JTERA (Jurnal Teknologi Rekayasa), Vol. 4, No. 2, Desember 2019, Hal. 157-166
Terakreditasi "**Peringkat 3"** oleh Kemenristekdikti, Nomor SK: 30/E/KPT/2018
DOI: 10.31544/jtera.v4.i2.2019.157-166

p-ISSN 2548-737X
e-ISSN 2548-8678

Perancangan *Disaster Recovery Plan* Sistem Informasi Akademik dengan Pendekatan Kerangka Kerja NIST 800-34

Muhammad Zakuan Agung
Program Studi Magister Teknik Informatika, Universitas Bina Darma
Jenderal Ahmad Yani No. 3, Palembang, Indonesia
Mzakuanagung30115@gmail.com

Abstrak

Politeknik Negeri Sriwijaya telah memiliki Sistem Informasi Akademik yang terintegrasi bernama SISAK POLSRI. Terdapat 8 (delapan) sub sistem di dalamnya yang meliputi Sistem Informasi Akademik (SIAK), Sistem Informasi Bimbingan Akademik (SIBA), *Learning Management System* Politeknik Negeri Sriwijaya (LMS Polsri), *E-Complaint* Politeknik Negeri Sriwijaya, *E-Library* Politeknik Negeri Sriwijaya, Sistem Informasi Kepegawaian (SIMPEG), Sistem Informasi Alumni dan *Tracer Study* (SIAT), dan Sistem Pendaftaran dan Pendataan Mahasiswa Baru *(E-Regist)*. SISAK POLSRI merupakan hal yang vital dalam keberlangsungan operasional Politeknik Negeri Sriwijaya, sehingga diperlukan suatu upaya preventif. Salah satu upaya yang dapat dilakukan adalah dengan merancang dokumen *Disaster Recovery Plan* yang bertujuan untuk menjaga keberlangsungan sistem, ketika sistem telah terkena dampak ancaman. Tahapan dalam perancangan *Disaster Recovery Plan* dengan pendekatan kerangka kerja NIST 800-34 yang diinisiasi oleh *Risk Assessment*, *Business Impact Analysis* dan *Strategy Recovery*. Hasil dari penelitian ini berupa dokumen *Disaster Recovery Plan* terhadap 9 ancaman dan 8 sub sistem SISAK POLSRI.

Kata kunci: *Disaster Recovery Plan (DRP),* Manajemen Resiko, Sistem Informasi Akademik

Abstract

Sriwijaya State Polytechnic already has an integrated Academic Information System named SISAK POLSRI. There are 8 (eight) sub systems in it which include Academic Information System (SIAK), Academic Guidance Information System (SIBA), Learning Management System of Sriwijaya State Polytechnic (LMS Polsri), E-Complaint Sriwijaya State Polytechnic, Sriwijaya State Polytechnic E-Librar , Employee Information System (SIMPEG), Alumni Information System and Tracer Study (SIAT), and New Student Registration and Data Collection System (E-Regist). SISAK POLSRI is vital in the sustainability of Sriwijaya State Polytechnic operations, so a preventive effort is needed. One effort that can be done is to design a Disaster Recovery Plan document that aims to maintain the sustainability of the system, when the system has been affected by threats. The stages in the design of the Disaster Recovery Plan with the NIST 800-34 framework approach were initiated by Risk Assessment, Business Impact Analysis and Strategy Recovery. The results of this study are in the form of Disaster Recovery Plan documents against 9 threats and 8 SISAK POLSRI sub-systems.

Keywords: *Disaster Recovery Plan (DRP), Risk Management, Academic Information System*

I. PENDAHULUAN

Sistem Informasi Akademik Politeknik Negeri Sriwijaya (SISAK POLSRI) adalah sistem yang mengintegrasikan seluruh proses bisnis pendidikan yang ada di Politeknik Negeri Sriwijaya ke dalam sebuah sistem informasi yang didukung oleh teknologi berbasis web maupun *mobile*. Sistem Informasi Akademik yang baik menjadi tolak ukur keberhasilan layanan suatu institusi [1]. Dengan penerapan SISAK POLSRI, sangat membantu dalam layanan secara keseluruhan, baik di luar institusi (*Front Office*) maupun di lingkungan internal (*Back Office*). SISAK POLSRI sudah dibangun sejak tahun 2012 yang mengintegrasikan data dosen, mahasiswa, tenaga kependidikan, pimpinan, akademik, dan jurusan. Pengembangan dan upaya pengamanan data/informasi terus

Diterima: 13 Agustus 2019; Direvisi: 11 November 2019; Disetujui: 21 November 2019
JTERA, Vol. 4, No. 2, Desember 2019

menerus dilakukan untuk menjamin validitas dan keakuratan data/informasi yang dihasilkan, karena data dan informasi merupakan aset dan syarat mutlak apakah institusi tersebut dapat berjalan dengan baik [2]-[4]. Selama proses pengembangan SISAK POLSRI, belum ada dokumentasi terkait dalam penyimpanan dan penjagaan infrastruktur maupun aset teknologi/sistem informasi, mengingat Indonesia merupakan negara rentan bencana alam dan juga rentan terhadap serangan *hacker* seperti SQL *Injection*, virus, dan *web deface* yang berdampak pada kerugian suatu organisasi [5]. Hal ini merupakan sebuah kerentanan yang memungkinkan berdampak kerugian suatu institusi, terutama bila sudah terjadi bencana alam maupun serangan *human caused* terhadap sistem maupun infrastruktur. Oleh karena itu, diperlukan sebuah pedoman untuk memitigasi resiko dan menjalankan proses bisnis ketika dalam kondisi kritis paska mengalami serangan, baik bencana maupun *human caused*. Salah satu dokumen yang digunakan ketika sistem telah mengalami serangan dan dalam kondisi kritis adalah *Disaster Recovery Plan* (DRP).

DRP merupakan bagian penting dalam langkah "mengasuransikan" data serta infrastruktur yang kita miliki agar tetap "hidup" dan berjalan sebagaimana mestinya [6]. DRP memuat proses, kebijakan, dan mekanisme yang berhubungan dengan bagaimana suatu institusi dapat melangsungkan bisnis prosesnya setelah terjadinya bencana, baik oleh bencana alam maupun *human caused* [7], [8]. Salah satu faktor utama dalam DRP adalah budaya organisasi, sehingga karakteristik personal dan gaya kepemimpinan sangat berpengaruh dalam penyusunan dan pengimplementasian DRP [9], [10]. Dalam penelitian ini kerangka kerja yang digunakan dalam penyusunan DRP adalah NIST 800-34 yang dirilis oleh National Institute of Standards and Technology [11]. Secara teknis tahapan dalam perancangan DRP dengan kerangka kerja NIST 800-34 terdapat dalam Gambar 1.

Dalam Kerangka Kerja NIST SP 800-34 tersebut memuat beberapa prosedur antara lain *Business Continuity Plan* (BCP) dan *Business Impact Analysis* (BIA), sehingga menghasilkan DRP. Ada beberapa hal yang harus diperhatikan dalam perancangan DRP, antara lain strategi apa yang digunakan dalam pemulihan aset teknologi/sistem informasi, teknologi apa yang digunakan pada masing-masing teknologi/sistem informasi, dan bagaimana SDM yang dilibatkan dalam pelaksanaan kegiatan.

Tujuan penelitian ini adalah memberikan rekomendasi rancangan DRP pada SISAK POLSRI

Gambar 1. Kerangka kerja NIST 800-4

menggunakan pendekatan kerangka kerja NIST 800-34 sehingga dapat menentukan tindakan apa dan bagaimana terhadap keberlangsungan sistem ketika mengalami serangan, baik bencana alam maupun serangan *human caused.*

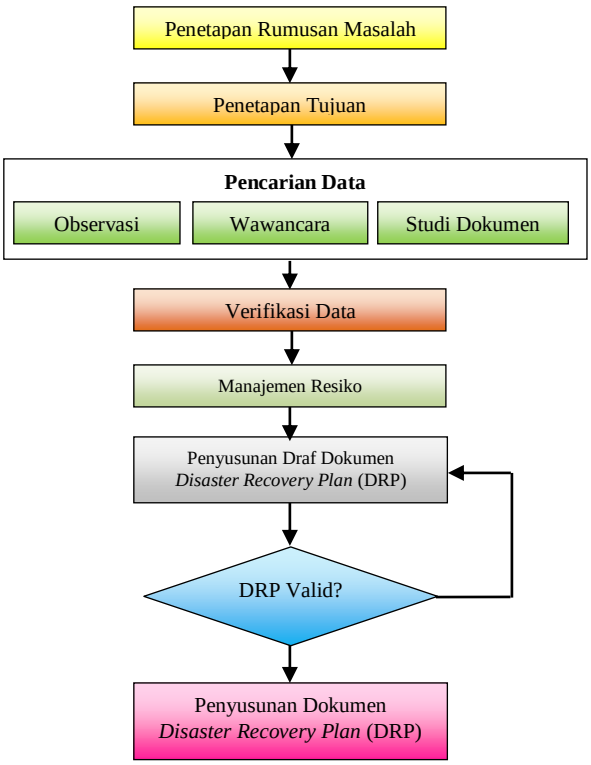
II. METODE PENELITIAN

Metode yang dilakukan pada penelitian, seperti pada Gambar 2. Secara umum tahapan yang dilakukan adalah observasi, wawancara, studi dokumen, dan perancangan DRP itu sendiri.

Observasi dilakukan untuk melihat kondisi eksisting sistem yang sedang berjalan. Dalam observasi ini menghasilkan data serangan yang disebabkan oleh bencana alam maupun serangan *human caused* yang pernah terjadi dalam SISAK POLSRI dan data perangkat lunak maupun perangkat keras teknologi/sistem informasi SISAK POLSRI. Dari data yang dihasilkan melalui observasi ini selanjutnya akan dilakukan pembobotan potensi resiko yang mungkin terjadi untuk dijadikan salah satu parameter dalam perancangan DRP.

Tahapan selanjutnya adalah wawancara. Dalam wawancara yang dilakukan melibatkan pihak-pihak yang berkepentingan dalam SISAK POLSRI. Adapun pihak yang diwawancarai antara lain: Tim IT POLSRI dan pengguna SISAK POLSRI (Dosen, Tenaga Kependidikan, dan Mahasiswa). Beberapa poin pertanyaan terkait tentang bagaimana jalannya sistem dan dukungan *stakeholder*, apa upaya yang dilakukan ketika terjadi bencana, baik yang disebabkan oleh bencana alam maupun *human caused*, dan tindakan preventif yang dilakukan dalam memitigasi bencana tersebut. Hasil dari wawancara ini akan dijadikan bahan pertimbangan dalam menentukan perancangan DRP.

Selanjutnya dilakukan studi dokumen dengan mengumpulkan data-data berupa dokumentasi baik *form* yang digunakan dalam *blueprint* SISAK POLSRI maupun dokumentasi topologi jaringan komputer. Studi dokumen digunakan sebagai acuan data dalam perancangan DRP.



Gambar 2. Metode penelitian

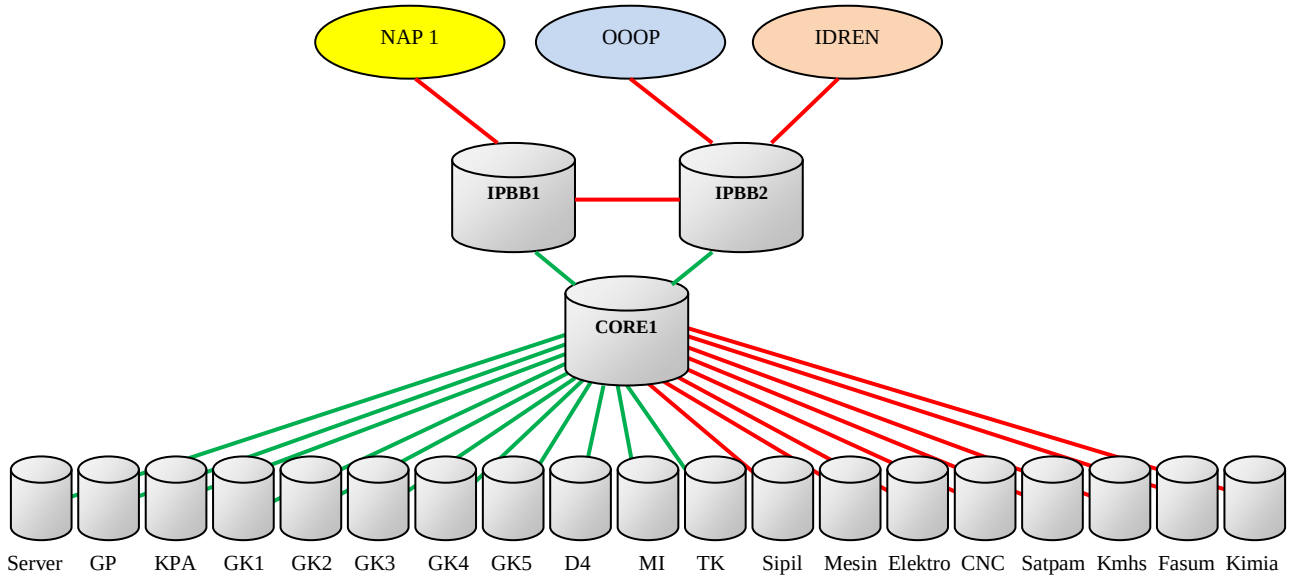
Tahap terakhir adalah merancang DRP. Kerangka kerja dalam perancangan DRP yang digunakan dengan pendekatan NIST 800-34. Tahapan yang dilakukan adalah melakukan *Risk Assessment* terhadap faktor-faktor kerentanan yang memiliki resiko tinggi hingga rendah, BIA yang digunakan untuk melihat bagaimana dampak resiko yang muncul terhadap kelangsungan jalannya proses bisnis, mengidentifikasi *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO), pemilihan prioritas dalam pemulihan sistem informasi, strategi *recovery* yang akan dilaksanakan, serta proses pendokumentasian yang menghasilkan dokumen rancangan DRP.

III. HASIL DAN PEMBAHASAN

A. Topologi Jaringan Komputer Polsri

Polsri memiliki jaringan komputer yang terintegrasi dalam menjalankan SISAK POLSRI. Jaringan komputer ini membentuk topologi jaringan yang menghubungkan seluruh divisi yang ada di Polsri. Dalam proses pengembangannya, topologi jaringan Polsri telah mengalami empat kali pengembangan dan perluasan jaringan, hingga pada tahun 2019 telah mengintegrasikan seluruh sub jaringan yang berjumlah 18 sub jaringan, antara lain:

1. Gedung Graha Pusat (GP)
2. Kantor Pusat Administrasi (KPA)
3. Gedung Kuliah 1 (GK 1)
4. Gedung Kuliah 2 (GK 2)
5. Gedung Kuliah 3 (GK 3)
6. Gedung Kuliah 4 (GK 4)
7. Gedung Kuliah 5 (GK 5)
8. Gedung Diploma IV (D4)
9. Gedung Manajemen Informatika (MI)
10. Gedung Teknik Komputer (TK)
11. Gedung Sipil (Sipil)
12. Gedung Mesin (Mesin)
13. Gedung Elektro (Elektro)
14. Ruang CNC (CNC)
15. Ruang Satpam (Satpam)
16. Ruang Kemahasiswaan (Kmhs)
17. Gedung Fasilitas Umum (Fasum)
18. Gedung Kimia (Kimia)



Gambar 3. Topologi jaringan komputer Polsri

Berdasarkan catatan observasi dan studi dokumen yang telah dilakukan, *server* jaringan Polsri pernah rusak di tahun 2014 karena terkena petir, yang mengakibatkan gangguan terhadap komputer jaringan di seluruh lingkungan Polsri selama hampir satu minggu. Secara detil topologi jaringan Polsri terdapat pada gambar 3:

Pada konfigurasi jaringan Polsri, setiap gedung memiliki *router* sendiri. Untuk *router* dengan sambungan kabel berwarna hijau memiliki *bandwidth* sebesar 10 Gbps dan untuk sambungan kabel berwarna merah memiliki *bandwidth* sebesar 1 Gbps. Setiap *router* gedung perkuliahan akan langsung terhubung ke *Core* pusat sebagai pengatur lalu lintas data.

Besar *bandwidth* dalam jaringan internet adalah 1.250 Mbps dengan *bandwidth* ke IIX = 500Mb (*Local* 500 Mbps & *redundant link* 100 Mbps, Internasional 150 Mbps & *redundant link* 100Mbps). Besar *bandwidth* VPN IP CCTV 512 Kbps per *site*. VPN Datawarehouse 2 Mbps *backhaul* 64 Kbps. Jaringan ini dibangun dengan menggunakan ISP dari PT. Telkom dengan layanan IDren.

B. Modul Sub Sistem Informasi Akademik Polsri

SISAK POLSRI merupakan sistem informasi yang terintegrasi, dimana di dalamnya memiliki tujuh sub sistem yang saling terkait terhadap seluruh kegiatan akademik maupun keuangan yang ada di Polsri. Adapun modul sub sistem yang ada di SISAK POLSRI terdapat dalam Tabel 1.

Tabel 1. Sub sistem SISAK POLSRI

No	Sub sistem
1	Sistem Informasi Akademik (SIAK)
2	Sistem Informasi Bimbingan Akademik (SIBA)
3	*Learning Management System* Politeknik Negeri Sriwijaya (LMS Polsri)
4	*E-Complaint* Politeknik Negeri Sriwijaya
5	*E-Library* Politeknik Negeri Sriwijaya
6	Sistem Informasi Kepegawaian (SIMPEG)
7	Sistem Informasi Alumni dan *Tracer Study* (SIAT)
8	Sistem Pendaftaran dan Pendataan Mahasiswa Baru *(E-Regist)*

Disamping sub sistem yang terdapat dalam SISAK POLSRI, juga hal lain yang menjadi pertimbangan dalam aset secara teknis fungsional antara lain:

1. *User base*/data user
2. *Source code* aplikasi
3. *Development Environment*
4. *Development Tools*/Perangkat yang digunakan dalam pengembangan sistem, baik perangkat lunak maupun perangkat keras

C. Risk Assessment Terhadap SISAK POLSRI

Risk Assessment dilakukan untuk menilai derajat tingkat resiko yang mungkin terjadi dalam perangkat teknologi/sistem informasi. Resiko dapat dimitigasi dengan menekan faktor *vulnerabilities* (kerentanan) ataupun menekan dampak dari resiko [12]. Dalam penelitian ini aspek *risk assessment* menilai potensi resiko terhadap perangkat lunak dan perangkat keras yang terkait dengan SISAK POLSRI. Salah satu acuan yang menjadi parameter dalam *risk assessment* adalah hasil observasi dan wawancara lapangan, dimana dihasilkan data-data kejadian yang pernah terjadi, seperti gangguan teknis, serangan *hacker*, maupun bencana alam/ *force majeur*.

Dalam perancangan DRP SISAK POLSRI, *risk assesment* menjadi sebuah prosedur awal, bagaimana menentukan ancaman dan menganalisis potensi resiko yang mungkin terjadi. Aspek yang dinilai dalam *risk assessment* meliputi *threats* (ancaman), potensi ancaman yang terjadi, *vulnerability* (potensi kerentanan), *critical assets* (aset kritis yang terdampak dari ancaman tersebut), dan *concequencies.*

Beberapa kejadian yang menimpa SISAK POLSRI dan menyebabkan gangguan teknis selama 7 tahun ini antara lain: gangguan petir, pemadaman listrik yang berulang, *fatal error* akibat komponen komputer rusak (*bad sector harddisk, failure memory, bluescreen*), dan serangan *virus/hacker*. Adapun potensi kejadian lainnya berupa bencana alam/*force majeur* mengingat Indonesia negara yang rawan bencana antara lain kebakaran, banjir, gempa bumi, dan badai. Tabel 2 merupakan hasil dari *risk assessment* SISAK POLSRI.

Tabel 2. *Risk assessment* SISAK POLSRI

No	*Threats*	*Potential Threats*	*Vulnerabilities*	*Critical Assets*	*Consequences*
1	Kebakaran	Dapat disebabkan kelalaian manusia seperti dari puntung rokok, korsleting / hubungan arus pendek listrik, ataupun kebakaran yang disebabkan dari eksternal lingkungan ruangan.	Terdapat material yang mudah terbakar, baik di dalam gedung maupun areal di luar gedung;	Gedung Perkantoran, sarana dan prasarana kantor	Dapat menghentikan kegiatan operasional
2	Banjir	Berdampak pada timbulnya kerusakan bangunan baik sarana & prasarana serta perangkat kantor lainnya	Sarana dan Prasarana berdampak rusak sedang hingga rusak parah paska banjir	Sarana dan prasarana perkantoran; perangkat komputer dan jaringan	Bila terkena sistem komputer dan jaringan, kegiatan operasional dapat terpaksa dihentikan;
3	Petir	Berdampak langsung terhadap jaringan *Local Area Network* dan komputer yang terkena sambaran petir, serta alat-alat listrik lainnya yang sedang terhubung dengan listrik	Perangkat komputer dan jaringan komputer, serta perangkat lainnya yang sedang terhubung dengan jaringan listrik	Sistem dan Jaringan komputer; perangkat kantor lainnya yang terhubung dengan jaringan listrik	Rusaknya perangkat kantor, komputer dan jaringan internet; kegiatan operasinal melambat atau terpaksa dihentikan.
4	Gempa Bumi	Berdampak pada kerusakan gedung, baik sarana dan prasarana ketika gempa bumi melebihi 5 skala richter	Dominan gedung dan ruangan di Politeknik Negeri Sriwijaya hanya mampu menahan gempa kurang dari 5 skala richter	Gedung, Sarana dan Prasarana maupun ruangan di Politeknik Negeri Sriwijaya	Dapat menghentikan kegiatan operasional
5	*Human Error*	Berdampak pada kerusakan ringan dan kerusakan menengah pada sistem komputer maupun sistem informasi; kesalahan informasi yang dihasilkan dari sistem	Kesalahan penginputan data; Terhapus data record maupun data sistem; *Bugs* akibat *slips / lapses*;	Data/ Informasi SISAK POLSRI	Memperlambat kinerja Sistem; Menghentikan kinerja sistem
6	*Virus / Worm /* Malware	Virus yang menyerang dan mencari *bugs* pada aplikasi maupun Sistem Operasi, worm yang dapat menginfeksi dari e-mail maupun *flashdisk* yang dimasukan ke dalam PC	Terdapat celah kerentanan yang dapat diinfeksi virus; Antivirus tidak selalu *update*;	Sistem Komputer dan SISAK POLSRI	Memperlambat kinerja Sistem; Menghentikan kinerja sistem
7	Gangguan Listrik Padam	Tegangan naik-turun / tidak stabil yang berdampak pada kerusakan perangkat keras seperti CPU (Harddisk / power supply)	Peralatan yang sedang terkoneksi listrik; Pemadaman listrik yang dilakukan berulang; Tidak semua komputer dihubungkan dengan UPS	Komputer yang terintegrasi dengan SISAK POLSRI	Merusak komputer; Memperlambat kinerja Sistem; Menghentikan kinerja Sistem

No	*Threats*	*Potential Threats*	*Vulnerabilities*	*Critical Assets*	*Consequences*
8	*Cyber Attact / Hacker*	Upaya serangan *cyber* dari pihak luar *(hacker/ cracker)* berupa SQL *Injection*, defacing, DDoS, Phising, Sniffing maupun Backdoor	*Server* masih memiliki celah kerentanan yang mudah terserang DDoS	Data/Informasi, Sistem Komputer SISAK POLSRI	Memperlambat kinerja Sistem; Menghilangkan data/informasi yang terdapat dalam sistem; Menghentikan kinerja sistem
9	*Serverdown*	Kerusakan pada *server* karena tingginya traffic maupun hal teknis lainnya, sehingga menjadi *down*	Terdapat celah kerentanan yang menyebabkan *server* menjadi *down*	Data/Informasi, Sistem Komputer SISAK POLSRI	Memperlambat kinerja Sistem; Menghentikan kinerja sistem

Tabel 3. Deskripsi layanan sub sistem SISAK POLSRI

No	Sub sistem	Layanan
1	Sistem Informasi Akademik (SIAK)	• Pendataan Dosen • Pendataan Mahasiswa • Kartu Hasil Studi • Presensi dan Agenda Perkuliahan • Pengolahan data Nilai
2	Sistem Informasi Bimbingan Akademik (SIBA)	• Bimbingan Akademik • Rencana Studi • Perwalian
3	*Learning Management System* Politeknik Negeri Sriwijaya (LMS Polsri)	• Pengolahan modul praktikum • Ujian Online • *Blended learning tools*
4	*E-Complaint* Politeknik Negeri Sriwijaya	• Pengolahan data keluhan • Grafik keluhan bulanan dan tahunan • Rekomendasi dan rencana tindak lanjut keluhan
5	*E-Library* Politeknik Negeri Sriwijaya	• Repository Buku • E-Journal POLSRI • Pengolahan data perpustakaan *online*
6	Sistem Informasi Kepegawaian (SIMPEG)	• Absensi Pegawai • BKD dan LKD Internal • KPI Pegawai • Pengolahan data kepegawaian
7	Sistem Informasi Alumni dan *Tracer Study* (SIAT)	• Pengolahan data alumni • Pengolahan data *Tracer Study* • Informasi Lowongan Kerja
8	Sistem Pendaftaran dan Pendataan Mahasiswa Baru *(E-Regist)*	• Pengolahan Data Mahasiswa Baru • Registrasi ulang Mahasiswa Baru

Data-data resiko pada Tabel 2 di atas selanjutnya dijadikan acuan pada tahapan berikutnya, yakni BIA. Penjelasan lebih detil mengenai BIA yang dikaitkan dengan *risk assessment* terhadap SISAK POLSRI dibahas pada poin berikutnya.

D. Business Impact Analysis (BIA)

Secara definisi BIA merupakan sebuah proses bagaimana penentuan dan pendokumentasian implikasi terhadap proses bisnis dari suatu ancaman atau resiko yang mengganggu dalam jalannya aktifitas suatu institusi [13]. Sebelum membuat BIA, hal yang perlu dilakukan adalah membuat pemetaan layanan apa saja yang dilaksanakan oleh masing-masing sub sistem dalam SISAK POLSRI. Tabel 3 adalah deskripsi dari layanan sub sistem SISAK POLSRI. Tahapan berikutnya adalah memetakan derajat dampak resiko terhadap layanan dari sub sistem SISAK POLSRI. Terdapat tiga kategori untuk derajat dampak resiko, yakni tinggi, rendah, dan sedang. Secara detil terdapat pada Tabel 4. Selanjutnya pemetaan dari dampak resiko terhadap layanan sub sistem berdasarkan derajat dampak resiko. Tabel 5 hingga Tabel 8 menunjukkan dampak resiko akibat *human error*, virus/worm/ malware, *cyber attack / hacker*, dan *serverdown*.

Tabel 4. Derajat dampak resiko

No	Derajat dampak	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

Tabel 5. *Human error*

No	Sub sistem	Dampak yang dialami	Tingkat dampak
1	SIAK	Kesalahan informasi seperti nilai, KHS, jadwal perkuliahan	Sedang
2	SIBA	Sistem tidak dapat memvalidasi data bimbingan akademik	Sedang
3	LMS POLSRI	*Mismatch* antara modul dengan mata kuliah yang diajarkan	Sedang
4	E-Complaint	*Mismatch* kategori komplain dengan konten komplain	Rendah
5	E-Library	Selisih data repository digital dengan repository fisik	Rendah
6	SIMPEG	Selisih perhitungan dan penggajian, berdampak dalam data kinerja pegawai yang dapat merugikan pegawai itu sendiri hingga tingkat berat	Tinggi
7	SIAT	*Mismatch* data alumni, data testimony dan informasi lowongan kerja	Rendah
8	E-Regist	Pendaftar tidak terakui sebagai mahasiswa baru	Tinggi

Tabel 6. Virus / Worm / Malware

No	Sub sistem	Dampak yang dialami	Tingkat dampak
1	SIAK	Melambatnya proses kegiatan akademik dalam sistem	Sedang
2	SIBA	Proses bimbingan tidak dapat dilakukan tepat waktu	Sedang
3	LMS POLSRI	Tidak bisa akses ke sistem dan modul hilang	Sedang
4	E-Complaint	Tidak bisa akses ke sistem dan data-data complain hilang	Tinggi
5	E-Library	Melambatnya proses pengunduhan dan pengunggahan data repository	Rendah
6	SIMPEG	Kehilangan data-data pegawai	Tinggi
7	SIAT	Tidak dapat akses ke sistem	Rendah
8	E-Regist	Kehilangan data mahasiswa baru	Tinggi

Tabel 7. *Cyber attack/hacker*

No	Sub sistem	Dampak yang dialami	Tingkat dampak
1	SIAK	Gangguan dalam absensi dan publikasi nilai	Tinggi
2	SIBA	Menghilangnya menu bimbingan dan konten data bimbingan	Sedang
3	LMS POLSRI	Tidak bisa akses ke sistem dan modul pembelajaran hilang	Sedang
4	E-Complaint	Terjadi *mismatch* data	Sedang
5	E-Library	Tidak bisa akses ke modul perpustakaan	Sedang
6	SIMPEG	Kehilangan data kepegawaian	Tinggi
7	SIAT	Terjadi perubahan dan manipulasi data yang tidak terkontrol	Sedang
8	E-Regist	Kehilangan data mahasiswa baru	Tinggi

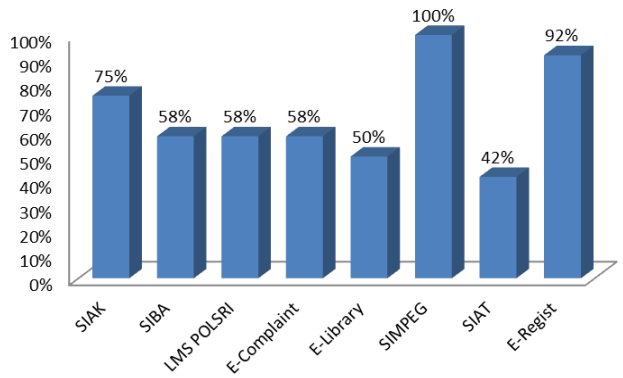
Tabel 8. *Serverdown*

No	Sub sistem	Dampak yang dialami	Tingkat dampak
1	SIAK	Terjadi kelambatan akses SIAK	Sedang
2	SIBA	Terjadi kelambatan akses SIBA	Rendah
3	LMS POLSRI	Terjadi kelambatan akses LMS POLSRI	Rendah
4	E-Complaint	Terjadi kelambatan akses eComplaint	Rendah
5	E-Library	Terjadi kelambatan akses eLibrary	Sedang
6	SIMPEG	Terjadi kelambatan akses SIMPEG	Tinggi
7	SIAT	Terjadi kelambatan akses SIAT	Rendah
8	E-Regist	Terjadi kelambatan akses eRegist	Sedang

Tahapan berikutnya adalah menentukan prioritas sistem mana yang memiliki nilai prioritas tertinggi. Pemberian prioritas adalah dengan menggabungkan nilai dampak dari masing-masing sub sistem, dengan penilaian:

- Tinggi : Penilaian 3
- Sedang : Penilaian 2
- Rendah : Penilaian 1

Penilaian yang dihasilkan dari perhitungan tingkat dampak dari sub sistem tersebut ditunjukkan pada Gambar 4.



Gambar 4. Grafik penilaian tingkat dampak

Tabel 9. Prioritas terdampak sub sistem SISAK POLSRI

No	Sub sistem	Rerata nilai dampak	%
1	SIMPEG	3	100%
2	E-Regist	2,75	92%
3	SIAK	2,25	75%
4	SIBA	1,75	58%
5	LMS POLSRI	1,75	58%
6	E-Complaint	1,75	58%
7	E-Library	1,5	50%
8	SIAT	1,25	42%

Adapun penilaian tingkat dampak dari prioritas tertinggi hingga terendah, dapat dilihat pada Tabel 9. Dari Tabel 9 di atas terlihat bahwa sub sistem yang memiliki tingkat dampak tertinggi dalam SISAK POLSRI adalah Sistem Informasi Kepegawaian (SIMPEG). Hal ini artinya adalah SIMPEG memiliki kerentanan yang tinggi bila terkena ancaman. Dampak yang dihasilkan sangat signifikan bagi kegiatan operasional institusi. Pada tingkat kedua adalah E-Regist, dimana sub sistem ini berkaitan langsung dengan mahasiswa baru. Sub

sistem yang memiliki dampak terendah terhadap ancaman adalah Sistem Informasi Alumni dan *Tracer Study* (SIAT).

E. Strategy Recovery

Tahapan *Strategy Recovery* merupakan inti dari perancangan dokumen DRP. Dalam tahapan ini dilakukan skenario bagaimana perbaikan dan mitigasi resiko paska sistem terkena ancaman. Tabel 10 menunjukkan *strategy recovery* terhadap salah satu ancaman, yakni *human error*:

IV. KESIMPULAN

Perlunya DRP dalam suatu sistem informasi dapat membantu pemulihan dan keberlanjutan suatu sistem informasi itu sendiri. Dalam penelitian ini telah dihasilkan dokumen DRP untuk SISAK POLSRI berdasarkan aspek ancaman dan terurut berdasarkan skala prioritas. Dua sub sistem skala prioritas dalam DRP adalah Sistem Kepegawaian (SIMPEG) dan *E-Regist* Mahasiswa Baru Polsri, dengan masing-masing bernilai 100% dan 92%. Adapun pendokumentasian DRP dilakukan setelah pembuatan *strategy recovery* sub sistem terhadap ancaman yang telah terjadi. Terdapat 9 rancangan *strategy recovery* berdasarkan ancaman yang terjadi.

REFERENSI

[1] W. Apri, Sowiyah, and A. Alben, *Implementasi Sistem Informasi Manajemen Akademik Berbasis Web*. Bandar Lampung: FKIP Unila, 2014.

[2] P. R. E. Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*. Yogyakarta: Graha Ilmu, 2014.

[3] R. Budiarto, "Manajemen Risiko Keamanan Sistem Informasi," *Journal of Computer Engineering System and Science*, vol. 2, no. 2, pp. 48–58, 2017.

[4] Yakub, *Pengantar Sistem Informasi*. Yogyakarta: Graha Ilmu, 2012.

Tabel 10. *Strategy recovery* ancaman *human error*

No	Sub sistem	Kendala	*Strategy recovery*
1	SIMPEG	Selisih perhitungan dan penggajian, berdampak dalam data kinerja pegawai yang dapat merugikan pegawai itu sendiri hingga tingkat berat	Terdapat multi validasi dalam proses perhitungan data, khususnya data-data yang memiliki tingkat kritis tinggi; Selalu melakukan *backup* data dalam server yang berbeda
2	E-Regist	Pendaftar tidak terakui sebagai mahasiswa baru	Penyimpanan data dilakukan di dalam sistem yang berbeda; melakukan audit ulang mengenai tata kelola eRegist
3	SIAK	Kesalahan informasi seperti nilai, KHS, jadwal perkuliahan	Perbaikan aspek Interaksi Manusia dan Komputer di SIAK
4	SIBA	Sistem tidak dapat memvalidasi data bimbingan akademik	Selalu menyertakan form manual dalam proses bimbingan agar tiap dosen memiliki data pribadi secara fisik
5	LMS POLSRI	*Mismatch* antara modul dengan mata kuliah yang diajarkan	Terdapat verifikator data untuk menverifikasi dosen, mata kuliah dan modul perkuliahan
6	E-Complaint	*Mismatch* kategori omplain dengan konten komplain	Dilakukan *backup* data secara berkala baik harian atau mingguan
7	E-Library	Selisih data repository digital dengan repository fisik	Pengecekan data fisik dengan data digital secara berkala
8	SIAT	*Mismatch* data alumni, data testimony dan informasi lowongan kerja	Tersedia fasilitas kanal lain selain sistem, seperti Instagram, Youtube, Facebook dan Twitter untuk kemudahan akses informasi alumni dan *tracer study*

[5] Pemerintah Republik Indonesia, *Undang-Undang Republik Indonesia Nomor 24 Tahun 2007 tentang Penanggulangan Bencana*. Indonesia, 2007.
[6] S. R. Wicaksono. *Disaster Recovery Planning*. Jakarta: Seribu Bintang. 2009.
[7] N. Rachmaningrum, "Studi Kelayakan Disaster Recovery Plan pada Infrastruktur Jaringan Komputer (Studi kasus Jaringan Komputer Universitas Widyatama)", in *semnas IF*, UPN Veteran Yogyakarta, pp. 30–36. 2011.
[8] A. F. U. Fahmawati, *Faktor-Faktor yang Mempengaruhi Disaster Recovery Plan dan Business Continuity Planning*, Bandar Lampung: Universitas Lampung. 2016.
[9] I. W. A. Yasa, "Perumusan *Disaster Recovery Plan* pada Infrastruktur Jaringan Komputer", Tesis, STMIK STIKOM Bali, 2016.
[10] R. Soetam. *Disaster Recovery Plan*. Jakarta: Prestasi Pustaka. 2009.
[11] (2002). The website NIST [Online]. Available: https://csrc.nist.gov.
[12] Gibson, *Managing Risk in Information System, 2nd Edition*, USA: Jones & Bartlett Learning. 2014.
[13] R. L. Tammineedi, "Business continuity management: A standards-based approach," *Information Security Journal*, vol. 19, no. 1, pp. 36–50, 2010.