p-ISSN: 2460-092X, e-ISSN: 2623-1662
Volume 6, Nomor 1, Juni 2020
Hal. 55 - 65

JUSIFO
JURNAL SISTEM INFORMASI

Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode *Octave* Pada Perguruan Tinggi Negeri X

RA Fitria Hamzah[1], Irfan Dwi Jaya[2], Utami Mizani Putri[3]
rafitriah13@gmail.com[1], irfan_dj@radenfatah.ac.id[2], utamiputri@radenfatah.ac.id[3]

[1]Sistem Informasi, Fakultas Sains dan Teknologi, UIN Raden Fatah Palembang
[2]Sistem Informasi, Fakultas Sains dan Teknologi, UIN Raden Fatah Palembang
[3]Sistem Informasi, Fakultas Sains dan Teknologi, UIN Raden Fatah Palembang

Diterima: 01 Mei 2020 | Direvisi: 18 Mei 2020 | Disetujui: 29 Mei 2020

Abstrak: *E-LKP adalah lembar kinerja pegawai yang diakses secara online dan berbasis web. Aplikasi E-LKP Perguruan Tinggi Negeri X tercipta untuk menghitung kinerja pegawai dimana hasil dari perhitungan tersebut akan diimplementasikan untuk remunerasi. Lembar kinerja pegawai dapat diakses secara online dan hanya pegawai yang dapat remunerasi beserta admin pada Perguruan Tinggi Negeri X saja yang bisa login atau menggunakannya. Tujuan dari penelitian ini adalah menganalisis risiko keamanan sistem informasi E-LKP Perguruan Tinggi Negeri X sesuai dengan metode OCTAVE. Hasil dari penelitian ini adalah dapat mengetahui risiko apa saja yang akan terjadi dan dapat mencegah risiko pada keamanan sistem informasi E-LKP Perguruan Tinggi Negeri X dan SOP (Standard Operating Procedure) yang direkomendasikan diharapkan dapat menjadi acuan dalam menangani risiko-risiko yang akan terjadi pada sistem informasi E-LKP Perguruan Tinggi Negeri X.*
Kata Kunci*: Risiko Keamanan, Octave, E-LKP*

Abstract: *E-LKP is an employee performance sheet that is accessed online and on a web-based basis. The E-LKP application of State University X was created to calculate employee performance where the results of the calculation will be implemented for remuneration. Employee performance sheets can be accessed online and only employees who can remuneration along with the admin at X State University can login or use it. The purpose of this study is to analyze the security risk of the State University X E-LKP information system according to the OCTAVE method. The results of this study are able to find out what risks will occur and can prevent risks to the security of the information system E-LKP State University X and the recommended SOP (Standard Operating Procedure) are expected to be a reference in dealing with risks that will occur in E-LKP information system State University X.*
Keywords***:*** *Security Risk, Octave, E-LKP*

1 PENDAHULUAN

E-LKP pertama kali digunakan pada bulan mei 2017. E-LKP merupakan laporan kinerja pegawai yang diakses secara online dan berbasis web. Sistem Informasi E-LKP Perguruan Tinggi Negeri X tercipta karena kampus perlu mengimplementasikan remunerasi dimana untuk menghitung kinerjanya harus menggunakan sistem informasi ini dan hasil dari perhitungan kinerja ini dapat dijadikan acuan untuk membayar tunjangan para pegawai. Laporan kinerja pegawai hanya dapat diakses secara *online* dan hanya pegawai yang dapat remunerasi beserta admin pada Perguruan Tinggi Negeri X saja yang bisa *login* atau menggunakannya. Sistem informasi E-LKP banyak memuat data pegawai tentang pencairan tunjangan serta hasil kinerja pegawai.

Permasalahan yang terjadi, berdasarkan hasil *interview* secara langsung dengan administrator sistem informasi E-LKP, pada 14 Juni 2017 terjadi gangguan keamanan informasi terhadap data-data pegawai. Hal ini mengakibatkan penundaan terhadap pemberian tunjangan pegawai. Gangguan keamanan ini memperlihatkan bahwa sistem informasi

memiliki celah terhadap keamanan sistem informasi. Berdasarkan ancaman tersebut juga perlu dilakukan analisis risiko keamanan pada sistem informasi E-LKP.

Metode yang dipakai untuk menganalisis risiko keamanan sistem informasi E-LKP dalam penelitian ini, yaitu *OCTAVE* (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) merupakan sebuah metode yang dikembangkan oleh *Software Engineering Institute (SEI)* pada tahun 2001. Metode OCTAVE merupakan sebuah *tool*, teknik dan metode yang digunakan untuk memberi penilaian dan perencanaan strategi keamanan sistem informasi berdasarkan pengidentifikasian risiko. Fokus dari metode *OCTAVE* adalah aset TI (Teknologi Informasi atau Sistem Informasi) kritis yang dimiliki oleh sebuah organisasi dalam melakukan pengidentifikasian, prioritas dan manajemen risiko keamanan informasinya. *OCTAVE* mendefinisikan komponen-komponen penting secara komprehensif, sistematis dan berbasis konteks evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi dengan mengambil keputusan risiko (Alberts, Christopher and Dorofee, Audrey, 2001).

Dengan analisis risiko keamanan sistem informasi E-LKP di Perguruan Tinggi Negeri X menggunakan metode *OCTAVE* ini kita dapat menemukan risiko apa saja yang mungkin akan terjadi dan bagaimana cara kita menjaga agar risiko yang akan terjadi nanti dapat kita tangani dengan cepat dan tanggap atau dapat diminimalisasi akibat dari risiko tersebut. Metode ini menggunakan 3 fase, fase pertama ini merupakan membangun profil ancaman, fase kedua merupakan tahap mengidentifikasi kerentanan infrastruktur dan fase ketiga ini merupakan tahap akhir dari metode octave yaitu membuat strategi perlindungan dan rencana (Alberts, Christopher and Dorofee, Audrey, 2001).

2 METODOLOGI PENELITIAN

2.1 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode analisis kualitatif. Metode penelitian kualitatif adalah metode penelitian yang berlandaskan pada filsafat post positivisme, digunakan untuk meneliti pada kondisi objek yang alamiah, (sebagai lawannya adalah eksperimen) dimana peneliti adalah sebagai instrumen kunci, teknik pengumpulan data dilakukan secara triangulasi (gabungan), analisis data bersifat induktif/kualitatif, dan hasil penelitian kualitatif lebih menekankan makna dari pada generalisasi (Sugiyono, 2017).

2.2 Metode Pengumpulan Data

Menurut Riduwan, mengungkapkan bahwa metode pengumpulan data adalah teknik atau cara-cara yang digunakan oleh peneliti untuk mengumpulkan data. Dalam hal ini, teknik pengumpulan data dalam penelitian adalah sebagai berikut (Riduwan, 2012):

a) Observasi

Metode observasi, peneliti mengamati secara langsung dan mempelajari permasalahan yang ada pada E-LKP Perguruan Tinggi Negeri X serta memberikan solusi dari permasalahan tersebut.

b) Wawancara

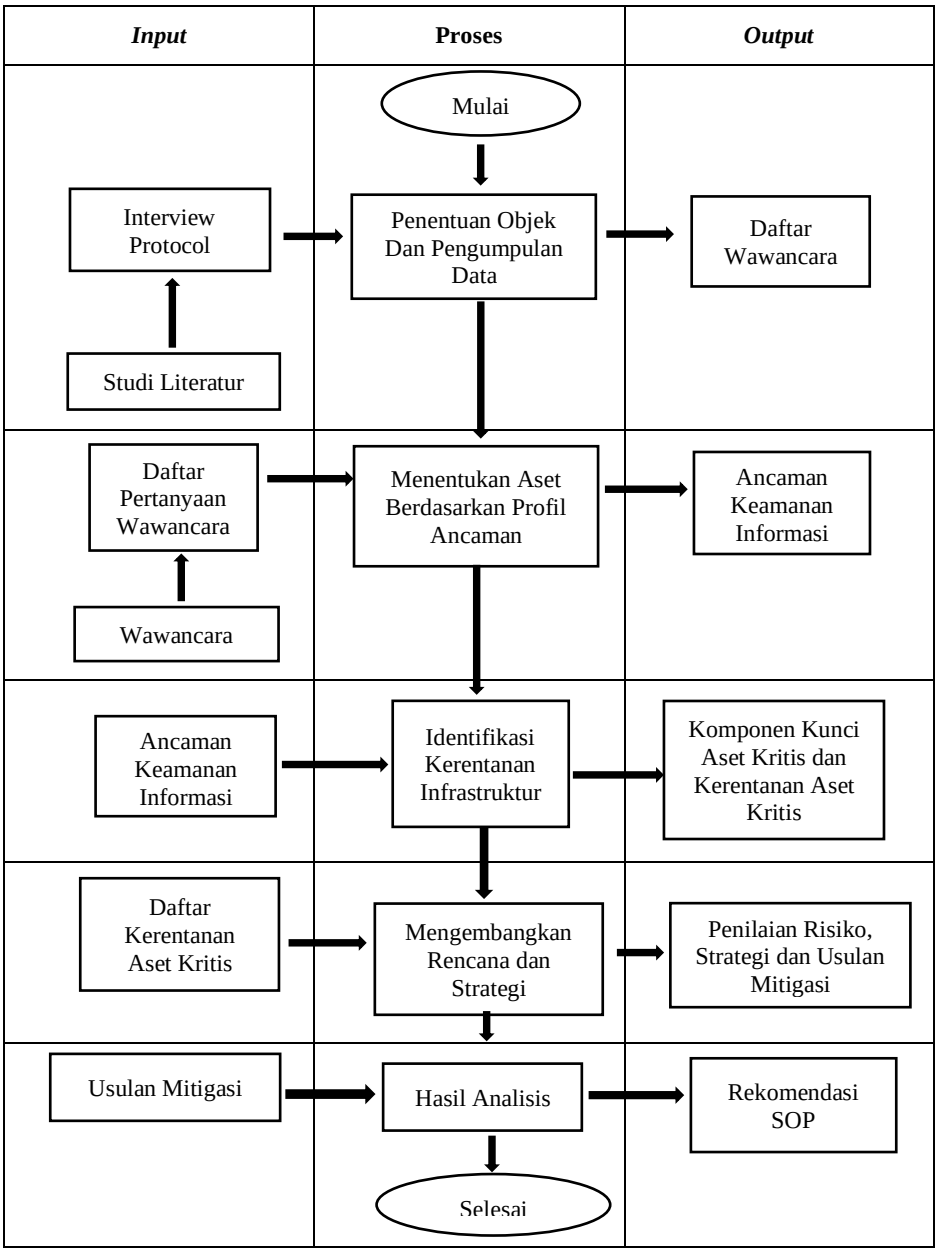
Dalam hal ini, bidang yang menjadi objek wawancara ada 3 (tiga) orang informan, yaitu Kepala Pusat Teknologi Informasi dan Pangkalan Data (PUSTIPD), divisi jaringan dan divisi pengembangan sistem.

c) Studi Kepustakaan

Studi kepustakaan adalah teknik pengumpulan data dengan mengadakan studi penelaahan terhadap buku-buku, literatur-literatur, catatan-catatan, dan laporan-laporan yang ada hubungannya dengan masalah yang dipecahkan (Nazir, 1988). Pengumpulan data yang dilakukan secara langsung dari sumber-sumber lain seperti buku, jurnal dan hasil penelitian yang berkaitan dengan penelitian ini.

2.3 Tahapan Penelitian

Metode analisis pada penelitian ini digambarkan melalui diagram alir pada Gambar 1 :



Gambar 1 Tahapan Penelitian

Berikut adalah paparan alur diagram dari gambar diatas:

A. Daftar Wawancara

Daftar wawancara dibuat berdasarkan hasil *output* yang terdapat di 3 fase yang ada pada metode *OCTAVE*.

B. Ancaman Pada Sistem Informasi E-LKP

Pada tahap ini kita mencari ancaman-ancaman yang dapat terjadi pada E-LKP melalui penentuan aset berdasarkan profil ancaman atau fase ke-1 metode OCTAVE.

Fase 1 Menentukan Aset Berdasarkan Profil Ancaman

1. Mendata Aset Kritis
2. Mengidentifikasi Kebutuhan Keamanan Aset Kritis
3. Mengidentifikasi Ancaman Aset Kritis
4. Mendata Keamanan Yang Sudah Diterapkan
5. Mengidentifikasi Kelemahan Perusahaan

C. Komponen Kunci Aset Kritis dan Kerentanan Aset Kritis

Hasil pada tahap ini didapatkan dari fase ke-2 metode OCTAVE.

Fase 2 Identifikasi Kerentanan Infrastruktur

1. Mengidentifikasi Komponen Kunci
2. Mengevaluasi Kerentanan Komponen Kunci

D. Penilaian Risiko, Strategi dan Usulan Mitigasi

Pada tahap ini kita melakukan pengukuran risiko menggunakan FMEA dan sekaligus melakukan rencana mitigasi berdasarkan fase 3 pada metode OCTAVE, penjelasannya sebagai berikut.

Fase 3 Mengembangkan Rencana dan Strategi

1. Mengidentifikasi Risiko
2. Melakukan Penilaian Risiko
3. Rencana Mitigasi Risiko

E. Rekomendasi SOP

Pada tahap ini peneliti akan membuat rekomendasi SOP untuk E-LKP berdasarkan dari hasil analisis dari risiko-risiko yang telah ditemukan, pengukuran risiko menggunakan FMEA serta rencana mitigasi yang telah ditentukan.

3 HASIL DAN PEMBAHASAN

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

Tabel 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

Aset	Kerentanan	Ancaman	Penyebab
	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

Aset	Kerentanan	Ancaman	Penyebab
	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 1 didapatkan penyebab dari kerentanan/kelemahan yang menjadi ancaman bagi 6 kategori aset kritis pada E-LKP Perguruan Tinggi Negeri X.

Berikut ini adalah identifikasi risiko berdasarkan penyebab yang terjadi pada E-LKP Perguruan Tinggi Negeri X berdasarkan hasil wawancara.

Tabel 2 Identifikasi Risiko

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

Aset	Penyebab	Risiko
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 2 setelah melakukan identifikasi penyebab kita menemukan risiko-risiko yang dirangkum pada Tabel 2 dan terdapat 17 risiko dari 6 aset kritis pada E-LKP Perguruan Tinggi Negeri X. 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 satu pun dari mereka mempunyai level tinggi yang dapat membahayakan aplikasi E-LKP.

Berikut ini merupakan penilaian risiko menggunakan FMEA untuk melihat seberapa besar dampak risiko tersebut terhadap sistem informasi E-LKP Perguruan Tinggi Negeri X.

Tabel 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*
	Server down	2	2	1	4	*Very Low*

Risiko	Potential Cause	S	O	D	RPN	Level
Aplikasi tidak bisa diakses	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 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. 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.

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.*

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 Perguruan Tinggi Negeri X. *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.

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 Perguruan Tinggi Negeri X.

Tabel 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 error*	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)

Rekomendasi SOP (*Standard Operating Procedures*)

Berikut ini adalah Rekomendasi SOP terhadap Risiko Keamanan Sistem Informasi E-LKP pada Perguruan Tinggi Negeri X 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 meng-update server sesuai dengan kebutuhan pada perusahaan.
e) Hard disk penuh rekomendasi SOP nya yaitu rutin melakukan pengecekan pada hard disk untuk melihat apakah ada redundansi (pengulangan) lalu menggunakan hardisk yang sesuai dengan kebutuhan.

2) Pada aset data

a) 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.

3) 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.

4) Pada aset pengguna dan admin

a) Penyalahgunaan hak akses rekomendasi SOP nya yaitu pengguna harus rutin mengganti/me-reset *password* minimal 2 minggu sekali dan melakukan *log out* ketika aplikasi sedang tidak digunakan.
b) *Human error* 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 tes kepada karyawan untuk melihat seberapa jauh pemahamannya.
g) Pembobolan data rekomendasi SOP nya yaitu memperkuat sistem keamanan internal terhadap aplikasi.

4 KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, diperoleh kesimpulan sebagai berikut:

1) Hasil Analisis Risiko Keamanan Sistem Informasi E-LKP menggunakan metode *OCTAVE* diperoleh 17 risiko dari 27 kejadian risiko dan mendapatkan 3 level pada pengukuran risiko yaitu *low, very low* dan *medium*. Berdasarkan hasil analisis tidak satu pun dari 27 kejadian risiko ini yang mempunyai level *high* dan *very high* dari sini kita dapat mengetahui bahwa risiko yang akan terjadi tidaklah dapat berdampak terlalu buruk

bagi sistem informasi E-LKP Perguruan Tinggi Negeri X karena sudah adanya penerapan pada kebutuhan keamanan sistem informasi E-LKP itu sendiri.

2) Dari mitigasi risiko menggunakan *Risk IT Framework* terdapat 3 *Risk Respons* yang digunakan untuk 17 risiko yaitu RR1.1, RR2.3, RR3.3, RR3.1 dan RR1.3 dan disesuaikan dengan data yang dibutuhkan untuk dilakukan mitigasi 17 risiko tersebut serta merekomendasikan SOP dari hasil analisis.

DAFTAR RUJUKAN

ISACA. (2009). *The Risk IT Framework*. Retrieved from www.isaca.org

Supradono, B. 2009. *Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation).* Media Elektrika, 2(1).

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S Implementation Guide, Version 1.0*. Pittsburgh: Carnegie Mellon Software Engineering Institute.

Alberts, Christopher and Dorofee, Audrey (2001). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Criteria SM (CMU/SEI-01-TR-016)*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001.

Carl S. Carlson, "Understanding and Applying the Fundamentals of FMEAs," 2014 Reliability and Maintainability Symposium, January, 2014.

Whitman, ME, Mattord, HJ (2012) *Principles of Information Security*. Boston (US): Course Technology, Thomson

Innike Desy, Bekti Cahyo Hidayanto, Hanim Maria Astuti. *Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis Di Divisi Ti Pt. Bank Xyz Surabaya* (Seminar Nasional Sistem Informasi Indonesia, 22 September 2014)