BAB IV
HASIL DAN PEMBAHASAN

4.1 E-LKP (*Electronic*-Laporan Kinerja Pegawai)

Kinerja adalah hasil seseorang secara keseluruhan selama periode tertentu di dalam melaksanakan tugas, seperti standar hasil kerja, target atau sasaran atau kriteria yang telah ditentukan terlebih dahulu dan telah disepakati bersama (Rivai & Basri, 2004, p.14). Kinerja karyawan adalah perbandingan hasil yang dicapai dengan peran serta tenaga kerja persatuan waktu (lazimnya per jam) (Kusriyanto, 2006, p.9). Kinerja karyawan adalah hasil pekerjaan yang mempunyai hubungan kuat dengan tujuan strategis, kepuasan konsumen dan memberikan kontribusi ekonomi (Amstrong dan Baron, 2012, p.7).

Berdasarkan teori di atas, maka dapat disimpulkan bahwa kinerja pegawai adalah hasil kerja baik dari kualitas maupun kuantitas yang dicapai pegawai per satuan periode waktu pada pelaksanaan tugas kerjanya seseorang sesuai dengan tanggung jawab yang diberikan kepadanya.

E-LKP adalah sebutan UIN Raden Fatah untuk laporan kinerja pegawai yang diakses secara online dan berbasis web. Sistem informasi E-LKP UIN Raden Fatah Palembang tercipta untuk menghitung kinerja pegawai dimana hasil perhitungannya akan diimplementasikan untuk remunerasi dan hasil dari perhitungan kinerja ini dapat dijadikan acuan untuk membayar tunjangan para pegawai. E-LKP ini baru terbentuk sekitar 2 tahun yang lalu (2017) dan baru 2 kali direvisi atau baru 2 kali ada pengembangan, pengembangan itu tergantung dari peraturan kementrian. E-LKP ini adalah laporan kinerja pegawai dapat diakses secara online dan hanya pegawai yang dapat remunerasi beserta admin pada UIN

Raden Fatah saja yang bisa login atau menggunakannya. Fungsi E-LKP ini adalah untuk menghitung kinerja pegawai dan absensi pegawai. Tujuan E-LKP ini adalah untuk mengetahui kinerja pegawai. Pengguna E-LKP ini berkisar 300 orang karena setiap bulannya ada penambahan bahkan pengurangan, tergantung dari pegawai yang meninggal ataupun cuti pindah (wawancara dengan Kemas Jumansyah HM, S.SI., 26 April 2019).

4.2 Aset Kritis E-LKP UIN Raden Fatah Palembang

Berikut ini adalah aset kritis pada E-LKP UIN Raden Fatah Palembang:

a. *Hardware* : Server, *Hardisk*, UPS, *Core Switch*, LAN, dan Router.
b. *Software* : *Firewall*, OS Server, Apache, *MySQL*, Php dan Ativirus.
c. Data : Data karyawan, data nilai capaian, data sasaran kinerja harian dan data kinerja bulanan.
d. *Network* : Jaringan internet dan intranet.
e. People : Admin IT dan jaringan, admin sistem, *software development*, data center, IT *support* dan admin database.

4.3 Hasil

Penelitian ini menerapkan beberapa seluruh tahapan yang ada pada OCTAVE. Proses penilaian risiko sesuai dengan tahapan risiko, dimana tahapan risiko di dapat dari FMEA. Berikut hasil dari langkah-langkah OCTAVE.

4.3.1 Menentukan Aset Berdasarkan Profil Ancaman

Dari fase I OCTAVE yang dibagi jadi 5 proses yaitu mendata aset kritis, mengidentifikasi kebutuhan keamanan aset kritis, mengidentifikasi ancaman aset kritis, mendata keamanan yang sudah diterapkan dan mengidentifikasi kelemahan

perusahaan. Berikut ini merupakan tabel penelitian Aset Berdasarkan Profil Ancaman berdasarkan hasil wawancara (terlampir).

Tabel 4.1 Aset Berdasarkan Profil Ancaman

Aset	Kerentanan	Ancaman	Penyebab
Hardware Server CCTV	Kurangnya pemeliharaan secara rutin	Kerusakan peralatan/media	Perawatan yang tidak teratur
	Kerentanan terhadap kelembapan, debu dan kotoran	Korosi, berembun, dan debu pada hardware	Kerusakan fisik pada server
	Kerentanan terhadap nilai informasi pada server	Pencurian data	Kurangnya pengamanan organisasi
	Kerentanan terhadap voltase yang bervariasi Turunnya daya listrik	Hilangnya pasokan listrik	Kerusakan arus listrik (terjadi lonjakan)
	Supply listrik yang tidak stabil	Hilangnya pasokan listrik	Pemadaman listrik
	Beban kerja server yang tinggi	Server lemot	Spesifikasi server yang sudah tidak memenuhi kebutuhan organisasi
	Pertambahan kapasitas data dalam pemrosesan	Kinerja server menjadi berat	Kapasitas backup data yang sudah tidak memenuhi kebutuhan organisasi
Data sasaran kinerja harian, sasaran kinerja bulanan	Data terlalu sering diupdate	Duplikat data	Kesalahan dalam penginputan dan penghapusan data
Data karyawan, nilai capaian, sasaran kinerja bulanan dan sasaran kinerja harian	Kurangnya backup secara rutin	Data hilang	Tidak adanya prosedur backup ketika server down
Data karyawan	Penempatan hak akses yang salah	Penyalahgunaan wewenang pada hak akses yang dimiliki	Kurangnya mekanisme pemantauan

Data karyawan, nilai capaian, sasaran kinerja bulanan dan sasaran kinerja harian	Terlalu banyak data yang diinputkan	Database penuh	Server down
	Software tidak diupdate	Pembobolan data	Kesalahan pada fungsional software
	Jaringan internet kurang optimal	Data korup	Aplikasi down
Perangkat Jaringan (*network*)	Kualitas jaringan yang kurang baik	Terputusnya koneksi	Kerusakan pada kabel
	Jalur komunikasi yang tidak dilindungi (disadap)	Penggunaan data yang ilegal	Kesalahan dalam melakukan konfigurasi
	Jalur komunikasi yang tidak dilindungi	Penyadapan informasi	Tidak ada pengamanan di sistem internal
	Bencana alam dan kejadian yang tidak terduga (banjir, gempa)	Koneksi terputus	Kerusakan pada infrakstruktur jaringan
	Sumber daya manusia yang tidak kompeten	Kesalahan pengguna	Kesalahan dalam melakukan konfigurasi
	Peletakan kabel yang sembarangan (tidak ada pelindung kabel)	Koneksi terputus	Kerusakan pada kabel
People : Pengguna dan admin	Ketidakhadiran karyawan	Penyalahgunaan wewenang	Adanya share login atau password
	Kurangnya pelatihan peningkatan keamanan	Kesalahan penggunaan	Kurangnya pelatihan prosedur penggunaan TI
	Kurangnya kesadaran akan keamanan	Kesalahan penggunaan	Kurangnya sosialisasi tentang keamanan komputer
	Kurangnya mekanisme pemantauan terkait keamanan informasi	Pengolahan data ilegal	Pengolahan data ilegal oleh karyawan
	Karyawan yang kurang teliti	Kesalahan penginputan data	Kesalahan penginputan data
	Pelatihan keamanan yang tidak cukup	Penyalahgunaan wewenang	Tidak keluar atau logout ketika meninggalkan komputer

	Kurangnya pengetahuan tentang keamanan	Penyalahgunaan wewenang	Password disimpan pada dekstop komputer
	Kurangnya kesadaran akan keamanan	Penyalahgunaan wewenang pada akses yang dimiliki	Tidak ada penggantian password secara berkala
	Kurangnya dokumentasi untuk penggunaan sistem	Kesalahan pengguna	Kurangnya dokumentasi untuk penggunaan sistem untuk pengguna baru
	Kurangnya kesadaran akan keamanan	Penyalahgunaan aplikasi	Pengguna mengetahui kelemahan pada aplikasi

Dari tabel 4.1 didapatkan penyebab dari kerentanan/kelemahan yang menjadi ancaman bagi 6 kategori aset kritis pada E-LKP UIN Raden Fatah Palembang dan dapat ditarik kesimpulan sebagai berikut:

a. Aset informasi yang kritis yakni data karyawan dan data nilai capaian karena apabila aset informasi ini disalahgunakan atau hilang dapat mengganggu proses penginputan data pencairan dana karyawan.
b. Kebutuhan keamanan / persyaratan dan keamanan yang sudah diterapkan.
    a) Kerahasiaan : Memastikan bahwa hanya orang yang berwenang yang memiliki akses ke informasi. Keamanan yang sudah diterapkan dalam hal ini seperti adanya CCTV pada ruang server, *Door Acces* dan penggantian password secara berkala oleh pengguna dan admin.
    b) Integritas : Memastikan bahwa aset informasi tetap dalam kondisi yang dimaksudkan oleh pemilik dan untuk tujuan yang dimaksudkan oleh pemiliknya. Keamanan yang sudah diterapkan dalam hal ini seperti pemasangan *firewall* dan pembatasan hak akses pada penginputan data.
    c) Ketersediaan : Memastikan bahwa aset informasi tetap dapat diakses oleh pengguna yang berwenang. Keamanan yang sudah diterapkan dalam hal ini

seperti proses backup data secara rutin dan melakukan update sistem operasi secara berkala.

4.3.2 Identifikasi Kerentanan Infrastruktur

4.3.2.1 Komponen Kunci

1. *Hardware :* Server dan *core switch*
2. *Software* : OS Server, dan HARIS (*Human Resources Information System*)
3. *People :* IT *support, server development* dan *Analyst* Jaringan.
4. Data : *Database.*
5. *Network* : Jaringan Internet dan Intranet.

4.3.2.2 Kerentanan Komponen Kunci

1. Server dan *core switch* : serangan DOS, pemadaman listrik dan bencana alam.
2. OS Server : virus dan serangan hacker.
3. IT *support, software development* dan *Analyst* jaringan : *Social enginering.*
4. *Database* : SQL *Injection.*
5. Jaringan : Terputusnya koneksi jaringan.

4.3.3 Mengembangkan Rencana dan Strategi

4.3.3.1 Identifikasi Risiko

Berikut ini adalah identifikasi risiko berdasarkan penyebab yang terjadi pada E-LKP UIN Raden Fatah Palembang berdasarkan hasil wawancara (terlampir).

Tabel 4.2 Identifikasi Risiko

Aset	Penyebab	Risiko
Hardware	Perawatan yang tidak teratur	Kerusakan pada perangkat keras (hardware)

Server CCTV	Kerusakan fisik pada server	
	Kurangnya pengamanan organisasi	Pencurian data/kehilangan informasi penting
	Kerusakan arus listrik (terjadi lonjakan)	Kebakaran
	Pemadaman listrik	
	Spesifikasi server yang sudah tidak memenuhi kebutuhan organisasi	Lambat koneksi terhadap server
	Kapasitas backup data yang sudah tidak memenuhi kebutuhan organisasi	Hardisk penuh
Data sasaran kinerja harian, sasaran kinerja bulanan	Kesalahan dalam penginputan dan penghapusan data	Kehilangan dan tidak validnya data
Data karyawan, nilai capaian, sasaran kinerja bulanan dan sasaran kinerja harian	Tidak adanya prosedur backup ketika server down	Kehilangan data
Data karyawan	Kurangnya mekanisme pemantauan	
Data karyawan, nilai capaian, sasaran kinerja bulanan dan sasaran kinerja harian	Server down	Aplikasi tidak bisa diakses
	Kesalahan pada fungsional software	
	Aplikasi down	
Perangkat Jaringan (*network)*	Kerusakan pada kabel Kesalahan dalam melakukan konfigurasi Kerusakan pada infrakstruktur jaringan Kerusakan pada kabel Kesalahan dalam melakukan konfigurasi	Terkendala koneksi internet
	Tidak ada pengamanan di sistem internal	Serangan hacker

People : Pengguna dan admin	Adanya share login atau password Tidak keluar atau logout ketika meninggalkan komputer Password disimpan pada dekstop komputer Tidak ada penggantian password secara berkala	Penyalahgunaan hak akses
	Kurangnya pelatihan prosedur penggunaan TI	Human eror
	Kurangnya sosialisasi tentang keamanan komputer	Pelanggaran terhadap aturan/regulasi (aturan) yang berlaku
	Pengolahan data ilegal oleh karyawan	Pencurian *database*
	Kesalahan penginputan data	Kehilangan dan tidak validnya data
	Kurangnya dokumentasi untuk penggunaan sistem untuk pengguna baru	Kurangnya pemahaman karyawan terhadap aplikasi
	Pengguna mengetahui kelemahan pada aplikasi	Pembobolan data

Dari tabel 4.1 setelah melakukan identifikasi penyebab kita menemukan risiko-risiko yang dirangkum pada tabel 4.2 dan terdapat 17 risiko dari 6 aset kritis pada E-LKP UIN Raden Fatah Palembang.

4.3.3.2 Penilaian Risiko

Berikut ini merupakan penilaian risiko menggunakan FMEA untuk melihat seberapa besar dampak risiko tersebut terhadap sistem informasi E-LKP UIN Raden Fatah Palembang. Dimana tingkat *severity*, digunakan untuk menganalisa risiko dengan menghitung seberapa besar dampak kejadian mempengaruhi output proses. Tingkat *occurrence*, menunjukan seberapa sering / intensitas risiko terjadi, serta menjabarkan skala pengukuran risiko berdasarkan peluang terjadinya dan

tingkat *detection*, pengukuran terhadap kemampuan mengendalikan atau mengontrol kegagalan yang dapat terjadi. Dan RPN itu didapat dari hasil perkalian *severity* (S), *occurrence* (O), dan *detection* (D). Hasil RPN untuk menentukan prioritas dari kegagalan, RPN tidak memiliki nilai atau arti. Nilai tersebut digunakan untuk meranking kegagalan proses yang potensial.

Tabel 4.3 Penilaian Risiko

Risiko	Potential Cause	S	O	D	RPN	Level
Kerusakan pada perangkat keras (hardware)	Perawatan yang tidak teratur	5	3	3	45	*Low*
	Kerusakan fisik pada server	10	1	1	10	*Very Low*
Pencurian data/kehilangan informasi penting	Kurangnya pengamanan organisasi	8	1	7	56	*Low*
Kebakaran	Kerusakan arus listrik (terjadi lonjakan)	10	1	1	10	*Very Low*
	Pemadaman listrik	2	1	1	2	*Very Low*
Lambat koneksi terhadap server	Spesifikasi server yang sudah tidak memenuhi kebutuhan organisasi	1	1	1	1	*Very Low*
Hardisk penuh	Kapasitas backup data yang sudah tidak memenuhi kebutuhan organisasi	2	1	1	2	*Very Low*
Kehilangan dan tidak validnya data	Kesalahan dalam penginputan dan penghapusan data	5	5	3	75	*Low*
Kehilangan data	Tidak adanya prosedur backup ketika server down	5	1	3	15	*Very Low*
	Kurangnya mekanisme pemantauan	5	1	3	15	*Very Low*
Aplikasi tidak bisa diakses	Server down	2	2	1	4	*Very Low*
	Kesalahan pada fungsional software	2	2	3	12	*Very Low*
	Aplikasi down	2	2	3	12	*Very Low*
Terkendala koneksi internet	Kerusakan pada kabel	5	5	3	75	*Low*
	Kesalahan dalam melakukan konfigurasi	5	1	2	10	*Very Low*

	Kerusakan pada infrastruktur jaringan	6	1	3	18	*Very Low*
Serangan hacker	Tidak ada pengamanan di sistem internal	10	1	5	50	*Low*
Penyalahgunaan hak akses	Adanya share login atau password	4	2	2	16	*Very Low*
	Tidak keluar atau logout ketika meninggalkan komputer	3	10	3	90	*Medium*
	Password disimpan pada dekstop komputer	4	10	2	80	*Medium*
	Tidak ada penggantian password secara berkala	1	10	2	20	*Low*
Human eror	Kurangnya pelatihan prosedur penggunaan TI	1	5	2	10	*Very Low*
Pelanggaran terhadap aturan/regulasi (aturan) yang berlaku	Kurangnya sosialisasi tentang keamanan komputer	1	2	3	6	*Very Low*
Pencurian *database*	Pengolahan data ilegal oleh karyawan	10	1	5	50	*Low*
Kehilangan dan tidak validnya data	Kesalahan penginputan data	5	9	2	90	*Medium*
Kurangnya pemahaman karyawan terhadap aplikasi	Kurangnya dokumentasi untuk penggunaan sistem pada pengguna baru	1	9	1	9	*Very Low*
Pembobolan data	Pengguna mengetahui kelemahan pada aplikasi	10	1	3	30	Low

Pada tabel 4.3 didapat bahwa risiko yang paling tinggi penilaiannya berada pada level *medium* RPN nya 90 pada risiko penyalahgunaan hak akses dan risiko kehilangan dan tidak validnya data, lalu risiko yang paling rendah berada pada level *very low* RPN nya 1 pada risiko lambat koneksi terhadap server. (Sumber : C.S. Carlson, "Understanding and Applying the Fundamentals of FMEAs," 2014 Annu. Reliab. Maintainab. Symp., 2014)

Setelah melakukan identifikasi aset berdasarkan profil ancaman, identifikasi risiko dan penilaian risiko selanjutnya adalah melakukan mitigasi terhadap risiko tersebut. Mitigasi dilakukan dengan menggunakan *Risk IT Framework*.

4.3.4 Mitigasi Risiko menggunakan *Risk IT Framework*

Pada tabel *responsible Risk IT Framework* terdapat penanggung jawab, yang terdiri dari CRO, CIO, CFO, dan HR (*Human Resource*) pada E-LKP UIN Raden Fatah Palembang. CIO (Chief Information Officer) dalam hal ini merupakan Kepala Bagian IT, CFO *(Chief Financial Officer)* sebagai Kepala Keuangan, CRO (*Customer Relation* Officer) sebagai Admin, dan *Human Resource* sebagai Humas.

Tabel 4.4 Pengurutan Risiko dan Pengelompokan *Risk IT Framework*

No.	Risiko (dari level tertinggi ke rendah)	*Risk IT Framework (Risk Response)*
1	Penyalahgunaan hak akses yang terjadi pada aset pengguna atau admin (*people)*	RR1.1 *Communicate IT risk analysis results* (Mengkomunikasikan Hasil Analisis Risiko TI)
2	Kehilangan dan tidak validnya data yang terjadi pada aset pengguna atau admin (*people)*	RR1.1 *Communicate IT risk analysis results* (Mengkomunikasikan Hasil Analisis Risiko TI)
3	Terkendala koneksi internet yang terjadi pada aset perangkat jaringan	RR2.3 *Respond to discovered risk exposure and opportunity* (Menanggapi Paparan Risiko Yang Ditemukan Dan Peluang)
4	Pencurian data/kehilangan informasi penting yang terjadi pada aset hardware, cctv dan server	RR2.3 *Respond to discovered risk exposure and opportunity* (Menanggapi Paparan Risiko Yang Ditemukan Dan Peluang)
5	Serangan hacker yang terjadi pada aset perangkat jaringan	RR3.3 *Initiate incident response* (Mulai Merespon Kejadian).
6	Pencurian *database* yang terjadi pada aset *people* (pengguna atau admin)	RR2.3 *Respond to discovered risk exposure and opportunity* (Menanggapi Paparan Risiko Yang Ditemukan Dan Peluang)
7	Kerusakan pada perangkat keras (hardware)	RR1.1 *Communicate IT risk analysis results* (Mengkomunikasikan Hasil Analisis Risiko TI)

8	Pembobolan data yang terjadi pada aset *people* (pengguna atau admin)	RR3.1 *Maintain incident response plans* (Pertahankan Rencana Dalam Merespon Kejadian)
9	Aplikasi tidak bisa diakses	RR3.1 *Maintain incident response plans* (Pertahankan Rencana Dalam Merespon Kejadian)
10	Kebakaran yang terjadi pada aset server	RR3.3 *Initiate incident response* (Mulai Merespon Kejadian).
11	Human eror	RR1.3 *Interpret independent IT assessment findings* (Menafsirkan Temuan Penilaian TI Sendiri)
12	Kurangnya pemahaman karyawan terhadap aplikasi	RR1.3 *Interpret independent IT assessment findings* (Menafsirkan Temuan Penilaian TI Sendiri)
13	Pelanggaran terhadap aturan/regulasi (aturan) yang berlaku yang terjadi pada *people* (pengguna atau admin)	RR1.3 *Interpret independent IT assessment findings* (Menafsirkan Temuan Penilaian TI Sendiri)
14	Hardisk penuh yang terjadi pada hardware	RR1.3 *Interpret independent IT assessment findings* (Menafsirkan Temuan Penilaian TI Sendiri)

4.4 Pembahasan

Berdasarkan hasil penelitian yang telah dilakukan dengan menganalisis risiko keamanan sistem informasi E-LKP menggunakan metode OCTAVE pada UIN Raden Fatah Palembang diperoleh data sebagai berikut.

1. Mengidentifikasi Risiko

Dari proses identifikasi risiko diperoleh 17 risiko dari 27 kejadian risiko dikarenakan memiliki lebih dari satu perbedaan penyebab. Karena diantara 17 risiko itu ada yang sama walaupun penyebab yang menjadikannya berbeda akhirnya peneliti menjadikan 14 risiko untuk dimitigasi dan dari risiko tersebut tidak satupun dari mereka mempunyai level tinggi yang dapat membahayakan aplikasi E-LKP.

2. Melakukan Pengukuran Risiko

Pada pengukuran risiko ini kami kelompokkan berdasarkan level dan jumlah risiko yang telah teridentifikasi.

Tabel 4.5 Pengukuran Risiko

No	Level	Jumlah Risiko
1	Very Low	16 risiko
2	Low	8 risiko
3	Medium	3 risiko
4	High	0 risiko
5	Very High	0 risiko

Dari tabel 4.5 hasil penilaian dikategorikan dalam tiga level penilaian risiko yaitu *medium, low* dan *very low*.

a. Level *medium* mempunyai 3 risiko dengan nilai RPN antara 80-91.
b. Level *low* mempunyai 8 risiko dengan nilai RPN antara 20-76.
c. Level *very low* mempunyai 16 risiko dengan nilai RPN antara 0-19.

Level *high* dan *very high* tidak terukur risikonya karena masih belum ada perhatian khusus dari pihak pimpinan di UIN Raden Fatah Palembang seperti contohnya belum adanya genset dan keamanan lainnya.

3. Rencana Mitigasi Risiko

Dari hasil identifikasi risiko terdapat 3 *Risk Respon* dalam *Risk IT Framework* yang dapat dijadikan acuan penentuan mitigasi risiko dan merekomendasikan SOP dari hasil analisis terhadap sistem informasi E-LKP UIN Raden Fatah Palembang. Dibawah ini merupakan pembahasan dari mitigasi risiko atau respon terhadap risiko yang teridentifikasi.

a) Risiko Penyalahgunaan Hak Akses Yang Terjadi Pada Aset Pengguna Atau Admin (*People),* Risiko Kehilangan Dan Tidak Validnya Data Yang Terjadi Pada Aset Pengguna Atau Admin (*People)* dan Risiko Kerusakan Pada Perangkat Keras (Hardware).

Pada risiko ini peneliti menggunakan *Risk IT Framework* RR1.1 *Communicate IT risk analysis results* (mengkomunikasikan hasil analisis risiko TI) karena pada RR1.1 ini berkomunikasi dengan jelas konteks perbaikan risiko yang jika memungkinkan akan menyertakan probabilitas kerugian atau keuntungan, rentang dan tingkat kepercayaan diri yang memungkinkan manajemen untuk keseimbangan perbaikan risiko. Untuk merespon risiko ini data yang dibutuhkan adalah *integrated risk management strategy* (strategi manajemen risiko terintegrasi), *risk analysis deficiencies* (defisiensi analisis risiko), *risk analysis results* (hasil analisis risiko) dan *peer-review recommendations* (rekomendasi ulasan rekan). Setelah data yang dibutuhkan terpenuhi didapatkan hasil dari respon risiko ini yakni *IT risk issues and opportunities* (masalah dan peluang risiko TI), *risk analysis report* (laporan analisis risiko), *loss/gain probabilities and ranges, risk response options, cost/benefit expectations* (probabilitas dan rentang kerugian / perolehan, opsi respons risiko, ekspektasi biaya / manfaat), *IT risk profile changes* (perubahan profil risiko TI) dan *business case opportunity* (peluang kasus bisnis). Berikut ini adalah Tabel *Responsible* terhadap respon risiko.

Tabel 4.6 RR1 (Tabel *Responsible)*

Key Activities (Kegiatan Utama)	CRO	CIO	CFO	HR
RR1.1 Mengkomunikasikan hasil analisis risiko TI.			**R**	
RR1.2 Laporkan aktivitas manajemen risiko TI dan status kepatuhan.			**R**	

RR1.3 Menafsirkan temuan penilaian TI sendiri.		**R**		
RR1.4 Identifikasi peluang terkait TI.		**R**		

Keterangan R : Responsible (Penanggung Jawab)

Tabel diatas merupakan pengelolaan mitigasi risiko pada E-LKP UIN Raden Fatah Palembang dimana CFO bertanggung jawab dalam mengkomunikasikan hasil analisis risiko TI dan melaporkan aktivitas manajemen risiko TI dan status kepatuhan dan CIO bertanggung jawab dalam menafsirkan temuan penilaian TI sendiri dan mengidentifikasi peluang terkait TI.

b) Risiko Terkendala Koneksi Internet Yang Terjadi Pada Aset Perangkat Jaringan, Risiko Pencurian Data/Kehilangan Informasi Penting Yang Terjadi Pada Aset *Hardware*, Cctv Dan Server dan Risiko Pencurian *Database* Yang Terjadi Pada Aset *People* (Pengguna Atau Admin).

Pada risiko ini peneliti menggunakan *Risk IT Framework* RR2.3 *Respond to discovered risk exposure and opportunity* (Menanggapi Paparan Risiko Yang Ditemukan Dan Peluang) untuk mengelola risiko ini karena menekankan proyek yang diharapkan untuk mengurangi potensi risiko frekuensi dan besarnya dampak kerugian dan menyeimbangkan proyek yang memungkinkan perebutan peluang bisnis yang strategis. Untuk merespon risiko ini data yang dibutuhkan adalah *Full economic life cycle cost and benefits* (Biaya dan manfaat siklus hidup ekonomi penuh), *Risk response requirements* (Persyaratan respons risiko), *Risk management benefits assigned to IT portfolio* (Manfaat manajemen risiko ditugaskan untuk portofolio TI), *risk response priority (risk disposition)* (prioritas respons risiko (disposisi risiko)), *IT risk issues and opportunities* (Masalah dan peluang risiko TI), *Control gaps and policy exceptions* (Kontrol kesenjangan dan pengecualian kebijakan), *Vulnerability events* (Kejadian kerentanan), *Key IT risk indicators and*

escalation triggers (Indikator kunci dan eskalasi risiko TI pemicu), *Programme plan* (Rencana program), *Strategic IT plan, tactical IT plans, IT project portfolio, IT service portfolio, IT sourcing strategy, IT acquisition strategy* (Rencana TI strategis, rencana TI taktis, portofolio proyek TI, portofolio layanan TI, strategi sumber TI, strategi akuisisi TI), *Information architecture, assigned data classifications, classification procedures and tools* (Arsitektur informasi, klasifikasi data yang ditugaskan, prosedur dan alat klasifikasi), *Technology opportunities* (Peluang teknologi), *IT budgets* (Anggaran TI), dan *Enterprise architecture road map or blueprint, business operational risk profiles* (Peta jalan atau cetak biru arsitektur perusahaan, profil risiko operasional bisnis). Setelah data tersebut terpenuhi maka akan didapatkan hasil dari merespon risiko ini yakni *IT risk action plans* (Rencana tindakan risiko TI) dan *IT risk response definition* (Definisi respons risiko TI). Berikut ini adalah Tabel *Responsible* terhadap respon risiko.

Tabel 4.7 RR2 (Tabel *Responsible)*

Key Activities (Kegiatan Utama)	**CRO**	**CIO**	**CFO**	**HR**
RR2.1 Kontrol Inventaris		**R**		
RR2.2 Pantau Penyelarasan Operasional Dengan Ambang Toleransi Risiko		**R**		
RR2.3 Menanggapi Paparan Peluang Risiko Yang Ditemukan		**R**		
RR2.4 Terapkan Kontrol				**R**
RR2.5 Melaporkan Kemajuan Rencana Tindakan Risiko TI		**R**		

Keterangan R : Responsible (Penanggung Jawab)

Tabel diatas merupakan pengelolaan mitigasi risiko pada E-LKP UIN Raden Fatah Palembang dimana CIO bertanggung jawab dalam kontrol inventaris, memantau penyelarasan operasional dengan ambang toleransi risiko, menanggapi

paparan peluang risiko yang ditemukan dan melaporkan kemajuan rencana tindakan risiko TI dan HR bertanggung jawab dalam menerapkan kontrol.

c) Risiko Serangan *Hacker* Yang Terjadi Pada Aset Perangkat Jaringan dan Risiko Kebakaran Yang Terjadi Pada Aset Server

Pada risiko ini peneliti menggunakan *Risk IT Framework* RR3.3 *Initiate incident response* (Mulai Merespon Kejadian) dimana pada risiko ini kita harus mengambil tindakan untuk meminimalkan dampak dari insiden yang sedang berlangsung dengan mengidentifikasi kategori kejadian dan mengikuti langkah-langkah dalam rencana merespon risiko ini dan harus memastikan bahwa tindakan yang diambil telah benar. Untuk merespon risiko ini data yang dibutuhkan adalah *Incident response plans* (Rencana respons insiden) dan *Risk event alert* (Peringatan peristiwa risiko). Setelah data tersebut terpenuhi maka hasil yang akan didapatkan yakni *Incident response actions taken* (Tindakan respons kejadian yang diambil) dan *Incident tickets* (tiket kejadian). Berikut ini adalah Tabel *Responsible* terhadap respon risiko.

Tabel 4.8 RR3 (Tabel *Responsible)*

Key Activities (Kegiatan Utama)	CRO	CIO	CFO	HR
RR3.1 Pertahankan Rencana Dalam Merespon Kejadian		**R**		
RR3.2 Pantau Risiko TI		**R**		
RR3.3 Mulai Merespon Kejadian		**R**		
RR3.4 Komunikasikan Pelajaran Yang Didapat Dari Peristiwa Berisiko		**R**		

Keterangan R : Responsible (Penanggung Jawab)

Tabel diatas merupakan pengelolaan mitigasi risiko pada E-LKP UIN Raden Fatah Palembang dimana CIO bertanggung jawab dalam mempertahankan rencana

dalam merespon kejadian, memantau risiko TI, mulai merespon kejadian dan mengkomunikasikan pelajaran yang didapat dari peristiwa berisiko.

d) Risiko Pembobolan Data Yang Terjadi Pada Aset *People* (Pengguna Atau Admin) dan Risiko Aplikasi Tidak Bisa Diakses

Pada risiko ini peneliti menggunakan *Risk IT Framework* RR3.1 *Maintain incident response plans* (menjaga rencana dalam merespon kejadian) dimana pada risiko ini harus mempersiapkan materialisasi ancaman melalui rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan dampak bisnis operasional, pengembangan terkait TI atau telah menyebabkan dampak bisnis. Pertahankan juga komunikasi terbuka tentang penerimaan risiko, kegiatan manajemen risiko, teknik analisis, dan hasil yang tersedia untuk membantu persiapan rencana. Untuk merespon risiko ini data yang dibutuhkan untuk memitigasi risiko ini adalah *IT risk action plans* (Rencana tindakan risiko TI), *Operating environment data*, *historical IT risk and loss data* (Data lingkungan operasi, data risiko dan kerugian TI historis) *Real-time problem and loss data, root-cause analysis and loss trends, emerging threats* (Data masalah dan kerugian waktu-nyata, analisis akar-penyebab, dan tren kerugian, ancaman yang muncul), *Emerging threats* (Ancaman yang muncul), *Risk analysis report* (Laporan analisis risiko), *IT risk issues and opportunities* (Masalah dan peluang risiko TI) dan *IT risk action plan progress/deviations* (Kemajuan / penyimpangan rencana tindakan risiko IT). Setelah data tersebut terpenuhi akan didapatkan hasil dari respon risiko ini yakni *Incident response plans* (Rencana respons insiden), *Risk analysis request* (Permintaan analisis risiko) dan *Availability, continuity and*

recovery specification (Spesifikasi ketersediaan, kontinuitas, dan pemulihan). Berikut ini adalah Tabel *Responsible* terhadap respon risiko.

Tabel 4.9 RR3 (Tabel *Responsible)*

Key Activities (Kegiatan Utama)	CRO	CIO	CFO	HR
RR3.1 Pertahankan Rencana Dalam Merespon Kejadian		**R**		
RR3.2 Pantau Risiko TI		**R**		
RR3.3 Mulai Merespon Kejadian		**R**		
RR3.4 Komunikasikan Pelajaran Yang Didapat Dari Peristiwa Berisiko		**R**		

Keterangan R : Responsible (Penanggung Jawab)

Tabel diatas merupakan pengelolaan mitigasi risiko pada E-LKP UIN Raden Fatah Palembang dimana CIO bertanggung jawab dalam mempertahankan rencana dalam merespon kejadian, memantau risiko TI, mulai merespon kejadian dan mengkomunikasikan pelajaran yang didapat dari peristiwa berisiko.

e) Risiko *Human Eror*, Risiko Kurangnya Pemahaman Karyawan Terhadap Aplikasi, Risiko Pelanggaran Terhadap Aturan/Regulasi (Aturan) Yang Berlaku Yang Terjadi Pada *People* (Pengguna Atau Admin) dan Risiko *Hardisk* Penuh Yang Terjadi Pada *Hardware*

Pada risiko ini peneliti menggunakan *Risk IT Framework* RR1.3 *Interpret independent IT assessment findings* (Menafsirkan Temuan Penilaian TI Sendiri) dimana pada respon risiko ini meninjau hasil dan temuan spesifik dari pihak ketiga yang objektif, audit internal, penjaminan kualitas, kegiatan penilaian diri dan lain-lain sambil mempertimbangkan toleransi risiko yang ditetapkan. Untuk merespon risiko ini data yang dibutuhkan adalah *Model for data collection* (Model untuk pengumpulan data), *Incident response actions taken* (Tindakan respons insiden diambil), *Root cause of incidents* (Akar penyebab insiden), *Project performance*

reports (Laporan kinerja proyek), *Process performance reports, supplier risks* (Memproses laporan kinerja, risiko pemasok), *Contingency test results* (Hasil tes kontingensi), *process performance reports* (memproses laporan kinerja), *Security threats and vulnerabilities* (Ancaman dan kerentanan keamanan), *Incident reports* (Laporan insiden*), Process performance reports* (Memproses laporan kinerja), *Problem records , known problems, known errors and workarounds* (Catatan masalah, masalah yang diketahui, kesalahan yang diketahui dan solusi) dan *Historical risk trends and events* (Tren dan peristiwa risiko historis). Setelah data tersebut terpenuhi maka hasil dari dari respon risiko ini yakni *Real-time problem and loss data, root-cause analysis and loss trends* (Data masalah dan kerugian waktu-nyata, analisis akar-penyebab, dan tren kerugian). Berikut ini adalah Tabel *Responsible* terhadap respon risiko.

Tabel 4.10 RR1 (Tabel *Responsible)*

Key Activities (Kegiatan Utama)	**CRO**	**CIO**	**CFO**	**HR**
RR1.1 Mengkomunikasikan hasil analisis risiko TI.			**R**	
RR1.2 Laporkan aktivitas manajemen risiko TI dan status kepatuhan.			**R**	
RR1.3 Menafsirkan temuan penilaian TI sendiri.		**R**		
RR1.4 Identifikasi peluang terkait TI.		**R**		

Keterangan R : Responsible (Penanggung Jawab)

Tabel diatas merupakan pengelolaan mitigasi risiko pada E-LKP UIN Raden Fatah Palembang dimana CFO bertanggung jawab dalam mengkomunikasikan hasil analisis risiko TI dan melaporkan aktivitas manajemen risiko TI dan status kepatuhan dan CIO bertanggung jawab dalam menafsirkan temuan penilaian TI sendiri dan mengidentifikasi peluang terkait TI.

4.5 Rekomendasi SOP (*Standard Operating Procedures*)

Berikut ini adalah Rekomendasi SOP terhadap Risiko Keamanan Sistem Informasi E-LKP pada UIN Raden Fatah Palembang berdasarkan hasil analisis sebagai berikut:

1. Pada aset *hardware*, server dan CCTV

a. Risiko kerusakan pada perangkat keras (hardware) rekomendasi SOP nya yaitu harus rutin melakukan pemeliharaan terhadap *hardware* minimal satu minggu sekali.

b. Pencurian data / kehilangan informasi penting rekomendasi SOP nya yaitu memberikan pedoman dan panduan bagi divisi dalam melakukan perbaikan hardware.

c. Kebakaran rekomendasi SOP nya yaitu para pegawai mematikan arus listrik untuk mengurangi penyebaran api yang terlalu cepat, lalu mencari sumber api, setelah itu pegawai memadamkan api menggunakan alat pemadam kebakaran yang khusus untuk ruangan server dan setelah itu mencari barang-barang yang masih bisa diselamatkan dari ruang server.

d. Lambat koneksi terhadap server rekomendasi SOP nya yaitu pegawai harus mengupdate server sesuai dengan kebutuhan pada perusahaan.

e. Hardisk penuh rekomendasi SOP nya yaitu rutin melakukan pengecekan pada hardisk untuk melihat apakah ada redudansi (pengulangan) lalu menggunakan hardisk yang sesuai dengan kebutuhan.

a. Pada aset data

Kehilangan dan tidak validnya data rekomendasi SOP nya yaitu admin harus mengganti *password* secara berkala minimal 2 minggu sekali dan rutin melakukan pengecekan terhadap data yang diupdate.

b. Aplikasi tidak bisa diakses rekomendasi SOP nya yaitu admin mencari penyebab kenapa aplikasi tersebut tidak dapat diakses, setelah menemukan penyebabnya segera melakukan perbaikan pada aplikasi agar masalah tidak berangsur lama dan rutin juga melakukan backup data agar ketika masalah ini terjadi perusahaan ada data cadangan apabila aplikasi mengalami masalah yang berangsur lama.

2. Pada aset perangkat jaringan (*network*)

a. Terkendala koneksi internet rekomendasi SOP nya yaitu rutin melakukan pengecekan terhadap kabel yang menjadi sumber internet minimal sehari sekali.

b. Serangan *hacker* rekomendasi SOP nya yaitu admin segera mengamankan data yang mungkin masih bisa diselamatkan selama proses *hacking* berlangsung dan melakukan pengamanan sistem internal.

3. Pada aset pengguna dan admin

a. Penyalahgunaan hak akses rekomendasi SOP nya yaitu pengguna harus rutin mengganti/mereset *password* minimal 2 minggu sekali dan melakukan *log out* ketika aplikasi sedang tidak digunakan.

b. *Human eror* rekomendasi SOP nya yaitu rutin mengadakan pelatihan prosedur penggunaan TI agar pegawai lebih memahami aplikasi.

c. Pelanggaran terhadap aturan/regulasi (aturan) yang berlaku rekomendasi SOP nya yaitu rutin melakukan sosialisasi tentang keamanan komputer.

d. Pencurian *database* rekomendasi SOP nya yaitu memberikan keamanan tambahan secara internal pada aplikasi E-LKP tersebut.
e. Kehilangan dan tidak validnya data rekomendasi SOP nya yaitu memeriksa kembali data yang kita input sebelum mengirimkannya dan melakukan *backup* data.
f. Kurangnya pemahaman karyawan terhadap aplikasi rekomendasi SOP nya yaitu melakukan test kepada karyawan untuk melihat seberapa jauh pemahamannya.
g. Pembobolan data rekomendasi SOP nya yaitu memperkuat sistem keamanan internal terhadap aplikasi.