti: validasi presensi, pengisian KRS, profil mahasiswa, pengajuan akademik.	Tinggi
2.	*E-Learning*	*Mismatch* kelas dengan materi yang di-*share*. Sehingga, terkadang membuat mahasiswa sulit mengetahui materi yang sudah dibagikan.	Rendah
3.	Absensi Perkuliahan	Sistem tidak memvalidasi presensi yang di-*input*-kan.	Tinggi
4.	*Website Profile* (kampus)	Adanya kesalahan informasi yang disediakan, seperti: *file download* yang disediakan lawas.	Sedang
5.	*Smart* Dosen	*Mismatch* data mahasiswa pada jumlah siswa yang diampu.	Rendah

Pada tabel 5 analisis dampak risiko dari *Human Error* terdapat beberapa item yang dianalis yang mengarah pada kesalahan pada akses atau pada saat mengoperasikan sistem-sistem yang ada. Sistem informasi *web student* dan absensi perkuliahan terlihat memiliki dampak risiko yang tinggi. Hal tersebut berdampak pada kesalahan informasi yang diterima oleh pengguna. Pada sistem informasi web student terdapat inkonsistensi data pada validasi presensi mahasiswa.

Tabel 6. Analisis dampak dari *Server Down*

No	Sistem Informasi	Dampak yang terjadi	Tingkat Dampak
1.	*Website Student*	Sulit untuk memvalidasi saat pengisian KRS atau presensi.	Tinggi
2.	*E-Learning*	Sulit melakukan akses *E-Learning* yang berdampak berkurangnya waktu KBM Mahasiswa.	Tinggi
3.	Absensi Perkuliahan	Ketertundaan absensi yang dilkukan oleh Dosen.	Sedang
4.	*Website Profile* (kampus)	Tidak bisa mengakses *website* kampus.	Rendah
5.	*Smart* Dosen	Keterlambatan *update* materi atau pembelajaran.	Sedang

Pada tabel 6 analisis dampak risiko dari *server down* salah satunya yaitu berdampak pada mahasiswa dan dosen. Dampak yang terjadi adalah pada saat pengisian KRS seringkali mahasiswa mengalami kendala saat proses penentuan jadwa mata kuliah. Selain itu dampak dari *serverdown* kadangkala mengakibatkan sistem *elearning* tidak dapat diakses pada jam-jam lalu lintas jaringan yang padat.

Tabel 7. Analisis dampak dari *Cyber Attack* atau *Hacker*

No	Sistem Informasi	Dampak yang terjadi	Tingkat Dampak
1.	*Website Student*	Tidak dapat mengakses sistem yang ada di *web student*.	Tinggi
2.	*E-Learning*	Tidak dapat mengakses dan modul pembelajaran hilang.	Sedang
3.	Absensi Perkuliahan	Hilangnya data presensi mahasiswa.	Rendah
4.	*Website Profile* (kampus)	Hilangnya konten yang terdapat di *web profile* kampus.	Rendah
5.	*Smart* Dosen	Tidak bisa mengakses sistem, hilangnya data akademik.	Tinggi

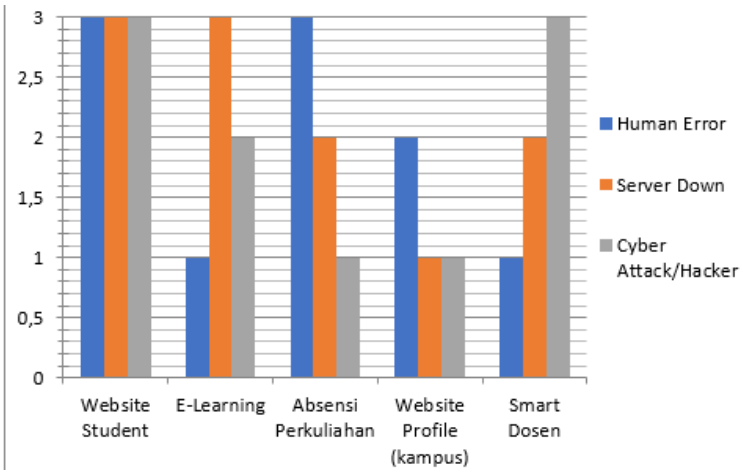
Pada tabel 7 analisis dampak risiko *Cyber Attack* atau *Hacker* memuat beberapa dampak di antaranya hilangnya data-data penting seperti data presensi mahasiswa maupun akses yang ditutup oleh hacker. Pada masing-masing hasil analisis dampak risiko telah dikategorikan berdasarkan kategori dampak risiko yang terdapat pada tabel 3.

Setelah melakukan analisis dampak risiko yang memungkin terjadi pada suatu bisnis, selajutnya penentuan *Recovery Objective* yang meliputi *Recovery Time Objective* (RTO) merupakan waktu maksimum sebuah sistem untuk *down* sebelum adanya dampak yang tidak diinginkan dari rangkaian sistem lainnya yang mendukung proses bisnis dan *Recovery Point Objective* (RPO) merupakan tentang jumlah toleransi minimum data dari sebuah sistem yang bisa direstorasi dari proses pemulihan yang akan dilakukan. Berikut hasil kebutuhan RTO dan RPO terhadap pengelolaan sistem informasi di Universitas Amikom Purwokerto yang terdapat pada tabel 8.

Tabel 8. Identifikasi RTO dan RPO

No.	Sistem	RTO / Menit	RPO / Menit	Tingkat Dampak
1.	*Website Student*	60	30	Tinggi
2.	*E-Learning*	45	15	Tinggi
3.	Absensi Perkuliahan	120	60	Sedang
4.	*Website Profile* (kampus)	120	60	Sedang
5.	*Smart* Dosen	60	30	Tinggi

Selanjutnya menentukan prioritas pemulihan dari sistem berdasarkan hasil pada gambar 6 dan tabel 9 untuk menetukan prioritas sistem dengan nilai tertinggi. Cara membuat tingkat prioritas yaitu menggabungkan nilai dampak dari setiap sistem, penjabarannya sebagai berikut adalah Tinggi: 3 poin, Sedang : 2 poin, Rendah : 1 poin.



Gambar 6. Grafik Penilaian Terdampak Sistem Informasi

Gambar 6 memperlihatkan hasil dari dampak penilain risiko sistem yang ada di universitas purwokerto. Penilaian dampak risiko dilihat berdasarkan sistem informasi yang menjadi acuan penilaian yaitu *website student,* e-learning, *website profile*, smart dosen, dan absensi perkuliahan. Penilaian urutan prioritas berdasarkan acuan tinggi hingga rendah dengan rentang nilai angka 3 ke angka 1.

Tabel 9. Prioritas Sistem Informasi yang Terdampak

No.	Sistem	Rerata Nilai Dampak	%	Urutan Prioritas
1.	*Website Student*	3	100%	1
2.	*E-Learning*	2	67%	3
3.	Absensi Perkuliahan	2	67%	4
4.	*Website Profile* (kampus)	1,33	44%	5
5.	*Smart* Dosen	2	67%	2

Pada tabel 9 memperlihatkan hasil dari penilaian urutan prioritas dengan cara mencari nilai rata-rata dari setiap acuan sistem yang dinilai. Hasilnya terlihat bahwa *website student* memiliki dampak risiko yang paling besar, kemudian smart dosen, elearning dan absensi perkuliahan . Berdasarkan nilai dampak yang ada maka di tentukan prioritas pemulihan sistem. Apabila nilai rerata dampak memiliki nilai tinggi maka diasumsikan menjadi urutan prioritas pemulihan yang utama seperti halnya website *student* yang memiliki urutan prioritas pertama.

Recovery Strategy adalah proses dalam melakukan pemulihan pada saat terjadinya suatu kegagalan sistem. Di dalam melakukan proses *Recovery* terdapat beberapa hal yang perlu diketahui seperti penyediaan fasilitas baik *hardware* maupun *software* yang dapat digunakan untuk pemulihan layanan. Dari hasil *Risk Assessment* dan *Business Impact Analysis* dapat ditarik garis besar ancaman-ancaman yang dapat menjadi acuan untuk melakukan proses *recovery*. Ancaman terhadap SI/TI Universitas Amikom Purwokerto dapat dilihat dari ancaman pada *Risk Assessment* pada aplikasi atau sistem informasi yang memerlukan suatu strategi pemulihan. Berikut tabel 10 hingga tabel 12 mengenai proses *recovery strategy* sistem informasi.

Tabel 10. *Recovery Strategy* Sistem Informasi Risiko *Human Error*

No	Sistem Informasi	Dampak yang terjadi	*Strategy Recovery*
1.	*Website Student*	Ketidaksesuaian informasi data, misalnya: validasi presensi, pengisian KRS, profil mahasiswa, pengajuan akademik.	Memberikan *manual book* atau fitur bantuan yang berfungsi.
2.	*E-Learning*	*Mismatch* kelas dengan materi yang di-*share*. Sehingga, terkadang membuat mahasiswa sulit mengetahui materi yang sudah dibagikan.	Adanya perbaikan mengenai aspek Interaksi Manusia dan Komputer.
3.	Absensi Perkuliahan	Sistem tidak memvalidasi presensi yang di-*input*-kan.	Notifikasi presensi apabila belum tervalidasi atau *reupdate*.
4.	*Website Profile* (kampus)	Adanya kesalahan informasi yang disediakan, seperti: *file download* yang disediakan sudah lawas.	Pengecekan berkala terhadap file yang sudah lewat ≥ 5 tahun. Dan di update kembali file yang perlu dibutuhkan bagi Dosen, Calon Mahasiswa, dan Mahasiswa.
5.	*Smart* Dosen	*Mismatch* data mahasiswa pada jumlah siswa yang diampu.	Memiliki backup data ganda seperti menyimpan pada penyimapnan cloud, maupun bcakup data secara fisik.

Pada tabel 10 *recovery strategy* sistem informasi pada sub bagian *human error* diantaranya perbaikan manual book dan backup data. Selain itu informasi absensi yang tervalidasi. Hal ini sesuai dengan nilai dampak risiko yang paling tinggi yaitu *website student* dan absensi perkuliahan.

Tabel 11. *Recovery Strategy* Sistem Informasi Risiko *Server Down*

No	Sistem Informasi	Dampak yang terjadi	*Strategy Recovery*
1.	*Website Student*	*Server* sering mengalami *down* apabila *traffic* semakin penuh, sehingga tidak bisa diakses oleh mahasiswa untuk cek dan men-*input* data.	Diganti menggunakan *server* cadangan atau pindah menggunakan sistem *cloud* agar lebih terintegrasi dan aman.
2.	*E-Learning*	Sulit melakukan akses *E-Learning* yang berdampak pada menguras jadwal kuliah.	Rajin melakukan *maintenance server* atau membuat penjadwalan *maintenance* karena proses pembelajaran menggunakan daring maka perlu pengecekan terhadap *server*.
3.	Absensi Perkuliahan	Ketertundaan absensi yang dilkukan oleh Dosen.	Yang sering terjadi di presensi Amikom adalah *syntax error* sehingga perlu pengecekan kesalahancoding yang membuat error.
4.	*Website Profile* (kampus)	Tidak bisa mengakses *website* kampus.	Diganti dengan menggunakan *server* cadangan atau *cloud.*
5.	*Smart* Dosen	Keterlambatan *update* materi atau pembelajaran.	Diganti dengan menggunakan *server* atau *cloud*.

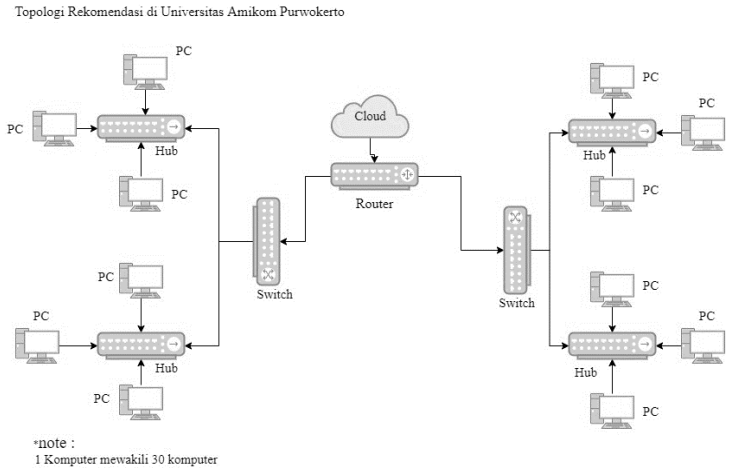
Pada Tabel 11 *recovery strategy* sistem informasi sub bagian *server down* diantaranya yaitu pengadaan server cadangan atau penggunaan cloud serta maintenance server secara kontinyu. Hal ini sesuai dengan nilai dampak risiko yang paling tinggi yaitu *website student* dan e-learning.

Tabel 12. *Recovery Strategy* Sistem Informasi Risiko *Cyber Attack* atau *Hacker*

No	Sistem Informasi	Dampak yang terjadi	*Strategy Recovery*
1.	*Website Student*	Tidak bisa mengakses sistem yang ada di *web student*.	Sering melakukan pembaharuan *password.*
2.	*E-Learning*	Tidak bisa akses dan modul pembelajaran hilang.	Harus melakukan *backup* data secara berkala agar data dalam *e-learning* dapat terjaga.
3.	Absensi Perkuliahan	Hilangnya data presensi mahasiswa.	Melakukan *backup* data presensi secara rutin dan membuat form manual untuk bukti nyata.
4.	*Website Profile* (kampus)	Hilangnya konten yang terdapat di *web profile* kampus.	Prioritaskan sistem *online security.*
5.	*Smart* Dosen	Tidak bisa mengakses sistem, hilangnya data akademik.	Harus melakukan *backup* data dan selalu melakukan pengecekan untuk mengantisipasi kehilangan data akademik yang sudah ter-*input.*

Pada tabel 12 *recovery strategy* sistem informasi sub bagian *cyber attack* atau *hacker* diantaranya *website student* yaitu pembaharuan password secara berkala. Pada bagian *smart dosen* strateginya adalah melakukan backup data dan evaluasi untuk mencegah kehilangan data. Hal ini sesuai dengan nilai dampak risiko tertinggi yaitu *website student* dan smart dosen.

Pada tahap ini pula penulis memberikan rekomendasi atas hasil *Risk Assesment* atau kendala yang muncul pada infrastruktur IT di Universitas Amikom Purwokerto berdasarkan NIST SP 800-34 agar dapat mengurangi tingkat risiko pada sistem TI dan data yang diterima kampus sebagai sistem informasi. Salah satu rekomendasi tersebut tersaji pada gambar 7.

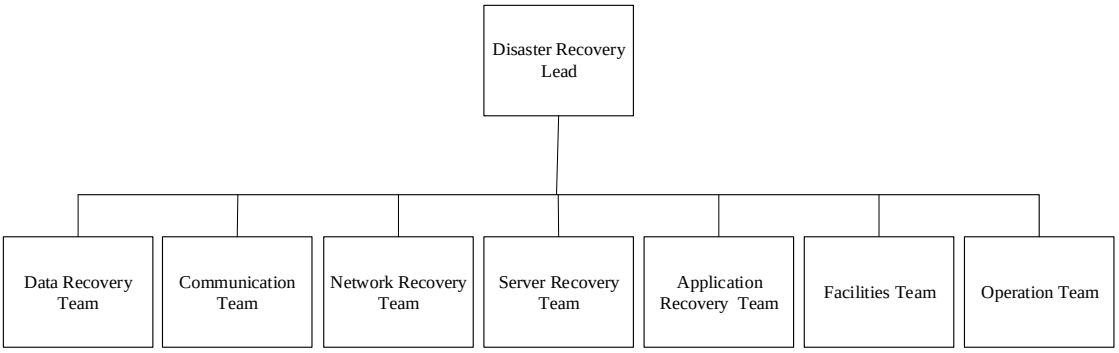


Gambar 7. Topologi Rekomendasi di Universitas Amikom Purwokerto

Dapat dilihat pada gambar 7 sudah memiliki perubahan topologi yang mana menggunakan sistem *cloud* berbasis *private cloud* agar lebih praktis, efektif, efisien dan ekonomis untuk menunjang kebutuhan operasional kampus. Manfaat *cloud* itu sendiri akan disimpan dalam bentuk virtual dengan memanfaatkan jaringan berbasis internet dengan berpusat pada satu *server*, sistem keamanannya pun dapat dipastikan akan terkontrol lebih baik, memiliki kapasitas penyimpanan yang cukup besar, dan akan meminimalisir terjadinya *down server*, terdapat beberapa cara-cara pengujian *Disaster Recovery Plan* antara lain:

1. *Check List Test*: Unit-unit manajemen akan meninjau ulang agar perencanaan tepat dan sesuai.
2. *Structured Walk-Through Test*: Bertemuanya perwakilan antar unit pada manajemen yang membahas perencanaan.
3. *Simulation Test*: Tes simulasi seolah-olah terjadi dampak dari bencana yang menguji kesiapan perosnil.
4. *Paralel Test*; Tes simulasi yang diterapkan di semua *recovery plan* yang bertujuan untuk memberi kepastian apabila terjadi bencana, sistem utama tetap berjalan melalui media *backup*.
5. *Full-Interuption Test*: Pengujian ini digunakan secara keseluruhan pada *recovery plan* yang dibuat.

Langkah-langkah penyusunan dokumentasi DRP menggunakan standar framework NIST SP 800-34 dan nantinya dokumen ini akan diterapkan di Universitas Amikom Purwokerto untuk mendukung proses penanggulangan jika terjadi gangguan atau bencana. Maka, diperlukannya sebuah tim yang mengatur mengenai *Disaster Recovery Plan* yaitu *Disaster Recovery Team* beserta dengan tanggung jawabnya yang dapat dilihat pada tabel 8.



Gambar 8. Struktur Organisasi *Disaster Recovery Team*

Tanggung jawab per masing-masing *job description* adalah *Disaster Recovery Lead yaitu* pengambilkeputusan, menghubungi anggota *Disaster Recovery Team*, pemandu semua anggota yang terlibat dalam pemulihan atau penanggulan bencana dan memimpin pertemuan rutin *Disaster Recovery Team* selama bencana berlangsung dan melakukan *Disaster Recovery Call Tree*, *Data Recovery Team* yaitu penyelamatan data, menangani insiden kecil yang berkaitan dengan data saat normal dan melakukan backup data berkala dan saat terjadi bencana, *Comunication Team* penyampaian tugas, komunikasi dengan karyawan dan klien serta media jika itu dibutuhkan, mengkomunikasikan ke pihak klien, mitra kerja, dan vendor jika terjadi bencana, *Network Recovery Team*; mengutamakan proses pemulihan layanan dengan cara dan urutan yang berpengaruh terhadap dampak bisnis paling tinggi, dan juga melihat serta menentukan koneksi jaringan yang terkena dampak serta menentukan lokasi lain sebagai alternatif, *Server Recovery Team* perbaikan dari server yang memiliki dampak besar bagi proses bisnis, melihat dan menentukan server yang tidak berfungsi dan kemudian menentukan lokasi lain sebagai alternatif server, *Application Recovery Team* melihat serta menentukan aplikasi yang tidak berfungsi dan melakukan pemulihan aplikasi dengan mengurutkan dari aplikasi yang memiliki dampak bisnis yang tinggi, *Facilities Team* menyediakan transportasi dan akomodasi untuk karyawan yang bekerja pada saat siaga bencana serta lokasi alternatifnya, melakukan penilaian terkait kerusakan fisik pada fasilitas utama, berkoordinasi dengan perusahaan asuransi yang berkaitan dengan asset organisasi dan memberikan laporan kepada *Disaster Recovery Lead*, *Operation Team* menjaga dan memastikan daftar perlengkapan penting yang dibutuhkan dan digunakan oleh organisasi termasuk komputer cadangan yang tersedia dan tidak terkena dampak ketika terjadi bencana serta memberikan laporan kepada *Disaster Recovery Lead*.

DRP atau *Disaster Recovery Plan* adalah *recovery plan* dari kemungkinan dampak-dampak bencana yang terjadi. Ketika bencana terjadi, maka *Disaster recovery team* bertugas untuk proses pemulihan sistem jika terjadi sesuatu. Dimana tindakan yang segera dilakukukan setelah terjadi bencana adalah pengecekan awal pada jaringan seperti pengecekan lokasi, pengecekan sumber listrik maupun seluruh perangkat komputer yang ada. Jika yang terjadi kerusakan ringan, maka *Disaster recovery team d*engan cepat memperbaiknya. Namun, jika yang terjadi kerusakan besar seperti fasilitas bangunan hancur maka perlu solusi lain dan di saat yang sama perlu segera melakukan perbaikan hingga kegiatan dapat dikembalikan ke lokasi utama dan berjalan secara normal. Selain itu, perlu dilakukan evaluasi untuk pencegahan bencana lainnya.

4. KESIMPULAN

Berdasarkan dari hasil analisis yang telah dilakukan maka dapat ditarik kesimpulan yaitu dokumen *Disaster Recovery Plan* dapat membantu memulihkan sistem informasi apabila terjadi suatu bencana berdasarkan tingkat prioritas risiko dampak yang terjadi. Urutan tingkat prioritasnya antara lain *Website Student* dengan nilai 100% dan masing-masing 67% untuk *E-Learning*; Absensi Perkuliahan; dan *Smart Dosen*. *Recovery Strategy* digunakan untuk memberikan rekomendasi pemulihan dari bencana berdasarkan urutan prioritas dampak risiko. Rekomendasi yang diberikan salah satunya membuat topologi dengan sistem *private cloud* untuk lancarnya kegiatan operasional di Universitas Amikom Purwokerto. Saran penelitian selanjutnya adalah pengukuran dan evaluasi dari penerapan sistem *private cloud* yang digunakan menggunakan *framework* yang sesuai.

UCAPAN TERIMA KASIH

Terima kasih atas dukungan tim dari Pusat Studi Jaringan Berbasis Informasi yang turut mendukung terselesainya penelitian ini.

REFERENSI

[1] J. J. Kassema, “Information Technology (IT) Contingency Plan as part of the Business Continuity Plan: Case of IT Services Delivery Industry,” Rochester, New York, 2019.

[2] J. S. Patel and K. V, “Disaster Recovery in Business Continuity Management,” *International Journal of Trend in Scientific Research and Development.*, vol. 3, no. 4, pp. 319–322, 2019.

[3] M. L. Sartwell, “Strategies for the Development of IT Disaster Recovery Plans in the Manufacturing Industry Walden University,” 2020.

[4] A. Srinivas, Y. S. Ramayya, and B. Venkatesh, “A Study on Cloud Computing Disaster Recovery,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 6, pp. 1380–1389, 2013.

[5] L. Nurtanzila, “Penerapan Disaster Recovery and Contigency Planning pada Perlindungan Arsip Vital di BPN DIY,” *Diplomatika: Jurnal Kearsipan Terapan*, vol. 1, no. 2, pp. 82–92, 2018.

[6] F. K. L. E. N. S. S. Kusumawardani, “Risk Assessment dan Business Impact Analysis BPK RI dalam Pengembangan DRP BPK RI dengan Standar NIST 800-30 Rev 1.,” in *Seminar Nasional Teknik Industri 2017 Universitas Gadjah Mada*, 2017.

[7] B. Yuliadi and A. Nugroho, “Rancangan Disaster Recovery Pada Instansi Pendidikan Studi Kasus Universitas Mercu Buana,” *Jurnal Teknik Informatika*, vol. 9, no. 1, pp. 30–39, 2016.

[8] Yulhendri, “Penerapan Business Continuity Plan / Disaster Recovery Plan (BCP / DRP) Pada BUMN Dalam Rangka Sustainability : Studi Kasus Pada Pt . X Wilayah Jakarta Raya,” *Jurnal Ilmu Komputer.*, vol. 12, no. 1, pp. 65–78, 2016.

[9] A. Arief and I. H. A. Wahab, “Information Technology Audit For Management Evaluation Using COBIT and IT Security,” *2016 3rd International Journal of Scientific & Engineering Research*, pp. 388–392, 2016.

[10] G. Budi and S. Dhimas, “Disaster Recovery Plan dalam Kantor Samisami,” *Seminar Nasioanal Cendekiawan Ke-3*, pp. 63–70, 2017.

[11] Isa, Indra Griha Tofik “Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akadem,” *Jurnal Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, vol. 15, no. 2, pp. 103–113, 2020.

[12] W. A. Prabowo dan M. E. Saputri, “Pemetaan Resiko Teknologi Informasi dengan Integrasi IT Balanced Scorecard dan NIST SP 800-,” *Jurnal Edukasi dan Penelitian Informatika.*, vol. 6, no. 3, pp. 370–378, 2020.

[13] Agung, Muhammad Zakuan “Perancangan Disaster Recovery Plan Sistem Informasi Akademik dengan Pendekatan Kerangka Kerja NIST 800-34,” *JTERA (Jurnal Teknologi Rekayasa)*, vol. 4, no. 2, p. 157, 2019.

[14] S. Anitha, “The Importance of Disaster Recovery Planning,” *IJARIIE*, vol. 6, no. 4, pp. 193–196, 2020.

[15] A. Supriyanto, I. Aknuranda, W. Hayuhardhika, and N. Putra, “Penyusunan Disaster Recovery Plan (DRP) berdasarkan Framework NIST SP 800-34 (Studi Kasus : Departemen Teknologi Informasi PT Pupuk Kalimantan Timur),” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 8, pp. 8212–8219, 2019.

[16] H. N. Prasetyo, N. Supriatna, A. P. Raharjo, and W. Wikusna, “Information Technology Disaster Recovery Plan (IT-DRP) Model-Based on NIST Framework in Indonesia,” *IJAIT (International Journal of Applied Information Technology)*, vol. 3, no. 1, pp. 34–45, 2020.

[17] W. A. Prabowo and R. D. Ramadhani, “Perancangan Contingency Planning Disaster Recovery Unit Teknologi Informasi Perguruan Tinggi menggunakan,” *Techno.COM*, vol. 20, no. 1, pp. 38–49, 2021.

[18] Kemendikbud, *Peraturan Menteri Pendidikan Nasional Republik Indonesia Nomor 38 Tahun 2008 tentang Pengelolaan Teknologi Informasi Dan Komunikasi di Lingkungan Departemen Pendidikan Nasional*. Jakarta: Kementerian Pendidikan, 2008.