e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan *Disaster Recovery Plan* pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi

Indra Griha Tofik Isa
Program Studi Manajemen Informatika, Jurusan Manajemen Informatika, Politeknik Negeri Sriwijaya
Jl. Srijaya Negara Bukit Besar, Kota Palembang, 30139
e-mail: indra_isa_mi@polsri.ac.id

ABSTRAK

Disaster Recovery Plan (DRP) merupakan upaya keberlanjutan sebuah sistem atau proses bisnis ketika menghadapi sebuah ancaman. Objek penelitian ini adalah Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi yang bertujuan untuk merancang *Disaster Recovery Plan* (DRP) dengan pendekatan kerangka kerja NIST 800-34. Tahapan penelitian dimulai dengan penetapan permasalahan yang akan diteliti; Pengumpulan data melalui observasi, wawancara dan studi lapangan; Identifikasi dan penilaian aset terdiri dari 4 aspek yakni Data, Perangkat Keras, Perangkat Lunak, dan Jaringan; *Risk Assessment* yang melihat potensi ancaman yang terjadi berdasarkan penilaian *Likelihood, Restoration* dan *Predictability*, diklasifikasikan menjadi 9 ancaman yakni Banjir, Petir/Badai, Gempa Bumi, Kebakaran, Gangguan Server, Gangguan Listrik, Serangan *Hacker / Cybercrime*, Kesalahan Manusia *(Human Error)* dan Serangan Virus, Malware, Worm; tahapan berikutnya *Business Impact Analysis* dengan melihat dampak yang terjadi pada SIAK UMMI dilihat dari ancaman. Dari tahapan ini dihasilkan sub sistem yang memiliki dampak terbesar adalah Sistem Keuangan Mahasiswa dengan nilai persentasi 99%, sedangkan sub sistem yang memiliki nilai terendah adalah Sistem Pembimbingan Akademik dengan nilai dampak persentasi 62%. Hasil akhir dari penelitian ini berupa dokumen *Disaster Recovery Plan* (DRP) yang memuat 9 kategory *Strategy recovery* terhadap potensi ancaman yang terjadi pada SIAK UMMI.

Kata Kunci – *Disaster Recovery Plan* (DRP), NIST 800-34, Sistem Informasi Akademik

1. PENDAHULUAN

SIAK UMMI atau Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi merupakan Sistem yang mengintegrasikan seluruh kegiatan akademik yang ada di Universitas Muhammadiyah Sukabumi. SIAK UMMI yang ada pada saat ini berjalan dalam platform berbasis web dengan melibatkan elemen atau sivitas akademik yang terdiri dari dosen, tenaga kependidikan, mahasiswa maupun pimpinan. Penerapan Sistem Informasi Akademik sendiri bertujuan untuk membantu dan mempercepat informasi akademik kepada mahasiswa (Siagian & Effiyaldi, 2018), sehingga layanan mahasiswa tercapai dengan baik. SIAK UMMI sudah mulai diimplementasikan sejak tahun 2013, dimana komponen sistem informasi akademik yang dibangun meliputi sistem pengisian KRS, pembimbingan mahasiswa, pengisian nilai, sistem keuangan mahasiswa, sistem penerimaan mahasiswa baru dan sistem administrasi fakultas (Asriyanik, 2016).

Salah satu keberhasilan dalam upaya keberlanjutan dari sistem yang diimplementasikan tersebut adalah bagaimana bertahan dengan menjaga data dan informasi yang merupakan aset dan syarat mutlak apakah institusi tersebut dapat berjalan dengan baik (Indrajit, 2014), (Budiarto, 2017), (Yakub, 2012). Berbagai upaya perbaikan dan meminimalisir kerentanan terus menerus dilakukan, baik dalam aspek prosedural, teknis dan kenyamanan pengguna dari segi interaksi manusia dan komputer (IMK) (Isa, 2018). Secara teknis SIAK UMMI mengimplementasikan teknologi keamanan data yang meminimalisir terjadinya pembobolan data oleh pihak-pihak yang tidak bertanggung jawab. Didalam perjalannya, SIAK UMMI pernah mengalami beberapa serangan, baik yang diakibatkan oleh *human caused* berupa *cyber attack* maupun bencana alam.

Beberapa dampak yang terjadi dari gangguan tersebut antara lain:

1. Terjadi penurunan layanan kepada mahasiswa, dosen dan *stakeholder* yang terkait di dalamnya
2. Potensi hilang maupun rusaknya data dan informasi yang bersifat kritis.
3. Penurunan kredibilitas atau kepercayaan terhadap pengelola Sistem Informasi
4. Potensi kerugian secara finansial (materi), sumber daya maupun waktu sebagai dampak dari rusaknya data dan sistem informasi.

Dari histori serangan yang telah terjadi baik berupa *cyber attact* maupun bencana alam, saat ini SIAK UMMI belum memiliki dokumentasi strategi penanganan serangan ataupun mekanisme penanganan bencana yang mampu mengatasi dampak dari kerusakan bencana baik itu bencana alam dan kerusakan akibat perbuatan manusia. Sehingga perlu dibuatkan sebuah mekanisme untuk meminimalisir kerugian akibat bencana tersebut (Rivai et al,2018). Salah satu persiapan dalam penanganan permasalahan ketika sistem menghadapi kondisi kritis setelah terjadi bencana adalah dengan pembuatan dokumen *Disaster Recovery Plan* (DRP). DRP sudah banyak diterapkan pada institusi koorporat maupun perguruan tinggi mengingat

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

bagaimana menyelamatkan aset data dan informasi yang bersifat kritikal dan penting.

Beberapa penelitian sebelumnya terkait penyusunan DRP yakni dengan menggunakan kerangka kerja NIST 800-34 salah satunya di Institusi Politeknik Negeri Sriwijaya, dimana dalam penelitian ini dihasilkan DRP terhadap 9 ancaman serta 8 sub-sistem dengan dua prioritas utamanya, yakni Sistem Kepegawaian (SIMPEG) dan E-Regist mahasiswa baru dengan tahapan yang dimulai dari penetapan permasalahan, Penetapan Tujuan, Pengumpulan Data, Verifikasi Data, Manajemen Resiko, Penyusunan draf DRP, validitas draf DRP dan Penetapan dokumen DRP (Agung, 2019).

Penelitian lainnya dilakukan pada BUMN PT. X, dengan menghasilkan DRP yang disesuaikan dengan situasi dan kondisi perusahaan sekarang agar perencanaan dilakukan tidak salah dan penanganan masalah dilakukan dengan tepat. DRP yang dihasilkan terdiri dari 7 rekomendasi (Yulhendri, 2016) yakni:

1. Menjalankan *Backup & Recovery Data* berkelanjutan
2. Penggunaan *Backup Tape* dan Penjadwalan *Backup*
3. Penggunaan *Backup Assist* dalam basis data
4. Penyusunan SOP penanganan *Backup & Recovery*
5. Simulasi *recovery* yang melibatkan staf *backup* dalam mencapai RTO
6. Penerapan rotasi *backup tape*
7. Pembangunan *data center*

Pada penelitian ini penyusunan dokumen DRP menggunakan kerangka kerja NIST 800-34 yang merupakan dokumen standarisasi dirilis oleh *National Institute of Standards and Technology* NIST), dengan beberapa tahapan yang dimulai dengan Penetapan Permasalahan dan Tujuan; Pengumpulan Data melalui Observasi, Wawancara dan Studi Lapangan; Penentuan dan Identifikasi Aset, *Risk Assessment;* dan Penyusunan Disaster Recovery Plan (DRP). Sehingga dengan adanya DRP ini, dapat meminimalisir maupun memitigasi dampak yang terjadi terutama ketika sistem dalam kondisi kritis setelah terjadi bencana

A. Identifikasi Permasalahan

Berdasarkan latar belakang yang telah dijelaskan di atas, identifikasi masalah dalam penelitian ini adalah:

1. Bagaimana potensi kerentanan yang terjadi dalam SIAK UMMI melalui *risk assessment* yang dilakukan pada tahapan perancangan *Disaster Recovery Plan*
2. Belum adanya dokumentasi *Disaster Recovery Plan* berupa strategi dalam menangani ancaman yang mungkin terjadi dalam SIAK UMMI
3. Mengimplementasikan kerangka kerja NIST 800-34 dalam perancangan dokumen *Disaster Recovery Plan* pada SIAK UMMI

B. Rumusan Masalah

Berdasarkan identifikasi permasalahan yang diuraikan di atas, maka rumusan masalah dalam penelitian ini adalah "Bagaimana Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan *Disaster Recovery Plan* pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi".

C. Batasan Masalah

Untuk membatasi penelitian agar fokus dan terarah, maka diperlukan ruang lingkup sebagai berikut:

1. Penelitian ini dilakukan di Universitas Muhammadiyah Sukabumi dan berfokus pada Sistem Informasi Akademik
2. Kerangka Kerja yang digunakan dalam perancangan *Disaster Recovery Plan* adalah dengan 800-34
3. Penelitian ini menghasilkan luaran berupa dokumen *Disaster Recovery Plan* berupa strategi recovery yang dihasilkan melalui *Risk Assessmen* pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi

2. TINJAUAN PUSAKA

A. NIST 800-34

Kerangka kerja NIST 800-34 dirilis oleh *National Institute of Standards and Technology* (NIST) yang di dalamnya memuat pedoman dalam penyusunan *Contingency Planning* atau rencana penanganan darurat. Aspek tahapan dalam kerangka kerja NIST 800-34 hingga dihasilkan dokumen *Disaster Recovery Plan* (DRP) pada gambar 1:

Gambar 1. Kerangka Kerja NIST 800-34
(Sumber: NIST 800-34 *Framework*)

Kerangka Kerja NIST SP 800-34 memuat beberapa tahapan prosedur seperti *Business Impact Analysis* (BIA), *Business Continuity Plan* (BCP), yang menjadi landasan dalam perancangan *Disaster Recovery Plan (DRP)* (NIST, 2020).

B. *Business Impact Analysis*

Business Impact Analysis (BIA) digunakan untuk mengevaluasi proses kritis (dan komponen TI yang mendukungnya) dan untuk menentukan waktu

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

pemulihan, prioritas, sumber daya dan ketergantungannya (Muhaemin, 2018). BIA melihat aspek dampak yang terjadi terhadap berjalannya sistem dalam mendukung proses bisnis, dimana terdapat 3 tahapan utama yakni:

1. Menentukan Misi/Bisnis Proses yang akan dianalisis
2. Mengidentifikasikan sumber daya
3. Mengidentifikasikan tingkatan pemulihan atau prioritas sumber daya dalam pemulihan sistem

C. *Disaster Recovery Plan*

Disaster Recovery Plan merupakan upaya penyelamatan data serta infrastruktur yang dimiliki agar tetap berjalan sebagaimana mestinya (Wicaksono, 2010). DRP adalah rencana yang berfokus pada sistem informasi yang dirancang untuk memulihkan pengoperasian sistem target, aplikasi, atau infrastruktur fasilitas komputer di lokasi alternatif setelah keadaan darurat (Swanson, et al, 2010).

Dalam perancangan DRP perlu memperhatikan aspek terkait di dalamnya, antara lain strategi apa yang digunakan dalam pemulihan aset IT/IS, teknologi apa yang digunakan pada masing-masing IT/IS dan bagaimana SDM yang dilibatkan dalam pelaksanaan kegiatan (Agung, 2019).

D. *Risk Assessment*

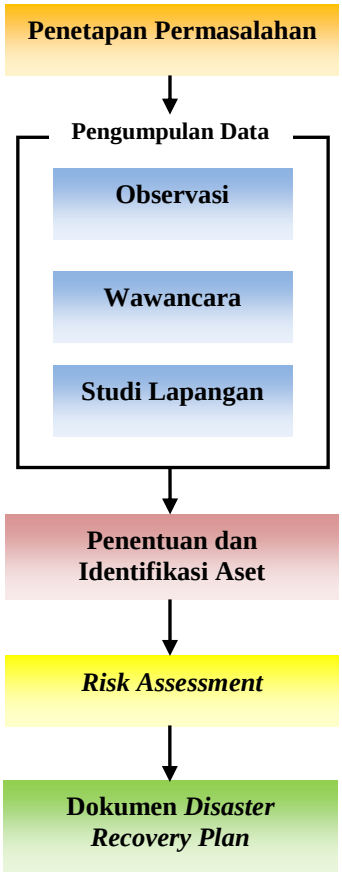
Risk Assessment merupakan bagian dari tahapan dalam manajemen resiko. Tujuan dengan adanya *risk management* ini adalah mengetahui potensi resiko/dampak yang akan terjadi dan bagaimana terhadap proses bisnis serta mengidentifikasi apa saja strategi yang akan mengurangi resiko/dampak tersebut.

Tujuan dari *Risk Assessment* adalah melihat gambaran dari seberapa besar dampak yang akan dialami oleh organisasi jika ancaman terjadi yang menyebabkan kegagalan maupun terhambatnya suatu proses bisnis (CDA, 2013). Ada 2 metode yang dapat dilakukan dalam *risk assessment*, yaitu:

1. Metode kualitatif
   Dilakukan dengan melakukan perkiraan terhadap biaya yang akan ditanggung oleh suatu organisasi sebagai akibat dari risiko yang diterima dengan membuat patokan terlebih dahulu. Asesmen resiko dilakukan dengan pemberian kategori nilai, yakni rendah, sedang dan tinggi
2. Metode kuantitatif
   Metode kuantitatif dilakukan dengan melakukan perhitungan matematis dengan mengakumulasi Nilai risiko berdasarkan nilai ancaman, nilai aset dan nilai analisis dampak bisnis.

3. METODE PENELITIAN

Metode yang dilakukan dalam penelitian ini terdapat pada gambar 2 di bawah ini:



Gambar 2. Metodologi Penelitian

Secara garis besar, tahapan dalam penelitian ini mengikuti kerangka kerja NIST 800-34. Di dalam pengumpulan data dilakukan dengan 3 tahapan sebagai berikut:

A. Observasi

Observasi dilakukan dengan mengamati langsung bagaimana berjalannya SIAK UMMI, dengan melihat user/aktor berinteraksi dengan sistem, bagaimana prosedur-prosedur mendasar yang digunakan di dalam sistem, bagaimana penanganan dasar sistem ketika terjadi serangan, data dan informasi penting apa sajakah yang menjadi prioritas dalam penanangan dan mitigasi bencana. Informasi yang dihasilkan dalam observasi ini menjadi landasan awal dalam kegiatan analisis selanjutnya

B. Wawancara

Merupakan kegiatan diskusi mendalam kepada beberapa pihak, antara lain operator SIAK UMMI, programmer dan analis, serta user yang terdiri dari Ketua Program Studi, Dosen maupun Mahasiswa. Beberapa pertanyaan yang diajukan dalam wawancara seperti terkait bagaimana jalannya sistem dan

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

peranan *stakeholder* di dalamnya, selama ini apa saja yang dilakukan ketika terjadi bencana yang disebabkan oleh *cyber attack by human caused* maupun bencana alam *(force majeur)*, bagaimana langkah preventif yang dilakukan dalam upaya pencegahan maupun memitigasi bencana.

C. Studi Lapangan

Studi lapangan dilakukan dengan melihat dokumen-dokumen apa saja terkait dengan SIAK UMMI, *blueprint* struktur sistem SIAK UMMI maupun topologi jaringan yang terkait dengan sistem

Selanjutnya menentukan dan mengidentifikasi aset yang terdiri dari Perangkat Lunak, Perangkat Keras, data dan file, dokumen serta jaringan. Dalam tahapan ini dilakukan analisis sub sistem yang terintegrasi dengan masing-masing unit kerja/ departemen. Sehingga dihasilkan penjabaran keterhubungan aset terhadap masing-masing unit kerja/ departemen.

Risk Assessment diawali dengan mengidentifikasi ancaman, baik yang sudah terjadi maupun potensi ancaman yang akan terjadi. Kemudian ancaman tersebut diberikan penilaian berdasarkan 3 aspek, yakni *Likelihood, Restoration Time,* dan *Predictability*. Dan yang terakhir diurutkan berdasarkan penilaian resiko terbesar hingga terkecil

Dokumentasi DRP disusun berdasarkan ancaman yang sudah diidentifikasi dan diberi skala penilaian dalam *risk assessment.* Dalam penyusunan dokumentasi DRP juga dilakukan penilaian terhadap aset berdasarkan 3 aspek yakni *Necessity, Recoverability, Replaceability* yang dikombinasikan dengan bobot persentasi penilaian sub sistem SIAK UMMI, sehingga dihasilkan skala prioritas berdasarkan subsistem prioritas teratas hingga terbawah. Dalam tahapan ini juga dihasilkan strategi terhadap ancaman dari masing-masing sub sistem yang ada dalam SIAK UMMI.

4. HASIL DAN PEMBAHASAN

A. Modul SIAK UMMI

SIAK UMMI terdiri dari 6 modul sub sistem yang mengakomodir kegiatan akademik mahasiswa, dosen dan pimpinan. Berikut modul detil dari SIAK UMMI ditunjukkan pada tabel 1

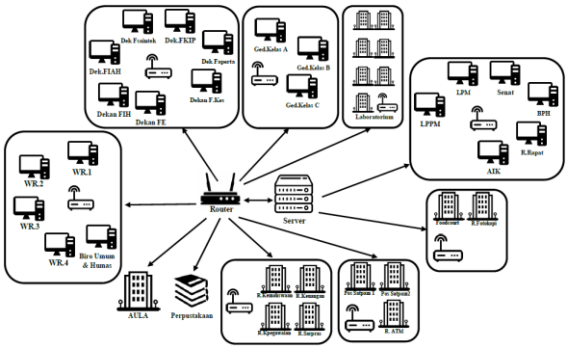
Tabel 1. Modul SIAK UMMI

No	Sub Sistem	Proses
1	Sistem Pengisian KRS	- Penginputan Data Mahasiswa - Pengisian Mata Kuliah - Validasi Pengambilan KRS oleh Dosen - Penyetujuan KRS oleh Dosen - KRS Disetujui
2	Sistem Pembimbingan Akademik Mahasiswa	- Ploting DPA oleh Fakultas - DPA melakukan penjadwalan Bimbingan Akademik melalui Sistem - Mahasiswa Bimbingan menerima jadwal Bimbingan - Pelaksanaan Jadwal bimbingan *offline* yang divalidasi secara *online* dengan mengisi hasil resume kegiatan, temuan dan solusi - Pelaksanaan Pembimbingan Akademik dilaksanakan minimal 3 kali/ semester - Pembimbingan yang bersifat insidentil diinput oleh mahasiswa YBS yang akan melakukan pembimbingan dengan DPA
3	Sistem penilaian mahasiswa	- Dosen membuka mata kuliah yang diampu - Dosen menginput data nilai mahasiswa berdasarkan mata kuliah yang diampu - Sistem akan men-*generate* nilai mahasiswa tersebut masuk predikat A / B / C / D / E
4	Sistem Keuangan Mahasiswa	- Fakultas mendata pembayaran mahasiswa - Tunggakan maupun pelunasan otomatis berubah sesuai dengan status pembayaran dengan pihak ketiga (Bank) - Untuk mahasiswa yang masih memiliki tunggakan, maka mahasiswa tersebut tidak bisa melakukan penginputan KRS
5	Sistem PMB	- Calon mahasiswa mendaftar pada akun siak.ummi.ac.id dengan mengisi data diri pada formulir pendaftaran - Calon mahasiswa mendapatkan token pembayaran, yang harus diinput dalam proses pembayaran dengan pihak bank - Aktivasi akun oleh calon mahasiswa setelah melakukan pembayaran - Calon mahasiswa mendapatkan nomor peserta ujian dan tanggal pelaksanaan ujian
6	Sistem Administrasi Fakultas	Data terkait fakultas yang terdiri dari data mahasiswa, data mata kuliah, data program studi, data dosen

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

B. Topologi Jaringan UMMI

Jaringan UMMI terdiri dari 10 area yang dapat dilihat pada gambar 3 berikut :



Gambar 3. Topologi Jaringan UMMI

Keterangan gambar 3 pada tabel 2 :

Tabel 2. Keterangan Gambar Topologi Jaringan UMMI

No Area	Keterangan	No Area	Keterangan
1	Rektorat	5	Aula
	Biro Umum dan Humas	6	Ruang Kemahasiswaan
	WR 1		Bagian Kepegawaian
	WR 2		Bagian Keuangan
	WR 3		Bagian Sarana dan Prasarana
	WR 4	7	Pos Satpam 1
2	Dekan F.Saintek		Pos Satpam 2
	Dekan FIAH		Ruang ATM
	Dekan FIH	8	Perpustakaan
	Dekan FE	9	Ruang LPPM
	Dekan F Kes		Ruang LPM
	Dekan FKIP		Ruang Rapat
	Dekan Faperta		Ruang AIK
3	Gedung Kelas A		Ruang Senat
	Gedung Kelas B		Ruang BPH
	Gedung Kelas C	10	Foodcourt
4	Gedung Lab F.Saintek		Ruang fotokopi
	Gedung Lab FIAH		
	Gedung Lab FIH		
	Gedung Lab FE		
	Gedung Lab F Kes		
	Gedung Lab FKIP		
	Gedung Lab Faperta		

C. Identifikasi Aset

Terdapat 5 aset utama yang terintegrasi dengan SIAK UMMI, yakni Perangkat Lunak, Perangkat Keras, Data/File, Dokumen dan Jaringan. Secara terperinci aset dan sub sistem yang terkait terdapat dalam tabel 3 :

Tabel 3. Identifikasi aset dan Sub Sistem yang terkait

No	Jenis	ID	Daftar Aset	Proses Bisnis Terkait
1	Perangkat Lunak	SW-UMMI-01	Windows Operating System	Sistem Pengisian KRS; Sistem Pembimbing an Akademik Mahasiswa; Sistem Penilaian Mahasiswa; Sistem Keuangan Mahasiswa; Sistem PMB; Sistem Administrasi Fakultas
		SW-UMMI-02	Windows Server	
		SW-UMMI-03	Web Browser	
		SW-UMMI-04	Microsoft Office	
		SW-UMMI-05	SQL Server	
		SW-UMMI-06	Antivirus	
2	Perangkat Keras	HW-UMMI-01	Komputer Gedung Lab F.Saintek	Sistem Pengisian KRS; Sistem Pembimbing an Akademik Mahasiswa; Sistem Penilaian Mahasiswa; Sistem Keuangan Mahasiswa; Sistem PMB; Sistem Administrasi Fakultas
		HW-UMMI-02	Printer dan periferal Gedung Lab F.Saintek	
		HW-UMMI-03	Komputer Gedung Lab FIAH	
		HW-UMMI-04	Printer dan periferal Gedung Lab FIAH	
		HW-UMMI-05	Komputer Gedung Lab FIH	
		HW-UMMI-06	Printer dan periferal Gedung Lab FIH	
		HW-UMMI-07	Komputer Gedung Lab FE	
		HW-UMMI-08	Printer dan periferal Gedung Lab FE	
		HW-UMMI-09	Komputer Gedung Lab F Kes	
		HW-UMMI-10	Printer dan periferal Gedung Lab F Kes	
		HW-UMMI-11	Komputer Gedung Lab FKIP	
		HW-UMMI-12	Printer dan periferal Gedung Lab FKIP	
		HW-UMMI-13	Komputer Gedung Lab Faperta	
		HW-UMMI-14	Printer dan periferal Gedung Lab Faperta	
		HW-UMMI-15	Komputer Ruang Kemahasiswaan	Sistem PMB
		HW-UMMI-16	Printer dan periferal Ruang Kemahasiswaan	
		HW-UMMI-17	Komputer Bagian Kepegawaian	Sistem Administrasi Fakultas; Sistem Pembimbing an Akademik Mahasiswa
		HW-UMMI-18	Printer dan periferal Bagian Kepegawaian	
		HW-UMMI-19	Komputer Bagian Keuangan	Sistem keuangan Mahasiswa
		HW-UMMI-20	Printer dan periferal Bagian Keuangan	
		HW-UMMI-21	Komputer Bagian Sarana dan Prasarana	Sistem Administrasi Fakultas
		HW-UMMI-22	Printer dan periferal Bagian Sarana dan Prasarana	

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

No	Jenis	ID	Daftar Aset	Proses Bisnis Terkait
		HW-UMMI-23	Komputer Perpustakaan	Sistem PMB
		HW-UMMI-24	Printer dan periferal Perpustakaan	
		HW-UMMI-25	Komputer Ruang LPPM	Sistem Penilaian Mahasiswa
		HW-UMMI-26	Printer dan periferal Ruang LPPM	
		HW-UMMI-27	Komputer Ruang LPM	Sistem Administrasi Fakultas; Sistem PMB
		HW-UMMI-28	Printer dan periferal Ruang LPM	
		HW-UMMI-29	Komputer Ruang AIK	Sistem Penilaian Mahasiswa
		HW-UMMI-30	Printer dan periferal Ruang AIK	
		HW-UMMI-31	Komputer Ruang BPH	Sistem Pengisian KRS; Sistem Pembimbingan Akademik Mahasiswa; Sistem Penilaian Mahasiswa; Sistem Keuangan Mahasiswa; Sistem PMB; Sistem Administrasi Fakultas
		HW-UMMI-32	Printer dan periferal Ruang BPH	
3	Data/ File	F-UMMI-01	Data Mahasiswa	Sistem Pengisian KRS; Sistem Pembimbingan Akademik Mahasiswa; Sistem Penilaian Mahasiswa; Sistem Keuangan Mahasiswa; Sistem PMB
…	…	…	…	…
5	Jaringan	AR-UMMI 10	Pos Satpam	

Dari aset yang sudah didata tersebut, dilakukan asesmen untuk menentukan skala prioritas, dengan menggunakan penilaian dengan parameter *Necessity*, *Recoverability*, *Replaceability* sehingga menghasilkan nilai skala prioritas / *Priority Value.* Penilaian dilakukan dengan skala 1 – 5, dengan nilai terendah 1 dan nilai tertinggi 5. Berikut hasil Asesmen dari penilaian aset pada tabel 4 dan tabel 5:

Tabel 4. Assesmen Skala Prioritas Aset

No	Elemen	Necessity	Recover ability	Replace ability	Priority Value
1	Perangkat Keras	2.44	2.08	2.85	**2.45**
2	Perangkat Lunak	2.71	1.71	1.71	**2.00**
3	Jaringan	2.06	2.00	2.00	**2.02**
4	Data	2.84	2.88	2.00	**2.57**

Tabel 5. Skala Prioritas Aset berdasarkan nilai terbesar

No	Elemen	Necessity	Recover ability	Replace ability	Priority Value
1	Data	2.84	2.88	2.00	2.57
2	Perangkat Keras	2.44	2.08	2.85	2.45
3	Jaringan	2.06	2.00	2.00	2.02
4	Perangkat Lunak	2.71	1.71	1.71	2.00

D. *Risk Assessment*

Risk Assessment dilakukan dengan menilai 3 aspek yakni *Likelihood*, *Restoration Time*, dan *Predictability* yang secara rinci dapat dilihat pada tabel 6 dan tabel 7 berikut:

Tabel 6. Deskripsi Atribut *Risk Assessment*

No	Keterangan	Deskripsi
1	Likelihood (0 - 10)	Nilai yang semakin tinggi akan menunjukkan bahwa ancaman akan semaki mungkin terjadi
2	Restoration Time (0 - 10)	Nilai yang semakin tinggi akan menunjukkan semakin lamanya waktu yang diperlukan mengembalikan sistem beroperasi seperti sedia kala
3	Predictability (0 - 3)	Nilai yang semakin tinggi akan menunjukkan semakin sulitnya memprediksi datangnya ancaman, sehingga semakin sedikit waktu dan usaha yang bisa dialokasikan untuk menghindarinya

Tabel 7. Deskripsi Penilaian Atribut

No	Kolom		
	Likelihood	Restoration Time	Predictability
0	Tidak Mungkin Terjadi	Tidak Ada	Dapat diprediksi dengan pasti bahka sebelum bencana terjadi
1	Terjadi > 5 tahu sekali	1 - 4 menit	Prediksi dapat dilakukan sebelum bencana terjadi, namun dengan tingkat kepercayaan yang rendah
2	Terjadi 2 - 5 tahun sekali	5 menit - 1 jam	Prediksi hanya dapat dilakukan setelah terjadi tanda-tanda awal bencana
3	Terjadi 1 - 2 tahun	1 - 6 jam	Tidak dapat diprediksi
4	Terjadi 6 - 12 bulan sekali	6 - 12 jam	
5	Terjadi 2 - 6 bulan sekali	12 - 24 jam	
6	Terjadi 1 - 2 bulan sekali	1 - 4 Hari	
7	Terjadi 2 - 4 Minggu sekali	5 - 9 Hari	
8	Terjadi 1 - 2 Minggu sekali	10 - 14 Hari	
9	Terjadi 1 - 7 Hari sekali	15 - 30 Hari	
10	Terjadi beberapa kali dalam 24 jam	Membutuhkan waktu > 1 bulan	

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

Ancaman yang terjadi maupun potensi ancaman yang akan terjadi dilakukan dengan melihat kondisi lapangan (observasi), wawancara kepada pihak terkait dan melihat dokumen-dokumen histori maupun catatan kerusakan. Dari hasil pengamatan yang dilakukan, terdapat lebih dari 20 ancaman yang terjadi yang kemudian dikelompokan ke dalam 9 ancaman secara garis besar. Tabel 8 menunjukkan identifikasi ancaman pada SIAK UMMI:

Tabel 8. Identifikasi Ancaman SIAK UMMI

ID	Jenis	Ancaman	Penyebab	Dampak
01	Banjir	1 Merusak Gedung Perkantoran 2 Merusak Sarana 3 Merusak Prasarana 4 Merusak Komputer dan Jaringan	1 Drainase yang kurang 2 Tersumbat saluran air 3 Hujan Terus menerus	Kegiatan operasional terpaksa dihentikan bila terkena sistem komputer dan jaringan
02	Petir/Badai	1 Merusak Jaringan *Local Area Network* (LAN) 2 Merusak Komputer Client 3 Merusak Periferal dan perangkat yang terhubung dalam jaringan listrik 4 Merusak Komputer Server	1 Kejadian Alam	
03	Gempa Bumi	1 Merusak Gedung Perkantoran 2 Merusak Sarana 3 Merusak Prasarana	1 Kejadian Alam	Menghentikan kegiatan operasional
04	Kebakaran	1 Merusak Gedung Perkantoran 2 Merusak Sarana 3 Merusak Prasarana	1 Hubungan Arus Singkat 2 Kelalaian Manusia 3 Kebakaran dari Eksternal	
05	Gang guan server	1 *System Crash* 2 *System Error* 3 *Undefined Error* 4 *Unstoppable Looping*	1 Traffic Data tinggi 2 Server Rusak 3 Serangan Virus/ Worm/ Malware	Memperlambat kinerja Sistem, Dapat menghentikan kegiatan operasional, Merusak Komputer
06	Gang guan Listrik	1 *System Crash* 2 *System Error* 3 *Undefined*	1 Tegangan Naik Turun/ Tidak Stabil 2 Listrik Padam 3 Kelalaian Manusia	
07	Serangan *Hacker/ Cybercrime*	1 Serangan Hacker 2 SQL Injection 3 Defacing 4 DDoS 5 Sniffing 6 Backdoor	1 Serangan Virus/ Worm/ Malware 2 Tidak ada Antivirus 3 Antivirus belum update 4 Single Server 5 System Vulnerability	
08	Kesalahan Manusia *(Human Error)*	1 Output dari sistem tidak valid 2 Redudansi Data 3 System Crash 4 System Error 5 Undefined Error 6 Unstoppable Looping	1 Kesalahan Penginputan Data 2 Kesalahan Prosedur 3 Kesalahan Input Password 4 Kelalaian Manusia yang merusak komputer & Sistem	Memperlambat kinerja Sistem, Dapat menghentikan kegiatan operasional
09	Serangan Virus, malware, Worm	1 Output dari sistem tidak valid 2 *System Crash* 3 *System Error* 4 *Undefined Error* 5 *Unstoppable Looping*	1 Serangan Virus/ Worm/ Malware 2 Tidak ada Antivirus 3 Antivirus belum update 4 Single Server 5 System Vulnerability	

Setelah dilakukan indentifikasi ancaman, tahapan berikutnya adalah proses *risk assessment* dengan penilaian yang dijelaskan pada tabel Deskripsi Penilaian Atribut. Berikut hasil *Risk Assessment* ditunjukkan pada tabel 9 :

Tabel 9. Hasil *Risk Assessment* SIAK UMMI

ID	Jenis	Ancaman	Likehood	Restoration Time	Predictability	Score
01	Banjir	1 Merusak Gedung Perkantoran 2 Merusak Sarana 3 Merusak Prasarana 4 Merusak Komputer dan Jaringan	2	9	1	12
02	Petir/Badai	1 Merusak Jaringan *Local Area Network* (LAN)	6	6	0	12

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

ID	Jenis	Ancaman	Likehood	Restoration Time	Predictability	Score
		2 Merusak Komputer Client 3 Merusak Periferal dan perangkat yang terhubung dalam jaringan listrik 4 Merusak Komputer Server				
03	Gempa Bumi	1 Merusak Gedung Perkantoran 2 Merusak Sarana 3 Merusak Prasarana	1	10	3	14
04	Kebakaran	1 Merusak Gedung Perkantoran 2 Merusak Sarana 3 Merusak Prasarana	1	10	2	13
05	Kelambatan Server / serverdown	1 *System Crash* 2 *System Error* 3 *Undefined Error* 4 *Unstoppable Looping*	10	3	0	13
06	Gangguan Listrik Padam	1 *System Crash* 2 *System Error* 3 *Undefined Error* 4 *Unstoppable Looping*	5	4	0	9
07	Serangan *Hacker/ Cybercrime*	1 Serangan Hacker 2 SQL Injection 3 Defacing 4 DDoS 5 Sniffing 6 Backdoor	7	5	1	13
08	Kesalahan Manusia *(Human Error)*	1 Output dari sistem tidak valid 2 Redudansi Data 3 System Crash 4 System Error 5 Undefined Error 6 Unstoppable Looping	7	3	1	11
09	Serangan Virus, malware, Worm	1 Output dari sistem tidak valid 2 *System Crash* 3 *System Error* 4 *Undefined Error* 5 *Unstoppable Looping*	7	5	0	12

Dari hasil *Risk Assessment* tersebut, selanjutnya adalah pengurutan dari penilaian terbesar hingga terendah sehingga dapat diketahui prioritas ancaman mana yang harus didahulukan. Tabel 10 menunjukkan penilaian *Risk Assessmen* berdasarkan penilaian terbesar hingga terendah:

Tabel 10. Penilaian *Risk Assessment* berdasarkan urutan terbesar-terendah

ID	Jenis	Likehood	Restoration Time	Predictability	Score
03	Gempa Bumi	1	10	3	14
04	Kebakaran	1	10	2	13
05	Kelambatan Server / serverdown	10	3	0	13
07	Serangan *Hacker/ Cybercrime*	7	5	1	13
01	Banjir	2	9	1	12
02	Petir/Badai	6	6	0	12
09	Serangan Virus, malware, Worm	7	5	0	12
08	Kesalahan Manusia *(Human Error)*	7	3	1	11
06	Gangguan Listrik Padam	5	4	0	9

E. *Business Impact Analysis*

Business Impact Analysis (BIA) dilakukan untuk melihat dampak yang terjadi pada SIAK UMMI dilihat dari ancaman. Berikut ini adalah tabel yang menunjukkan dampak terhadap masing-masing modul yang ada di SIAK UMMI:

Tabel 11. Ancaman Gempa Bumi

No	Sub Sistem	Dampak yang dialami	Tingkat Dampak
1	Sistem Pengisian KRS	Melumpuhkan Kegiatan Operasional	**3**
2	Sistem Pembimbingan Akademik Mahasiswa	Melumpuhkan Kegiatan Operasional	**3**
3	Sistem penilaian mahasiswa	Melumpuhkan Kegiatan Operasional	**3**
4	Sistem Keuangan Mahasiswa	Melumpuhkan Kegiatan Operasional	**3**
5	Sistem PMB	Melumpuhkan Kegiatan Operasional	**3**
6	Sistem Administrasi Fakultas	Melumpuhkan Kegiatan Operasional	**3**

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

Tabel 12. Ancaman Kebakaran

No	Sub Sistem	Dampak yang dialami	Tingkat Dampak
1	Sistem Pengisian KRS	Melumpuhkan Kegiatan Operasional	**3**
2	Sistem Pembimbingan Akademik Mahasiswa	Melumpuhkan Kegiatan Operasional	**3**
3	Sistem penilaian mahasiswa	Melumpuhkan Kegiatan Operasional	**3**
4	Sistem Keuangan Mahasiswa	Melumpuhkan Kegiatan Operasional	**3**
5	Sistem PMB	Melumpuhkan Kegiatan Operasional	**3**
6	Sistem Administrasi Fakultas	Melumpuhkan Kegiatan Operasional	**3**

Tabel 13. Serangan *Hacker / Cybercrime*

No	Sub Sistem	Dampak yang dialami	Tingkat Dampak
1	Sistem Pengisian KRS	Perubahan Data mahasiswa dan dosen tanpa kendali	**3**
2	Sistem Pembimbingan Akademik Mahasiswa	Kehilangan data historis pembimbingan akademik mahasiswa	**2**
3	Sistem penilaian mahasiswa	Gangguan publikasi nilai dan nilai menjadi tidak kredibel	**3**
4	Sistem Keuangan Mahasiswa	Terjadi perubahan dan manipulasi data yang tidak terkontrol	**3**
5	Sistem PMB	Data mahasiswa baru mengalami perubahan tanpa kendali	**2**
6	Sistem Administrasi Fakultas	Terjadi perubahan dan manipulasi data yang tidak terkontrol	**3**

Tabel 14. Petir/ Badai

No	Sub Sistem	Dampak yang dialami	Tingkat Dampak
1	Sistem Pengisian KRS	Memperlambat Kinerja Sistem	**3**
2	Sistem Pembimbingan Akademik Mahasiswa	Memperlambat Kinerja Sistem	**3**
3	Sistem penilaian mahasiswa	Memperlambat Kinerja Sistem	**3**
4	Sistem Keuangan Mahasiswa	Memperlambat Kinerja Sistem	**3**
5	Sistem PMB	Memperlambat Kinerja Sistem	**3**
6	Sistem Administrasi Fakultas	Memperlambat Kinerja Sistem	**3**

Tabel 15. Serangan Virus, Malware, Worm

No	Sub Sistem	Dampak yang dialami	Tingkat Dampak
1	Sistem Pengisian KRS	Melambatnya proses Pengisian KRS	**2**
2	Sistem Pembimbingan Akademik Mahasiswa	Pembimbingan Akademik sulit dilakukan tepat waktu sesuai agenda yang sudah ditetapkan	**2**
3	Sistem penilaian mahasiswa	Terjadi kelambatan dalam proses penilaian akademik mahasiswa	**3**
4	Sistem Keuangan Mahasiswa	Berpengaruh kepada kinerja keuangan	**3**
5	Sistem PMB	Data mahasiswa baru mengalami perubahan tanpa kendali	**3**
6	Sistem Administrasi Fakultas	Terjadi kelambatan dalam proses administrasi fakultas	**2**

Tabel 16. Gangguan Listrik Padam

No	Sub Sistem	Dampak yang dialami	Tingkat Dampak
1	Sistem Pengisian KRS	Memperlambat Kinerja Sistem	**2**
2	Sistem Pembimbingan Akademik Mahasiswa	Memperlambat Kinerja Sistem	**2**
3	Sistem penilaian mahasiswa	Memperlambat Kinerja Sistem	**2**
4	Sistem Keuangan Mahasiswa	Memperlambat Kinerja Sistem	**3**
5	Sistem PMB	Memperlambat Kinerja Sistem	**2**
6	Sistem Administrasi Fakultas	Memperlambat Kinerja Sistem	**3**

Bila dirata-ratakan secara keseluruhan dari dampak tersebut, masing-masing modul memiliki nilai yang berbeda yang ditunjukkan oleh tabel berikut:

Tabel 17. Rerata dan Bobot Persentasi nilai dampak Modul SIAK UMMI

No	Sub Sistem	Rerata	%
1	Sistem Pengisian KRS	2.33	78%
2	Sistem Pembimbingan Akademik Mahasiswa	1.87	62%
3	Sistem penilaian mahasiswa	2.11	70%
4	Sistem Keuangan Mahasiswa	2.97	99%
5	Sistem PMB	2.56	85%
6	Sistem Administrasi Fakultas	2.67	89%

Dilihat dari rerata nilai tabel di atas, sub sistem yang memiliki dampak terbesar adalah Sistem Keuangan Mahasiswa dengan nilai persentasi 99%, sedangkan sub sistem yang memiliki nilai terendah adalah Sistem Pembimbingan Akademik dengan nilai dampak persentasi 62%.

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

F. *Strategi Recovery* dalam dokumen DRP

Tahapan terakhir dalam penyusunan dokumen DRP adalah pembuatan *strategy recovery*. *Strategy Recovery* disusun berdasarkan aset yang terintegrasi dengan SIAK UMMI berdasarkan ancaman. Sehingga terdapat 9 *Strategy Recovery*, Tabel 18 menunjukkan *Strategy Recovery* terhadap Ancaman Serangan *Hacker / Cybercrime* dan Tabel 19 *Strategy Recovery* terhadap Ancaman Kelambatan Server / *Serverdown*

Tabel 18. *Strategy Recovery* terhadap Ancaman Serangan *Hacker / Cybercrime*

No	Aspek		Strategi
1	Data	1	Instalasi Antivirus
		2	Back up data dilakukan secara berkala
		3	Updating Antivirus Secara berkala
		4	Terdapat form manual sebagai pendamping data digital
2	Perangkat Keras	1	Terdapat petunjuk/ prosedur dalam mengoperasikan sistem
		2	Operator hanya yang berkepentingan langsung terhadap sistem
		3	Dilakukan perawatan dan stok opname secara berkala
3	Jaringan	1	Pengecekan secara berkala
		2	Penggantian Komponen yang rusak
		3	Terdapat manual dan petunjuk penggunaan
4	Perangkat Lunak	1	Terdapat instruksi manual dalam penggunaan software
		2	Operator hanya yang berkepentingan langsung terhadap sistem

Tabel 19. *Strategy Recovery* terhadap Ancaman Kelambatan Server / *Serverdown*

	Aspek		Strategi
1	Data	1	Backup Data rutin harian dan mingguna
		2	Refresh Data
		3	Reload Data
		4	Memory Eficiency
2	Perangkat Keras	1	Terdapat petunjuk/ prosedur dalam mengoperasikan sistem
		2	Operator hanya yang berkepentingan langsung terhadap sistem
		3	Dilakukan perawatan dan stok opname secara berkala
3	Jaringan	1	Pengecekan secara berkala
		2	Perbesar Bandwidth
		3	Terdapat manual dan petunjuk penggunaan
4	Perangkat Lunak	1	Terdapat instruksi manual dalam penggunaan software
		2	Operator hanya yang berkepentingan langsung terhadap sistem

5. KESIMPULAN

Disaster Recovery Plan (DRP) merupakan langkah preventif untuk keberlangsungan suatu sistem terutama dalam menghadapi ancaman. Di dalam penyusunan DRP SIAK UMMI dilakukan dengan beberapa tahapan yang dimulai dengan identifikasi aset, *business process analysis, risk assessment* dan *strategy recovery.* Sehingga dari penelitian ini dihasilkan beberapa kesimpulan, yakni:

1. Dalam identifikasi aset dihasilkan penilaian skala prioritas dengan nilai tertinggi : data sebesar 2.57 dan nilai terendah Perangkat Lunak sebesar 2.00. Identifikasi aset menjadi dasar prioritas mana yang harus didahulukan ketika terjadi ancaman terhadap SIAK UMMI
2. *Risk Assessment* menghasilkan 9 ancaman yang terdiri dari Banjir, Petir/Badai, Gempa Bumi, Kebakaran, Kelambatan Server / *Serverdown*, Gangguan Listrik Padam, Serangan *Hacker (Cybercrime), Human Error* dan Serangan Virus/ Worm/ Malware. Dari ancaman tersebut berdasarkan parameter *Likelihood, Restoriation Time* dan *Predictability* didapatkan Gempa Bumi memiliki nilai tertinggi sebesar 14 dan Gangguan padam Listrik sebesar 9
3. *Business Impact Analysis* (BIA) dilakukan untuk melihat dampak yang terjadi pada SIAK UMMI dilihat dari ancaman. Dari sub sistem SIAK UMMI, sub sistem yang memiliki dampak terbesar adalah Sistem Keuangan Mahasiswa dengan nilai persentasi 99%, sedangkan sub sistem yang memiliki nilai terendah adalah Sistem Pembimbingan Akademik dengan nilai dampak persentasi 62%.
4. *Strategy Recovery* disusun berdasarkan aset yang terintegrasi dengan SIAK UMMI berdasarkan ancaman dimana terdapat 9 *Strategy Recovery* (salah satunya ditunjukkan pada tabel XXX)

DAFTAR PUSTAKA

Siagian, S.H.T., & Effiyaldi. (2018). Analisis dan Perancangan Sistem Informasi Akademik pada STIKES Jambi. *Jurnal Manajemen Sistem Informasi*. Vol 3 (4)

Asriyanik. 2016. Penilaian Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi dengan Menggunakan ISO 27001. *Jurnal SANTIKA: Jurnal Ilmiah Sains dan Teknologi.* Vol 6 (2)

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

Budiarto, R. (2017). Manajemen Risiko Keamanan Sistem Informasi. *Journal of Computer Engineering System and Science*. Vol 2 (2). pp. 48–58.

Yakub. (2012). *Pengantar Sistem Informasi*. Yogyakarta: Graha Ilmu.

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI: http://dx.doi.org/10.30872/jim.v15i2.3724

Rifai, Z., Maydina, A., Kurniawan A. A. (2018). Rancangan Dokumen Disaster Recovery Plan pada IS / IT di Dinas XYZ. *CESS (Journal of Computer Engineering System and Science).* Vol 3 (2).

Agung, M. Z. (2019). Perancangan Disaster Recovery Plan Sistem Informasi Akademik dengan Pendekatan Kerangka Kerja NIST 800-34. *JTERA (Jurnal Teknologi Rekayasa).* Vol 4 (2).

Yulhendri. (2016). Penerapan Business Continuity Plan/ Disaster Recovery Plan pada BUMN dalam Rangka Sustainability: Studi Kasus pada PT. X Wilayah Jakarta Raya. *Jurnal Ilmu Komputer*. Vol 12 (1).

Isa, I. G. T. (2017). Kansei Engineering Approach in Software Interface Design. *Jurnal of Science Innovare*, 1(1), 22-26.

Swanson, M., et all. (2010). *Contingency Planning Guide for Federal Information System*. USA: National Institute of Standards and Technology

NIST. In *Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, version 1.0*, Retrieved From https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf. [Accessed: 20 April 2020]

Wicaksono, S. R. (2010). *Disaster Recovery Planning*. Jakarta: Seribu Bintang.

Muhaemin. (2018). Mengembangkan *Business Continuity Planning* (BCP) dengan Pendekatan Kuantitatif Studi Kasus: Siak – Ditjen Adminduk Kemendagri. *Jurnal Sistem Informasi, Teknologi Informatika dan Komputer*. Vol 9 (1)

Cyber Defense Academy. (2013). *IT Risk Management*. Jakarta : Diklat Teknis Kementerian Sekretariat Negara.