BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

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

Beberapa ciri khas karakteristik kualitatif dapat dikemukakan sebagai berikut:

1. Dilakukan pada kondisi yang alamiah.
2. Penelitian kualitatif bersifat deskriptif. Data yang terkumpul berbentuk kata-kata atau gambar, sehingga tidak menekankan pada angka.
3. Penelitian kualitatif lebih menekankan pada proses daripada produk atau *outcome*.
4. Penelitian kualitatif melakukan analisis data sesuai data secara dedukatif.
5. Penelitian kualitatif lebih menekankan makna (data dibalik yang teramati).

3.2 Waktu dan Tempat Penelitian

Waktu penelitian dilakukan mulai dari 21 Februari 2019 dengan tempat penelitian di UIN Raden Fatah Palembang pada PUSTIPD, dengan judul penelitian analisis risiko keamanan sistem informasi E-LKP dengan metode OCTAVE.

3.3 Alat dan Bahan Penelitian

Untuk mengolah data hasil dari penelitian menggunakan Microsoft Word yang digunakan untuk membuat laporan penelitian. Dalam penelitian ini yang akan dianalisis yaitu E-LKP UIN Raden Fatah Palembang menggunakan metode OCTAVE dimana fokus penelitian ini adalah risiko apa saja yang akan mengganggu keamanan pada sistem ini dan data didapatkan dari hasil wawancara secara mendalam terhadap narasumber yang benar-benar paham terhadap sistem informasi E-LKP UIN Raden Fatah Palembang.

3.4 Metode Pengumpulan Data

Riduwan (2012) 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:

a. Observasi

Metode Observasi merupakan metode yang digunakan oleh peneliti yang melakukan pengamatan dan pencatatan langsung secara sistematis terhadap gejala atau fenomena yang diselidiki (Mukhtar, 2013). Metode observasi, peneliti mengamati secara langsung dan mempelajari permasalahan yang ada pada E-LKP UIN Raden Fatah Palembang serta memberikan solusi dari permasalahan tersebut.

b. Wawancara

Wawancara merupakan suatu cara pengumpulan data yang digunakan untuk memperoleh informasi langsung dari sumbernya (Riduwan, 2012). Wawancara adalah percakapan dengan maksud tertentu. Percakapan itu dilakukan oleh dua pihak, yaitu pewawancara (*interviewer*) yang mengajukan pertanyaan dan

terwawancara (*interviewer*) yang memberikan jawaban atas pertanyaan itu (Patton, 2006). 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.

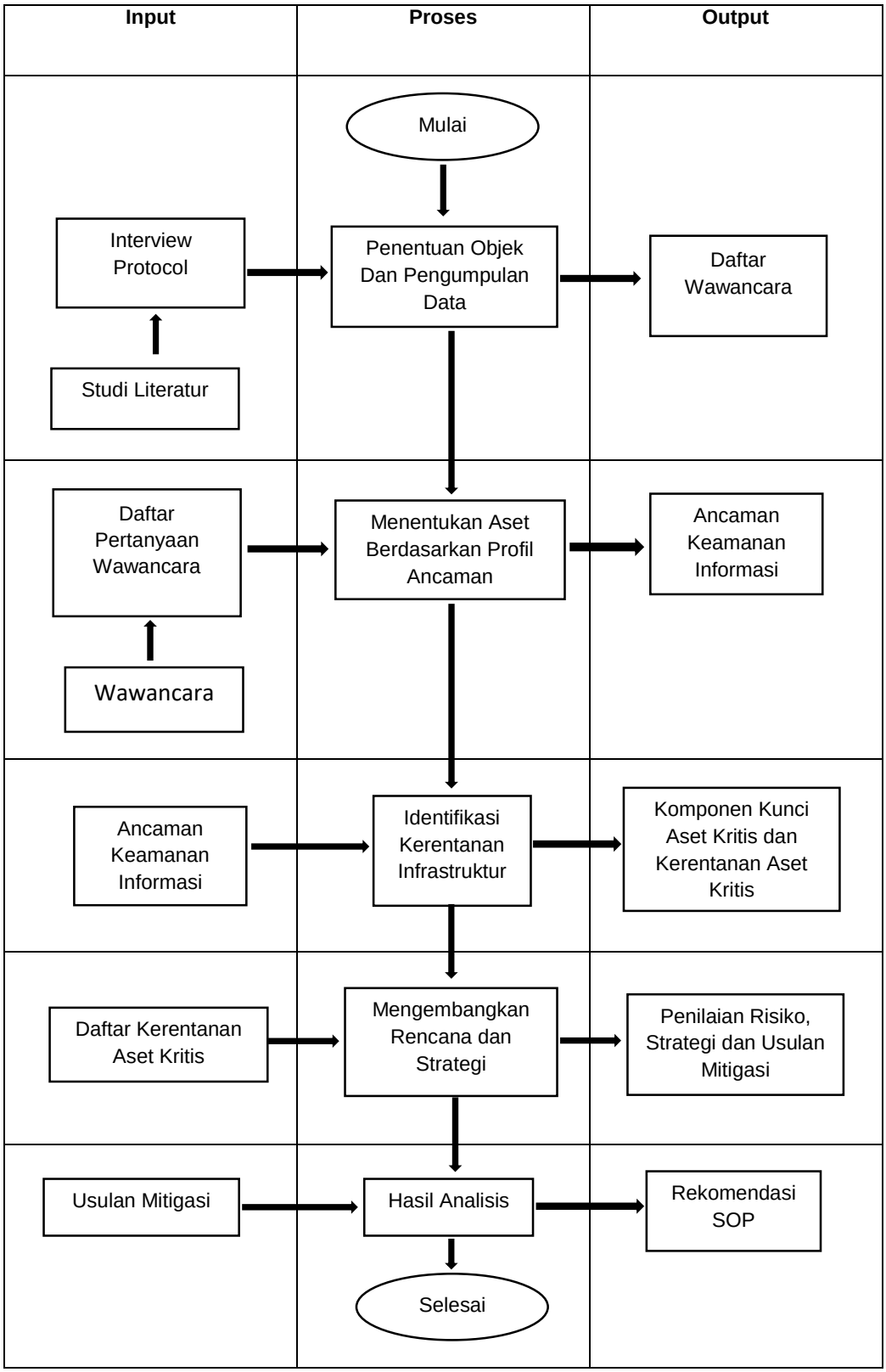
Langkah pertama yang dilakukan peneliti yaitu melakukan wawancara terlebih dahulu informan divisi pengembangan sistem dan divisi jaringan tentang sistem informasi Elektronik Laporan Kinerja Pegawai (E-LKP), tidak hanya pada ke dua orang informan tersebut akan tetapi Kepala Pusat Teknologi Informasi dan Pangkalan Data (PUSTIPD) juga dilakukan wawancara untuk mengetahui lebih lanjut tentang sistem tersebut. Selain itu bukan hanya pada sistem dan informasi yang ada saja tetapi juga perangkat keras dan fasilitas-fasilitas pendukung pada sistem dengan tujuan mendapatkan data yang akurat sesuai dengan keadaan yang sesungguhnya.

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.

3.5 Tahapan Penelitian

Metode analisis pada penelitian ini akan digambarkan melalui diagram alur sebagai berikut:



Gambar 3.1 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 E-LKP UIN Raden Fatah Palembang

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

Fase 1 Menentukan Aset Berdasarkan Profil Ancaman

1. Mendata Aset Kritis

Aset kritis diperoleh dari wawancara yang sudah dilakukan dengan pihak terkait di perusahaan.

2. Mengidentifikasi Kebutuhan Keamanan Aset Kritis

Berdasarkan hasil wawancara yang sudah dilakukan sebelumnya, maka akan dilakukan identifikasi mengenai kebutuhan keamanan pada masing-masing aset kritis teknologi informasi di perusahaan tersebut dengan menyertakan CIA Triad, yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas) dan *Availability* (ketersediaan).

3. Mengidentifikasi Ancaman Aset Kritis

Identifikasi ancaman terhadap aset kritis dilakukan dengan mengacu pada hasil analisis kebutuhan keamanan aset kritis di perusahaan.

4. Mendata Keamanan Yang Sudah Diterapkan

Pendataan dilakukan berdasarkan dari hasil wawancara yang sudah dilakukan sebelumnya kepada pihak terkait.

5. Mengidentifikasi Kelemahan Perusahaan

Proses identifikasi kelemahan perusahaan dilakukan berdasarkan hasil wawancara yang sudah dilakukan sebelumnya kepada pihak terkait.

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

Berdasarkan data aset penting, kebutuhan keamanan dan daftar ancaman yang sudah di peroleh tahap berikutnya adalah melakukan identifikasi komponen penting dari masing-masing aset kritis.

2. Mengevaluasi Kerentanan Komponen Kunci

Evaluasi kerentanan dari masing-masing komponen kunci dilakukan setelah memperoleh daftar komponen kunci pada proses sebelumnya.

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

Proses identifikasi risiko dilakukan pada komponen penting yang berkaitan dengan aset kritis perusahaan yang dapat mempengaruhi proses bisnis perusahaan. Identifikasi risiko ini dilakukan berdasarkan hasil identifikasi dan evaluasi yang sebelumnya telah dilakukan.

2. Melakukan Penilaian Risiko

Penilaian risiko dilakukan dengan menggunakan metode FMEA berdasarkan daftar kemungkinan risiko yang telah dibuat sebelumnya. Dari hasil penilaian risiko ini nantinya dapat diketahui seberapa besar tingkat risiko yang dihadapi perusahaan. Penilaian risiko dengan metode FMEA didasari oleh 3 faktor yaitu *Severity, Occurrence, Detection*. Nilai dari masing-masing faktor kemudian dikalian, nantinya akan diperoleh *Risk Priority Number*. Kemudian risiko dikategorikan berdasarkan levelnya.

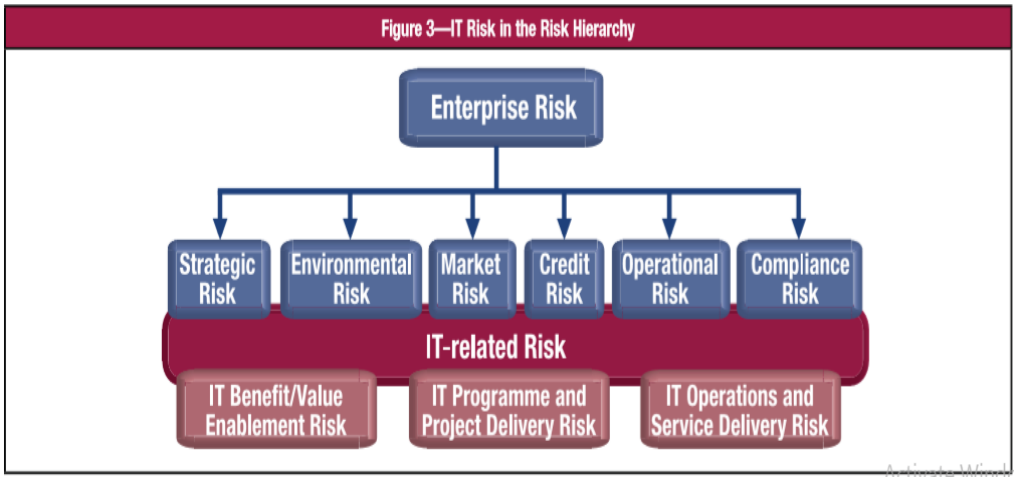
3. Rencana Mitigasi Risiko

Rencana mitigasi risiko dibuat untuk melakukan pengamanan terhadap masing-masing komponen aset kritis perusahaan dari risiko yang mungkin dapat terjadi. Rencana mitigasi risikonya menggunakan *Risk IT Framework.*

a) Pengertian *Risk IT Framework*

Risk IT Framework adalah komponen dari keseluruhan risiko perusahaan, seperti yang ditunjukkan pada Gambar 3.2. risiko lainnya merupakan wajah perusahaan termasuk risiko strategis, risiko lingkungan, risiko pasar, risiko kepercayaan, risiko operasional dan risiko kepatuhan. Banyak diperusahaan risiko TI terkait dianggap komponen risiko operasional, misalnya, dalam industri keuangan yaitu *Basel II framework*. Namun, bahkan risiko strategis dapat memiliki komponen TI untuk itu, terutama di mana TI adalah *enabler* kunci dari inisiatif bisnis baru. Hal yang sama berlaku untuk risiko kepercayaan, di mana kerusakan TI (keamanan) dapat menyebabkan menurunnya kepercayaan. Untuk alasan bahwa lebih baik tidak untuk menggambarkan risiko TI dengan ketergantungan hierarki

pada salah satu kategori risiko lain, tapi mungkin seperti yang ditunjukkan pada contoh (industri berorientasi keuangan) yang diberikan dalam Gambar 3.2.



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

Gambar 3.2 Risiko TI dalam Susunan Risiko

Risk IT Framework adalah bisnis risiko khusus, risiko bisnis yang terkait dengan penggunaan, kepemilikan, operasi, keterlibatan, pengaruh dan adopsi TI dalam suatu perusahaan. Ini terdiri dari peristiwa dan kondisi yang berkaitan dengan TI yang berpotensi berdampak bisnis. Hal ini dapat terjadi dengan kedua frekuensi dan besarnya yang menentu, serta menciptakan tantangan dalam memenuhi tujuan strategis dan tujuan. Risiko TI dapat dikategorikan dalam berbagai cara:

1. Risiko yang dapat diperoleh dengan peluang yang diberikan dengan teknologi untuk efisiensi atau lebih banyak efektifitas proses bisnis, atau sebagai pendorong untuk inisiatif bisnis baru.
2. Program dan proyek pengiriman yang terkait dengan ketiga kontribusi oleh orang yang menyediakan bisnis, pemecahan masalah, tidak punya rencana proyek dan program. Ini terkait dengan manajemen portofolio investasi (seperti yang dijelaskan dalam kerangka kerja TI).

3. Risiko pengoperasian dan perlindungan terlebih dahulu ditempatkan dengan semua aspek kinerja sistem dan layanan yang menghasilkan perusakan atau pengurangan nilai bagi perusahaan.

b) Tujuan *IT Risk Framework*

Manajemen risiko bisnis merupakan komponen penting dari administrasi yang bertanggung jawab dari perusahaan apapun. Hampir setiap keputusan bisnis membutuhkan eksekutif atau manajer risiko keseimbangan dan reward.

Kerangka kerja risiko TI menjelaskan risiko TI dan memungkinkan pengguna untuk:

1. Integrasi manajemen risiko ke dalam keseluruhan usaha, ini mengizinkan usaha untuk membuat risiko kembali sadar akan keputusan.
2. Baik keputusan terkait tentang perjanjian risiko dan keinginan risiko dan toleransi risiko dari perusahaan.
3. Memahami bagaimana cara menanggung risiko.

Secara singkat, kerangka ini memungkinkan perusahaan untuk membuat keputusan sadar risiko yang sesuai.

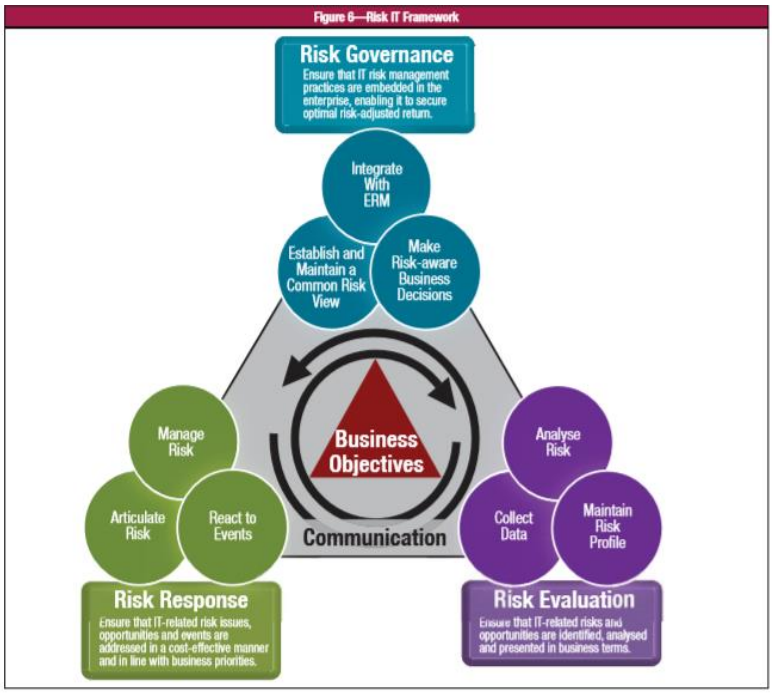
c) *IT Risk Framework*

Kerangka kerja Risiko TI dibangun di atas prinsip-prinsip yang ditetapkan dalam bab sebelumnya dan dikembangkan lebih lanjut menjadi model proses yang komprehensif (gambar 3.3).

Model proses manajemen risiko mengelompokkan kegiatan utama ke dalam sejumlah proses. Proses-proses ini dikelompokkan menjadi tiga domain. Model proses akan tampak akrab bagi pengguna COBIT dan Val IT: pedoman substansial

diberikan pada kegiatan utama dalam setiap proses, tanggung jawab untuk proses, arus informasi antara proses dan kinerja manajemen proses.

Tiga domain dari kerangka kerja Risiko TI - Tata Kelola Risiko, Evaluasi Risiko dan Respons Risiko - masing-masing berisi tiga proses, seperti yang ditunjukkan pada gambar 3.3.



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

Gambar 3.3 *IT Risk Framework*

Kerangka Risiko TI terdiri dari:

1. Domain - *Risk Governance:* Tata Kelola Risiko (RG)

   RG1 Membangun dan memelihara pandangan risiko umum

   RG2 Mengintegrasikan dengan ERM

   RG3 Membuat keputusan bisnis yang sadar risiko

2. Domain - *Risk Evaluation:* Evaluasi Risiko (RE)

   RE1 Mengumpulkan data

   RE2 Menganalisis risiko

RE3 Menjaga profil risiko

3. Domain – *Risk Response:* Respon Risiko (RR)

RR1 *Articulate Risk* (Mengartikulasikan Risiko)

Pastikan bahwa informasi tentang keadaan sebenarnya dari eksposur dan peluang yang berhubungan dengan ti tersedia secara tepat waktu dan kepada orang yang tepat untuk tanggapan yang sesuai.

RR1.1 *Communicate IT Risk Analysis Results* (Mengkomunikasikan Hasil Analisis Risiko TI)

Laporkan hasil analisis risiko dalam bentuk dan format yang berguna untuk mendukung keputusan bisnis. Koordinasikan kegiatan analisis risiko tambahan seperti yang disyaratkan oleh pembuat keputusan (mis., penolakan laporan, penyesuaian ruang lingkup). Komunikasikan dengan jelas konteks risiko-pengembalian. Jika memungkinkan, sertakan probabilitas kehilangan dan / atau perolehan, rentang, dan tingkat kepercayaan yang memungkinkan manajemen menyeimbangkan pengembalian risiko. Identifikasi dampak negatif dari peristiwa / skenario yang harus mendorong keputusan respons dan dampak positif dari peristiwa / skenario yang mewakili peluang manajemen harus menyalurkan kembali ke dalam strategi dan proses penetapan tujuan. Memberikan pemahaman kepada pengambil keputusan.

RR1.2 *Report IT risk management activities and state of compliance* (Laporkan Aktivitas Dan Kondisi Manajemen Risiko TI)

Memenuhi kebutuhan pelaporan risiko dari berbagai pemangku kepentingan (mis., dewan, komite risiko, fungsi kontrol risiko, manajemen unit bisnis). Untuk

memastikan pelaporan yang strategis dan efisien tentang masalah dan status risiko TI, terapkan prinsip-prinsip relevansi, efisiensi, ketepatan waktu, dan akurasi. Termasuk efektivitas dan kinerja kontrol, masalah dan kesenjangan, status remediasi, peristiwa dan insiden, dan dampaknya terhadap profil risiko. Termasuk kinerja proses manajemen risiko. Memberikan masukan untuk pelaporan perusahaan terintegrasi.

RR1.3 *Interpret Independent IT Assessment Findings* (Menafsirkan Temuan Penilaian TI Sendiri)

Tinjau hasil dan temuan spesifik dari pihak ketiga yang objektif, audit internal, penjaminan kualitas, kegiatan penilaian diri, dll. Peta mereka ke profil risiko dan garis dasar risiko dan kontrol, sambil mempertimbangkan toleransi risiko yang ditetapkan. Ambillah celah dan keterpaparan terhadap bisnis.

RR1.4 *Identify It-Related Opportunities* (Identifikasi Peluang Terkait TI)

Secara berulang, pertimbangkan tingkat relatif risiko TI terhadap kapasitas manajemen risiko TI untuk proses bisnis, unit bisnis, produk, dll. Khusus untuk area dengan risiko relatif dan paritas kapasitas risiko (yaitu, menunjukkan kemampuan untuk mengambil risiko lebih besar), mengidentifikasi peluang terkait TI yang dapat memungkinkan daerah untuk menerima risiko yang lebih besar dan meningkatkan pertumbuhan dan pengembalian.

RR2 *Manage Risk* (Mengelola Risiko)

Pastikan bahwa langkah-langkah untuk merebut peluang strategis dan mengurangi risiko ke tingkat yang dapat diterima dikelola sebagai portofolio.

RR2.1 *Inventory Controls* (Kontrol Inventaris)

Di seluruh area fokus risiko, inventarisasi kontrol untuk mengelola risiko dan memungkinkan risiko diambil sesuai dengan selera dan toleransi risiko. Klasifikasi kontrol (mis., prediktif, preventif, detektif, korektif) dan memetakannya ke pernyataan risiko TI khusus dan agregasi risiko TI. Kembangkan tes untuk desain kontrol dan tes untuk mengontrol efektivitas operasi. Identifikasi prosedur dan teknologi yang digunakan untuk memantau operasi kontrol (mis., pemantauan kontrol ketika TI terlibat atau otomatisasi proses pemantauan perusahaan).

RR2.2 *Monitor Operational Alignment With Risk Tolerance Thresholds* (Pantau Penyelarasan Operasional Dengan Ambang Toleransi Risiko)

Pastikan bahwa setiap lini bisnis menerima pertanggungjawaban untuk beroperasi dalam level toleransi individual dan portofolionya dan untuk memasukkan alat pemantauan ke dalam proses operasi utama. Pantau kinerja kontrol, dan ukur varians dari ambang terhadap sasaran.

RR2.3 *Respond To Discovered Risk Exposure And Opportunity* (Menanggapi Paparan Risiko Yang Ditemukan Dan Peluang)

Menekan proyek yang diharapkan untuk mengurangi potensi frekuensi dan besarnya peristiwa / kerugian yang merugikan, dan menyeimbangkannya dengan proyek yang memungkinkan perebutan peluang bisnis strategis. Mengadakan diskusi biaya / manfaat terkait kontribusi kontrol baru atau yang ada terhadap pengoperasian dalam toleransi risiko TI.

RR2.4 *Implement Controls* (Terapkan Kontrol)

Ambil langkah-langkah yang tepat untuk memastikan penyebaran efektif kontrol baru dan penyesuaian ke kontrol yang ada. Berkomunikasi dengan pemangku kepentingan utama di awal proses. Sebelum mengandalkan kontrol, lakukan uji coba dan tinjau data kinerja untuk memverifikasi operasi terhadap desain. Memetakan kontrol operasional baru dan yang diperbarui ke mekanisme pemantauan yang akan mengukur kinerja kontrol dari waktu ke waktu, dan tindakan korektif manajemen yang cepat bila diperlukan. Identifikasi dan latih staf tentang prosedur baru saat digunakan.

RR2.5 *Report It Risk Action Plan Progress* (Laporkan Kemajuan Rencana Tindakan Risiko TI)

Memantau rencana tindakan risiko TI di semua tingkatan untuk memastikan efektivitas tindakan yang diperlukan dan menentukan apakah penerimaan risiko residual telah diperoleh. Pastikan bahwa tindakan yang dilakukan dimiliki oleh pemilik proses yang terkena dampak dan penyimpangan dilaporkan kepada manajemen senior.

RR3 *React To Events* (Bereaksi Terhadap Peristiwa)

Pastikan bahwa langkah-langkah untuk meraih peluang langsung atau membatasi besarnya kerugian dari peristiwa terkait ti diaktifkan tepat waktu dan efektif.

RR3.1 *Maintain Incident Response Plans* (Pertahankan Rencana Dalam Merespon Kejadian)

Mempersiapkan materialisasi ancaman melalui rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat

menyebabkan dampak bisnis operasional, pengembangan dan / atau strategis (mis., insiden terkait TI) atau telah menyebabkan dampak bisnis. Pertahankan komunikasi terbuka tentang penerimaan risiko, kegiatan manajemen risiko, teknik analisis, dan hasil yang tersedia untuk membantu persiapan rencana. Ketika mengembangkan rencana aksi, pertimbangkan berapa lama perusahaan dapat terekspos dan berapa lama untuk pulih.

RR3.2 *Monitor It Risk* (Pantau Risiko TI)

Pantau lingkungan. Ketika batas kontrol telah dilanggar, naik ke langkah berikutnya atau konfirmasikan bahwa ukuran kembali dalam batas. Mengkategorikan insiden (mis., kehilangan bisnis, pelanggaran kebijakan, kegagalan sistem, penipuan, gugatan), dan membandingkan eksposur aktual dengan ambang batas yang dapat diterima. Mengkomunikasikan dampak bisnis kepada pengambil keputusan. Terus mengambil tindakan dan mendorong hasil yang diinginkan. Pastikan kebijakan dipatuhi dan bahwa ada akuntabilitas yang jelas untuk tindakan tindak lanjut.

RR3.3 *Initiate Incident Response* (Mulai Merespon Kejadian)

Ambil tindakan untuk meminimalkan dampak dari insiden yang sedang berlangsung. Identifikasi kategori insiden dan ikuti langkah-langkah dalam rencana respons. Beri tahu semua pemangku kepentingan dan pihak-pihak yang terkena dampak bahwa suatu insiden sedang terjadi. Identifikasi jumlah waktu yang diperlukan untuk melaksanakan rencana dan buat penyesuaian, jika perlu, untuk situasi yang dihadapi. Pastikan bahwa tindakan yang benar telah diambil.

RR3.4 *Communicate Lessons Learned From Risk Events* (Komunikasikan Pelajaran Yang Didapat Dari Peristiwa Berisiko)

Periksalah peristiwa / kerugian buruk masa lalu dan peluang yang hilang. Tentukan apakah ada kegagalan yang berasal dari kurangnya kesadaran, kemampuan atau motivasi.

E. Rekomendasi SOP

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

Standar Operasional Prosedur (SOP) adalah dokumen yang berkaitan dengan prosedur yang dilakukan secara kronologis untuk menyelesaikan suatu pekerjaan yang bertujuan untuk memperoleh hasil kerja yang paling efektif dari para pekerja dengan biaya yang serendah-rendahnya. SOP biasanya terdiri dari manfaat, kapan dibuat atau direvisi, metode penulisan prosedur, serta dilengkapi oleh bagan *flowchart* di bagian akhir (Laksmi, 2008, p.52).

Tujuan *Standar Operasional Prosedur* (SOP) adalah sebagai berikut (Indah Puji, 2014, p.30):

1. Untuk menjaga konsistensi tingkat penampilan kinerja atau kondisi tertentu dan kemana petugas dan lingkungan dalam melaksanakan sesuatu tugas atau pekerjaan tertentu.
2. Sebagai acuan dalam pelaksanaan kegiatan tertentu bagi sesama pekerja, dan supervisor.
3. Untuk menghindari kegagalan atau kesalahan (dengan demikian menghindari dan mengurangi konflik), keraguan, duplikasi serta pemborosan dalam proses pelaksanaan kegiatan.

4. Merupakan parameter untuk menilai mutu pelayanan.
5. Untuk lebih menjamin penggunaan tenaga dan sumber daya secara efisien dan efektif.
6. Untuk menjelaskan alur tugas, wewenang dan tanggung jawab dari petugas yang terkait.
7. Sebagai dokumen yang akan menjelaskan dan menilai pelaksanaan proses kerja bila terjadi suatu kesalahan atau dugaan mal praktek dan kesalahan administratif lainnya, sehingga sifatnya melindungi rumah sakit dan petugas.
8. Sebagai dokumen yang digunakan untuk pelatihan.
9. Sebagai dokumen sejarah bila telah di buat revisi SOP yang baru.

Sedangkan fungsi SOP adalah sebagai berikut (Indah Puji, 2014, p.35):

1. Memperlancar tugas petugas/pegawai atau tim/unit kerja.
2. Sebagai dasar hukum bila terjadi penyimpangan.
3. Mengetahui dengan jelas hambatan-hambatannya dan mudah dilacak.
4. Mengarahkan petugas/pegawai untuk sama-sama disiplin dalam bekerja.
5. Sebagai pedoman dalam melaksanakan pekerjaan rutin.

Manfaat SOP atau yang sering disebut sebagai prosedur tetap (protap) adalah penetapan tertulis mengenai apa yang harus dilakukan, kapan, dimana dan oleh siapa dan dibuat untuk menghindari terjadinya variasi dalam proses pelaksanaan kegiatan oleh pegawai yang akan mengganggu kinerja organisasi (instansi pemerintah) secara keseluruhan. SOP memiliki manfaat bagi organisasi antara lain (Permenpan No.PER/21/M-PAN/11/2008):

1. Sebagai standarisasi cara yang dilakukan pegawai dalam menyelesaikan pekerjaan khusus, mengurangi kesalahan dan kelalaian.

2. SOP membantu staf menjadi lebih mandiri dan tidak tergantung pada intervensi manajemen, sehingga akan mengurangi keterlibatan pimpinan dalam pelaksanaan proses sehari-hari.
3. Meningkatkan akuntabilitas dengan mendokumentasikan tanggung jawab khusus dalam melaksanakan tugas.
4. Menciptakan ukuran standar kinerja yang akan memberikan pegawai. cara konkret untuk memperbaiki kinerja serta membantu mengevaluasi usaha yang telah dilakukan.
5. Menciptakan bahan-bahan training yang dapat membantu pegawai baru untuk cepat melakukan tugasnya.
6. Menunjukkan kinerja bahwa organisasi efisien dan dikelola dengan baik.
7. Menyediakan pedoman bagi setiap pegawai di unit pelayanan dalam melaksanakan pemberian pelayanan sehari-hari.
8. Menghindari tumpang tindih pelaksanaan tugas pemberian pelayanan.
9. Membantu penelusuran terhadap kesalahan-kesalahan prosedural dalam memberikan pelayanan. Menjamin proses pelayanan tetap berjalan dalam berbagai situasi.

Prinsip-prinsip SOP dalam PERMENPAN PER/21/M-PAN/11/2008 disebutkan bahwa penyusunan SOP harus memenuhi prinsip-prinsip antara lain: kemudahan dan kejelasan, efisiensi dan efektivitas, keselarasan, keterukuran, dimanis, berorientasi pada pengguna, kepatuhan hukum, dan kepastian hukum.

1. Konsisten. SOP harus dilaksanakan secara konsisten dari waktu ke waktu, oleh siapapun, dan dalam kondisi apapun oleh seluruh jajaran organisasi pemerintahan.

2. Komitmen. SOP harus dilaksanakan dengan komitmen penuh dari seluruh jajaran organisasi, dari level yang paling rendah dan tertinggi.
3. Perbaikan berkelanjutan. Pelaksanaan SOP harus terbuka terhadap penyempurnaan-penyempurnaan untuk memperoleh prosedur yang benar-benar efisien dan efektif.
4. Mengikat. SOP harus mengikat pelaksana dalam melaksanakan tugasnya sesuai dengan prosedur standar yang telah ditetapkan.
5. Seluruh unsur memiliki peran penting. Seluruh pegawai peran-peran tertentu dalam setiap prosedur yang distandarkan. Jika pegawai tertentu tidak melaksanakan perannya dengan baik, maka akan mengganggu keseluruhan proses, yang akhirnya juga berdampak pada proses penyelenggaraan pemerintahan.
6. Terdokumentasi dengan baik. Seluruh prosedur yang telah distandarkan harus didokumentasikan dengan baik, sehingga dapat selalu dijadikan referensi bagi setiap mereka yang memerlukan.