ANALISIS MANAJEMEN RISIKO PADA PENGGUNAAN SISTEM INFORMASI PERPUSTAKAAN MENGGUNAKAN METODE *OCTAVE ALLEGRO* (STUDI KASUS : PERPUSTAKAAN UIN RADEN FATAH PALEMBANG)

SKRIPSI

Oleh

AFRIANI RIZKIKA
NIM. 13540007

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI RADEN FATAH

PALEMBANG

2018

ANALISIS MANAJEMEN RISIKO PADA PENGGUNAAN SISTEM INFORMASI PERPUSTAKAAN MENGGUNAKAN METODE *OCTAVE ALLEGRO* (STUDI KASUS : PERPUSTAKAAN UIN RADEN FATAH PALEMBANG)

SKRIPSI

Sebagai salah satu syarat untuk memperoleh gelar

Sarjana Sains dalam bidang Sistem Informasi

Oleh

AFRIANI RIZKIKA
NIM. 13540007

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI RADEN FATAH

PALEMBANG

2018

HALAMAN PENGESAHAN

ANALISIS MANAJEMEN RISIKO PADA PENGGUNAAN SISTEM INFORMASI PERPUSTAKAAN MENGGUNAKAN METODE *OCTAVE ALLEGRO*

Oleh :

Afriani Rizkika

13540007

Telah dipertahankan di depan sidang penguji skripsi

pada tanggal 7 Maret 2018

dan dinyatakan memenuhi syarat untuk memperoleh gelar

Sarjana Sains dalam bidang sistem informasi

PEMBIMBING I	PEMBIMBING II
Rusmala Santi, M.Kom	**Evi Fadilah, M.Kom**
NIP. 197911252014032002	**NIDN: 0215108502**

Mengetahui,

Kepala Program Studi Sistem Informasi

Fakultas Sains dan Teknologi

UIN Raden Fatah Palembang

Ruliansyah, M.Kom

NIP.197511222006041003

PERSETUJUAN

TIM PENGUJI SKRIPSI

Judul Skripsi	:	Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro
Nama	:	Afriani Rizkika
NIM	:	13540007
Program	:	Sarjana (S1) Fakultas Sains dan Teknologi

Telah disetujui oleh tim penguji sidang skripsi.

1. Ketua	:	Gusmelia Testiana, M.Kom NIP. 197508012009122001	(.....)
2. Sekretaris	:	Evi Fadilah. M.Kom NIDN. 021508502	(.....)
3. Penguji I	:	Gusmelia Testiana, M.Kom NIP. 197508012009122001	(.....)
4. Penguji II	:	Irfan Dwi Jaya, M.Kom NIDN. 0208018701	(.....)

Diuji di Palembang pada tanggal 7 Maret 2018

Waktu	: 09.00 – 10.00 WIB
Hasil/ IPK	: 3,12
Predikat	: Amat Baik

Dekan,
Fakultas Sains dan Teknologi
UIN Raden Fatah

KEMENTERIAN AGAMA R.I. uin RADEN FATAH PALEMBANG FAKULTAS SAINS DAN TEKNOLOGI PALEMBANG

Dr. Dian Erlina, SPd. M.Hum.
NIP.197101021999032001

MOTO DAN PERSEMBAHAN

MOTTO :

“Masalah Adalah Proses Menjadikan Diri Lebih Baik Lagi”

(Afriani Rizkika 07-04-1995)

Skripsi ini kupersembahkan :

ALLAH SWT.

mamaku Wanikma dan papaku Ismail Ishak yang tersayang

Saudara-saudariku Aghta Andrian, Ade Puspita Sari dan Ahmad Septian yang selalu memberikan dukungan, semangat, senyum dan do’anya untuk keberhasilan ini.

Serta Keluarga Besarku tercinta.

Agung Prandiko yang sudah menemaniku dari awal kuliah sampai sekarang, terima kasih juga untuk canda tawanya selama ini semoga impian kita selama ini dapat terwujud..

Sahabat kecilku Rabiah Al-Adawiyah dan Nadyah Khairiah

Sahabat kuliahku Anwar Sidik, Adholf Afriatama, Armansyah, Ade Sukmawati, Rika Seftiana, Atika Arpan dan Ardian Saputra terima kasih untuk canda tawa dan perjuangan yang kita lewati bersama dan terima kasih untuk kenangan manis yang telah mengukir selama ini.

Untuk teman-temanku SI angkatan 2013 khususnya kelas SI.A, terima kasih atas semuanya, semoga silaturahmi kita tetap terjaga dan sukses untuk kita semua baik dunia maupun akhirat.

Dan terakhir untuk ALMAMATER kebanggaanku, Agama, Bangsa dan Negaraku INDONESIA.

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Afriani Rizkika
Tempat dan tanggal lahir	: Palembang, 07 April 1995
Program Studi	: Sistem Informasi
NIM	: 13540007

Menyatakan dengan sesungguhnya bahwa:

1. Seluruh data, informasi, interprestasi serta pernyataan dalam pembahasan dan kesimpulan yang disajikan dalam Skripsi ini, kecuali yang disebutkan sumbernya ditulis dalam daftar pustaka adalah merupakan hasil pengamatan, penelitian, pengolahan, serta pemikiran saya dengana pengarahan dari para pembimbing yang ditetapkan.
2. Skripsi yang saya tulis ini adalah asli, bukan jiplakan dan belum pernah diajukan untuk mendapat gelar akademik, baik di UIN Raden Fatah maupun perguruan tingi lainnya.
3. Apabila dikemudian hari ditemukan adanya bukti ketidakbenaran dalam pernyataan tersebut diatas, maka saya bersedia menerima sanksi akademis berupa pembatalan gelar yang saya peroleh melalui pengajuan karya ilmiah ini.

Demikian pernyataan ini dibuat dengan penuh kesadaran dan dapat dipertanggungjawabkan.

Palembang, 7 Maret 2018

Afriani Rizkika
NIM.13540007

RISK MANAGEMENT ANALYSIS ON USING LIBRARY INFORMATION SYSTEM USING OCTAVE ALLEGRO METHOD

ABSTRACT

SLIMS (Senayan Library Management System) is an open source library management system software licensed under GPL v3. The SLIMS feature is the Online public Acess catalog (OPAC), the circulation of lending and return, lending rules, membership management, inventory collection, reports and statistics, barcode making. Protection of information assets is necessary in maintaining information security because in the process of storage and use, threats that may affect the confidentiality, integrity and availability of information may invade information assets. The rapid implementation of library information systems poses a risk that can be threatened by librarian failure in assessing the source of the threat. Risk assessment is part of risk management, undertaken to assess how likely it is to threat and vulnerability to the information system and its assets. OCTAVE Allegro is a framework that focuses on risk assessment of critical information assets and is relatively easy to use because it does not require a lot of resources to do so. The end result of the risk assessment is a recommendation on the steps to be taken for the protection of the information system and its assets.

Keywords: Analysis, Risk Management, *OCTAVE Allegro*, SLiMS

ANALISIS MANAJEMEN RISIKO PADA PENGGUNAAN SISTEM INFORMASI PERPUSTAKAAN MENGGUNAKAN METODE *OCTAVE ALLEGRO*

ABSTRAK

SLiMS (Senayan Library Management System) adalah perangkat lunak sistem manajemen perpustakaan (library management system) sumber terbuka yang dilisensikan di bawah GPL v3. Adapun fitur SLIMS yaitu, Online public Acess catalog (OPAC), sirkulasi pinjam dan kembali, aturan peminjaman, manajemen keanggotaan, inventaris koleksi, laporan dan statistik, pembuatan barcode. Perlindungan terhadap aset informasi sangat diperlukan dalam menjaga keamanan informasi karena dalam proses penyimpanan serta penggunaannya, ancaman yang dapat mempengaruhi kerahasiaan, integritas dan tersedianya dari informasi dapat menyerang aset informasi. Penerapan sistem informasi perpustakaan yang berkembang pesat menimbulkan risiko yang dapat mengancam disebabkan kegagalan pustakawan dalam menilai sumber ancaman. Penilaian risiko merupakan bagian dari manajemen risiko, dilakukan untuk menilai seberapa besar kemungkinan adanya ancaman dan kerentanan terhadap sistem informasi beserta aset-asetnya. OCTAVE Allegro merupakan framework yang fokus pada penilaian risiko terhadap aset informasi kritikal dan relatif mudah digunakan karena tidak membutuhkan banyak resource untuk melakukannya. Hasil akhir dari penelitian ini menunjukkan bahwa pada perpustakaan UIN Raden Fatah Palembang dampak yang paling tinggi risiko berdasarkan OCTAVE Allegro yaitu pada *IT Risk* dan Financial, karena belum adanya anggaran khusus untuk pembiayaan dalam pengelolaan dan perawatan untuk sistem SLiMS (*Senayan Library Management System*) di perpustakaan UIN Raden Fatah Palembang .

Kata Kunci : Analisis, Manajemen Risiko, *OCTAVE Allegro*, SLiMS

KATA PENGANTAR

Assalamu'alaikum, Wr. Wb

Alhamdulillah, Segala puji kehadirat Allah Subhanahu Wa Ta'ala karena atas berkat rahmat dan hidayah-Nya sehingga skripsi ini dapat terselesaikan sebagai salah satu syarat untuk menyelesaikan studi Strata Satu (S-1) pada Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Raden Fatah Palembang. Shalawat beserta salam semoga senantiasa tercurah kepada junjungan kita Baginda Rasulullah Shalallahu Alaihi Wassalam beserta para keluarga, sahabat dan para pengikut Beliau hingga akhir zaman.

Setelah melakukan kegiatan penelitian akhirnya laporan skripsi yang berjudul **"Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode *OCTAVE Allegro* (Studi Kasus : Perpustakaan UIN Raden Fatah Palembang)".** Pembuatan skripsi ini mendapatkan banyak bantuan dan bimbingan dari berbagai pihak dengan memberikan banyak masukan dan nasehat, serta mendukung dan menjadi motivasi tersendiri. Maka dari itu ucapan terima kasih penulis haturkan kepada yang terhormat:

1. Bapak Prof. Drs. H. Muhammad Sirozi, Ph.D selaku Rektor Universitas Islam Negeri Raden Fatah Palembang.
2. Ibu Dr. Dian Erlina, S.Pd, M.Hum selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Raden Fatah Palembang.
3. Bapak Ruliansyah, S.T, M.Kom selaku Ketua Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Raden Fatah Palembang.
4. Ibu Rusmala Santi M.Kom selaku Sekretaris Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Raden Fatah Palembang dan Dosen Pembimbing I (Satu).
5. Ibu Evi Fadilah, M.Kom selaku Dosen Pembimbing II (Dua).
6. Bapak Opi Palopi M.Ag selaku Dosen Pembimbing Akademik.
7. Kedua Orang tua saya Bapak Ismail Ishak (Alm) dan Ibu Wanikma.

8. Ibu Nurmalina. S.Ag., SS. M.Hum selaku kepala perpustakaan.
9. Agung Prandiko yang selalu menemani dari awal kuliah sampai sekarang.
10. Rekan mahasiswa/I Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Raden Fatah Palembang Angkatan 2013, khususnya kelas 1354-A serta rekan bimbingan periode 2017-2018.

Semoga Allah SWT senantiasa melimpahkan rahmat dan hidayah-Nya kepada kita semua, Amin Yaa Rabbal Alamin.

Wassalamu'alaikum, Wr.Wb

Palembang, 7 Maret 2018

Afriani Rizkika

Nim 13540007

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Manajemen risiko telah menjadi bagian penting dari strategi manajemen semua organisasi. Manajemen risiko sangatlah penting untuk menjalankan tujuan bisnis pada organisasi, diperlukan manajemen risiko untuk menghindari hal yang tidak diinginkan pada organisasi yang dapat merugikan organisasi itu sendiri jika manajemen risiko diabaikan.

Dalam manajemen risiko organisasi mulai dengan melihat seperti apa perencanaan manajemen risiko, dan bagaimana organisasi dapat melakukan risiko untuk menjalankan tujuan pada organisasi. Kemudian organisasi melihat pilihan yang dimiliki dalam menangani setiap risiko tersendiri, dan bagaimana organisasi dapat menentukan strategi mana yang digunakan. Dan akhirnya akan melihat bagaimana suatu organisasi dapat memonitor risiko dalam mengidentifikasi dan menangani risiko yang baru.

Terdapat banyak metode yang digunakan dalam menganalisis manajemen risiko. Salah satu cara untuk melaksanakan kegiatan manajemen risiko teknologi informasi adalah dengan menggunakan metode atau framework penilaian risiko Framework NIST SP 800-30 membahas manajemen risiko yang behubungan dengan model proses analisis secara rinci dalam tingkat praktek manajemen sesuai dengan siklus hidup pengembangan sistem (*System Development Life Cycle).* Perumusan manajemen risiko teknologi informasi berbasis ISO 31000 dilaksanakan melalui tahapan-tahapan penentuan konteks dan kriteria risiko,

identifikasi risiko, analisa risiko, evaluasi risiko dan penentuan perlakukan risiko. Teknik yang digunakan untuk melakukan identifikasi, analisa dan juga evaluasi risiko sangat bergantung pada kondisi masing-masing lembaga dan juga ketersediaan data yang berkaitan dengan risiko teknologi informasi. Pada *OCTAVE Allergo* penelitian memfokuskan pada identifikasi, analisis dan penilaian risiko, *OCTAVE Allegro* dapat dilakukan dalam bentuk workshop, setting bersama yang didukung dengan panduan, lembar kerja, dan kuesioner, yang terdapat dalam lampiran *OCTAVE Allegro*. Salah satu kelebihan *OCTAVE Allegro* selain cocok untuk digunakan oleh individu yang ingin melakukan penilaian risiko yang komprehensif tanpa keterlibatan yang luas dari organisasi, ahli atau sumber daya yang ada juga memiliki kelebihan lainnya yaitu *OCTAVE Allegro* direkomendasikan untuk peniaian risiko container informasi

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Allegro merupakan metodologi untuk merampingkan dan mengoptimalkan proses penilaian risiko keamanan informasi sehingga organisasi dapat memperoleh hasil yang cukup dengan investasi waktu yang singkat, orang dan sumber daya yang terbatas dalam hubungannya dengan informasi, layanan dan proses bisnis. Metodologi ini berbeda dari pendekatan-pendekatan lain karena fokus utamanya adalah pada aset informasi yang digunakan, di mana informasi disimpan, dipindahkan dan diproses, dan bagaimana informasi mempunyai dampak ancaman, kerentanan dan gangguan, pengguna *OCTAVE Allegro* memetakan aset informasi ke semua wadah tempat penyimpanan, transportasi, atau pemrosesan dan mempertimbangkan ancaman terhadap masing-masing wadah tersebut. Proses pengumpulan data berbasis lokakarya yang melekat pada

metode *OCTAVE Allegro* yang ada telah dieliminasi dan diganti dengan lembar kerja yang disederhanakan dan panduan terstruktur. Di *OCTAVE Allegro* semua informasi yang relevan tentang risiko spesifik untuk aset informasi ditangkap di lembar kerja risiko aset informasi. Pada lembar kerja ini, informasi ancaman dan dampak yang terkait dengan risiko ditangkap, skor risiko relatif dihitung, dan rencana dan kegiatan mitigasi didokumentasikan. Hal ini secara signifikan mengurangi manipulasi dokumentasi, organisasi, dan data yang diperlukan untuk melakukan penilaian risiko dan menghasilkan pandangan risiko yang jauh lebih singkat yang dapat dikomunikasikan dan dibagi.

Pepustakaan UIN Raden Fatah berdiri seiring dengan diresmikannya IAIN Raden Fatah pada tanggal 13 November 1964 bertepatan dengan tanggal 8 Rajab 1384 H. Perpustakaan UIN Raden Fatah telah mengaplikasikan sistem informasi yang dilatarbelakangi oleh pengetahuan, perkembangan ilmu dan teknologi. Perpustakaan UIN Raden Fatah yang pemenuhan kebutuhannya bertumpu pada sistem informasi pada setiap layanannya yang memuat aset informasi dalam melindungi sistem informasi yang ada di dalamnya perlu sebuah manajemen risiko untuk menanggulangi berbagai ancaman yang dapat mengganggu sistem informasi dan jaringannya. Untuk mengetahui proses penerapan manajemen risiko sistem informasi perpustakaan tersebut, diperlukan penelitian sejauh mana penerapan manajemen risiko sistem informasi perpustakaan dalam menilai sumber ancaman dan kerentanan, menganalisis, mengurangi, serta mengevaluasi risiko terhadap asset informasi perpustakaan UIN Raden Fatah.

Oleh karena itu, penelitian ini akan memberikan hasil penilaian terhadap risiko yang dimiliki oleh perpustakaan dan sebuah rekomendasi dalam mengelola

manajemen risiko. Rekomendasi yang dilakukan menggunakan *OCTAVE Allegro*. Rekomendasi yang diberikan tersebut berfungsi sebagai bantuan dalam mengatasi manajemen risiko untuk kedepannya.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan permasalahan dalam penelitian ini adalah :

1. Bagaimana penilaian terhadap manajemen risiko yang telah dilakukan di perpustakaan UIN Raden Fatah?
2. Bagaimana memberikan rekomendasi dalam mengelola manajemen risiko di perpustakaan UIN Raden Fatah?

1.3 Batasan Masalah

Penelitian yang dilakukan perlu dibatasi masalah yang akan dibahasnya, agar dalam penelitian dapat lebih terarah, batasan masalah diantaranya sebagai berikut:

1. Penilaian risiko ini berfokus pada 4 tahap dan 8 langkah.
2. Analisis manajemen risiko sistem informasi menggunakan metode *OCTAVE Allegro.*
3. Hasil dari penelitian ini berupa pendekatan pengurangan risiko sesuai dengan hasil yang diberikan oleh metode *OCTAVE Allegro.*

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Memberikan penilaian terhadap manajemen risiko yang telah dilakukan di Perpustakaan UIN Raden Fatah.
2. Memberikan rekomendasi dalam mengelola manajemen risiko di perpustakaan UIN Raden Fatah.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

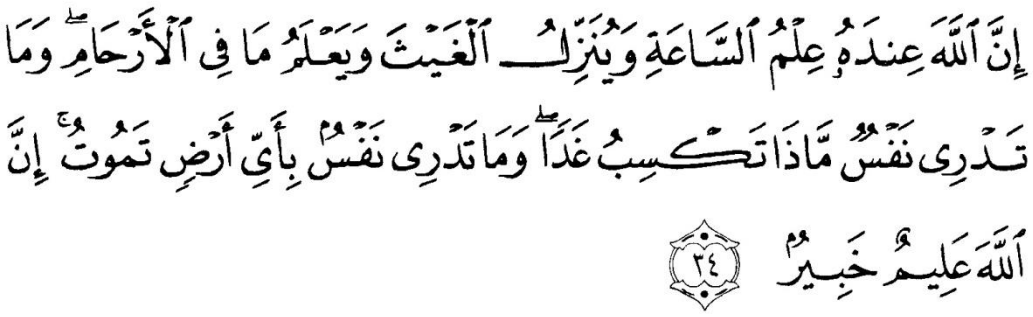
1. Mengurangi risiko terjadinya kerusakan pada sistem informasi perpustakaan beserta asetnya.
2. Mengurangi dampak kerugian akibat kerusakan sistem informasi perpustakaan.
3. Memudahkan penyusunan rencana kegiatan sehingga membuat kinerja organisasi menjadi lebih baik lagi kedepannya.
4. Dapat mengidentifikasikan keamanan dengan penilaian risiko.

BAB II

LANDASAN TEORI

2.1 Ayat Al-Qur'an Berkenaan dengan Penelitian

Dalam menjalankan usaha, seorang muslim dihadapkan pada ketidakpastian terhadap apa yang akan terjadi. Seseorang boleh saja merencanakan suatu usaha tapi tidak dapat memastikan apakah usahanya itu akan beruntung atau merugi. Sebagaimana dijelaskan dalam Al-Quran surat Luqman ayat 34 :


إِنَّ ٱللَّهَ عِندَهُۥ عِلْمُ ٱلسَّاعَةِ وَيُنَزِّلُ ٱلْغَيْثَ وَيَعْلَمُ مَا فِى ٱلْأَرْحَامِ ۖ وَمَا
تَدْرِى نَفْسٌ مَّاذَا تَكْسِبُ غَدًا ۖ وَمَا تَدْرِى نَفْسٌۢ بِأَىِّ أَرْضٍ تَمُوتُ ۚ إِنَّ
ٱللَّهَ عَلِيمٌ خَبِيرٌ ٣٤

Artinya:

"Sesungguhnya Allah, hanya pada sisi-Nya sajalah pengetahuan tentang Hari Kiamat; dan Dialah Yang menurunkan hujan, dan mengetahui apa yang ada dalam rahim. Dan tiada seorangpun yang dapat mengetahui (dengan pasti) apa yang akan diusahakannya besok. Dan tiada seorangpun yang dapat mengetahui di bumi mana dia akan mati. Sesungguhnya Allah Maha Mengetahui lagi Maha Mengenal". (QS. Luqman: 34)

Sudah menjadi sunatullah bahwa dalam menjalankan usaha maupun berinvestasi terkandung risiko di dalamnya. Tidak ada di dalam kehidupan ini yang bebas dari risiko. Oleh karena itu mengantisipasi dan mensiasati risiko agar tidak menimbulkan kerugian yang lebih besar diperbolehkan. Hal ini dijelaskan dalam Al-Qur'an surat Al Hasyr ayat 18 :

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱتَّقُواْ ٱللَّهَ وَلۡتَنظُرۡ نَفۡسٞ مَّا قَدَّمَتۡ لِغَدٖۖ
وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ خَبِيرُۢ بِمَا تَعۡمَلُونَ ١٨

Artinya :

"Hai orang-orang yang beriman, bertakwalah kamu pada Allah dan hendaklah setiap diri memperhatikan apa yang telah diperbuatnya untuk hari esok dan bertakwalah kepada Alloh. Sesungguhnya Alloh Maha Mengetahui apa yang kamu kerjakan".

Ayat tersebut menjelaskan bahwa seorang muslim diperbolehkan mempersiapkan apa yang diperbuat untuk hari esok dengan mengetahui, mempelajari dan menganalisa risiko yang akan terjadi dengan menerapkan manajemen risiko. Selanjutnya kita disuruh untuk bertawakal kepada Alloh terhadap apa yang terjadi setelah melakukan berbagai usaha tersebut. Karena manusia hanya bisa meramalkan dan memprediksi, selanjutnya Allah yang menetapkan terjadinya segala sesuatu.

Hubungan kedua ayat Al-Qur'an diatas dengan penelitian yang dilakukan yaitu pentingnya dalam melakukan manajemen risiko. Pada surat Luqman Ayat

34 menyatakan bahwa dalam menjalankan usaha terdapat risiko di dalamnya, dan tidak ada dalam kehidupan yang bebas dari risiko. Dan juga pada surat Al Hasyr ayat 18 menyatakan bahwa tiada seorangpun di alam semesta ini yang dapat mengetahui apa yang akan diperbuat, diusahakan, serta kejadian apa yang akan terjadi pada hari esok.

2.2 Teori yang Berhubungan dengan Penelitian

2.2.1 Manajemen Risiko

Manajemen risiko telah menjadi bagian penting dari strategi manajemen semua organisasi. Karena dalam manajemen risiko organisasi mulai dengan melihat seperti apa perencanaan manajemen risiko, dan bagaimana organisasi dapat melakukan risiko untuk menjalankan tujuan pada organisasi.

Tujuan dari manajemen risiko adalah untuk mengenali risiko dalam sebuah proyek dan mengembangkan strategi untuk mengurangi atau bahkan menghindarinya, dilain sisi juga harus dicari cara untuk memaksimalkan peluang yang ada (Nasrul, 2015).

Proses yang dilalui dalam manajemen risiko adalah:

1. Identifikasi Risiko. Proses identifikasi risiko dilakukan dengan menganalisis sumber risiko dari akrivitas perpustakaan.
2. Pengukuran risiko. Pengukuran risiko digunakan untuk mengukur ekspouser risiko perpustakaan sebagai acuan untuk memutuskan apakah perlu dilakukan proses pengendalian.

3. Pemantauan Risiko. Pemantaun risiko dilakukan terhadap besarnya eksposur risiko, toleransi risiko, kepatuhan limit internal, dan hasil stress *testing* maupun konsistensi pelaksanaa dengan kebijakan dan prosedur yang diterapkan.
4. Pengendalian Risiko. Pengendalian risiko adalah upaya untuk mengurangi atau menghilangkan risiko, disesuaikan dengan eksposur risiko dan tingkat risiko yang terjadi

Manajemen risiko memfasilitasi terjadinya perbaikan dan perkembangan organisasi / perusahaan secara berkelanjutan. Manajemen harus senantiasa mengembangkan dan menerapkan perbaikan strategi manajemen risiko serta meningkatkan maturitas dan kualitas pelaksanaan manajemen risiko.

Manajemen risiko melindungi dan menciptakan nilai tambah, manajemen risiko memberikan kontribusi melalui peningkatan tercapainya sasaran organisasi / perusahaan, dan perbaikan dalam aspek keselamatan kerja, kesehatan kerja, kepatuhan terhadap peraturan perundangan, perlindungan lingkungan hidup, persepsi publik, kualitas produk, reputasi, *corporate governance,* efisiensi operasi dan lain-lain (Hery, 2015: 29).

Dari pendapat diatas peneliti menyimpulkan bahwa manajemen risiko bagian dari tanggung jawab manajemen yang tidak terpisahkan dari proses bisnis dan proyek organisasi / perusahaan dalam mencapai sasaran.

2.2.2 Sistem Informasi Perpustakaan

Sistem Informasi Perpustakaan menurut Gordon B.davis (2003) : “Sistem Informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan

kebutuhan pengolahan data harian, penunjang kegiatan dalam penyimpanan data, dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan."

Sistem informasi perpustakaan merupakan sistem automasi perpustakaan. Di dalam sistem perpustakaan terdapat modul-modul yang terintegrasi dari sistem yang satu ke sistem yang lain. Adapun modul-modul yang dapat terintegrasi yaitu: (Harmawan, 2009).

1. Modul Pengadaan. Pengadaan merupakan kegiatan pokok dari perpustakaan atau puast dokumentasi karena kegiatan ini mengusahakan buku-buku yang dibutuhkan ada dalam koleksi. Modul pengadaan ini berfungsi untuk membuat daftar usulan buku dan daftar pengadaan buku.
2. Modul Pengatalogan. Katalog adalah daftar barang yang berada pada suatu tempat, sedangkan katalog perpustakaan adalah daftar bahan pustaka yang ada dalam perpustakaan. Yang tujuannya adalah untuk memudahkan para anggota perpustakaan untuk mengetahui koleksi perpustakaan dengan cepat. Adapun fungsi modul pengatalogan adalah untuk mengelola data koleksi buku maupun koleksi berkala.
3. Modul keanggotaan. Keanggotaan perpustakaan sagat perlu untuk mempermudah pengguna dalam meminjam koleksi perpustakaan. Untuk pengurusan keanggotaan setiap perpustakaan memiliki kebijakan sendiri. Modul keanggotaan berfungsi untuk mengelola data anggota seperti penambahan, pengeditan dan penghapusan data anggota.
4. OPAC Menurut Darmono (2007, 155) *Online Public Access Catalog* atau katalog *online* adalah sistem katalog perpustakaan yang menggunakan

komputer. Pangkalan data dirancang dan dibuat sendiri oleh perpustakaaan dengan menggunakan perangkat buatan sendiri, maupun menggunakan perangkat lunak komersial. Sesuai dengan namanya katalog online ini berfungsi seperti layaknya sebuah katalog yaitu sebagai sarana penelusuran koleksi milik suatu perpustaakaan. Katalog ini memberikan informasi bibliografis serta lokasi suatu buku di perpustakaan. katalog online merupakan suatu terobosan yang luar biasa di bidang kepustakawanan karena dapat memberikan titik cari (access point) dari segala aspek pendekatan pada data katalog. Otomasi perpustakaan akan memudahkan pengguna/pustakawan dalam menelusur informasi khususnya katalog melalui OPAC. Pengguna/pustakawan dapat menelusur suatu judul buku secara bersamaan. Disamping itu, mereka juga dapat menelusur buku dari berbagai pendekatan. Misalnya melalui judul, kata kunci, pengarang, kata kunci pengarang, subyek, kata kunci subyek dsb. Sedangkan apabila menggunakan katalog manual, pengguna/pustakawan hanya dapat akses melalui tiga pendekatan yaitu judul, pengarang, dan subyek.

2.2.3 *OCTAVE Allegro*

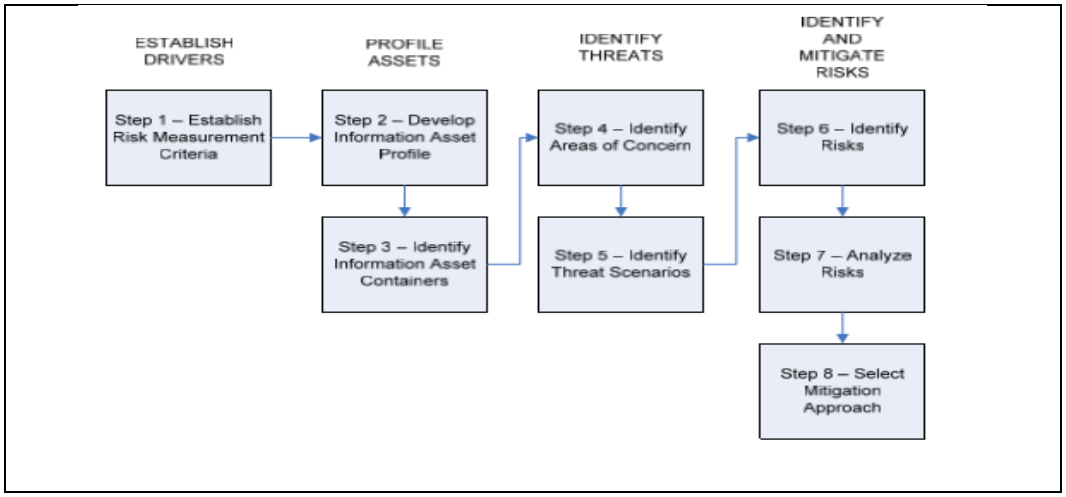
OCTAVE adalah metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan informasi. Hal ini dimaksudkan untuk membantu sebuah organisasi

1. mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi.

2. mengidentifikasi aset yang penting bagi misi organisasi.
3. mengidentifikasi kerentanan dan ancaman terhadap aset tersebut.
4. menentukan dan mengevaluasi konsekuensi potensial terhadap organisasi jika ancaman direalisasikan.

OCTAVE Allegro merupakan sebuah *framework* yang menggunakan pendekatan *OCTAVE* dan didesain untuk melakukan penilaian risiko terhadap operasional organisasi atau perusahaan dengan tujuan untuk menghasilkan hasil yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait penilaian risiko.

Kerangka konseptual yang membentuk dasar pendekatan *OCTAVE* asli diterbitkan oleh. (1999). Bekerja sama dengan *Telemedicine* dan *Advanced Technology Research Center (TATRC), SEI* mengembangkan metode *OCTAVE* untuk mengatasi tantangan kepatuhan keamanan yang dihadapi oleh Departemen Pertahanan AS (DoD) dalam menangani ketentuan-ketentuan Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) 1 untuk privasi dan keamanan kesehatan pribadi. Sejak diluncurkan pertama kali pada bulan September 1999, telah terjadi sejumlah pembaruan dan perubahan metodologi *OCTAVE*.



Sumber : Caralli,dkk. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.2007:4

Gambar 2.1 Langkah-langkah *OCTAVE Allegro*

Pendekatan *OCTAVE Allegro* terdiri dari delapan langkah yang disusun dalam empat tahap, seperti yang diilustrasikan pada diatas. Pada tahap 1, organisasi mengembangkan kriteria pengukuran risiko yang konsisten dengan pengemudi organisasi. Selama fase kedua, aset informasi yang dipastikan kritis diprofilkan. Proses pembuatan profil ini menetapkan batasan yang jelas untuk aset tersebut, mengidentifikasi persyaratan keamanannya, dan mengidentifikasi semua lokasi penyimpanan, pengiriman, atau pemrosesan aset. Pada fase 3, ancaman terhadap aset informasi diidentifikasi dalam konteks lokasi penyimpanan, pengiriman, atau pemrosesan aset. Pada tahap akhir, risiko terhadap aset informasi diidentifikasi dan dianalisis dan pengembangan pendekatan mitigasi dimulai. Keluaran dari setiap langkah dalam proses ditangkap pada serangkaian lembar kerja yang kemudian digunakan sebagai masukan ke langkah berikutnya dalam proses.

OCTAVE Allegro menyediakan analisis risiko kuantitatif sederhana dengan memperkenalkan konsep skor risiko relatif. Nilai risiko relatif adalah nilai yang diperoleh dari pertimbangan deskripsi kualitatif probabilitas risiko yang dikombinasikan dengan prioritas dampak risiko organisasi dalam hal kriteria pengukuran risiko organisasi. Skor dapat digunakan untuk membandingkan signifikansi relatif dari risiko individu. Persyaratan umum untuk *OCTAVE Allegro*

1. meningkatkan kemudahan penggunaan
2. menyempurnakan definisi lingkup penilaian
3. mengurangi persyaratan pelatihan dan pengetahuan
4. mengurangi komitmen sumber daya
5. mendorong pelembagaan dan pengulangan
6. menghasilkan hasil yang konsisten dan sebanding di seluruh perusahaan
7. memfasilitasi pengembangan kompetensi inti penilaian risiko
8. Mendukung persyaratan kepatuhan perusahaan Masing-masing persyaratan umum ini dibahas pada bagian berikut.

Pada *OCTAVE Allegro* semua informasi yang relevan tentang risiko spesifik untuk aset informasi ditangkap di lembar kerja risiko aset informasi. Pada lembar kerja ini, informasi ancaman dan dampak yang terkait dengan risiko ditangkap, skor risiko relatif dihitung, dan rencana dan kegiatan mitigasi didokumentasikan. Ini secara signifikan mengurangi manipulasi dokumentasi, organisasi, dan data yang diperlukan untuk melakukan penilaian risiko dan menghasilkan pandangan risiko yang jauh lebih ringkas yang dapat dikomunikasikan dan dibagi. Ini juga membantu organisasi untuk mengatur informasi risiko dengan cara yang

memungkinkan analisis akar permasalahan dan pengembangan strategi mitigasi, terutama di mana strategi ini dapat mengatasi lebih dari satu risiko. Selain itu, pengembangan lembar kerja memfasilitasi kemampuan organisasi untuk melakukan analisis kecenderungan di seluruh unit organisasi karena format standar dan konsisten untuk mendokumentasikan dan mengurangi risiko.

2.3 Teknik Analisis Data

2.3.1 Populasi

Populasi diartikan sebagai wilayah generalisasi yang terdiri atas: obyek/subyek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya. Jadi populasi bukan hanya orang, tetapi juga obyek dan benda-benda alam lain. Populasi juga bukan sekedar jumlah yang ada pada obyek/subyek yang dipelajari, tetapi meliputi seluruh karakteristik/sifat yang dimiliki oleh subyek atau obyek itu (Sugiyono, 2016:80).

Menurut Sudjana (2000), populasi merupakan totalitas semua nilai yang mungkin dapat dihitung atau dapat diukur, baik secara kuantitatif maupun kualitatif terhadap karakteristik tertentu mengenai sekumpulan objek yang lengkap dan jelas yang ingin dipelajari sifat-sifatnya, kedudukan populasi dalam suatu penelitian memegang peran yang sangat penting sebab populasi inilah yang kelak akan dikenai generalisasi.

Berdasarkan beberapa pendapat para ahli,maka penulis menyimpulkan bahwa populasi adalah jumlah keseluruhan dari semua objek yang akan dihitung

2.3.2 Teknik Pengambilan Sampel

Teknik pengambilan sampel yang digunakan dalam penelitian yaitu *Nonprobability Sampling*, dimana teknik pengambilan sampel yang tidak memberikan peluang/kesempatan sama bagi setiap unsur atau anggota populasi untuk dipilih menjadi sampel (Sugiyono, 2016:84).

Untuk menentukan sampel yang akan digunakan dalam penelitian, maka digunakan teknik sampling, sampel jenuh. Sampel jenuh adalah teknik penentuan sampel bila semua anggota populasi digunakan sebagai sampel. Hal ini sering dilakukan bila jumlah populasi relative kecil, kurang dari 30 orang atau penelitian yang ingin membuat generalisasi dengan kesalahan yang sangat kecil (Sugiyono, 2012:85).

2.4 Penelitian Terdahulu

Beberapa tinjaun pustakan yang berkaitan dengan manajemen risiko, berisi beberapa dari jurnal yang terdiri dari 4 jurnal berdasarkan penelitian yang telah dilakukan.

Rosini, dkk. Melakukan penelitian berjudul " Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode OCTAVE Allegro". Penelitian tersebut bertujuan untuk mengidentifikasi potensi kerawanan informasi yang ada sehingga informasi yang tersedia perpustakaan selalu mutakhir , siap dan dapat diakses dengan mudah ketika diperlukan sesuai dengan kebutuhan pemustakanya. Setelah melakukan identifikasi potensi kerawanan informasi Rosini, dkk. Memberikan hasil penilaian risiko yang dapat dilakukan dengan mengurangi atau menghilangkan risiko sebanyak 21 *area of concern*, memindahkan risiko

(transfer) atau mitigate sebanyak 16 *area of concern*, menunda risiko (*defer*) sebanyak 12 *area of concern*, dan menerima risiko (*accept*) atau menunda sebanyak 3 *area of concern.*

Nyoman Ayu Nila Dewi dan Gusti Putu Hardi Yudana melakukan penelitian dengan melakukan suatu pengukuran untuk menganalisa beberapa kemungkinan resiko yang akan muncul dalam suatu sistem dengan menggunakan metode OCTAVE Allegro. Dalam penelitiannya, Nyoman Ayu Nila Dewi dan Gusti Putu Hardi Yudana membahas tentang penilaian risiko yang mungkin akan terjadi dalam sistem dan memberikan penilaian dan rekomendasi mengenai langkah-langkah yang harus diambil untuk perlindungan sistem. Penelitian ini akan menilai dari sisi pengguna sistem dan pengelola sistem. Hasil penelitian ini akan menggambarkan suatu resiko yang mungkin akan terjadi dalam sistem e-learning dan penanganan dari resiko tersebut serta penilaian resiko yang terjadi. Judul penelitian yang dilakukan pada tahun 2016 saat itu ialah " Analisis Manajemen Risiko Pada Sistem Akademik di STMIK STIKOM BALI".

Penelitian yang dilakukan oleh Anita Wulansari pada tahun 2013 dengan judul " Analisis Penilaian Risiko Keamanan untuk Aset Informasi pada Usaha Kecil dan Menengah Bidang Finansial B2B". Dalam penelitian tersebut Anita Wulansari melakukan penilaian risiko terhadap asset teknologi informasi yang dimiliki oleh perusahaan keuangan kecil dan menengah. Penelitian ini akan memperlihatkan risiko-risko apa saja yang teridentifikasi dari aspek *technical, physical,* dan *people* pada asset informasi kritikal milik perusahaan serta pendekatan mitigasi yang sesuai untuk masing-masing risiko. Hasil penelitian ini adalah risiko-risko yang

teridentifikasi untuk masing-masing *container* dari asset informasi kritikal dan skor untuk tiap risiko sehingga perusahaan dapat menentukan strategi mitigasi yang tepat.

Deni Ahmad Jakaria, dkk melakukan penelitian dengan judul " Manajemen Risiko Sistem Informasi Akademik Pada Perguruan Tinggi Menggunakan Octave Allegro". Penelitian ini bertujuan untuk mengidentifikasi, menganalisis dan melakukan penilaian risiko agar dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada asset kritikal dan mengambil langkah-langkah pencegahan yang tepat. Selanjutnya hasil dari penilaian risiko dapat membuat perencanaan strategi untuk menjaga asset informasi kritikal secara tepat serta langkah-langkah pemulihan jika scenario ancaman benar-benar terjadi.

Dalam penelitian ini penulis melakukan suatu pengukuran untuk menganalisa beberapa kemungkinan risiko yang akan muncul dalam suatu sistem dengan menggunakan metode *OCTAVE Allegro*. Dalam penelitiannya penulis membahas tentang penilaian risiko yang mungkin akan terjadi dalam sistem dan memberikan penilaian dan rekomendasi mengenai langkah-langkah yang harus diambil untuk perlindungan sistem. Penelitian ini akan memberikan hasil penilaian terhadap risiko yang dimiliki oleh perpustakaan dan sebuah rekomendasi dalam mengelola manajemen risiko. Rekomendasi yang dilakukan menggunakan *OCTAVE Allegro*. Rekomendasi yang diberikan tersebut berfungsi sebagai bantuan dalam mengatasi manajemen risiko untuk kedepannya

BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah pendekatan kualitatif. Dimana metode kualitatif digunakan untuk penelitian yang bersifat seni (kurang terpola), dan disebut sebagai metode interpretive karena data dan hasil lebih berkenaan dengan interprestasi terhadap data yang ditemukan di lapangan. Filsafat positivisme memandang realitas/ gejala/ fenomena itu dapat diklasifikasikan, relative tetap, konkrit, teramati, terukur dan hubungan gejala bersifat sebab akibat. Penelitian pada umumnya dilakukan pada populasi atau sampel tertentu yang resprentif (Sugiyono, 2012:7). Beberapa ciri khas karakteristik kualitatif dapat dikemukakan sebagai berikut ini :

1. Dilakukan pada kondisi yang alamiah.
2. Penelitian kualitatif lebih 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 deduktif.
5. Penelitian kualitatif lebih menekankan makna (data dibalik yang teramati) (Sugiyono,2012:13)

3.2 Lokasi Penelitian

Lokasi penelitian dilakukan di UPT.Perpustakaan UIN Raden Fatah Palembang Jalan Prof. K.H. Zainal Abidin Fikri KM. 3,5, Pahlawan, Kemuning, Pahlawan, Kemuning, Kota Palembang, Sumatera Selatan 30126, Indonesia

3.3 Bahan Penelitian

Dalam penelitian ini bahan penelitian yang digunakan untuk kemudian diolah menjadi acuan adalah sebagai berikut :

1. Data yang berhubungan dengan penelitian yang tersedia di Perpustakaan UIN Raden Fatah Palembang.
2. Sistem Informasi Perpustakaan sebagai objek penelitian.
3. Karyawan perpustakaan UIN Raden Fatah Palembang yang menggunakan sistem informasi yang dimiliki oleh perpustakaan.

3.4 Metode Pengumpulan Data

3.4.1 Data Primer

Data primer adalah data informasi yang diperoleh tangan pertama yang dikumpulkan secara langsung dari sumbernya. Data primer ini adalah sumber data yang memberikan data kepada pengumpulan data melalui teknik observasi, wawancara, diskusi terfokus, dan penyebaran *kuesioner*. (Sugiyono, 2016:137).

1. *Interview* (Wawancara), Wawancara digunakan sebagai teknik pengumpulan data apabila peneliti ingin melakukan studi pendahuluan untuk menemukan

permasalahan yang harus diteliti, dan juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam dan jumlah respondennya sedikit/kecil. (Sugiyono, 2016: 137). Pada penelitian ini peneliti melakukan wawancara langsung kepada kepala perpustakaan.

2. Kuesioner (Angket), Angket atau kuesioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawab. (Sugiyono, 2016:142). Dilihat dari jumlah responden yang berjumlah 14 orang dan Kuesioner yang disebarkan, ditujukan kepada bagian-bagian responden yang memang benar-benar menggunakan layanan sistem informasi perusahaan dan bagian penyedia layanan. Ditetapkanya populasi dan sampel tersebut agar kusioner yang disebarkan tertuju pada sasaran yang tepat. Apabila sasaran kuesioner telah tepat, maka hasil dari perhitungan kusioner tidak dapat diragukan lagi.
3. *Observasi* (Pengamatan), Observasi dilakukan oleh peneliti dengan mengamati secara langsung mengenai perilaku manusia, proses kerja, gejala-gejala alam dan bila responden yang diamati tidak terlalu besar (Sugiyono, 2012:145).Observasi dalam penelitian ini adalah dengan mengamati secara langsung kejadian di Perpustakaaan UIN Raden Fatah Palembang.

3.4.2 Data Sekunder

Data sekunder sumber yang tidak langsung memberikan data kepada pengumpul data, misalnya lewat orang lain atau lewat dokumen (Sugiyono, 2012:137). Untuk mendapatkan data sekunder, peneliti mengumpulkan data-data yang berkaitan dengan penelitian, Data sekunder yang digunakan seperti data aset

informasi perpustakaan, dokumen-dokumen, baik dokumen tertulis atau *softcopy* maupun dokumen elektronik yang dapat mendukung dalam proses penulisan.

3.5 Populasi Dan Sampel

3.5.1 Populasi

Populasi yang digunakan dalam penelitian ini adalah karyawan perpustakaan pada perpustakaan UIN Raden Fatah Palembang. Adapun jumlah populasi pada perpustakaan UIN Raden Fatah Palembang sebanyak 14 orang. Karakteristik yang ditetapkan dalam penelitian ini adalah sebagai berikut ini :

1. Karyawan yang aktif dalam menggunakan sistem informasi perpustakaan.
2. Karyawan berjenis kelamin laki-laki dan perempuan
3. Karyawan yang berumur mulai dari 22 sampai 51 tahun keatas.
4. Pendidikan terakhir karyawan dari SMA sampai S3.
5. Karyawan yang sehat secara jasmani dan rohani saat pelaksanaan penelitian.

3.5.2 Sampel

Penelitian menggunakan teknik sampel jenuh, dimana sampel jenuh adalah seluruh jumlah populasi dijadikan sebagai sampel. Diambilnya seluruh jumlah populasi sebagai sampel karena jumlah populasi pada penelitian ini kurang dari 100 responden. Sehingga dapat dikatakan jumlah responden tidak terlalu banyak. Populasi yang ada ditujukan kepada bagian-bagian yang memang mengelola sistem informasi di perpustakaan. Sehingga berdasarkan pada populasi yang ada ialah 14 responden. Berikut rekap data karyawan Perpustakaan UIN Raden Fatah Palembang. Pada Tabel 3.1 sebagai berikut ini :

Tabel 3.1 Rekap Data Karyawan Perpustakaan UIN Raden Fatah 2017

No	Bagian	Jumlah
1	Kepala Perpustakaan	1 orang
2	Bagian Pengadaan dan Pengolahan Bahan Pustaka	3 orang
3	Layanan Local Content dan Koleksi Tandon	1 orang
4	Layanan sirkulasi dan Multimedia	5 orang
5	Referensi dan Jurnal Ilmiah	1 orang
6	Automasi / Jaringan dan Kerjasama	1 orang
7	Tata Usaha dan Umum	2 orang
Jumlah		14 orang

Sumber : Kepala Perpustakaan, UIN Raden Fatah Palembang.

3.6 Tahapan *Octave Allegro*

Didalam *OCTAVE Allegro* terdapat langkah-langkah yang digunakan untuk mengukur risiko yaitu :

1. Membangun Kriteria Pengukuran Risiko
2. Mengembangkan Profil Aset Informasi
3. Identifikasi Informasi Wadah Aset
4. Mengidentifikasi Area yang diperhatikan
5. Identifikasi Skenario Ancaman
6. Identifikasi Risiko
7. Analisis Risiko
8. Pendekatan Mitigasi

3.6.1 Membangun Kriteria Pengukuran Risiko

Pada Langkah 1 terdapat dua aktivitas yang dilakukan pada tahap ini, menetapkan penggerak organisasi yang akan digunakan untuk mengevaluasi dampak risiko terhadap misi dan tujuan bisnis organisasi. Driver ini tercermin dalam seperangkat kriteria pengukuran risiko yang akan dikembangkan.

Dalam penilaian *Allegro* akan menciptakan serangkaian kriteria pengukuran risiko yang mencerminkan berbagai area dampak yang penting (dan mungkin unik) untuk organisasi. Misalnya, area dampak dapat mencakup kesehatan dan keselamatan pelanggan dan karyawan, keuangan, reputasi, dan undang-undang dan peraturan. Satu set standar template lembar kerja akan digunakan untuk membuat kriteria ini di beberapa area dampak dan kemudian memprioritaskannya.

Langkah 1 Kegiatan 1

Tentukan seperangkat ukuran kualitatif (kriteria pengukuran risiko) yang dengannya dapat mengevaluasi dampak risiko terhadap misi dan tujuan bisnis organisasi. Dokumentasikan kriteria di Lembar Kerja Kriteria Pengukuran Risiko. Minimal, perhatikan area dampak berikut ini:

1. Reputasi / kepercayaan pelanggan (Lembar kerja 1, Lampiran B)
2. Keuangan (Lembar kerja 2, Lampiran B)
3. Produktivitas (Lembar Kerja 3, Lampiran B)
4. Keselamatan dan Kesehatan Kerja (Lembar Kerja 4, Lampiran B)
5. Denda / denda hukum (Lembar kerja 5, Lampiran B)
6. Area dampak yang ditentukan pengguna (Lembar kerja 6, Lampiran B)

Langkah 1 Aktivitas 2

Memprioritaskan area dampak dari yang paling penting hingga yang tidak penting dengan menggunakan lembar kerja peringkat area dampak (Lembar Kerja 7, Lampiran B). Kategori yang paling penting harus mendapat nilai tertinggi dan paling tidak penting yang paling rendah.

3.6.2 Mengembangkan Profil Aset Informasi

Penilaian risiko yang dilakukan difokuskan pada aset informasi organisasi. Pada langkah 2 terdapat delapan aktivitas yang dilakukan, memulai proses mendefinisikan aset informasi tersebut. Kemudian, mengidentifikasi wadah di mana aset informasi "hidup" dan kustodian dari kontainer tersebut. Ini akan membantu untuk sepenuhnya mengidentifikasi semua poin di mana aset informasi mungkin rentan terhadap pengungkapan, modifikasi, kehilangan / penghancuran, atau gangguan. Profil dibuat untuk setiap aset informasi, membentuk dasar untuk identifikasi ancaman dan risiko dalam langkah selanjutnya.

Langkah 2 Kegiatan 1

Kegiatan pertama dalam tahap penilaian risiko ini melibatkan identifikasi kumpulan aset informasi dimana penilaian dapat dilakukan. Penilaian tersebut memberikan sebagian besar utilitas bila berfokus pada aset informasi yang paling penting bagi organisasi. Bergantung pada tingkat di mana akan melakukan penilaian risiko ini, "organisasi" mungkin diganti oleh departemen, divisi, atau sublevel organisasi lainnya.

Langkah 2 Kegiatan 2

"Berfokus pada beberapa kritis" adalah prinsip manajemen risiko yang penting. Dengan demikian, harus melakukan penilaian risiko terstruktur hanya pada aset-aset yang penting untuk mencapai tujuan dan mencapai misi organisasi, dan juga hal-hal yang penting karena faktor-faktor seperti kepatuhan terhadap peraturan.

Langkah 2 Kegiatan 3

Dalam kegiatan berikut (3-8) harus mengumpulkan informasi tentang aset informasi yang diperlukan untuk memulai proses penilaian risiko terstruktur. Gunakan *Critical Information Asset Profile* (Lembar Kerja 8, Lampiran B) untuk mencatat informasi ini.

Untuk memulai, catat nama aset informasi penting di kolom (1) dari *Critical Information Asset Profile*.

Langkah 2 Kegiatan 4

Dokumentasikan dasar pemikiran untuk memilih aset informasi penting di kolom (2) dari *Critical Information Asset Profile*.

Langkah 2 Kegiatan 5

Catatlah deskripsi untuk aset informasi penting di kolom (3) profil aset informasi kritis. Menentukan ruang lingkup aset informasi dan menggunakan definisi umum yang disepakati.

Langkah 2 Kegiatan 6

Mengidentifikasi dan mendokumentasikan pemilik aset informasi penting. (Lihat definisi yang diberikan di atas untuk menentukan siapa pemiliknya. Catatlah informasi ini di kolom (4) dari *Critical Information Asset Profile*.

Langkah 2 Kegiatan 7

Catat persyaratan keamanan untuk kerahasiaan, integritas, dan ketersediaan di kolom (5) Lembar kerja informasi kritis. Mulailah dengan memeriksa persyaratan yang berlaku untuk aset informasi, dan lanjutkan dengan mengisi informasi yang melengkapi setiap pernyataan persyaratan keamanan.

Langkah 2 Kegiatan 8

Identifikasi persyaratan keamanan terpenting untuk aset informasi dengan menandai 'X' di kotak di samping kategori persyaratan keamanan di kolom (6) Lembar kerja informasi kritis. Menggunakan informasi ini saat Anda menentukan dampak potensial dari risiko, jadi penting untuk memilih persyaratan keamanan ini dengan hati-hati.

3.6.3 Mengidentifikasi Informasi Wadah Aset

Pada langkah 3 hanya ada satu aktivitas yang dilakukan. Tempat penyimpanan aset, penyimpanan, atau pemrosesan informasi dapat menjadi titik kerentanan dan ancaman yang membahayakan aset informasi. Wadah biasanya dikenali sebagai beberapa jenis aset teknis - perangkat keras, perangkat lunak, atau sistem - namun wadah juga dapat menjadi benda fisik seperti selembar kertas

atau orang yang penting bagi organisasi. Wadah orang sangat penting sehubungan dengan kekayaan intelektual atau informasi yang umumnya sensitif atau rahasia.

Dalam penilaian risiko keamanan informasi, identifikasi kontainer sangat penting untuk mengidentifikasi risiko terhadap aset informasi itu sendiri. Dengan memetakan aset informasi ke semua kontainer Yang dijalaninya, kegiatan ini mendefinisikan batasan lingkungan dan infrastruktur teknis yang harus diperiksa untuk risiko

Langkah 3 Kegiatan 1

Menggunakan peta lingkungan risiko aset informasi (Lembar Kerja 9a, 9b, dan 9c, Lampiran B) mengidentifikasi dan mendokumentasikan wadah dimana aset informasi disimpan, dikirim, atau diproses sebagai berikut:

1. Menggunakan Lembar Kerja 9a untuk mengidentifikasi wadah teknis yang berada di bawah kontrol langsung organisasi (internal) atau organisasi yang dikelola di luar organisasi (eksternal)
2. Gunakan Lembar Kerja 9b untuk mengidentifikasi lokasi fisik tempat aset informasi ada di dalam atau di luar organisasi
3. Lembar Kerja Pengguna 9c untuk mengidentifikasi orang-orang internal atau eksternal organisasi yang mungkin memiliki pengetahuan terperinci tentang aset informasi.

3.6.4 Mengidentifikasikan Area yang diperhatikan

Hanya ada satu aktivitas di langkah 4 , memulai proses pengembangan profil risiko aset informasi. Area yang menjadi perhatian dapat menjadi ciri

ancaman yang unik bagi organisasi dan kondisi pengoperasiannya yang unik. Tujuan dari langkah ini bukan untuk menangkap daftar lengkap semua skenario ancaman yang mungkin untuk aset informasi.

Langkah 4 Kegiatan 1

Untuk melakukan aktivitas ini, gunakan peta lingkungan informasi aset risiko untuk referensi dan lembar kerja risiko aset informasi (Lembar Kerja 10, Lampiran A) untuk mencatat bidang perhatian.

Untuk mengidentifikasi area yang menjadi perhatian, lakukan langkah-langkah berikut:

1. Menggunakan peta lingkungan risiko aset informasi, tinjau kembali setiap kontainer yang dicantumkan untuk membuat diskusi tentang area potensial yang menjadi perhatian.
2. Dokumentasikan setiap bidang perhatian yang diidentifikasi di lembar kerja risiko aset informasi. Pada lembar kerja, catat nama aset informasi dan dokumentasikan area yang menjadi perhatian sedetail mungkin. Lengkapi kolom yang diberi label "Aset Informasi" dan "Area Kepedulian" pada lembar kerja dan ingatlah untuk menggunakan lembar kerja terpisah untuk setiap area perhatian yang di identifikasi.
3. Perluas bidang perhatian untuk menciptakan skenario ancaman. Skenario ancaman adalah ekspresi sifat ancaman yang lebih rinci. Untuk setiap area perhatian yang telah di catat di lembar kerja risiko aset informasi, kolom

lengkap (1) sampai (4) dengan merekam aktor, maksud, motif, dan hasil. Jika tidak dapat menyelesaikan beberapa elemen ini, biarkan kosong.

4. Dalam kolom (5) mendokumentasikan bagaimana ancaman ini akan mempengaruhi persyaratan keamanan yang telah ditetapkan untuk aset informasi. Terus lakukan aktivitas ini untuk setiap lembar kerja risiko aset informasi sampai semua area perhatian yang telah diperluas. Informasi risiko yang tersisa akan dikumpulkan pada langkah selanjutnya.
5. Lanjutkan melalui masing-masing wadah yang terdaftar di peta lingkungan risiko aset informasi dan daftarkan sebanyak mungkin bidang yang menjadi perhatian. Ingat, satu wadah dapat menyebabkan identifikasi satu atau lebih area yang menjadi perhatian.

3.6.5 Identifikasi Skenario Ancaman

Pada Langkah 5 ada tiga aktivitas yang dilakukan yaitu mencatat area kekhawatiran yang dapat mempengaruhi aset informasi. Dalam langkah ini, area yang menjadi perhatian diperluas menjadi skenario ancaman yang lebih jauh menjelaskan sifat ancaman. Untuk memperluas area yang menjadi perhatian dalam skenario ancaman, harus terlebih dahulu memahami komponen dasar dari sebuah ancaman.

Langkah ini berguna untuk memberikan pertimbangan atas kemungkinan dalam skenario ancaman. Kemungkinan ini kemudian dibagi ke dalam *high*, *medium*, atau *low*.

Langkah 5 Kegiatan 1

Dalam kegiatan ini, akan mengidentifikasi skenario ancaman tambahan yang belum diunggulkan oleh area yang menjadi perhatian. Untuk melakukan ini, Gunakan "*Appendix C - Threat Scenarios Questionnaires*." Ada satu kuesioner untuk setiap jenis wadah (teknis, fisik, dan manusia). Setiap kuesioner berisi kumpulan skenario yang diikuti oleh pertanyaan yang dirancang untuk membantu benih identifikasi ancaman tambahan.

Untuk menyelesaikan aktivitas ini, gunakan peta lingkungan aset informasi yang di buat di Langkah 4 (Lembar Kerja 9a, 9b, dan 9c) sebagai panduan.

1. Lanjutkan ke skenario-skenario ancaman 1 - Wadah Teknis. Mengingat wadah teknis yang di cantumkan di Lembar Kerja 9a, jawablah pertanyaannya. Lingkari respon yang tepat.
2. Lanjutkan melalui scenario-skenario ancaman 2 - skenario fisik dan skenario ancaman 3 - Orang. Gunakan lembar kerja 9b dan 9c untuk membantu dalam menyelesaikan kuesioner.

Langkah 5 Kegiatan 2

Dalam kegiatan ini, melengkapi lembar kerja risiko aset informasi untuk masing-masing skenario ancaman generik yang di identifikasi untuk dipertimbangkan pada kuesioner.

1. Tinjau tanggapan pada scenario-skenario ancaman. Tidak perlu melakukan apapun lebih jauh untuk setiap skenario di mana Anda memutar "tidak".

2. Untuk semua jawaban "ya", catat lembar kerja risiko aset informasi baru. Lengkapi bagian (1) sampai (5) pada lembar kerja ini. Jika menemukan bahwa yang telah menjawab "ya" untuk sebuah pertanyaan, namun tidak dapat menemukan situasi kehidupan nyata yang sesuai, lanjutkan.
3. Terus sampai setidaknya ada satu Lembar Kerja Risiko Aset Informasi yang diselesaikan untuk setiap jawaban "ya" pada setiap kuesioner skenario ancaman.

Langkah 5 Kegiatan 3

Kegiatan ini bersifat opsional untuk semua profil risiko aset informasi. Jika memilih untuk melakukannya, Lakukan di semua profil. Dan juga harus memutuskan untuk menambahkan kemungkinan pada deskripsi skenario ancaman yang di tangkap di lembar kerja risiko aset informasi Probabilitas membantu menentukan skenario mana yang lebih mungkin diberikan pada konteks operasi unik. Ini akan berguna kemudian dalam menentukan bagaimana memprioritaskan kegiatan mitigasi risiko. Karena seringkali sangat sulit untuk mengukur probabilitas secara akurat (terutama berkenaan dengan kerentanan dan kejadian keamanan), probabilitas dinyatakan dalam penilaian risiko ini secara kualitatif seperti tinggi, sedang, atau rendah.

Dengan kata lain, menentukan apakah ada kemungkinan (tinggi) yang kuat bahwa skenario yang telah di dokumentasikan dapat terjadi, peluang menengah (netral), atau jika skenario tidak mungkin (rendah). Jika memilih untuk membuat

keputusan ini, harus memeriksa kotak probabilitas yang sesuai di kolom (6) untuk masing-masing lembar kerja risiko yang dibuat.

3.6.6 Identifikasi Risiko

Pada langkah keenam, konsekuensi bagi organisasi jika sebuah ancaman terjadi dicatat, dalam mendapatkan gambaran risiko secara lengkap. Sebuah ancaman dapat mempunyai akibat – akibat yang potensial bagi organisasi.

Langkah 6 Kegiatan 1

Dalam kegiatan ini, menentukan bagaimana skenario ancaman yang di catat di lembar kerja risiko aset informasi masing-masing dapat memengaruhi organisasi.

1. Untuk setiap skenario ancaman yang di dokumentasikan di lembar kerja risiko aset informasi, tentukan bagaimana organisasi akan terkena dampak jika skenario ancaman ini terwujud. Inilah konsekuensi dari ancaman dan melengkapi persamaan risiko.
2. Dokumentasikan minimal satu konsekuensi dalam bagian (7) lembar kerja risiko aset informasi. Konsekuensi tambahan dapat didokumentasikan seperlunya. Jadilah sespesifik mungkin. Cobalah untuk mempertimbangkan area dampak dari kriteria evaluasi risiko untuk mempertimbangkan konsekuensinya. Perhatikan juga hasil yang di pertimbangkan di Langkah 5, Aktivitas 5.

3.6.7 Analisis Risiko

Pada Langkah 7, secara kualitatif mengukur sejauh mana organisasi dipengaruhi oleh ancaman dengan menghitung nilai risiko untuk setiap risiko terhadap setiap aset informasi. Informasi penilaian ini digunakan untuk menentukan risiko yang harus segera diatasi dan untuk memprioritaskan tindakan mitigasi untuk sisa risiko pada Langkah 8.

Dalam kegiatan ini, akan menghasilkan skor risiko relatif. Skor risiko relatif diperoleh dengan mempertimbangkan sejauh mana konsekuensi dari risiko mempengaruhi organisasi dibandingkan dengan kepentingan relatif dari berbagai area dampak. Dengan kata lain, jika area "reputasi" paling penting bagi organisasi dan konsekuensi dari suatu risiko menyebabkan dampak yang luas terhadap reputasi, mungkin perlu mengambil tindakan untuk memastikan bahwa risiko ini dikurangi. Dengan menggunakan kriteria ini, memastikan bahwa risiko dinilai dalam konteks pengantar organisasi .

Langkah 7 Kegiatan 1

Mulailah dengan meninjau kriteria pengukuran risiko yang di buat di Langkah 1, Aktivitas 1. Fokus pada bagaimana mendefinisikan dampak tinggi, menengah, dan rendah untuk organisasi.

Dengan menggunakan kriteria pengukuran risiko sebagai panduan, evaluasi konsekuensi relatif terhadap masing-masing area dampak dan catat nilai "tinggi," "sedang," atau "rendah" di kolom "Nilai" kolom (8). Jika telah menulis lebih dari satu pernyataan konsekuensi, pastikan untuk mempertimbangkan

semuanya karena harus menugaskan nilai ke area dampak. kemudian mencatat nilai di masing-masing area dampak.

Langkah 7 Kegiatan 2

Pada langkah ini, skor risiko relatif akan dihitung yang dapat digunakan untuk menganalisis risiko dan membantu organisasi menentukan strategi risiko yang tepat. Anda akan melakukan langkah ini di kolom "Skor" kolom (8) pada masing-masing Lembar Kerja Risiko Aset Informasi.

1. Hitung skor untuk setiap area dampak dengan mengalikan luas area dampak dengan nilai dampak. (Lihat lembar kerja peringkat area dampak yang di buat di Langkah 1, Aktivitas 2.) Catat hasilnya di kolom "skor". Nilai dampak diberi nilai kuantitatif sebagai berikut: Tinggi - 3, Sedang - 2, dan Rendah - 1. Pastikan untuk menjaga nilai-nilai ini tetap konsisten di seluruh lembar kerja risiko.
2. Total kolom skor. Total ini adalah skor risiko relatif.
3. Perhatikan contoh berikut. Organisasi tersebut menempatkan area dampaknya seperti yang ditunjukkan di bawah ini. Area keuangan dianggap sebagai area dampak yang paling penting dan keamanan dan kesehatan yang paling tidak penting. Nilai dampak diberikan di Kegiatan 1 karena konsekuensinya dipertimbangkan.

3.6.8 Pendekatan Mitigasi

Pada Langkah 8 ada tiga aktivitas, pertimbangkan risiko mana yang perlu di manfaatkan dan bagaimana caranya. Hal ini dilakukan dengan memprioritaskan risiko, menentukan pendekatan untuk mengurangi risiko penting berdasarkan sejumlah faktor organisasi, dan mengembangkan strategi mitigasi yang mempertimbangkan nilai aset dan tempat tinggalnya.

Konsekuensi umum dari situasi ini adalah beberapa aset dalam wadah akan terlindungi karena kontrol lebih luas daripada yang diminta oleh persyaratan keamanan mereka. Paling sering, kontrol yang diterapkan pada wadah akhirnya gagal memenuhi kebutuhan keamanan semua aset informasi yang tersimpan, memproses, atau mengangkutnya secara akurat (terkadang karena kontrol *de facto* telah diterapkan di semua kontainer serupa). Salah satu cara untuk mengatasi masalah ini adalah dengan memindahkan aset informasi ke wadah lain (mis., Server) tempat mereka dapat dilindungi dengan cara yang lebih baik memenuhi persyaratan keamanan mereka.

Untuk mengurangi risiko secara tepat, harus mempertimbangkan pendekatan yang seimbang.

1. Dapat menghindari risiko dengan menerapkan kontrol yang tepat untuk mencegah ancaman dan kerentanan agar tidak dieksploitasi.
2. Dapat membatasi risiko dengan menerapkan strategi yang membatasi dampak buruk pada organisasi jika risiko direalisasikan.

Langkah 8 Kegiatan 1

Kegiatan pertama di Langkah 8 adalah memilah-milah masing-masing risiko yang telah Anda identifikasi dengan skor risikonya. Mengkategorikan risiko secara tertib akan membantu untuk mulai membuat keputusan mengenai status mitigasi.

Ada banyak cara bagi sebuah organisasi untuk mengkategorikan risikonya. Salah satu cara mudahnya adalah memulai dengan memilah risikonya dari yang tertinggi ke yang terendah. Kemudian pisahkan risikonya menjadi empat kolam dengan jumlah risiko yang sama. Risiko dengan skor tertinggi harus berada di area pertama (Pool 1), risiko dengan skor tertinggi berikutnya di urutan kedua (Pool 2), tertinggi berikutnya di ketiga (Pool 3), dan skor terendah di Keempat (kolam 4).

Skema kategorisasi lainnya mungkin masuk akal bagi organisasi. Jika organisasi menggunakan probabilitas, mungkin ingin mempertimbangkan untuk mengembangkan matriks risiko untuk mengkategorikan risiko yang teridentifikasi. Tabel matrik risiko relatif di bawah ini menunjukkan contoh bagaimana melakukan hal ini.

Langkah 8 Kegiatan 2

Tetapkan pendekatan mitigasi untuk setiap risiko. Pertimbangkan untuk menggunakan yang berikut sebagai panduan, namun ingatlah bahwa keputusan tentang pendekatan mitigasi sangat bergantung pada situasi operasi unik organisasi, jadi jangan gunakan bagan ini semata-mata untuk memutuskan bagaimana mengatasi risiko yang telah diidentifikasi.

Catatan: Dalam beberapa kasus dimungkinkan untuk mentransfer risiko ke pihak lain. Hal ini dapat dianggap sebagai pendekatan mitigasi untuk semua risiko yang sedang dipertimbangkan.

Tentukan bagaimana akan membahas setiap risiko pada lembar kerja risiko aset informasi masing-masing yang telah di buat dan dokumentasikan ini dengan memeriksa tindakan yang sesuai dalam kotak "Penanggulangan Risiko" di kolom (9). Setiap risiko pada setiap profil risiko harus memiliki pendekatan yang didokumentasikan. Untuk risiko yang di putuskan untuk diterima, pastikan untuk kembali dan meninjau kembali pernyataan dampak dan nilai dampak - jangan menerima risiko yang dapat menimbulkan konsekuensi serius pada organisasi.

Langkah 8 Kegiatan 3

Untuk semua profil risiko yang di putuskan untuk dikurangi, kemudian mengembangkan strategi mitigasi. Dengan mengingat tindakan yang dapat dilakukan untuk mengurangi risiko, mulailah mempertimbangkan strategi mitigasi untuk setiap risiko yang telah di putuskan untuk mengurangi, sebagai berikut:

1. Perhatikan wadah dimana kontrol akan diimplementasikan. (Wadah ini dapat ditemukan di Peta Lingkungan Risiko Aset Informasi.)
2. Jelaskan kontrol yang akan dilaksanakan dan risiko residual terhadap aset setelah kontrol diterapkan.

Berikut beberapa pertanyaan yang perlu dipertimbangkan pada saat mengembangkan strategi mitigasi risiko :

1. Bagaimana aktor dicegah untuk tidak mengeksploitasi kelemahan?
2. Bagaimana cara yang dapat dilakukan aktor tersebut dicegah?
3. Bagaimana motif dicegah?
4. Bagaimana hasilnya bisa dicegah?
5. Bisakah probabilitas ancaman dikurangi?
6. Jika tidak ada kegiatan proaktif yang dapat dilakukan, dapatkah dampak dari ancaman tersebut dikurangi?
7. Dapatkah organisasi meminimalkan dampak atau dampak dari risiko yang direalisasikan?
8. Bagaimana persyaratan keamanan untuk aset informasi ini dipenuhi oleh strategi mitigasi

BAB IV

HASIL DAN PEMBAHASAN

4.1 Gambaran Umum Objek Penelitian

4.1.1 Sejarah UPT Perpustakaan

Sejarah Perpustakaan UIN Raden Fatah Palembang Pepustakaan UIN Raden Fatah berdiri seiring dengan diresmikannya IAIN Raden Fatah pada tanggal 13 November 1964 bertepatan dengan tanggal 8 Rajab 1384 H. Koleksi awal berupa karya tulis dan karya cetak yang dimiliki perpustakaan sebanyak 7.943 exemplar yang diperoleh dari sumbangan suka rela para dermawan dan dari kalangan civitas akademika IAIN Raden Fatah. Kondisi perpustakaan saat itu masih sangan sederhana. Fasilitas, sarana dan prasarana perpustakaan masih sangan terbatas, koleksi perpustakaan masih dipajang dan ditempatkan dalam salah satu ruagan yang menyatu dengan tempat /ruang kuliah, karena perpustakaan belum memiliki gedung tersendiri. Manajemen dan organisasi perpustakaan belum memadai karena masih sangan terbatasnya tenaga pengelola dan belum ada karyawan yang memiliki dasar ilmu perpustakaan atau memperoleh pelatihan tentang perpustakaan. Periode ini (1964-1979), sejak mulai berdiri sampai dibangunnya gedug perpustakaan pada tahun 1979, sejak mulai berdiri sampai dibangunnya gedung perpustakaan pada tahun 1979, secara berturut-turut dipimpin oleh:

1. Bapak Hamid Nawawi (1964-1968)
2. Bapak Abbas Karib (1968-1972)
3. Ibu Dra.Maisaroh Nawawi (1972-1979)

Dua orang terakhir juga sebagai tenaga pengajar pada Fakultas Syari'ah) Seiring dengan perkembangan IAIN Al-Jami'ah Raden Fatah dari tahun ke tahun, maka pada masa kepemimpinan Rektor IAIN Raden Fatah dijabat oleh Bapak Prof.KH.Zainal Abidin Fikry dan pimpinan perpustakaan dipercayakan kepada Bapak Mazwar Gholib (1979-1983) maka dibangunlah gedung perpustakaan

tersendiri (1979) dengan luas bangunan kurang lebih 364 meter persegi dengan ruang baca berukuran 91 meter persegi. Dalam ruang baca hanya terdapat 40 kursi dan 20 buah meja baca. Tenaga pengelola perpustakaan hanya berjumlah 8 orang dan hanya tiga orang diantaranya yang pernah mendapatkan pelatihan tentang perpustakaan. Dalam perkembangan berikutnya, gedung ini perlu direnovasi dan disesuaikan dengan syarat-syarat dan standar yang biasanya digunakan dalam pembangunan gedung perpustakaan berdasarkan standar ISI, yaitu : Ruang dokemen atau bahan pustaka : 150 volume per meter persegi; ruang kepala 30 meter persegi, ruang pengadaan dan pengolahan bahan pustaka 9 meter persegi, ruang staf administrasi 5 meter persegi, ruang pengguna/pemustaka/user, luas rata-rata per pembaca di ruang baca 2,33 meter persegi dan ruang-ruang lain seperti : ruang untuk tangga, koridor, pintu masuk, lobi, toilet, tiang dan pengangkutan barang. Ruang untuk keperluan lain besarnya 30% hingga sepertiga dari ruangan untuk bahan pustaka, pembaca, jasa dan staf administrasi. Atas dasar standar tersebut, maka gedung perpustakaan yang dibangun pada tahun 1979 tersebut belum memenuhi standar minimal dan diperlukan gedung perpustakaan baru.

Masa kepemimpinan IAIN Raden Fatah Palembang dipegang oleh Bapak Drs. Usman Said (1985-1995), dibangunlah gedung perpustakaan yang mengacu kepada standar ISI di atas, walaupun belum sepenuhnya terpenuhi, setidaknya pemilihan lokasi sudah dianggab tepat dengan memperhitungkan kenyamanan pengguna/pemustaka/user, perluasan masa mendatang(konstruksi tanah bila dibangun gedung perpustakaan dengan perluasan bertingkat), lokasi yang strategis dan mudah dijangkau dari semua arah, serta terletak dijantung kampus IAIN Raden Fatah. Gedung perpustakaan ini dibangun pada tahun 1991/1992 dan mulai ditempati pada tahun 1993 pada masa kepemimpinan perpustakaaan dipercayakan pada Bapak Marus Bakri, BA. (1983-1996). Adapun gedung perpustakaan lama tidak lagi difungsikan untuk perpustakaan, tetapi sudah dialih fungsikan menjadi sentral pelayanan akademik (BAAK). selanjutnya perpustakaan IAIN Raden Fatah dipimpin secara berturut-turut oleh:

1. Bapak Drs.Balia Manaf (1996-2000)
2. Bapak Drs.Ruslan Muhayyan (200--2002)
3. Bapak Drs.Syafran Effendi (2002-2006)
4. Bapak Drs.H.Thohman Bahalik (2006-2010)
5. Ibu Herlina.S.Ag.,SS.,M.Hum (2010-2014)
6. Ibu Nurmalina, S.Ag.,SS.,M.Hum (2014-2018).

4.1.2 Visi dan Misi UPT Perpustakaan

1. Visi

Visi UPT Perpustakaan UIN Raden Fatah adalah "Mengembangkan perpustakaan sebagai informasi resource center berbasis ilmu-ilmu keislaman multidisiliner".

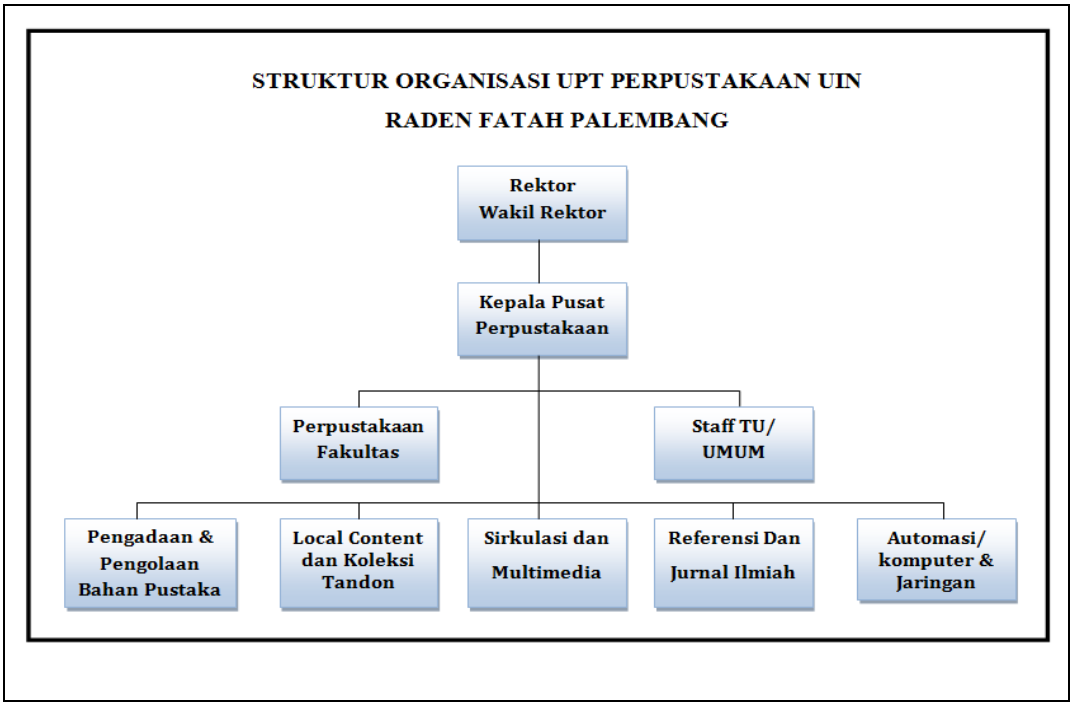
2. Misi

1. Menyediakan akses terhadap informasi dan layanan informasi untuk mendukung fungsi Tri Dharma Perguruan Tinggi.
2. Meningkatkan kualitas koleksi perpustakaan dalam bidang keislaman dan keilmuan agar lebih dapat berdaya guna bagi civitas akademika UIN Raden Fatah.
3. Meningkatakan kualitas layanan yang sesuai dengan perkembangan teknologi informasi.
4. Menjalin hubungan kerjasama dengan lembaga terkait untuk meningkatkan akses ke sumber-sumber yang relevan.

4.1.3 Struktur Organisasi UPT Perpustakaan

Struktur organisasi UPT perpustakaan UIN dapat dilihat pada gambar 4.1 yaitu terdiri dari rektor, wakil rektor, kepala pusat perpustakaan,selanjutnya terbagi dua bagian tingkatan perpustakaan fakultas dan staf tata usaha atau umum, bagian perpustakaan fakultas terdapat sub-sub bagian terdiri dari pengadaan dan

pengelolaan bahan pustaka, lokal content dan koleksi tandon, sirkulasi dan multimedia, referensi dan jurnal ilmiah serta automasi komputer dan jaringan.



Sumber : Dokumen Pedoman UPT perpustakaan

Gambar 4.1 Struktur Organisasi UPT Perpustakaan

Hasil observasi pada UPT perpustakaan UIN Raden fatah terdapat struktur organisasi pada gambar 4.1 dapat di analisa pada bagian perpustakaan fakultas terdiri dari sub-sub bagian yaitu pengadaan dan pengelolaan bahan pustaka, *local conten*t dan koleksi tandon, sirkulasi dan mutimedia, referensi dan jurnal ilmiah serta automasi komputer dan jaringan, pada bagian perpustakaan fakultas dari hasil observasi di lingkungan UIN Raden Fatah adanya berberapa perpustakaan terdiri dari berberapa perpustakaan fakultas yaitu perpustakaan fakultas syari‟‟ah, perpustakaan fakultas adab, perpustakaan tarbiyah, perpustakaan ushuluddin, perpustakaan fakultas febi, perpustakaan fakultas dakwah serta UPT perpustakaan dengan adanya berberapa perpustakaan yang ada di UIN Raden Fatah dari gambar 4.1 struktur organisasi untuk dapat di analisa diperjelas pada bagian perpustakaan fakultas bahwasanya terdapat berberapa perpustakaan sehingga perlu adanya penambahan konten yang diperjelaskan pada Gambar 4.1 struktur organisasi.

Automasi komputer dan jaringan dapat analisa untuk di spesifikasikan kembali dengan adanya penamabahan konten puskom pada struktur organisasai perpustakaan UPT dari hasil observasi dan wawancara kepada petugas UPT perpustakaan adanya peran dan kontribusi puskom pada perpustakaan seperti ketika gangguan pada website SLIMS perpustakaan, terjadi kesalahan-kesalahan program maupun *update* program pada perpustakaan UIN Raden Fatah sehingga dari hasil analisa dapat memberikan evolusi pada struktur organisasi UIN Raden Fatah.

4.2 Hasil Penelitian

4.2.1 Identitas Responden Berdasarkan Bagian

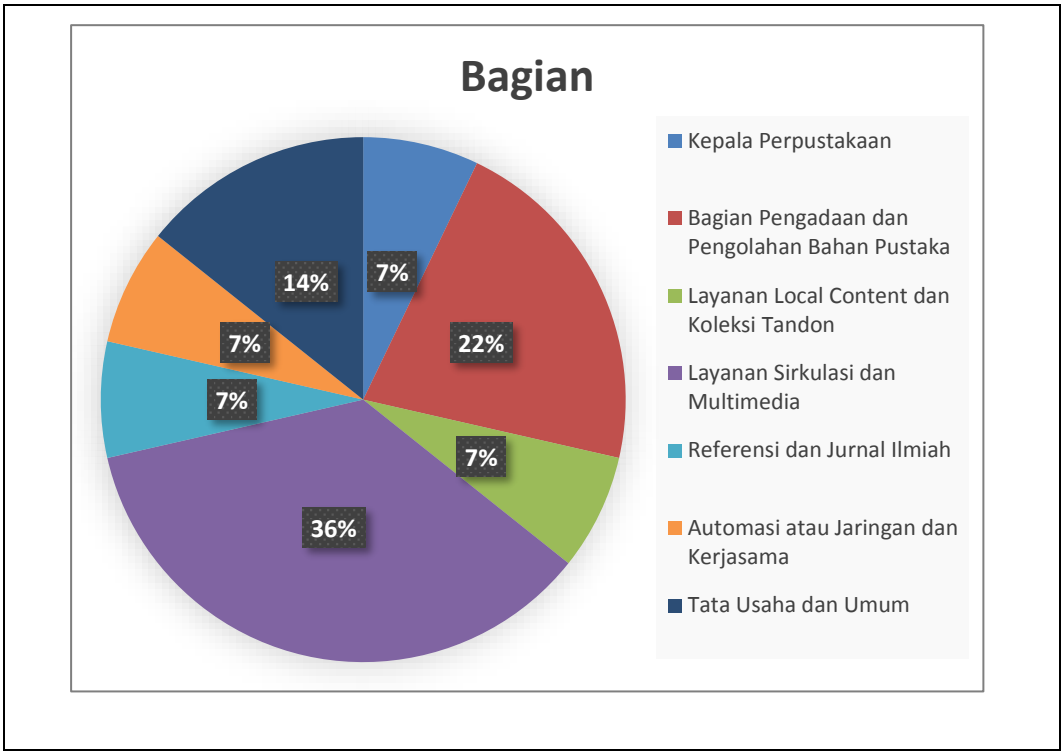
Dari hasil pengumpulan dan pengolahan data kuesioner dengan jumlah sampel sebanyak 14 responden. Pada Tabel 4.1 berikut ini merupakan data responden berdasarkan bagian jenis kelamin responden, dapat dilihat sebagai berikut :

Tabel 4.1 Rekapitulasi data responden berdasarkan bagian

No	Bagian	Jumlah	Persentase
1	Kepala Perpustakaan	1	7.14%
2	Bagian Pengadaan dan Pengolahan Bahan Pustaka	3	21.42%
3	Layanan Local Content dan Koleksi Tandon	1	7.14%
4	Layanan Sirkulasi dan Multimedia	5	35.71%
5	Referensi dan Jurnal Ilmiah	1	7.14%
6	Automasi atau jaringan dan kerjasama	1	7.14%
7	Tata Usaha dan umum	2	14.28%

Dari Tabel 4.1 di atas dapat diketahui bahwa responden yang mengisi kuesioner dari kepala perpustakaan berjumlah 1 orang atau 7.14%, Bagian Pengadaan dan Pengolahan Bahan Pustaka berjumlah 3 orang atau 21.42%, Layanan Local Content dan Koleksi Tandon berjumlah 1 orang atau 7.14%, Layanan Sirkulasi dan Multimedia berjumlah 5 orang atau 35.71%, Referensi dan

Jurnal Ilmiah berjumlah 1 orang atau 7.14%, Automasi atau jaringan dan kerjasama berjumlah 1 orang atau 7.14%, Tata Usaha dan umum berjumlah 2 orang atau 14.28%.



Sumber : Data Primer Diolah, 2017

Gambar 4.2 Data Responden Berdasarkan Bagian

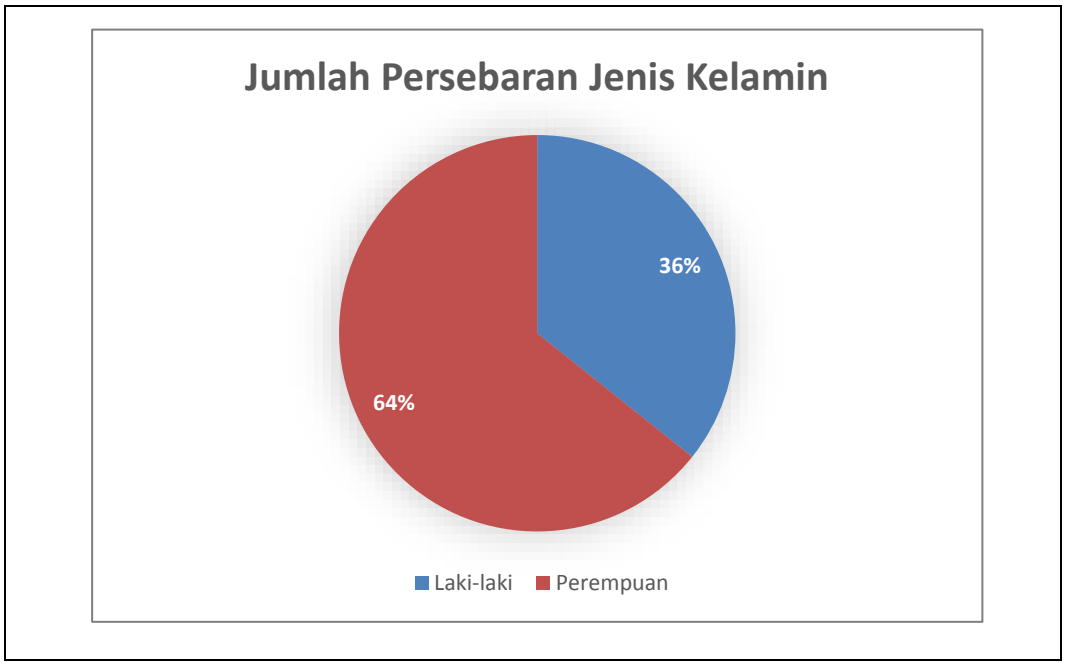
4.2.2 Identitas Responden Berdasarkan Jenis Kelamin

Dari hasil pengumpulan dan pengolahan data kuesioner dengan jumlah sampel sebanyak 14 responden didapatkan hasil persebaran jenis kelamin sebagai berikut seperti yang ditunjukkan pada Tabel 4.2 :

Tabel 4.2 Rekapitulasi data responden berdasarkan jenis kelamin

No	Bagian	Jumlah	Persentase
1	Perempuan	9	64.28%
2	Laki- Laki	5	35.71%

Hasil penelitian menunjukan bahwa terdapat 6 atau 17.64% responden berjenis kelamin perempuan, sedangkan 28 atau 82.34% responden berjenis kelamin laki-laki. Gambaran persantese diagram chart dapat dilihat sebagai berikut ini :



Gambar 4.3 Data Responden Berdasarkan Jenis Kelamin

4.3 Deskripsi *OCTAVE Allegro*

Penelitian ini menerapkan beberapa tahapan yang ada pada *OCTAVE Allegro*. Proses penilaian risiko sesuai dengan tahapan risiko, dimana tahapan risiko di dapat dari *OCTAVE Allegro*. Berikut tahapan *OCTAVE Allegro* :

4.3.1 Membangun Kriteria Pengukuran Risiko

. Dengan membangun kriteria risiko kita bisa mengetahui area dampak pada perpustakaan UIN Raden Fatah berdasarkan lembar kerja Allegro Pengukuran risiko merupakan tahap lanjutan setelah pengidentifikasian risiko. Hal ini dilakukan untuk menentukan relatif pentingnya resiko, untuk memperoleh informasi yang akan membantu perpustakaan untuk menetapkan risiko. Tujuan dari kriteria pengukuran risiko yaitu dapat mengetahui risiko yang terdapat pada perpustakaan agar dapat meminimalisir risiko berdasarkan lembar kerja allegro.

Dimana pada tahapan ini memiliki 1 langkah dan 2 aktivitas dalam membangun kriteria pengukuran risiko.

Langkah 1 aktivitas 1

Tabel 4.3 *Impact Area* Reputasi dan Keberhasilan Pelanggan

Lembar Kerja Allegro 1	**KRITERIA PENGUKURAN RISIKO - REPUTASI DAN KEBERHASILAN PELANGGAN**		
Area Dampak	Rendah	Sedang	Tinggi
Reputasi Sistem	Reputasi sedikit terpengaruh jika terjadi kerusakan terhadap sistem dengan usaha penanganan sistem yang dilakukan pada saat terjadi kerusakan	Reputasi sedikit terpengaruh jika terjadi kerusakan dalam sistem yang sedang dan dengan perbaikan dengan membutuhkan waktu yang singkat dengan biaya yang lebih	Reputasi pada tingkatan ini, dimana sangat mempengaruhi pengunjung dengan reputasi yang buruk dan mengganggu aktivitas utama pengunjung dan membutuhkan waktu yang lama dan biaya yang mahal
Kehilangan Pengunjung	Adanya pengurangan pengunjung yang diakibatkan hilangnya kepercayaan	Kurang dari 2% pengurangan pengunjung yang diakibatkan hilangnya kepercayaan	Tidak ada pengurangan pengunjung yang diakibatkan hilangnya kepercayaan

Pada **Tabel 4.3** *Impact Area* Reputasi dan Keberhasilan Pelanggan diatas berdasarkan hasil wawancara pada pihak perpustakaan dimana pada kriteria pengukuran risiko reputasi dan kehilangan pengunjung terdapat 2 area dampak yaitu reputasi sistem dan kehilangan pengunjung (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:67).

Pada Tabel 4.4 *Impact Area* Keuangan

Lembar Kerja Allegro 2	**KRITERIA PENGUKURAN RISIKO – KEUANGAN**		
Area Dampak	Rendah	Sedang	Tinggi
Biaya Operasional	Tidak ada kenaikan biaya dari perpustakaan pertahun	Kenaikan antara 2% dan 5% biaya dari perpustakaan pertahun	Kenaikan lebih dari 5% biaya dari perpustakaan pertahun

Pada Tabel 4.4 *Impact Area* keuangan diatas , berdasarkan hasil wawancara pada pihak perpustakaan, dimana pada bagian keuangan hanya terdapat satu area dampak yaitu biaya operasional (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:69).

Tabel 4.5 *Impact Area* Produktivitas

Lembar Kerja Allegro 3	**KRITERIA PENGUKURAN RISIKO PRODUKTIVITAS**		
Area Dampak	Rendah	Sedang	Tinggi
Jam Kerja karyawan	Jam kerja staff tidak meningkatkan biaya tenaga kerja	Jam kerja staff meningkatkan biaya tenaga kerja antara 2%	Jam kerja staff meningkatkan biaya tenaga kerja antara 2%- 5%

Pada **Tabel 4.5** *Impact Area* Produktivitas diatas hanya terdapat satu area dampak pada produktivitas , berdasarkan hasil wawancara pada pihak perpustakaan yang mana pada produktivitas area dampaknya berupa jam kerja karyawan (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:71).

Tabel 4.6 *Impact Area* Kehidupan dan Keamanan

Lembar Kerja Allegro 4	**KRITERIA PENGUKURAN RISIKO – KEAMANAN DAN KESEHATAN**		
Area Dampak	Rendah	Sedang	Tinggi
Kehidupan	Tidak ada ancaman yang signifikan terhadap kehidupan karyawan atas kerusakan pada system	Kehidupan karyawan terancam, namun Hanya sedikit respon peraturan	Kehilangan anggota pengunjung atau anggota karyawan
Keamanan	Keamanan dipertanyakan, tapi tidak ada tanggapan peraturan dan sedikit atau tidak ada biaya	Keamanan berdampak, minimal ada tanggapan peraturan	Keamanan dilanggar, tanggapan peraturan yang signifikan denga melibatkan biaya yang mahal

Pada **Tabel 4.6** *Impact Area* Kehidupan dan Keamanan diatas dimana pada kriteria pengukuran risiko kehidupan dan keamanan terdapat 2 area dampak yang terjadi di perpustakaan (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:73).

Tabel 4.7 *Impact Area* Denda dan Pinalti

Lembar Kerja Allegro 5	**KRITERIA PENGUKURAN RISIKO – DENDA DAN PINALTI**		
Area Dampak	Rendah	Sedang	Tinggi
Denda Buku	Denda kurang dari 500 di pungut	Denda antara 500 sampai 1000 di pungut	Denda yang lebih besar dari 1000 dipungut.
Tuntunan Hukum	Tidak ada tuntutan hukum atas kehilangan buku diajukan terhadap perpustakaan kepada pengunjung	Adanya tuntutan hukum atas kehilangan buku diajukan terhadap perpustakaan kepada pengunjung	Tuntutan hukum atas kehilangan buku diajukan kepada pengunjung dengan mengembalikan 1 buku yang sama atau mengembalikan 2 buku yang berbeda

Pada **Tabel 4.7** *Impact Area* Denda dan Pinalti diatas dimana pada bagian denda dan pinalti area dampak yang terjadi di perpustakaan yaitu denda buku dan tuntunan hukum (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:75).

Tabel 4.8 *Impact Area IT Risk*

Lembar Kerja Allegro 6	**KRITERIA PENGUKURAN RISIKO – *IT RISK***		
Area Dampak	Rendah	Sedang	Tinggi
Orang	Tidak ada data yang hilang jika pegawai perpustaaan pindah, perpustakaan harus memiliki pegawai yang ahli dalam bidangnya dan tidak kurangnya sumber daya manusia	Data tidak terdokumentasi dengan baik, pegawai kurang disiplin mengakibatkan keterlambatan proses pengelolaan data	Pegawai yang sudah tidak bekerja msih dapat mengakses data yang ada di perpustakaan dan penumpukan pekerjaan karena kurangnya pegawai
Aplikasi	Data sistem tersimpan dengan baik pada server jika terdapat virus data tetap aman karena terdapat data cadangan pada server. Ancaman berupa virus atau kegiatan hacking langsung di atasi dengan cepat	Jika terjadi ancaman terhadap sistem, perpustakaan hanya dapat mengandalkan data cadangan dan tidak dapat menjamin agar ancaman itu tidak terjadi lagi.	Data cadangan sistem tidak diolah dengan baik , jika terdapat ancaman pegawai tidak dapat menanganinya
Fasilitas	Komputer sudah cukup dan cara penggunaan sudah distandarisasikan secara luas kepada setiap masing-masing pegawai	Komputer sudah cukup tetapi cara penggunaan komputer masih belum di standarisasikan secara prosedur	Kurangnya komputer yang dapat mengakibatkan menumpuknya pekerjaan pada satu komputer

Pada **Tabel 4.8** *IT RISK* diatas terdapat 3 area dampak pada *IT RISK* yaitu orang , aplikasi dan fasilitas (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:77).

Langkah 1 aktivitas 2

Tabel 4.9 Skala Prioritas *Impact Area*

Lembar Kerja Allegro 7	**LAMPIRAN PRIORITISAS DAERAH DAMPAK**
Prioritas	Daerah Dampak
6	*Reputation and Customer Confidence*
5	*Financial*
1	*Produktivity*
3	*Safety and Health*
2	*Fines and Legal Penalties*
4	*IT Risk*

Dari **Tabel 4.9 Skala Prioritas *Impact Area*** diatas berdasarkan hasil wawancara di perpustakaan UIN Raden Fatah, *Financial* berada pada prioritas 5 karena karena sistem diperpustakaan sudah terkomputerisasi dan membutuhkan biaya yang cukup untuk memelihara sistem, agar selalu up to date dan berjalan dengan lancar, pada *Reputation and Customer Confidence* berada pada prioritas 4 Karena reputasi sistem mempengaruhi aktivitas pengolahan data, pada Safety and Health berada pada prioritas 3 karena aktivitas yang dilakukan akan tetap berjalan walaupun sistem yang digunakan bermasalah, pada *Fines and Legal Penalties* berada pada prioritas 2 karena tidak mempngaruhi sistem yang digunakan, sedangkan *Produktivity* berada pada priotitas 1 karena tidak terlalu berdampak kepada sistem (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:79).

4.3.2 Mengembangkan Profil Aset Informasi

Pada saat mengembangkan profil aset informasi dibutuhkan untuk mendefinisikan ancaman dan risiko terhadap aset apa saja yang ada di perpustakaan UIN Raden Fatah. Aset ini ditentukan dan mempertimbangkan dari segala aspek risiko aset yang ada. Pada tahapan ini dilakukan untuk mengetahui aset informasi apa yang dianggap paling penting pada perpustakaan dan mengetahui persyaratan keamanan apa yang harus dilakukan oleh pihak

perpustakaan agar aset informasi tersebut menjadi aman. Pada tahapan ini memiliki 1 langkah 8 aktivitas.

Tabel 4.10 *Information Asset Profilling*

Lembar Kerja Allegro 8	**INFORMASI AKTIVA INFORMASI KRITIS**	
(1) Aset Kritis Aset informasi apa yang paling penting ?	(2) Dasar Pemikiran untuk Seleksi Mengapa aset informasi ini penting bagi organisasi?	(3) Deskripsi Apa uraian yang disepakati tentang aset informasi ini?
Aset otomasi SLiMS	Karena semua data ada di asset tersebut jika aset otomasi SLiMS rusak maka tidak dapat melakukan pengolahan data	Aset informasi ini berisi semua data buku, pengunjung, peminjaman semua data ada di SLiMS.
(4) Pemilik (s) Siapa pemilik aset informasi ini?		
Pemilik aset informasi ini adalah perpustakaan		
(5) Persyaratan Keamanan Apa persyaratan keamanan untuk aset informasi ini?		
Kerahasiaan	Memastikan bahwa hanya orang yang berwenang yang memiliki akses ke aset informasi	Anggota staff yang memiliki bagian tersendiri yang bertanggung jawab atas sistem yang dikerjakan
Integritas	Memastikan bahwa aset informasi tetap dalam kondisi yang dimaksudkan oleh pemilik dan untuk tujuan yang dimaksudkan oleh pemiliknya	Staff yang berwenang yang dapat memperbarui / mengubah informasi, hanya staff di bagian tersebut yang dapat memasukkan dan memodifikasi aset informasi
Tersedianya	Memastikan bahwa aset informasi tetap dapat diakses oleh pengguna yang berwenang	SLiMS harus tersedia bagi petugas entri data untuk melakukan semua data yang ada.
(6) Persyaratan keamanan yang paling penting Apa persyaratan keamanan terpenting untuk aset informasi ini?		
• Kerahasiaan	✓ Integritas	• Tersediannya

Pada **Tabel 4.10** ***Information Asset Profilling*** diatas menjelaskan bahwa aset informasi yang paling penting di perpustakaan yaitu SliMS karena jika SLiMS tidak dapat digunakan maka pengolahan data tidak dapat berjalan dan akan berdampak buruk pada aktivitas kerja perpustakaan, sedangkan untuk persyaratan keamanan yang digunakan perpustakaan yaitu integritas karena hanya staff yang berwenang yang dapat memperbarui / mengubah informasi, hanya staff di bagian tersebut yang dapat memasukkan dan mengolah data (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:81).

4.3 3 Identifikasi Kontainer Wadah Aset

Tahapan ini menjelaskan tentang identifikasi suatu informasi aset dari suatu sistem mengenai tempat penyimpanan, pengiriman serta tempat pemprosesan sistem yang digambarkan dengan *worksheet Information Asset Risk Environment Map.* Tujuan dari tahapan ini yaitu untuk mengetahui tempat dimana aset informasi disimpan, dikirim, dan di proses.

Tabel 4.11 Peta Lingkungan Risiko Informasi Aset Informasi Teknikal

Lembar Kerja Allegro 9a	**PETA LINGKUNGAN RISIKO INFORMATION ASSET (Teknikal)**
Dalam	
Wadah Deskripsi	**PEMILIK (S)**
1. Server SLiMS	Dikelola oleh PUSTPD.
2. Workstation perpustakaan	Dikelola oleh PUSTPD
Luar	
Wadah Deskripsi	**PEMILIK (S)**
1 Sebagian besar informasi disimpan di server	Tidak diketahui

Pada tabel diatas menjelaskan tentang peta lingkungan informasi risiko (teknikal) yang berkaitan dengan prosedur teknik yang harus dijalankan pegawai dalam pengolahan data yang ada di SliMS (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:83).

Tabel 4.12 Peta Lingkungan Risiko Informasi Aset Informasi Fisik

Lembar Kerja Allegro 9B	**PETA LINGKUNGAN RISIKO INFORMASI (FISIK)**
Dalam	
Wadah Deskripsi	**PEMILIK (S)**
1. Salinan salinan ringkasan dan laporan dicetak dan disimpan oleh anggota pengolahan data secara berkala	Staff pengolahan data

Pada tabel diatas menjelaskan tentang peta lingkungan informasi risiko (fisik) yang berkaitan dengan laporan informasi yang ada pada perpustakaan UIN Raden Fatah Palembang (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:85)..

Tabel 4.13 Peta Lingkungan Risiko Informasi Aset Informasi Orang

Lembar Kerja Allegro 9c	**PETA LINGKUNGAN RISIKO INFORMASI (Orang)**
Dalam	
NAMA ATAU PERAN / RESPONSIBILITAS	**DEPARTEMEN ATAU UNIT**
1 Automasi / komputer dan jaringan	Layanan jaringan
2 Staf perpustakaan	Layanan pengolahan data
Luar	
KONTRAKTOR, VENDOR, DLL.	**ORGANISASI**
1. Vendor pihak kedua mengelola dan penyimpanan hardisk cadangan untuk sistem SLIMS. Hubungan dikelola via departemen IT di perpustakaan.	Penyimpanan data yang aman

Pada tabel diatas menjelaskan tentang peta lingkungan informasi risiko (orang) yang berkaitan dengan peran siapa saja yang terkait dalam mengelola dan bertanggung jawab untuk mengelola SliMS (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:87)..

4.3.4 Mengidentifikasikan Area Yang di Perhatikan

Pada tahapan ini digunakan untuk menjabarkan aktivitas-aktivitas dalam mengidentifikasikan *area of concern* dari penggunaan sistem. Identifikasi *areas of concern* dengan meninjau kembali setiap *container* untuk melihat dan menentukan areas of concern yang potensial dan melanjutkan dengan melakukan dokumentasi setiap *areas of concern* yang telah diidentifikasi. Tujuannya untuk mengetahui *areas of concern* apa yang terdapat pada perpustakaan

Tabel 4.14 *Areas of Concern*

No	Area Yang Menjadi Perhatian
1	Mengalami kerusakan pada aplikasi SLiMS sehingga pihak perpustakaan tidak dapat melakukan pengolahan data

Pada Tabel 4.14 *Area of Concern* diatas menjelaskan terdapat area yang menjadi pusat perhatian utama yang harus diperhatikan untuk meminimalisir dan mencegah risiko yang akan terjadi (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:46).

4.3.5 Mengidentifikasikan Skenario Ancaman

Pada tahap ini perpustakaan dapat membuat skenario-skenario yang dapat mempengaruhi aset informasi untuk masing-masing *container* yang telah ditetapkan dan mengidentifikasikan *actor*, *means*, *motive* dan *outcome* serta menentukan probabilitas terjadinya skenario ancaman. Adapun tujuan dari skenario ancaman yaitu memberikan gambaran secara rinci mengenai *property* dari skenario ancaman.

Tabel 4.15 *Properties of Threat*

	Area of Concern	**Threat of Properties**	
1	Mengalami kerusakan pada aplikasi SLiMS sehingga pihak perpustakaan tidak dapat melakukan	*1. Actors*	Eksternal / vendor
		2. Means	Melakukan perusakan pada aplikasi SLiMS
		3. Motives	Ingin Merusak SLiMS
		4. Outcome	Modifikasi Interupsi

	pengolahan data.	*5. Security requirements*	Melakukan evaluasi terhadap aplikasi SLiMS

Pada **Tabel 4.15** ***Properties of Threat*** diatas menunjukkan identifikasi skenario ancaman yang memberikan secara rinci mengenai *property* dari ancaman, antara lain *actor, means, motives, outcome,* dan *security requirements* (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:51).

4.3.6 Mengidentifikasi Risiko

Pada tahapan ini aktivitas yang dilakukan perpustakaan adalah menentukkan dampak dari skenario ancaman terhadap perpustakaan. Dimana untuk setiap skenario yang telah dibuat perpustakaan harus menentukkan dampak atau konsekuensi yang mungkin akan ditimbulkan ketika ancaman terjadi. Identifikasi risiko bertujuan untuk menentukan bagaimana skenario ancaman memberikan dampak atau konsekuensi bagi perpustakaan serta menentukan tingkatannya

Tabel 4.16 Identifikasi Risiko

Skenario Ancaman	**Konsekuensi**
Mengalami kerusakan pada aplikasi SLiMS sehingga pihak perpustakaan tidak dapat melakukan pengolahan data	Terganggunya aktivitas perpustakaan dalam pengelolaan data dan akan berakibat buruk pada perpustakaan

Pada Tabel 4.16 Identifikasi Risiko diatas menjelaskan bahwa adanya keterkaitan antara skenario ancaman dan konsekuensi yang akan dihadapi oleh pihak perpustakaan. (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:54).

4.3.7 Menganalisis Risiko

Dengan melakukan analisis risiko dapat mengidentifikasikan dan menghitung risiko, dengan mempertimbangkan bagaimana mengurangi probabilitas kegagalan dan dengan mempertimbangkan sejauh mana konsekuensi dari risiko mempengaruhi perpustakaan. Adapun tujuan dari analisis risiko yaitu

dapat mengetahui risiko dan konsekuesni yang akan dihadapi oleh perpustakaan dan dapat memberikan penilaian atas konsekuesi yang terjadi, pada analisis risiko terdapat 1 langkah dan 2 aktivitas.

Langkah 7 Aktivitas 1

Tabel 4.17 Analisis Risiko

Skenario Ancaman	**Konsekuensi**
Mengalami kerusakan pada jaringan sehingga menghalangi kemampuan perpustakaan untuk melakukan proses pengiriman data.	Terganggunya aktivitas perpustakaan dalam pengelolaan data dan akan berakibat buruk pada perpustakaan

Pada **Tabel 4.17** Analisis Risiko diatas menunjukkan bahwa konsekuensi tersebut berdampak langsung pada *financial* dan *IT Risk* perpustakaan UIN Raden Fatah. sedangkan pada **Tabel 4.18** dibawah menunjukkan nilai dampak dari konsekuensi (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:56).

Tabel 4.18 Nilai Dampak

Area Dampak	Nilai Dampak
Reputation and Customer Confidence	Tinggi
Financial	Tinggi
Produktivity	Rendah
Safety and Health	Sedang
Fines and Legal Penalties	Rendah
IT Risk	Sedang

Pada Tabel 4.18 diatas untuk mendapatkan nilai dampak tinggi, sedang, rendah pada area dampak harus melakukan tahapan pada langkah satu aktivitas satu, dimana pada tahapan satu memiliki lembar kerja kriteria pengukuran risiko untuk mengetahui risiko yang ada di perpustakaan. Pada langkah satu aktivitas dua digunakan untuk mengetahui area dampak yang paling penting. Dengan melakukan tahapan satu maka perpustakaan akan mendapatkan nilai dampak tinggi, sedang, rendah.

Langkah 7 aktivitas 2

Tabel 4.19 Menghitung *Score Impact Area*

Dampak Luas	Peringkat	Nilai Dampak	Nilai
Reputation and Customer Confidence	6	Tinggi (3)	12
Financial	5	Tinggi (3)	10
Produktivity	1	Rendah (1)	1
Safety and Health	3	Sedang (2)	6
Fines and Legal Penalties	2	Rendah (1)	2
IT Risk	4	Sedang (2)	12
		Skor Total	43

Pada Tabel 4.19 Menghitung *Score Impact Area* menunjukkan bahwa dari konsekuensi memberikan nilai dampak dan skor total yang dapat digunakan untuk menganalisis risiko dan membantu organisasi menentukan strategi risiko yang tepat (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:57).

4.3.8 Pendekatan Mitigasi

Berdasarkan perhitungan skor pada tahapan sebelumnya, perpustakaan dapat menentukan risiko mana yang perlu dimitigasi dan bagaimana caranya. Hal tersebut dilakukan dengan cara membuat prioritas dari risiko, menentukan pendekatan yang akan diambil untuk memitigasi risiko berdasarkan drivers dari perpustakaan dan mengembangkan strategi mitigasi dengan mempertimbangkan nilai dari aset. Terdapat tiga aktivitas yang perlu dilakukan pada tahapan ini

Langkah 8 aktivitas 1

Tabel 4.20 *Relative Risk Matrix*

RELATIF RISIKO MATRIX			
Kemungkinan	RISK SCORE		
	30 to 45	16 to 29	0 to 15
Tinggi	POOL 1	POOL 2	POOL 2
Sedang	POOL 2	POOL 2	POOL 3
Rendah	POOL 3	POOL 3	POOL 4

Pada Tabel 4.20 *Relative Risk Matrix* diatas Pool digunakan untuk mengkategorikan risiko berdasarkan pada skor risikonya (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:61).

Langkah 8 aktivitas 2

Tabel 4.21 *Mitigation Approch*

POOL	Pendekatan Mitigasi
1	Mengurangi
2	Menunda / Mengurangi
3	Mengurangi / Menerima
4	Menerima

Pada Tabel 4.21 *Mitigation Approch* digunakan untuk menentukan pendekatan mitigasi untuk setiap risiko berdasarkan *relative risk matrix* dari setiap risiko (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:62).

Langkah 8 aktivitas 3

Tabel 4.22 *Risk Mitigation*

Risk Mitigation	
Area yang menjadi perhatian	Mengalami kerusakan pada aplikasi SLiMS sehingga pihak perpustakaan tidak dapat melakukan pengolahan data
Tindakan	Mengurangi
Wadah	Kontrol
Solusi	1. Meningkatakan sistem keamanan pada aplikasi SLiMS 2. Melakukan evaluasi terhadap aplikasi yang digunakan

Pada Tabel 4.22 *Risk Mitigation* diatas merupakan pengembangan strategi mitigasi risiko karena perlu dibuat suatu strategi untuk memitigasi risiko tersebut (Carrali, RA, JF, Steven, R, Young, WR, Wilson., 2007:63).

4.4 Hasil Penelitian *OCTAVE Allegro*

Berdasarkan hasil penelitian menggunakan metode *OCTAVE Allegro* terdapat 5 area dampak yang berisiko pada perpustaaan UIN Raden Fatah Palembang. Pada lembar kerja allegro kriteria pengukuran risiko reputasi dan keberhasilan pelanggan berada pada level tinggi. Dikatakan level tinggi karena kerusakan yang terjadi pada aplikasi SLiMS dapat membuat pihak perpustakaan sulit melakukan pengolahan data. Pada lembar kerja allegro kriteria pengukuran risiko keuangan berada pada level tinggi karena sistem yang digunakan oleh perpustakaan UIN Raden Fatah Palembang sudah terkomputerisasi, jadi jika terjadi kerusakan pada sistem yang digunakan maka pihak perpustakaan UIN Raden Fatah Palembang membutuhkan biaya yang cukup besar untuk memperbaiki sistem jika terjadi kerusakan dan keuangan perpustakaan UIN Raden Fatah Palembang bisa dikatakan belum baik, karena setiap tahunnya perpustakaan UIN Raden Fatah Palembang belum memiliki anggaran tersendiri untuk pengelolaan dan perawatan teknologi informasi.

Pada lembar kerja allegro kriteria pengukuran risiko produktivitas berada pada level rendah, karena jam kerja karyawan tidak mempengaruhi jika terjadi kerusakan pada sistem yang digunakan. Pada lembar kerja allegro kriteria pengukuran risiko keamanan dan kehidupan berada pada level sedang, dikatakan level sedang karena tidak adanya ancaman yang signifikan terhadap kehidupan karyawan atas kerusakan pada sistem yang digunakan dan keamanan perpustakaan masih di pertanyakan jika terjadi kerusakan pada sistem yang digunakan. Sedangkan pada lembar kerja allegro kriteria pengukuran risiko denda dan pinalti

berada pada level rendah , karena tidak adanya pengaruh terhadap kerusakan terhadap sistem yang digunakan terhadap denda dan pinalti.

Dari hasil penilaian risiko maka pihak perpustakaan UIN Raden Fatah Palembang dapat membuat perencanaan strategi dalam mengelola manajemen risiko untuk melakukan pengelolaan dan perawatan sistem yang digunakan.

4.5 Pembahasan Hasil *OCTAVE Allegro*

Seperti yang dijelaskan pada BAB II skripsi ini , *OCTAVE Allegro* merupakan *framework* yang menggunakan pendekatan *OCTAVE* dan di desain untuk melakukan penilaian risiko terhadap operasional organisasi atau perusahaan dengan tujuan untuk menghasilkan hasil yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait penialain risiko.

4.5.1 Kriteria Pengukuran Risiko *Financial*

Berdasarkan hasil penelitian terhadap manajemen risiko menunjukkan bahwa *Reputation and Customer Confidence and financial* merupakan area dampak yang paling penting bagi perpustakaan UIN Raden Fatah Palembang. Dimana hasil penilaian risiko berdasarkan *OCTAVE Allegro* kondisi *financial* berada pada level tinggi. Dikatakan level tinggi karena belum adanya anggaran khusus untuk pembiayaan dalam pengelolaan dan perawatan untuk sistem SLiMS *(Senayan Library Management System)* di perpustakaan UIN Raden Fatah Palembang .

Permasalahan yang masih dialami pihak perpustakaan ialah belum adanya anggaran khusus untuk perawatan dan pengelolaan sistem. Karena biaya perawatan dan pembaharuan sarana dan prasarana untuk teknologi informasi membutuhkan biaya yang sangat besar. Hal ini dapat mempengaruhi sistem karena bila sarana dan prasarana sistem tidak bisa terpenuhi dengan baik maka proses pengelolaan data tidak berjalan dengan maksimal dan dapat menyebabkan kerugian langsung dan terhambatnya proses aktivitas perpustakaan.

Rekomendasi Dalam Mengelola Manajemen Risiko

Mengelola manajemen risiko yang baik berdasarkan *OCTAVE Allegro*, setiap program kerja atau perencanaan yang akan dibuat oleh perpustakaan sebaiknya :

1. Adanya penambahan anggaran khusus untuk sistem
2. Adanya rincian khusus dalam pengeluaran anggaran untuk menunjang kualitas sistem.
3. Mengalokasikan biaya khusus untuk sistem. Biaya-biaya yang dikeluarkan untuk menyediakan layanan, sebaiknya mengutamakan pengeluaran biaya yang memiliki fungsi jangka panjang. (Isaca, 2009)

4.5.2 Kriteria Pengukuran Risiko *Reputation and Customer Confidence*

Berdasarkan hasil penelitian terhadap manajemen risiko menunjukkan bahwa *Reputation and Customer Confidence* merupakan area dampak yang berisiko bagi perpustakaan UIN Raden Fatah Palembang. Dimana hasil penilaian

risiko berdasarkan *OCTAVE Allegro* kondisi *Reputation and Customer Confidence* berada pada level tinggi. Dikatakan level tinggi karena jika terjadi kerusakan pada sistem yang digunakan pihak perpustakaan maka pihak perpustakaan tetap dapat melayani pengunjung secara manual.

Permasalahan yang masih dialami pihak perpustakaan ialah kurangnya karyawan yang ahli dalam bidang TI. Hal ini dapat menyebabkan lambatnya proses pengolahan, dikarena pihak perpustakaan melayani pengunjung secara manual akibat data terjadi kerusakan pada sistem .

Rekomendasi Dalam Mengelola Manajemen Risiko

Mengelola manajemen risiko yang baik berdasarkan *OCTAVE Allegro*, setiap program kerja atau perencanaan yang akan dibuat oleh perpustakaan sebaiknya :

1. Perlu pengekrutan pegawai baru yang ahli pada bidangnya
2. Perpustakaan secara formal membutuhkan peningkatan keterampilan manajemen risiko TI secara berkala berbasis pada tujuan perpustakaan.

   (Isaca, 2009)

4.5.3 Kriteria Pengukuran Risiko *Produktivity*

Berdasarkan hasil penelitian terhadap manajemen risiko menunjukkan bahwa *Produktivity* merupakan area dampak yang memiliki risiko bagi perpustakaan UIN Raden Fatah Palembang. Dimana hasil penilaian risiko berdasarkan *OCTAVE Allegro* kondisi *Produktivity* berada pada level sedang.

Dikatakan level sedang karena jika terjadi kerusakan pada sistem yang digunakan maka jam kerja karyawan tidak berpengaruh dan jika terjadi kerusakan pada sistem yang digunakan tidak meningkatkan biaya tenaga kerja pada karyawan perpustakaan.

Permasalahan yang terjadi disebabkan karena kurangnya karyawan yang ahli dalam bidang TI dan kurangnya pengetahuan karyawan tentang sistem, hal ini mengakibatkan tumpang tindihnya pekerjaan yang ada di perpustakaan.

Rekomendasi Dalam Mengelola Manajemen Risiko

Mengelola Manajemen Risiko yang baik berdasarkan *OCTAVE Allegro*, setiap program kerja atau perencanaan yang akan dibuat oleh Perpustakaan sebaiknya :

1. Mengadakan pelatihan untuk memperoleh sumberdaya manusia yang ahli dalam mengelola integrasi TI.
2. Membuat pelatihan dan pendidikan untuk mendukung praktik manajemen risiko TI dan penggunaan konsep dan teknik terdepan. (Isaca, 2009)

4.5.4 Kriteria Pengukuran Risiko *Safety and Health*

Berdasarkan hasil penelitian terhadap manajemen risiko menunjukkan bahwa *Safety and Health* merupakan area dampak yang tidak terlalu berisiko bagi perpustakaan UIN Raden Fatah Palembang. Dimana hasil penilaian risiko berdasarkan *OCTAVE Allegro* kondisi *Safety and Health* berada pada level sedang. dikatakan level sedang karena tidak adanya ancaman yang signifikan

terhadap kehidupan karyawan atas kerusakan pada sistem yang digunakan dan keamanan perpustakaan masih di pertanyakan jika terjadi kerusakan pada sistem yang digunakan.

Pemasalahan yang dialami disebabkan karena kerusakan terjadi bukan karena karyawan jadi tidak ada ancaman yang signifikan kepada karyawan dan keamanan perpustakaan hanya sebatas menjalankan proses back up data untuk mengamankan data dimana hal itu belumlah cukup untuk mencegah agar sistem tersebut terhindar dari ancaman.

Rekomendasi Dalam Mengelola Manajemen Risiko

Mengelola manajemen risiko yang baik berdasarkan *OCTAVE Allegro*, setiap program kerja atau perencanaan yang akan dibuat oleh perpustakaan sebaiknya :

1. Perpustakaan harus melakukan pengawasan secara rutin terhadap sistem yang digunakan.
2. Perlunya penambahan sistem keamanan. (Isaca, 2009)

4.5.5 Kriteria Pengukuran Risiko *Fines and Pinalties*

Berdasarkan hasil penelitian terhadap manajemen risiko menunjukkan bahwa *Fines and Legal Pinalties* merupakan area dampak yang tidak terlalu berisiko bagi perpustakaan UIN Raden Fatah Palembang. Dimana hasil penilaian risiko berdasarkan *OCTAVE Allegro* kondisi *Fines and Legal Pinalties* berada

pada level rendah. dikatakan level rendah karena tidak adanya pengaruh terhadap kerusakan terhadap sistem yang digunakan terhadap denda dan hukuman.

Permasalahan yang terjadi dapat disebabkan masih kurangnya kesadaran pengunjung terhadap waktu yang diberikan ketika meminjam buku.Hal ini menyebabkan kurangnya koleksi buku yang ada di perpustakaan UIN Raden Fatah Palembang.

Rekomendasi Dalam Mengelola Manajemen Risiko

Mengelola manajemen risiko yang baik berdasarkan *OCTAVE Allegro*, setiap program kerja atau perencanaan yang akan dibuat oleh perpustakaan sebaiknya :

1. Perpustakaan perlu melakukan penegasan terhadap pengunjung yang me minjam buku. (Isaca, 2009)

4.5.5 Kriteria Pengukuran Risiko *IT Risk*

Berdasarkan hasil penelitian terhadap manajemen risiko menunjukkan bahwa *IT Risk* merupakan area dampak yang paling berisiko bagi perpustakaan UIN Raden Fatah Palembang. Dimana hasil penilaian risiko berdasarkan *OCTAVE Allegro* kondisi *IT Risk* berada pada level tinggi. dikatakan level tinggi karena kerusakan sistem atau kehilangan data pada perpustakaan dapat menyebabkan terganggunya proses pengolahan data di perpustakaan UIN Raden Fatah Palembang.

Permasalahan yang terjadi disebabkan karena kurangnya karyawan yang ahli dalam bidang TI dan kurangnya pengetahuan karyawan tentang sistem, hal ini mengakibatkan perpustakaan tidak dapat melakukan pengolahan data.

Rekomendasi Dalam Mengelola Manajemen Risiko

Mengelola manajemen risiko yang baik berdasarkan *OCTAVE Allegro*, setiap program kerja atau perencanaan yang akan dibuat oleh perpustakaan sebaiknya :

1. Perpustakaan harus mengamankan data pekerjaan jika terjadi pemberhentian terhadap pegawai
2. Harus memiliki pegawai yang ahli pada bidangnya dengan cara melakukan penambahan pegawai atau program pelatihan kepada pegawai.
3. Kepala perpustakaan harus melakukan pengawasan secara rutin kepada seluruh pegawai.

.

BAB V

PENUTUP

5.1 Simpulan

Berdasarkan hasil analisis risiko yang dilakukan pada tugas akhir ini dapat disimpulkan bahwa setelah melakukan serangkaian proses manajemen risiko maka didapatkan hasil tingkatan risiko pada sistem informasi perpustakaan :

1. Berdasarkan hasil penilaian risiko terdapat 5 area dampak yang berisiko pada perpustakaan UIN Raden Fatah Palembang. Hasil penilaian risiko berdasarkan *OCTAVE Allegro* kondisi, *Safety and Health, IT Risk,* berada pada level sedang, dan pada *Fines and Legal Pinalties*, *Productivity* berada pada level rendah, sedangkan pada kondisi *Financial, Reputation and Customer* berada pada level tinggi karena *Financial, Reputation and Customer Confidence* paling berisiko di perpustakaan.
2. Berdasarkan hasil analisis pada manajemen risiko, perpustakaan harus meningkatkan sistem keamanan dan melakukan evaluasi terhadap system informasi perpustakaan yang digunakan.

5.2 Saran

Peneliti menyarankan Perpustakaan UIN Raden Fatah Palembang, untuk melakukan :

1. Mengawasi secara rutin terhadap segala bentuk risiko TI yang ada pada perpustakaan dan Meningkatkan sarana dan prasarana untuk menunjang proses pengelolaan data.
2. Mempunyai strategi untuk menjalankan skenario manajemen risiko TI.
3. Menambah staff/karyawan yang ahli dalam bidang program.
4. Perpustakaan perlu menerapkan prediksi terhadap kemungkinan potensial masalah yang mungkin akan terjadi dan bagaimana cara mengantisipasinya serta menghadapinya.

DAFTAR PUSTAKA

Sugiyono. 2012. *Metode Penelitian Kuantitatif, Kualitatif, dan R & D*.Bandung : Alfabeta.

Hery. 2015. Manajemen Risiko Bisnis. Jakarta: Grasindo.

Carrali, RA, JF, Steven, R, Young, WR, Wilson. 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assesment Process.* Software Engineering Institude Carnegie Mellon University CMU/SEI Report Number : CMU/SEI-2007-TR-012 http://resources.sei.cmu.edu/library/asset-view.cfm assetid=8419. Diakses 13 Juni 2011.

Sugiyono. 2016. *Metode Penelitian Kuantitatif, Kualitatif, dan R & D*.Bandung : Alfabeta.

Siregar. 2014. Statistika Deskriptif untuk Penelitian.

Jakaria,dkk. 2013. Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda *OCTAVE Allegro.* Seminar Nasional Aplikasi Teknologi Informasi (SNATI). ISSN: 1907-5022.

Rosini, dkk. 2013. Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode *OCTAVE Allegro*. Jurnal Pustakawan Indonesia. Volume 14 No.1.

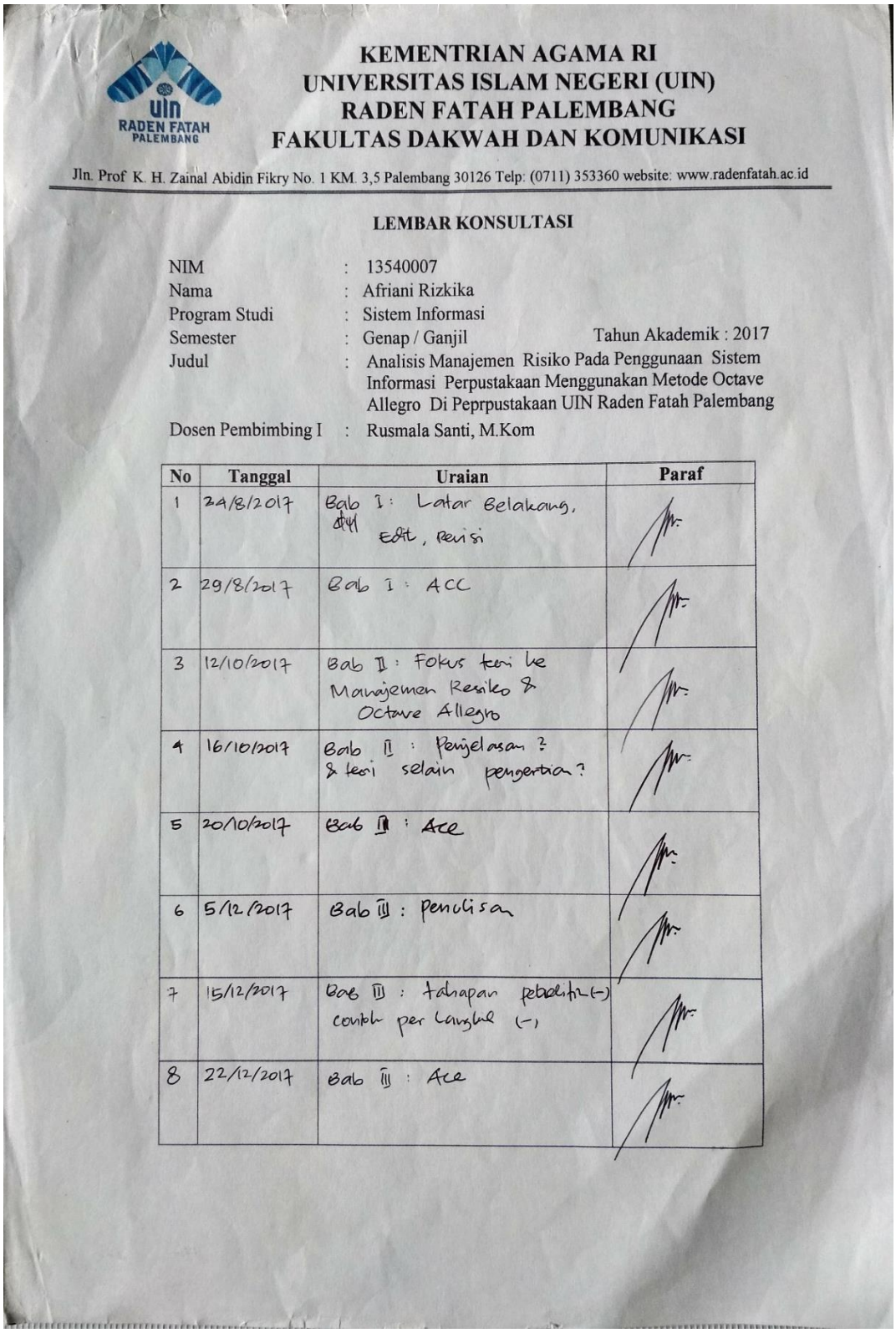
Nyoman Ayu Nila Dewi, I Gusti Putu Hardi Yudana.2016. Analisis Manajemen Risiko Pada Sistem Akademik Di STMIK STIKOM BALI. Seminar Nasional Teknologi Informasi dan Multimedia. ISSN : 2302-3805

Anita Wulansari, Putu Wuri Handayani. 2013. Analisis Penilaian Risiko Keamanan Untuk Aset Informasi Pada Usaha Kecil dan Menengah Bidang Fianansial B2B : Studi Kasus NgaturDuit.com

Isaca.2009. The Risk IT Framework. ISBN 978-1-60420-111-6

LAMPIRAN

Lampiran Konsultasi Pembimbing I



KEMENTRIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS DAKWAH DAN KOMUNIKASI

Jln. Prof K. H. Zainal Abidin Fikry No. 1 KM. 3,5 Palembang 30126 Telp: (0711) 353360 website: www.radenfatah.ac.id

LEMBAR KONSULTASI

NIM : 13540007
Nama : Afriani Rizkika
Program Studi : Sistem Informasi
Semester : Genap / Ganjil Tahun Akademik : 2017
Judul : Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode Octave Allegro Di Peprpustakaan UIN Raden Fatah Palembang
Dosen Pembimbing I : Rusmala Santi, M.Kom

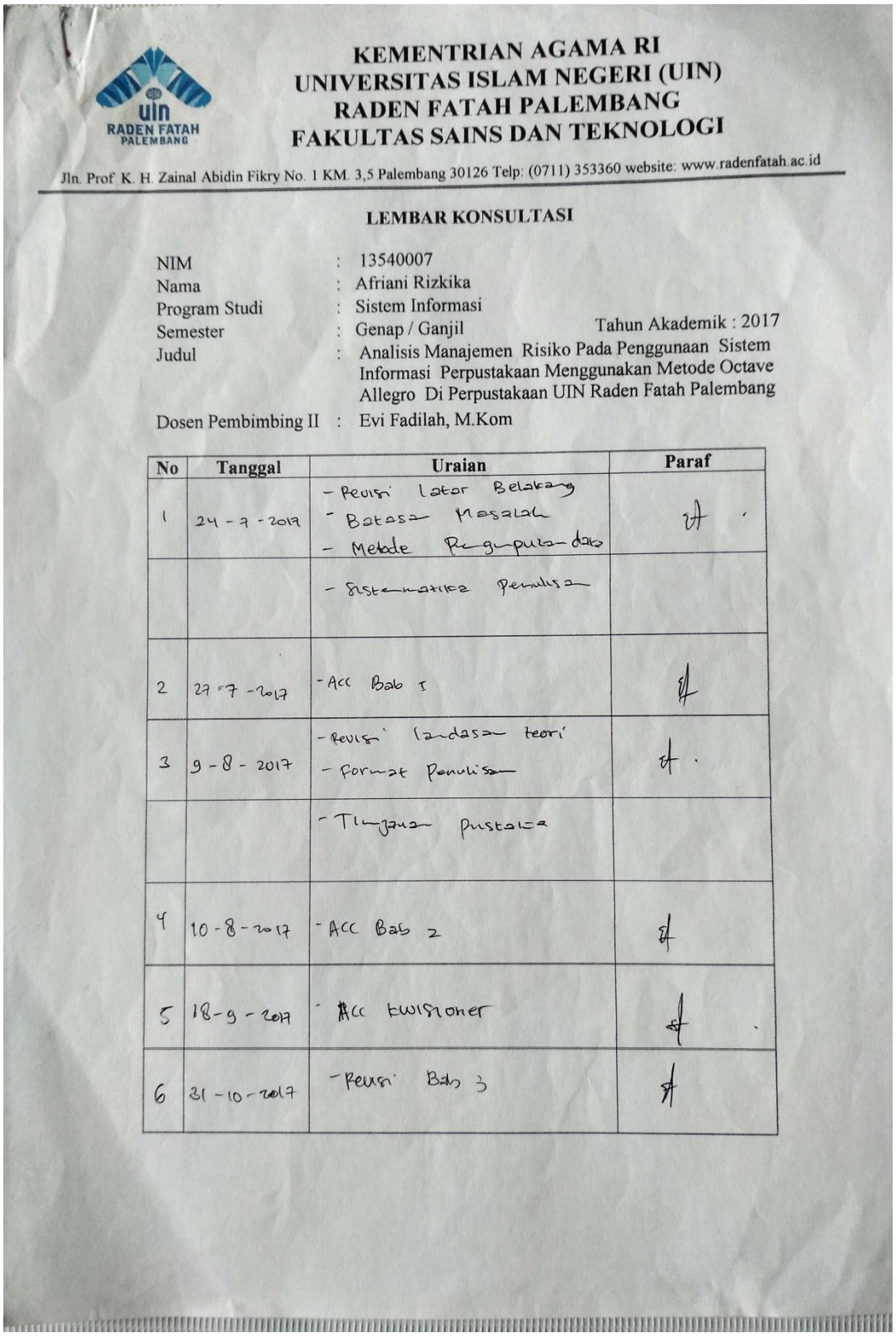
No	Tanggal	Uraian	Paraf
1	24/8/2017	Bab I : Latar Belakang, dll Edit, Revisi	
2	29/8/2017	Bab I : ACC	
3	12/10/2017	Bab II : Fokus teori ke Manajemen Resiko & Octave Allegro	
4	16/10/2017	Bab II : Penjelasan ? & teori selain pengertian ?	
5	20/10/2017	Bab II : Acc	
6	5/12/2017	Bab III : penulisan	
7	15/12/2017	Bab III : tahapan rebaliti (-) contoh per Langkah (-)	
8	22/12/2017	Bab III : Acc	

KEMENTRIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS DAKWAH DAN KOMUNIKASI

Jln. Prof K. H. Zainal Abidin Fikry No. 1 KM. 3,5 Palembang 30126 Telp: (0711) 353360 website: www.radenfatah.ac.id

No	Tanggal	Uraian	Paraf
9	28/12/2017	Bab IV : Penjelasan hasil & pembahasan hasil	
10	5/1/2018	Bab IV : tambahan penjelasan	
11	8/1/2018	Bab IV : penjelasan tiap tahapan octave	
12	18/1/2018	Bab IV : penjelasan tiap tahapan + tabel	
13	19/1/2018	Bab IV : Hasil & pembahasan	
14	23/1/2018	Bab IV : Pembahasan per area/lingkaran + rekomendasi yg. berdasarkan referensi	
15	1/2/2018	Bab IV : tambahkan referensi di rekomendasi	

Lampiran Konsultasi Pembimbing II



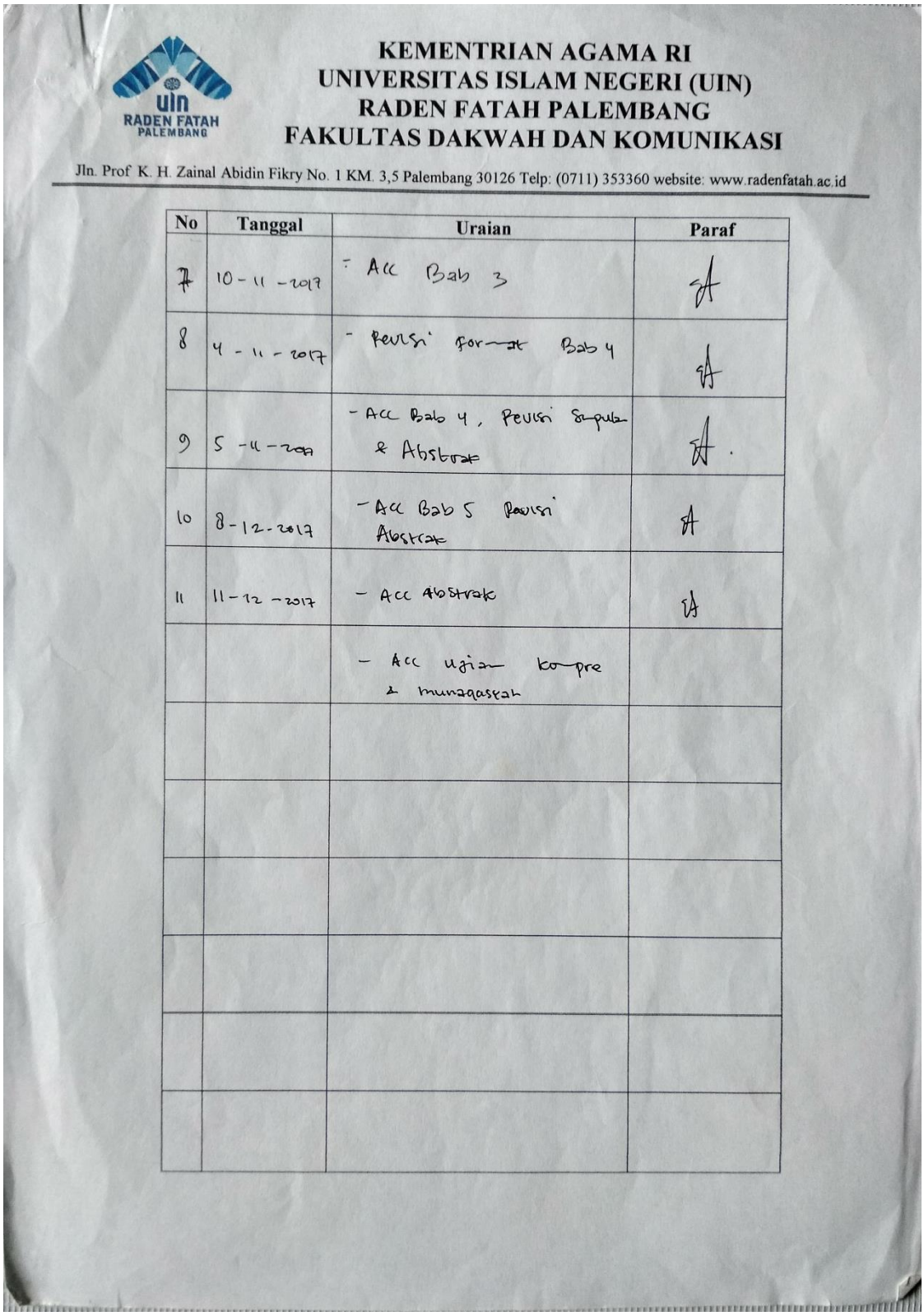
KEMENTRIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

Jln. Prof K. H. Zainal Abidin Fikry No. 1 KM. 3,5 Palembang 30126 Telp: (0711) 353360 website: www.radenfatah.ac.id

LEMBAR KONSULTASI

NIM : 13540007
Nama : Afriani Rizkika
Program Studi : Sistem Informasi
Semester : Genap / Ganjil Tahun Akademik : 2017
Judul : Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode Octave Allegro Di Perpustakaan UIN Raden Fatah Palembang
Dosen Pembimbing II : Evi Fadilah, M.Kom

No	Tanggal	Uraian	Paraf
1	24-7-2017	- Revisi Latar Belakang - Batasan Masalah - Metode Pengumpulan data	
		- Sistematika Penulisan	
2	27-7-2017	- Acc Bab I	
3	9-8-2017	- Revisi landasan teori - Format Penulisan	
		- Tinjauan pustaka	
4	10-8-2017	- Acc Bab 2	
5	18-9-2017	- Acc kuisioner	
6	31-10-2017	- Revisi Bab 3	

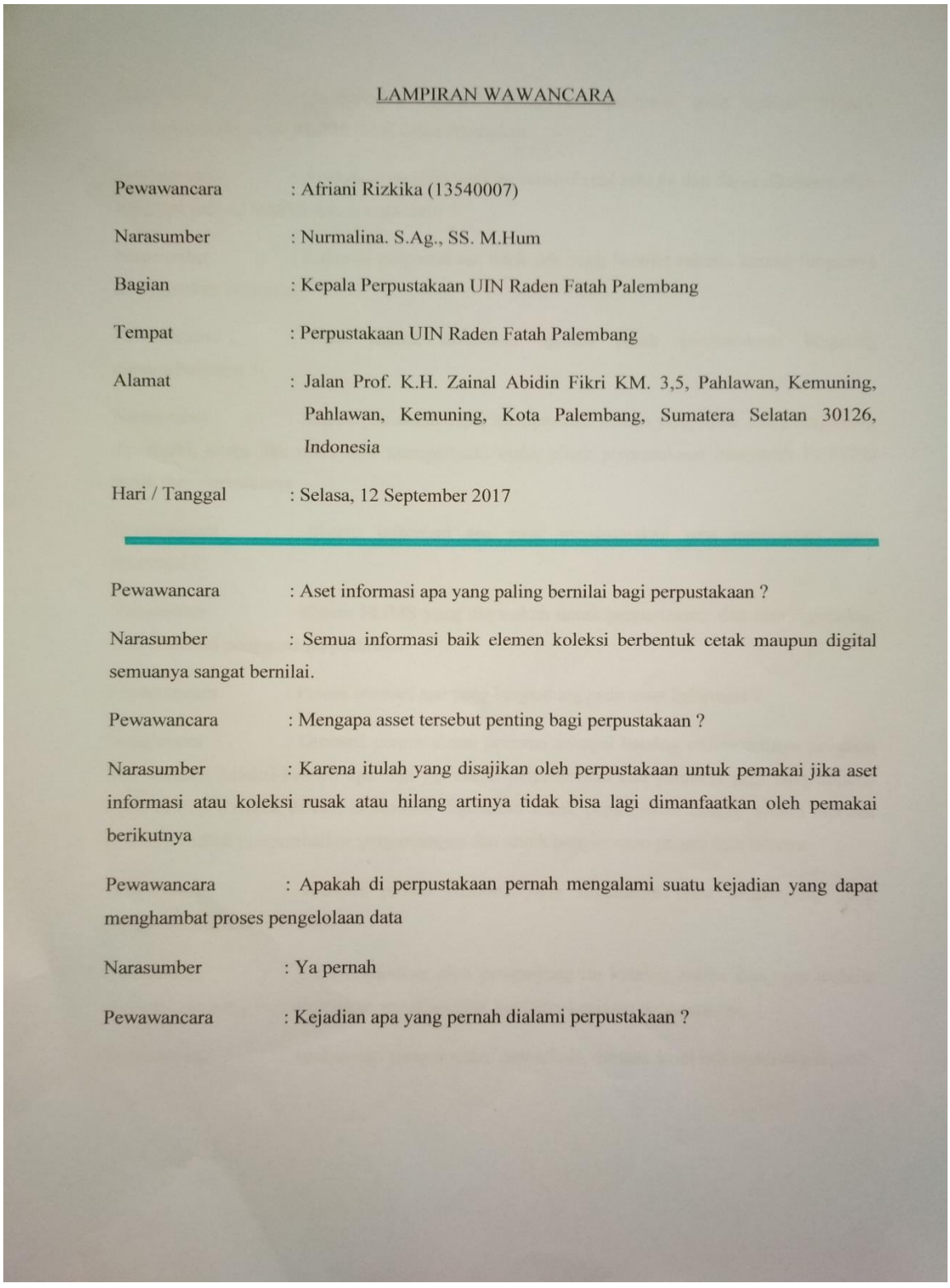


KEMENTRIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS DAKWAH DAN KOMUNIKASI

Jln. Prof K. H. Zainal Abidin Fikry No. 1 KM. 3,5 Palembang 30126 Telp: (0711) 353360 website: www.radenfatah.ac.id

No	Tanggal	Uraian	Paraf
7	10-11-2017	- Acc Bab 3	
8	4-11-2017	- Revisi format Bab 4	
9	5-11-2017	- Acc Bab 4, Revisi Simpulan & Abstrak	
10	8-12-2017	- Acc Bab 5 Revisi Abstrak	
11	11-12-2017	- Acc Abstrak	
		- Acc ujian kompre & munaqasah	

Lampiran Wawancara



LAMPIRAN WAWANCARA

Pewawancara : Afriani Rizkika (13540007)

Narasumber : Nurmalina. S.Ag., SS. M.Hum

Bagian : Kepala Perpustakaan UIN Raden Fatah Palembang

Tempat : Perpustakaan UIN Raden Fatah Palembang

Alamat : Jalan Prof. K.H. Zainal Abidin Fikri KM. 3,5, Pahlawan, Kemuning, Pahlawan, Kemuning, Kota Palembang, Sumatera Selatan 30126, Indonesia

Hari / Tanggal : Selasa, 12 September 2017

Pewawancara : Aset informasi apa yang paling bernilai bagi perpustakaan ?

Narasumber : Semua informasi baik elemen koleksi berbentuk cetak maupun digital semuanya sangat bernilai.

Pewawancara : Mengapa asset tersebut penting bagi perpustakaan ?

Narasumber : Karena itulah yang disajikan oleh perpustakaan untuk pemakai jika aset informasi atau koleksi rusak atau hilang artinya tidak bisa lagi dimanfaatkan oleh pemakai berikutnya

Pewawancara : Apakah di perpustakaan pernah mengalami suatu kejadian yang dapat menghambat proses pengelolaan data

Narasumber : Ya pernah

Pewawancara : Kejadian apa yang pernah dialami perpustakaan ?

Narasumber : Perpustakaan pernah mengalami gangguan pada aplikasi SLiMS sehingga pada saat itu SLiMS tidak dapat digunakan

Pewawancara : Apakah asset informasi ini sensitif atau rahasia dan dapat diketahui oleh beberapa individ terpilih dalam organisasi ?

Narasumber : Kalau di perpustakaan tidak ada yang bersifat rahasia karena fungsinya menyebarkan informasi

Pewawancara : Jika terjadi kerusakan apakah pihak perpustakaan langsung memperbaikinya ?

Narasumber : Jika perpustakaan dapat memperbaiki sistem yang rusak maka langusung diperbaiki, tetapi jika tidak bisa memperbaiki maka pihak perpustakaan menyuruh PUSTPD untuk memperbaikinya

Pewawancara : Sistem informasi apa yang menggunakan atau memproses asset informasi ?

Narasumber : Sistem SLIMS yang digunakan untuk perpustakaan dan bisa digunakan oleh eksternal pengguna perpustakaan

Pewawancara : Proses otomasi apa yang bergantung pada asset informasi ?

Narasumber : Otomasi perpustakaan pertama sebagai katalog online artinya pemakai bisa mencari koleksi-koleksi apa saja yg ada di perpustakaan dan pemakai juga tahu dimana letak koleksi tersebut di rak, kedua,bisa digunakan untuk peminjaman koleksi secara otomasi kemudian untuk pengembalian, perpanjangan dan untuk penginputan proses data lainnya.

Pewawancara : Adakah proses otomasi yang digunakan oleh pengunjung yang mengandalkan aset informasi ?

Narasumber : Yang digunakan oleh pengunjung itu katalog online dan juga website perpustakaan yang bisa digunakan untuk melihat kegiatan-kegiatan perpustakaan.

Pewawancara : Apakah ada tempat selain aset teknis, dimana asset informasi di simpan?

Narasumber : Informasi di simpan di dunia maya di internet dan kelola oleh server yang ada di PUSTPD, perpustakaan hanya mengelola data

Pewawancara : Apakah ada salinan kertas dari asset informasi yang dibagi atau disimpan di organisasi lain ?

Narasumber : Salinan kertas seperti membuat laporan pengunjung, jumlah anggota perpustakaan yang kemudian di print lalu kartu anggota di cetak dan diberikan kepada pemakai

Pewawancara : Apakah ada pihak eksternal yang mungkin memiliki akses terhadap informasi dan mungkin mempertahankannya atau mengungkapkannya jika mereka melihatnya ?

Narasumber : Menggunakan nya sudah pasti karena sudah online jadi bisa digunakan oleh semua orang tanpa batasan waktu dan tempat dan yang memanfaatkannya secara eksternal yang langsung berkunjung ke perpustakaan.

Narasumber : Aset informasi apa, jika hilang secara signifikan akan mengganggu kemampuan organisasi untuk mencapai tujuannya ?

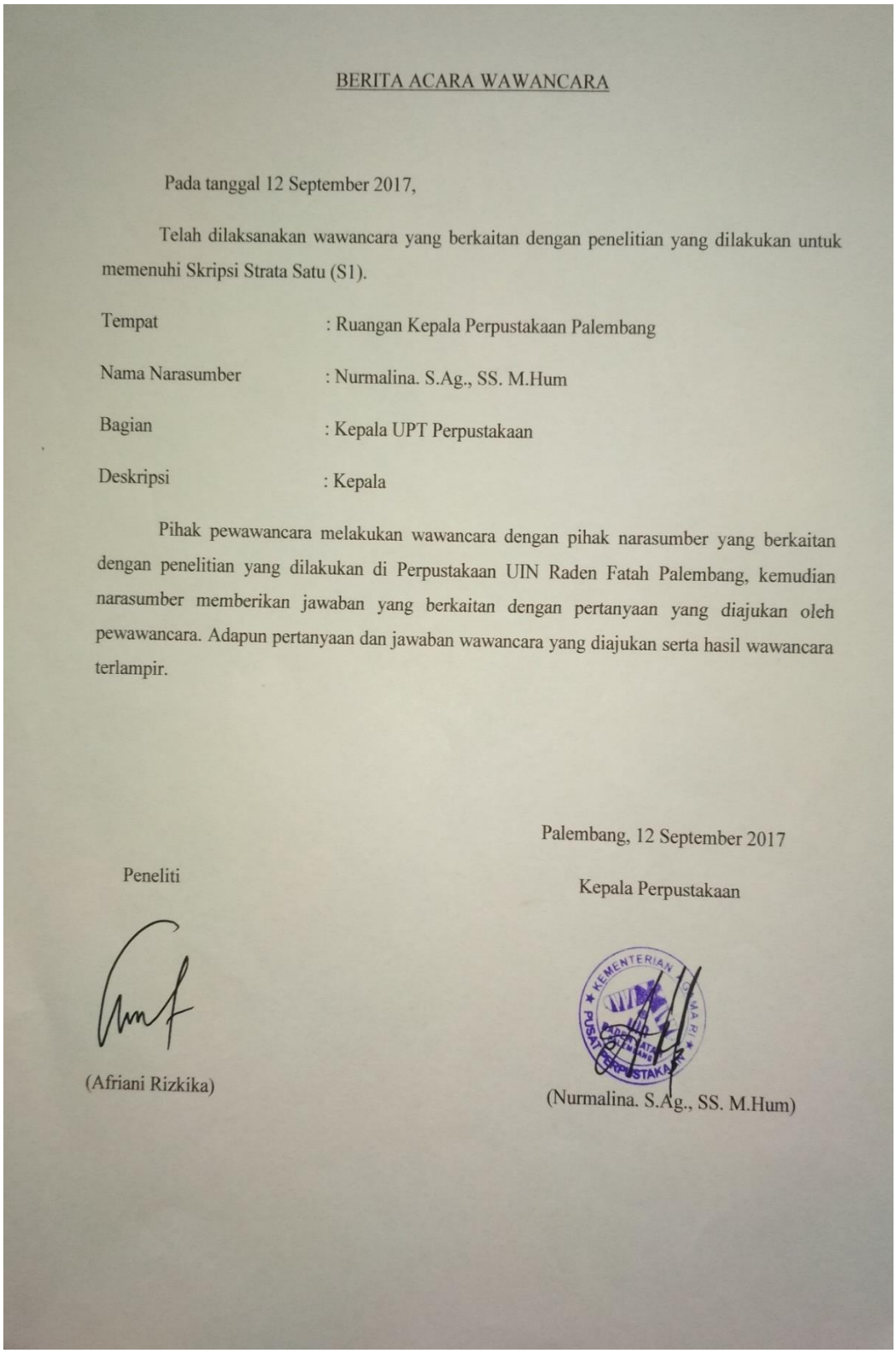
Pewawancara : Aset otomasi slims jika rusak bubar otomasi perpustakaan karena semua data buku, pengunjung, peminjaman semua data ada di SLIMS.

Palembang, 12 September 2017

Kepala Perpustakaan

(Nurmalina. S.Ag., SS. M.Hum)

Lampiran Berita Acara Wawancara



BERITA ACARA WAWANCARA

Pada tanggal 12 September 2017,

Telah dilaksanakan wawancara yang berkaitan dengan penelitian yang dilakukan untuk memenuhi Skripsi Strata Satu (S1).

Tempat : Ruangan Kepala Perpustakaan Palembang

Nama Narasumber : Nurmalina. S.Ag., SS. M.Hum

Bagian : Kepala UPT Perpustakaan

Deskripsi : Kepala

Pihak pewawancara melakukan wawancara dengan pihak narasumber yang berkaitan dengan penelitian yang dilakukan di Perpustakaan UIN Raden Fatah Palembang, kemudian narasumber memberikan jawaban yang berkaitan dengan pertanyaan yang diajukan oleh pewawancara. Adapun pertanyaan dan jawaban wawancara yang diajukan serta hasil wawancara terlampir.

Palembang, 12 September 2017

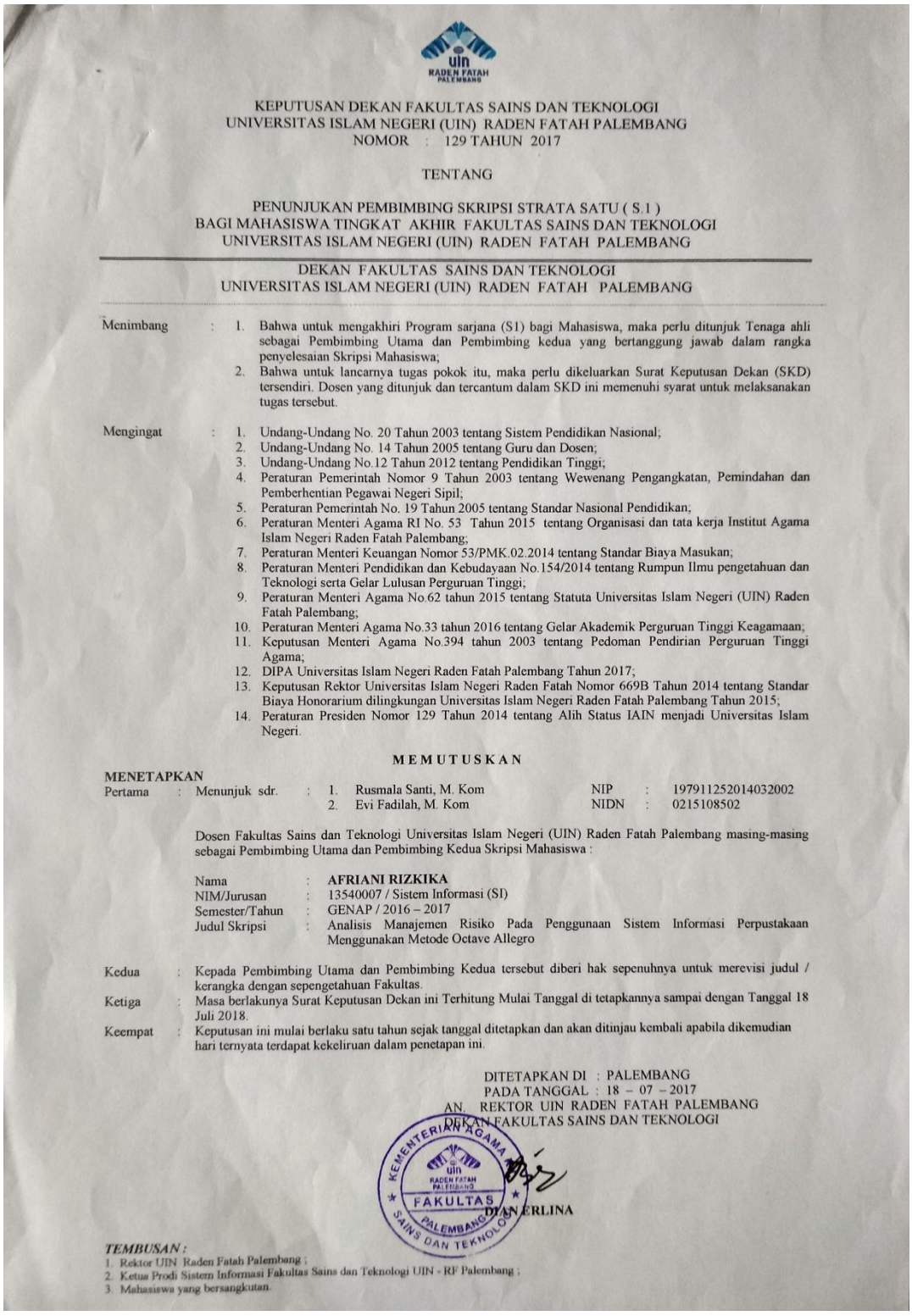
Peneliti

Kepala Perpustakaan

(Afriani Rizkika)

(Nurmalina. S.Ag., SS. M.Hum)

Lampiran SK Pembimbing



KEPUTUSAN DEKAN FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG
NOMOR : 129 TAHUN 2017

TENTANG

PENUNJUKAN PEMBIMBING SKRIPSI STRATA SATU (S.1)
BAGI MAHASISWA TINGKAT AKHIR FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG

DEKAN FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH PALEMBANG

Menimbang :
1. Bahwa untuk mengakhiri Program sarjana (S1) bagi Mahasiswa, maka perlu ditunjuk Tenaga ahli sebagai Pembimbing Utama dan Pembimbing kedua yang bertanggung jawab dalam rangka penyelesaian Skripsi Mahasiswa;
2. Bahwa untuk lancarnya tugas pokok itu, maka perlu dikeluarkan Surat Keputusan Dekan (SKD) tersendiri. Dosen yang ditunjuk dan tercantum dalam SKD ini memenuhi syarat untuk melaksanakan tugas tersebut.

Mengingat :
1. Undang-Undang No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
2. Undang-Undang No. 14 Tahun 2005 tentang Guru dan Dosen;
3. Undang-Undang No.12 Tahun 2012 tentang Pendidikan Tinggi;
4. Peraturan Pemerintah Nomor 9 Tahun 2003 tentang Wewenang Pengangkatan, Pemindahan dan Pemberhentian Pegawai Negeri Sipil;
5. Peraturan Pemerintah No. 19 Tahun 2005 tentang Standar Nasional Pendidikan;
6. Peraturan Menteri Agama RI No. 53 Tahun 2015 tentang Organisasi dan tata kerja Institut Agama Islam Negeri Raden Fatah Palembang;
7. Peraturan Menteri Keuangan Nomor 53/PMK.02.2014 tentang Standar Biaya Masukan;
8. Peraturan Menteri Pendidikan dan Kebudayaan No.154/2014 tentang Rumpun Ilmu pengetahuan dan Teknologi serta Gelar Lulusan Perguruan Tinggi;
9. Peraturan Menteri Agama No.62 tahun 2015 tentang Statuta Universitas Islam Negeri (UIN) Raden Fatah Palembang;
10. Peraturan Menteri Agama No.33 tahun 2016 tentang Gelar Akademik Perguruan Tinggi Keagamaan;
11. Keputusan Menteri Agama No.394 tahun 2003 tentang Pedoman Pendirian Perguruan Tinggi Agama;
12. DIPA Universitas Islam Negeri Raden Fatah Palembang Tahun 2017;
13. Keputusan Rektor Universitas Islam Negeri Raden Fatah Nomor 669B Tahun 2014 tentang Standar Biaya Honorarium dilingkungan Universitas Islam Negeri Raden Fatah Palembang Tahun 2015;
14. Peraturan Presiden Nomor 129 Tahun 2014 tentang Alih Status IAIN menjadi Universitas Islam Negeri.

M E M U T U S K A N

MENETAPKAN

Pertama : Menunjuk sdr. :
1. Rusmala Santi, M. Kom — NIP : 197911252014032002
2. Evi Fadilah, M. Kom — NIDN : 0215108502

Dosen Fakultas Sains dan Teknologi Universitas Islam Negeri (UIN) Raden Fatah Palembang masing-masing sebagai Pembimbing Utama dan Pembimbing Kedua Skripsi Mahasiswa :

Nama : **AFRIANI RIZKIKA**
NIM/Jurusan : 13540007 / Sistem Informasi (SI)
Semester/Tahun : GENAP / 2016 – 2017
Judul Skripsi : Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode Octave Allegro

Kedua : Kepada Pembimbing Utama dan Pembimbing Kedua tersebut diberi hak sepenuhnya untuk merevisi judul / kerangka dengan sepengetahuan Fakultas.

Ketiga : Masa berlakunya Surat Keputusan Dekan ini Terhitung Mulai Tanggal di tetapkannya sampai dengan Tanggal 18 Juli 2018.

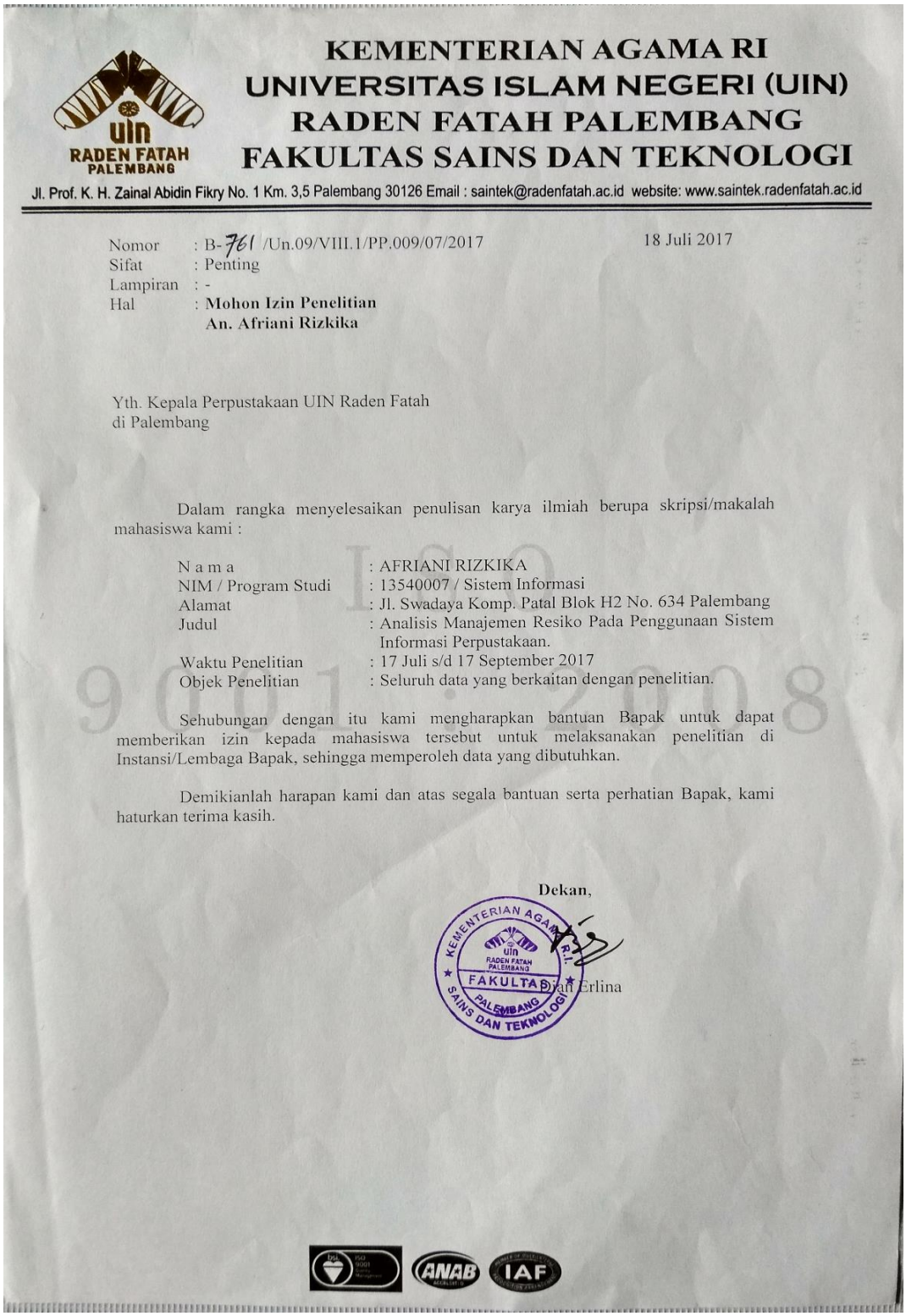
Keempat : Keputusan ini mulai berlaku satu tahun sejak tanggal ditetapkan dan akan ditinjau kembali apabila dikemudian hari ternyata terdapat kekeliruan dalam penetapan ini.

DITETAPKAN DI : PALEMBANG
PADA TANGGAL : 18 – 07 – 2017
AN. REKTOR UIN RADEN FATAH PALEMBANG
DEKAN FAKULTAS SAINS DAN TEKNOLOGI

DIAN ERLINA

TEMBUSAN :
1. Rektor UIN Raden Fatah Palembang ;
2. Ketua Prodi Sistem Informasi Fakultas Sains dan Teknologi UIN - RF Palembang ;
3. Mahasiswa yang bersangkutan.

Lampiran Surat Izin Penelitian



KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI (UIN)
RADEN FATAH PALEMBANG
FAKULTAS SAINS DAN TEKNOLOGI

UIN RADEN FATAH PALEMBANG

Jl. Prof. K. H. Zainal Abidin Fikry No. 1 Km. 3,5 Palembang 30126 Email : saintek@radenfatah.ac.id website: www.saintek.radenfatah.ac.id

Nomor : B-761 /Un.09/VIII.1/PP.009/07/2017 — 18 Juli 2017
Sifat : Penting
Lampiran : -
Hal : **Mohon Izin Penelitian**
An. Afriani Rizkika

Yth. Kepala Perpustakaan UIN Raden Fatah
di Palembang

Dalam rangka menyelesaikan penulisan karya ilmiah berupa skripsi/makalah mahasiswa kami :

N a m a	: AFRIANI RIZKIKA
NIM / Program Studi	: 13540007 / Sistem Informasi
Alamat	: Jl. Swadaya Komp. Patal Blok H2 No. 634 Palembang
Judul	: Analisis Manajemen Resiko Pada Penggunaan Sistem Informasi Perpustakaan.
Waktu Penelitian	: 17 Juli s/d 17 September 2017
Objek Penelitian	: Seluruh data yang berkaitan dengan penelitian.

Sehubungan dengan itu kami mengharapkan bantuan Bapak untuk dapat memberikan izin kepada mahasiswa tersebut untuk melaksanakan penelitian di Instansi/Lembaga Bapak, sehingga memperoleh data yang dibutuhkan.

Demikianlah harapan kami dan atas segala bantuan serta perhatian Bapak, kami haturkan terima kasih.

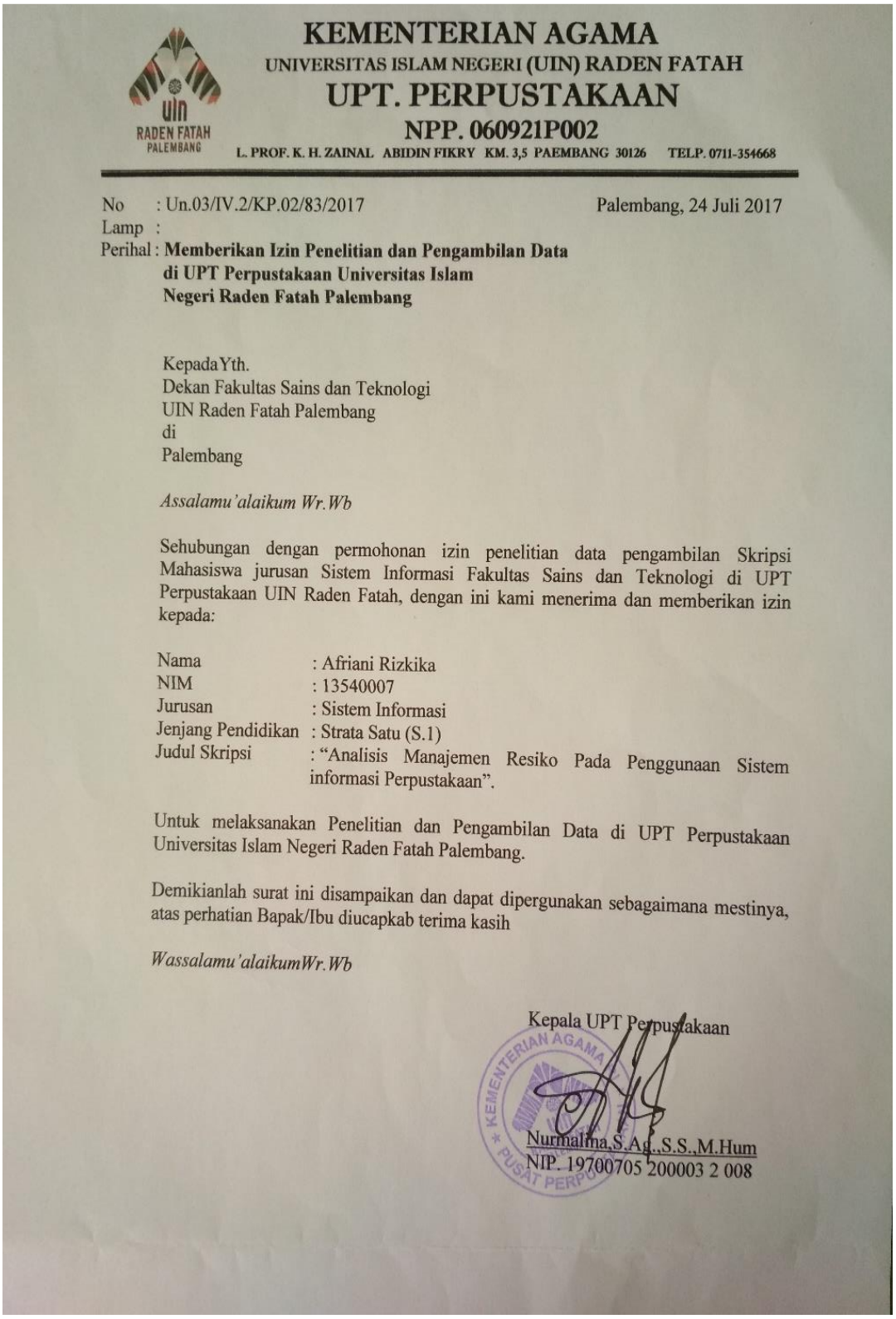
Dekan,

KEMENTERIAN AGAMA R.I. UIN RADEN FATAH PALEMBANG FAKULTAS SAINS DAN TEKNOLOGI PALEMBANG

Dian Erlina

ISO 9001:2008 ANAB IAF

Lampiran Balasan Izin Penelitian



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI (UIN) RADEN FATAH
UPT. PERPUSTAKAAN
NPP. 060921P002
L. PROF. K. H. ZAINAL ABIDIN FIKRY KM. 3,5 PAEMBANG 30126 TELP. 0711-354668

No : Un.03/IV.2/KP.02/83/2017 Palembang, 24 Juli 2017
Lamp :
Perihal : **Memberikan Izin Penelitian dan Pengambilan Data di UPT Perpustakaan Universitas Islam Negeri Raden Fatah Palembang**

Kepada Yth.
Dekan Fakultas Sains dan Teknologi
UIN Raden Fatah Palembang
di
Palembang

Assalamu'alaikum Wr.Wb

Sehubungan dengan permohonan izin penelitian data pengambilan Skripsi Mahasiswa jurusan Sistem Informasi Fakultas Sains dan Teknologi di UPT Perpustakaan UIN Raden Fatah, dengan ini kami menerima dan memberikan izin kepada:

Nama	: Afriani Rizkika
NIM	: 13540007
Jurusan	: Sistem Informasi
Jenjang Pendidikan	: Strata Satu (S.1)
Judul Skripsi	: "Analisis Manajemen Resiko Pada Penggunaan Sistem informasi Perpustakaan".

Untuk melaksanakan Penelitian dan Pengambilan Data di UPT Perpustakaan Universitas Islam Negeri Raden Fatah Palembang.

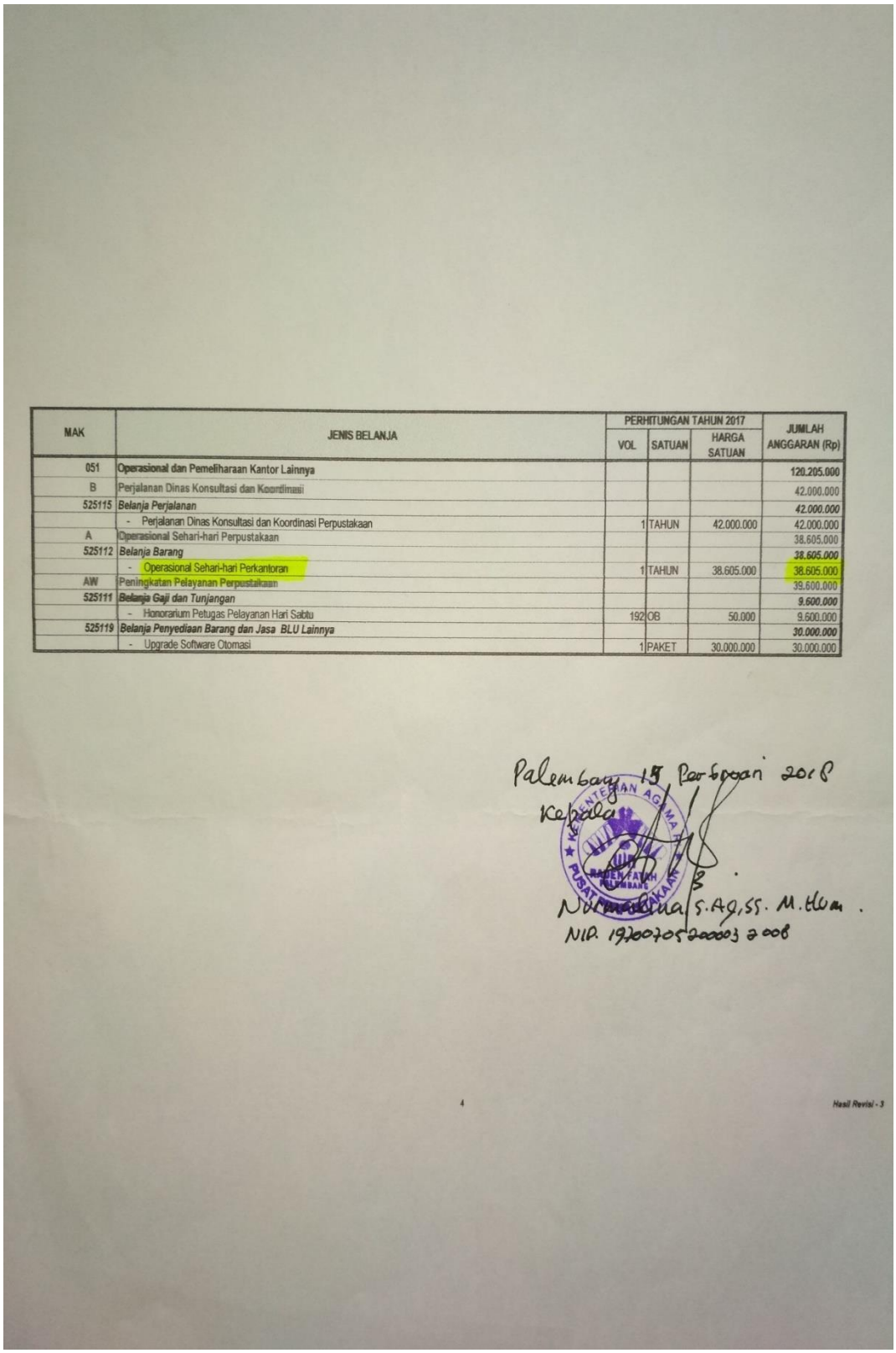
Demikianlah surat ini disampaikan dan dapat dipergunakan sebagaimana mestinya, atas perhatian Bapak/Ibu diucapkab terima kasih

Wassalamu'alaikumWr.Wb

Kepala UPT Perpustakaan

Nurmalina,S.Ag.,S.S.,M.Hum
NIP. 19700705 200003 2 008

Lampiran Biaya Operasional



MAK	JENIS BELANJA	PERHITUNGAN TAHUN 2017			JUMLAH ANGGARAN (Rp)
		VOL	SATUAN	HARGA SATUAN	
051	**Operasional dan Pemeliharaan Kantor Lainnya**				**120.205.000**
B	Perjalanan Dinas Konsultasi dan Koordinasi				42.000.000
525115	***Belanja Perjalanan***				***42.000.000***
	- Perjalanan Dinas Konsultasi dan Koordinasi Perpustakaan	1	TAHUN	42.000.000	42.000.000
A	Operasional Sehari-hari Perpustakaan				38.605.000
525112	***Belanja Barang***				***38.605.000***
	- Operasional Sehari-hari Perkantoran	1	TAHUN	38.605.000	38.605.000
AIW	Peningkatan Pelayanan Perpustakaan				39.600.000
525111	***Belanja Gaji dan Tunjangan***				***9.600.000***
	- Honorarium Petugas Pelayanan Hari Sabtu	192	OB	50.000	9.600.000
525119	***Belanja Penyediaan Barang dan Jasa BLU Lainnya***				***30.000.000***
	- Upgrade Software Otomasi	1	PAKET	30.000.000	30.000.000

Palembang, 15 Desember 2017
Kepala

Nurmadiah, S.Ag, S.S., M.Hum.
NIP. 19700705 200003 2 008

4

Hasil Revisi - 3

Lampiran Denda

PERPUSTAKAAN UIN RADEN FATAH PALEMBANG

4. Kewajiban Pemustaka

a) Berpakaian sopan, bersih, dan rapi.
b) Menjaga dan merawat koleksi yang telah dipinjam selama dalam pinjaman.
c) Menggunakan seluruh peralatan perpustakaan sesuai dengan peruntukan bukan untuk kepentingan diluar ketentuan yang ada.
d) Memasukkan buku cetak, binder, tas (termasuk tas laptop), dan jaket kedalam loker yang disediakan. Barang-barang berharga seperti laptop, dompet, handphone (HP), uang, perhiasan dan sejenisnya harap dibawa dan dijaga sendiri. Kehilangan barang di perpustakaan bukan menjadi tanggung jawab perpustakaan.
e) Menunjukkan identitas yang masih berlaku ketika menggunakan seluruh fasilitas di perpustakaan
f) Mematikan nada dering (silent) HP selama berada di perpustakaan.
g) Pemustaka selain sivitas akademika UIN Raden Fatah hanya boleh membaca di tempat
h) Mematuhi tata tertib sebagaimana yang ada dalam buku etika mahasiswa UIN Raden Fatah Palembang.

5. Larangan Anggota Perpustakaan

a) Membawa senjata tajam.
b) Merokok, membawa makanan, [illegible] ke dalam perpustakaan.
c) Memakai sandal jepit, baju kaos, [illegible] jaket ke dalam perpustakaan.
d) Berisik, gaduh, dan mengganggu [illegible] lain di dalam perpustakaan.
e) Merobek, merusak, mengotori dan mencoret-coret koleksi perpustakaan.
f) Mengubah, membuang identitas buku yang dipinjamnya.
g) Memakai kartu anggota perpustakaan milik anggota lain.

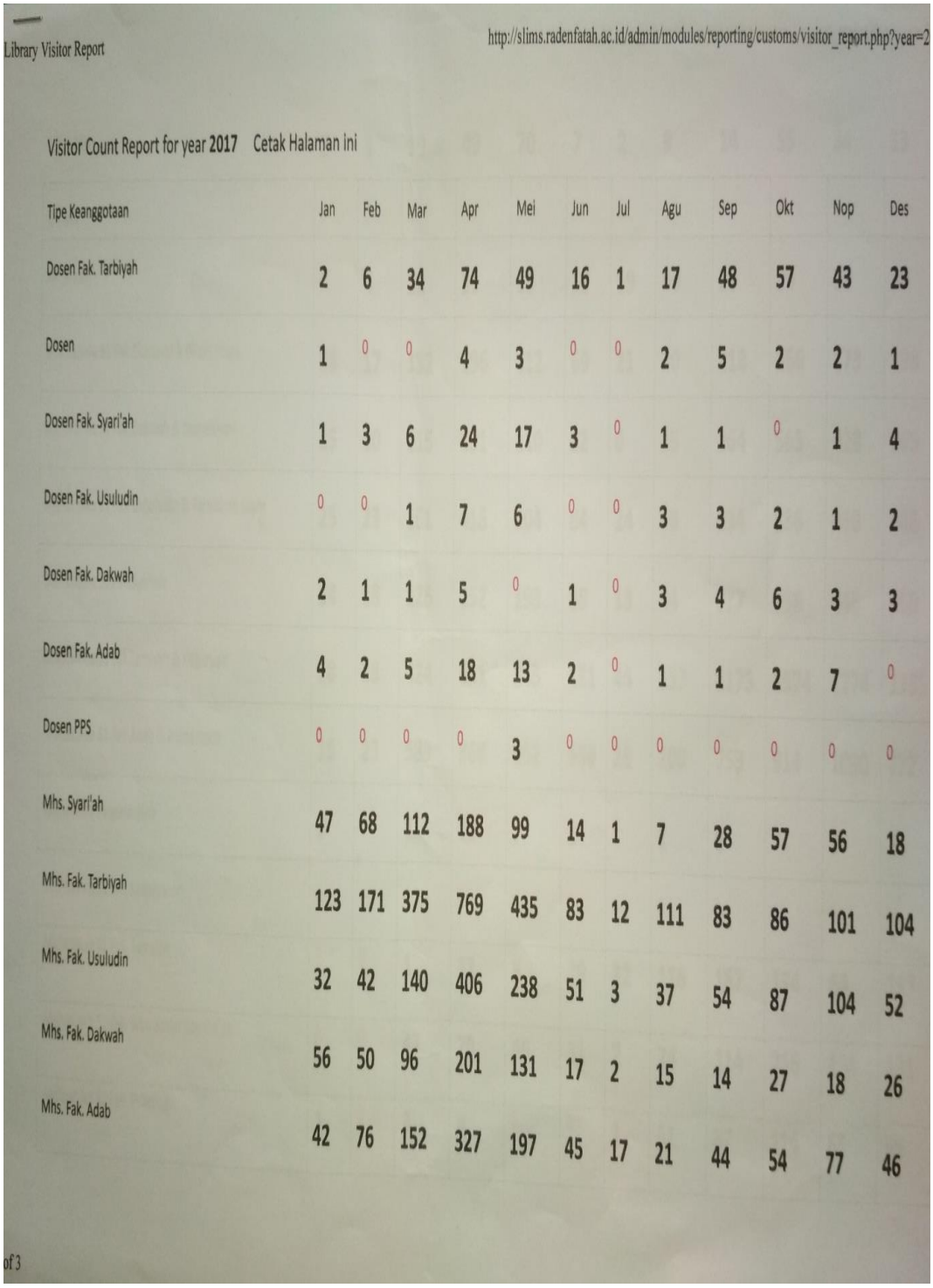
6. Denda/Sanksi

a. Denda uang sebesar Rp. 500,- per buku/hari
b. Mengganti dengan 2 buah buku dengan judul dan pengarang yang sama dan atau denda 4 kali harga buku jika buku yang dipinjam hilang.

B. SISTEM PELAYANAN

Sistem pelayanan yang diterapkan di perpustakaan UIN Raden Fatah adalah sistem pelayanan terbuka (open access). Dalam sistem ini para pemustaka dibenarkan untuk dapat secara langsung memilih, mencari/menemukan dan mengambil sendiri bahan pustaka yang dikehendaki dari jajaran koleksi perpustakaan yang ada di koreksi. Artinya para pemustaka dapat melakukan browsing bahan pustaka dari jajaran koleksi.

Lampiran Pengunjung



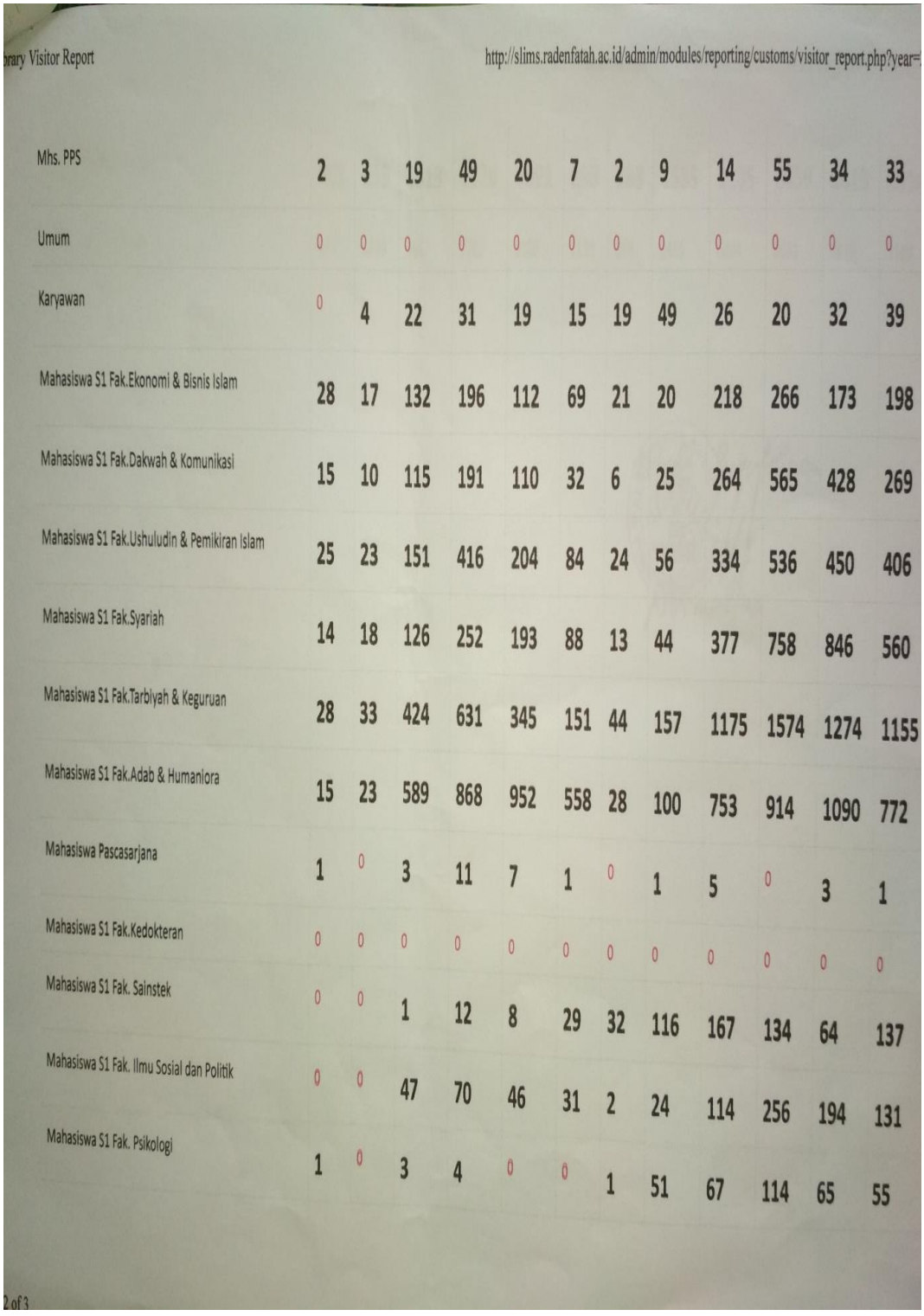
Library Visitor Report

http://slims.radenfatah.ac.id/admin/modules/reporting/customs/visitor_report.php?year=2

Visitor Count Report for year **2017** Cetak Halaman ini

Tipe Keanggotaan	Jan	Feb	Mar	Apr	Mei	Jun	Jul	Agu	Sep	Okt	Nop	Des
Dosen Fak. Tarbiyah	2	6	34	74	49	16	1	17	48	57	43	23
Dosen	1	0	0	4	3	0	0	2	5	2	2	1
Dosen Fak. Syari'ah	1	3	6	24	17	3	0	1	1	0	1	4
Dosen Fak. Usuludin	0	0	1	7	6	0	0	3	3	2	1	2
Dosen Fak. Dakwah	2	1	1	5	0	1	0	3	4	6	3	3
Dosen Fak. Adab	4	2	5	18	13	2	0	1	1	2	7	0
Dosen PPS	0	0	0	0	3	0	0	0	0	0	0	0
Mhs. Syari'ah	47	68	112	188	99	14	1	7	28	57	56	18
Mhs. Fak. Tarbiyah	123	171	375	769	435	83	12	111	83	86	101	104
Mhs. Fak. Usuludin	32	42	140	406	238	51	3	37	54	87	104	52
Mhs. Fak. Dakwah	56	50	96	201	131	17	2	15	14	27	18	26
Mhs. Fak. Adab	42	76	152	327	197	45	17	21	44	54	77	46

of 3



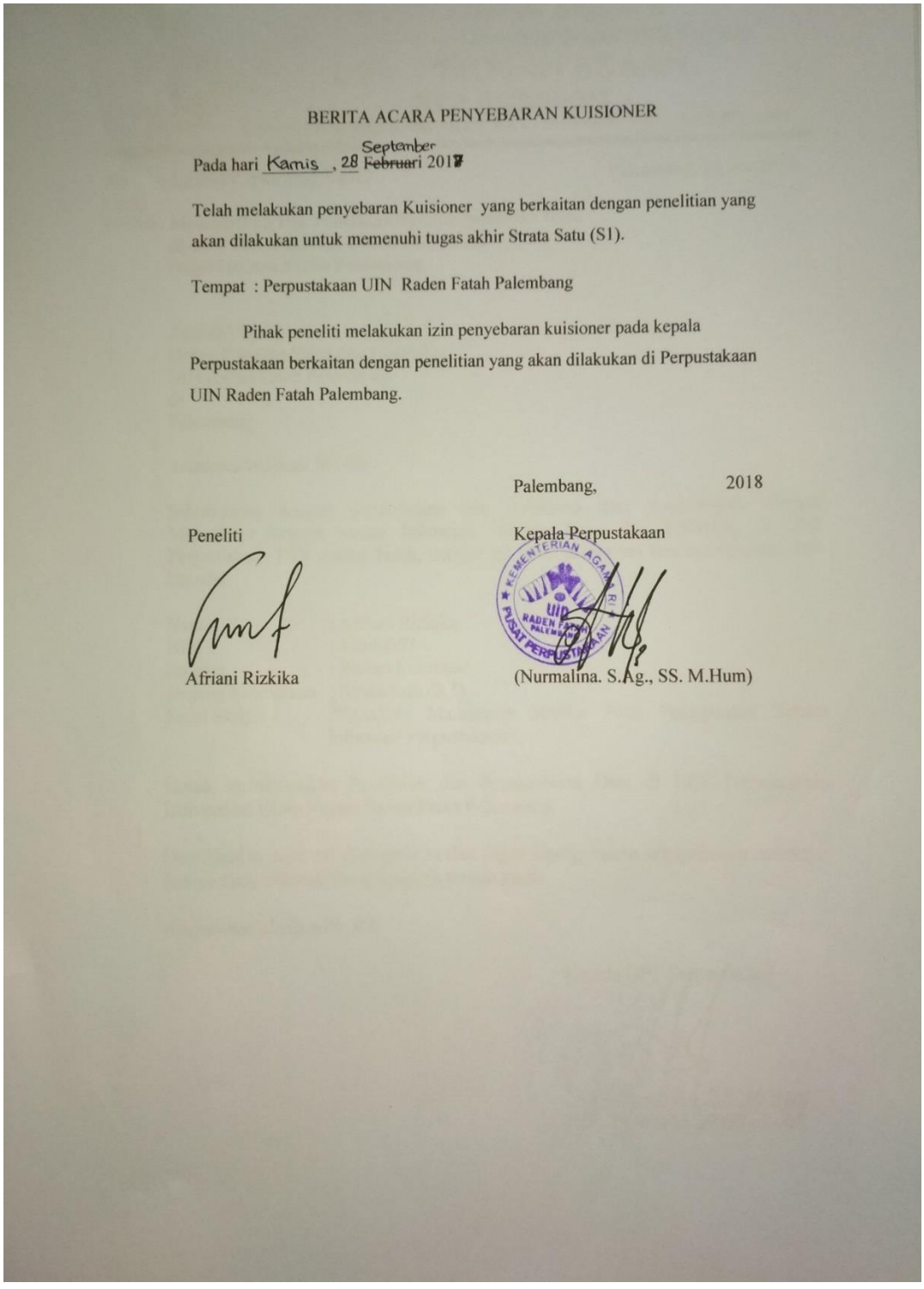
rary Visitor Report http://slims.radenfatah.ac.id/admin/modules/reporting/customs/visitor_report.php?year=

Mhs. PPS	2	3	19	49	20	7	2	9	14	55	34	33
Umum	0	0	0	0	0	0	0	0	0	0	0	0
Karyawan	0	4	22	31	19	15	19	49	26	20	32	39
Mahasiswa S1 Fak.Ekonomi & Bisnis Islam	28	17	132	196	112	69	21	20	218	266	173	198
Mahasiswa S1 Fak.Dakwah & Komunikasi	15	10	115	191	110	32	6	25	264	565	428	269
Mahasiswa S1 Fak.Ushuludin & Pemikiran Islam	25	23	151	416	204	84	24	56	334	536	450	406
Mahasiswa S1 Fak.Syariah	14	18	126	252	193	88	13	44	377	758	846	560
Mahasiswa S1 Fak.Tarbiyah & Keguruan	28	33	424	631	345	151	44	157	1175	1574	1274	1155
Mahasiswa S1 Fak.Adab & Humaniora	15	23	589	868	952	558	28	100	753	914	1090	772
Mahasiswa Pascasarjana	1	0	3	11	7	1	0	1	5	0	3	1
Mahasiswa S1 Fak.Kedokteran	0	0	0	0	0	0	0	0	0	0	0	0
Mahasiswa S1 Fak. Sainstek	0	0	1	12	8	29	32	116	167	134	64	137
Mahasiswa S1 Fak. Ilmu Sosial dan Politik	0	0	47	70	46	31	2	24	114	256	194	131
Mahasiswa S1 Fak. Psikologi	1	0	3	4	0	0	1	51	67	114	65	55

2 of 3

Pengunjung Bukan Anggota	402	659	3313	2528	1991	898	588	1585	3185	2459	1613	1514
Total kunjungan/bulan	841	1209	5867	7282	5198	2195	816	2455	6984	8031	6679	5549

Lampiran Penyebaran Kuesioner



BERITA ACARA PENYEBARAN KUISIONER

Pada hari Kamis, 28 ~~Februari~~ September 2017

Telah melakukan penyebaran Kuisioner yang berkaitan dengan penelitian yang akan dilakukan untuk memenuhi tugas akhir Strata Satu (S1).

Tempat : Perpustakaan UIN Raden Fatah Palembang

Pihak peneliti melakukan izin penyebaran kuisioner pada kepala Perpustakaan berkaitan dengan penelitian yang akan dilakukan di Perpustakaan UIN Raden Fatah Palembang.

Palembang, 2018

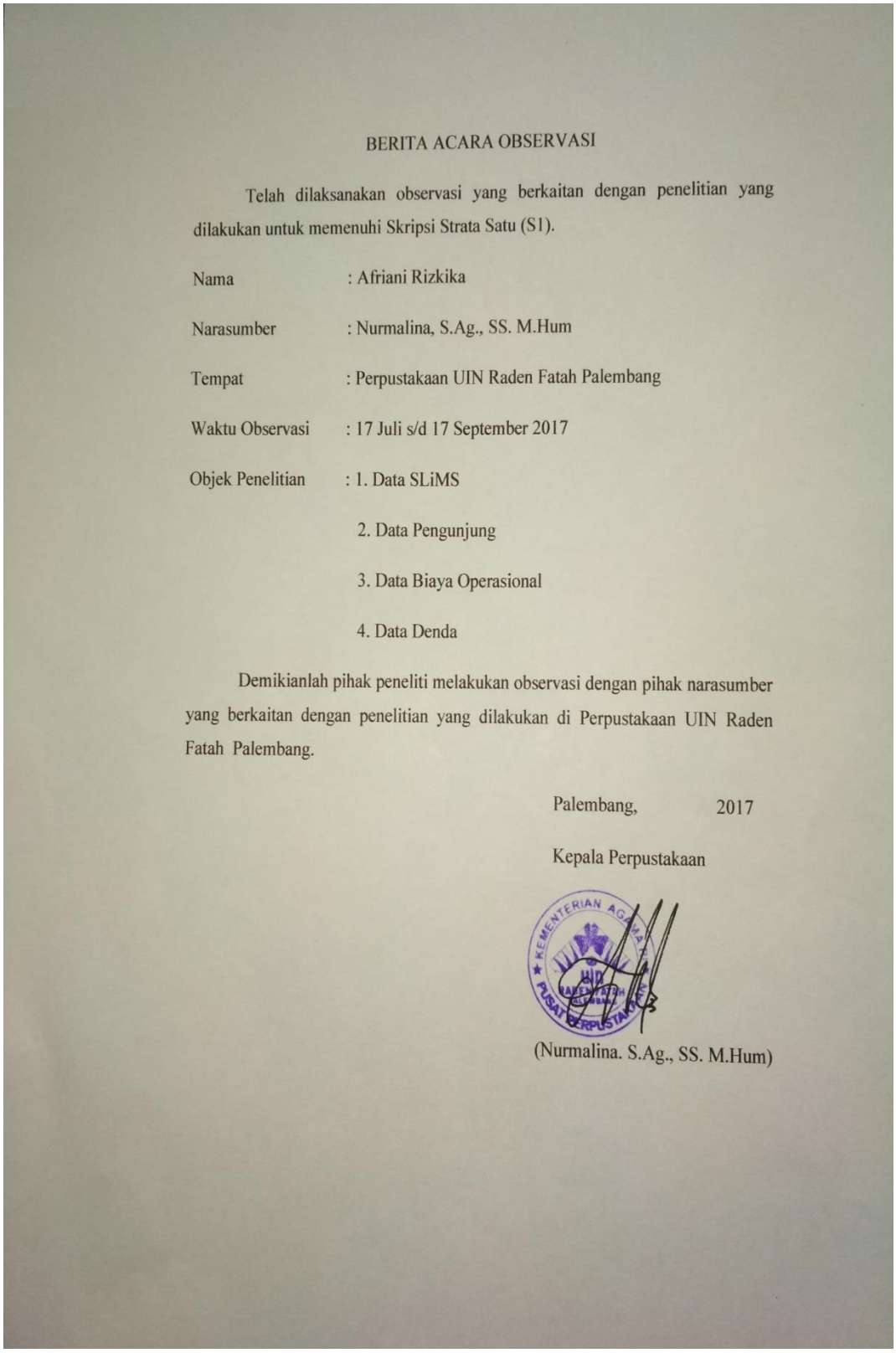
Peneliti

Afriani Rizkika

Kepala Perpustakaan

(Nurmalina. S.Ag., SS. M.Hum)

Lampiran Berita Acara Observasi



BERITA ACARA OBSERVASI

Telah dilaksanakan observasi yang berkaitan dengan penelitian yang dilakukan untuk memenuhi Skripsi Strata Satu (S1).

Nama : Afriani Rizkika

Narasumber : Nurmalina, S.Ag., SS. M.Hum

Tempat : Perpustakaan UIN Raden Fatah Palembang

Waktu Observasi : 17 Juli s/d 17 September 2017

Objek Penelitian : 1. Data SLiMS

2. Data Pengunjung

3. Data Biaya Operasional

4. Data Denda

Demikianlah pihak peneliti melakukan observasi dengan pihak narasumber yang berkaitan dengan penelitian yang dilakukan di Perpustakaan UIN Raden Fatah Palembang.

Palembang, 2017

Kepala Perpustakaan

(Nurmalina. S.Ag., SS. M.Hum)

Lampiran Kuesioner

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation).*Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	DIKY KURNIADI
Usia	27
Jenis Kelamin	Laki-Laki
Bagian / Departemen	UPT Perpustakaan UIN Raden Fatah Palembang

Skenario Pertanyaan Ancaman 1	Kontainer teknis

Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.

Skenario 1:

Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:

Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya ✓ (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya ✓ (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya ✓ (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario 2:

Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :

Diungkapkan kepada individu yang tidak berwenang?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)		Kontainer teknis			
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya ✓ (modifikasi)	Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	Ya ✓ (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya ✓ (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	✓ Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya ✓ (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya ✓ (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	✓ Ya (rugi)

Kuesioner Skenario Ancaman – 2	**Kontainer Fisik**

Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.

Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya ✓ (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya ✓ (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya ✓ (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario 2:

Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:

Diungkapkan kepada individu yang tidak berwenang?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)		Kontainer Fisik			
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Masalah pihak ketiga lainnya terjadi	Tidak	Ya ✓ (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya ✓ (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3		Orang-orang	
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya ✓ (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya ✓ (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya ✓ (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	✓ Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya ✓ (sengaja)

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation)*.Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	Gepin Yunaltra
Usia	25 tahun
Jenis Kelamin	Laki laki
Bagian / Departemen	Uin raden fatah Palembang

Skenario Pertanyaan Ancaman 1	Kontainer teknis		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2	**Kontainer Fisik**		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)		Kontainer Fisik			
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Masalah pihak ketiga lainnya terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3		Orang-orang	
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation).*Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	RIKA HANDAYANI
Usia	23 TAHUN
Jenis Kelamin	PEREMPUAN
Bagian / Departemen	SIRKULASI

Skenario Pertanyaan Ancaman 1	Kontainer teknis		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2		**Kontainer Fisik**	
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)	Kontainer Fisik				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Masalah pihak ketiga lainnya terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3	Orang-orang		
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation)*.Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	Ahmad Syarkowi
Usia	
Jenis Kelamin	Laki-laki
Bagian / Departemen	Tata Usaha

Skenario Pertanyaan Ancaman 1	Kontainer teknis		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya ✓ (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya ✓ (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :			
Diungkapkan kepada individu yang tidak berwenang?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2		**Kontainer Fisik**	
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)	Kontainer Fisik			
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda				
Masalah pihak ketiga lainnya terjadi	Tidak ✓	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi) ✓

Kuesioner Skenario Ancaman - 3	Orang-orang		
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja) ✓
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja) ✓
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja) ✓
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja) ✓

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation)*.Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	NURMALINA, S.Ag., SS. M. Hum
Usia	48 TAHUN
Jenis Kelamin	PEREMPUAN
Bagian / Departemen	KEPALA

Skenario Pertanyaan Ancaman 1	Kontainer teknis

Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.

Skenario 1:

Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:

Diungkapkan kepada individu yang tidak berwenang?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja) ✓	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja) ✓	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario 2:

Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :

Diungkapkan kepada individu yang tidak berwenang?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2		**Kontainer Fisik**	
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)	Kontainer Fisik			
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Masalah pihak ketiga lainnya terjadi	Tidak ✓	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak ✓	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3	Orang-orang		
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja) ✓	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja) ✓	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak ✓	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja) ✓	Ya (sengaja)

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation).*Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	Etti Puspita Sari, S.Sos
Usia	29 Tahun
Jenis Kelamin	Perempuan
Bagian / Departemen	STAFF UPT. Perpustakaan

Skenario Pertanyaan Ancaman 1	Kontainer teknis		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	~~Ya~~ (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	~~Ya~~ (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	~~Ya~~ (modifikasi)	Ya (interupsi)	Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	~~Ya~~ (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	~~Ya~~ (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	~~Ya~~ (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	~~Ya~~ (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2	**Kontainer Fisik**		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)			Kontainer Fisik		
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Masalah pihak ketiga lainnya terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3		Orang-orang	
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation).*Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	Asmaran
Usia	
Jenis Kelamin	Perempuan
Bagian / Departemen	Layanan Local Content & Tandon

Skenario Pertanyaan Ancaman 1	Kontainer teknis		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2		**Kontainer Fisik**	
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)					Kontainer Fisik
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Masalah pihak ketiga lainnya terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3			Orang-orang
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation).* Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	ROZALI
Usia	54 TAHUN
Jenis Kelamin	LAKI - LAKI
Bagian / Departemen	ADM

Skenario Pertanyaan Ancaman 1	Kontainer teknis		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	✓Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	✓Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	✓Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	✓Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	✓Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya (pengungkapan)	Ya (modifikasi)	✓Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	✓Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2	Kontainer Fisik		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)	Kontainer Fisik			
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda				
Masalah pihak ketiga lainnya terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3	Orang-orang		
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation).*Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	Rumila Shri. M.Hum
Usia	28 Tahun
Jenis Kelamin	perempuan
Bagian / Departemen	perpustkaan / pengolahan

Skenario Pertanyaan Ancaman 1	Kontainer teknis		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2 | **Kontainer Fisik**

Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.

Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario 2:

Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:

Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)	Kontainer Fisik				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Masalah pihak ketiga lainnya terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3	Orang-orang		
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

KUESIONER

Analisis Manajemen Risiko Pada Penggunaan Sistem Informasi Perpustakaan Menggunakan Metode OCTAVE Allegro

Kuesioner ini adalah bagian dari penelitian skripsi mahasiswa Jurusan Sistem Informasi Fakultas Sains dan Teknologi UIN Raden Fatah Palembang, yang bertujuan untuk mendapatkan data dan opini dari staff/karyawan Perpustakaan UIN Raden Fatah Palembang mengenai manajemen risiko di Perpustakan UIN Raden Fatah.

Kuesioner ini dikembangkan dari standar manajemen risiko sistem informasi perpustaakan yaitu OCTAVE Allegro *(Operationally Critical Threat, Assets and Vulnerability Evaluation)*.Untuk itu mohon kiranya bapak/ibu dapat memberikan opini dan pendapatnya akan pertanyaan-pertanyaan yang akan diberikan dalam kuesioner ini.

PETUNJUK PENGISIAN KUESIONER

Responden dapat memberikan jawaban dengan memberikan tanda centang (√) pada salah satu pilihan jawaban yang tersedia. Hanya satu jawaban saja yang dimungkinkan untuk setiap pertanyaan.

IDENTITAS RESPONDEN

Nama	Ulmi Kalsum.
Usia	26
Jenis Kelamin	Perempuan
Bagian / Departemen	UPT. Perpustakaan UIN RF.

Skenario Pertanyaan Ancaman 1	Kontainer teknis		
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah teknis tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan dapat mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Apakah ada situasi di mana orang luar bisa mengakses satu atau lebih wadah teknis, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi :			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman - 1 (lanjutan)	Kontainer teknis				
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi aset informasi Anda pada kontainer teknis yang Anda identifikasi. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset informasi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja • Gangguan yang tidak disengaja terhadap ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda					
Sebuah cacat perangkat lunak terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sistem crash diketahui atau tidak diketahui asal terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Sebuah cacat perangkat keras terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Kode berbahaya (seperti virus, worm, trojan horse, atau back door) dieksekusi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah dengan telekomunikasi terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Masalah atau sistem pihak ketiga lainnya	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman – 2		**Kontainer Fisik**	
Lembar kerja ini akan membantu Anda memikirkan skenario yang dapat mempengaruhi aset informasi Anda pada wadah fisik tempat penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus Anda hadapi. Pertimbangkan setiap skenario dan lingkari respons yang tepat. Jika jawaban Anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak disengaja atau sengaja atau keduanya.			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario 2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa mengakses satu atau lebih wadah fisik, secara tidak sengaja atau sengaja, sehingga menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang diinginkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

Skenario Pertanyaan Ancaman -2 (lanjutan)					
Skenario 3: Dalam skenario ini, pertimbangkan situasi yang dapat mempengaruhi wadah fisik Anda dan, secara default, memengaruhi aset informasi Anda. Tentukan apakah salah satu dari hal berikut dapat terjadi, dan jika ya, tentukan apakah situasi ini akan menyebabkan satu atau lebih dari hasil berikut: • Pengungkapan aset inform asi Anda yang tidak disengaja • Modifikasi aset informasi Anda yang tidak disengaja Interupsi yang tidak disengaja dari ketersediaan aset informasi Anda • Penghancuran permanen yang tidak disengaja atau kehilangan sementara aset informasi Anda			**Kontainer Fisik**		
Masalah pihak ketiga lainnya terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)
Bencana alam atau buatan manusia (banjir, api, tornado, ledakan, atau angin topan) terjadi	Tidak	Ya (pengungkapan)	Ya (modifikasi)	Ya (interupsi)	Ya (rugi)

Kuesioner Skenario Ancaman - 3			**Orang-orang**
Skenario 1: Pikirkan orang-orang yang bekerja di organisasi Anda. Adakah situasi di mana seorang karyawan memiliki pengetahuan terperinci tentang aset informasi Anda dan dapat, secara tidak sengaja atau sengaja, menyebabkan aset informasi menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Diubah agar tidak digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Terganggu sehingga tidak bisa diakses untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksud?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)
Skenario2: Pikirkan orang-orang yang berada di luar organisasi Anda. Ini bisa mencakup orang-orang yang mungkin memiliki hubungan bisnis yang sah dengan organisasi Anda atau tidak. Adakah situasi di mana orang luar bisa, secara tidak sengaja atau sengaja, menyebabkan aset informasi Anda menjadi:			
Diungkapkan kepada individu yang tidak berwenang?	Tidak	Ya (secara tidak sengaja)	Ya (sengaja)

RIWAYAT HIDUP

Nama Afriani Rizkika. Saya lahir di Palembang, tepatnya pada tanggal 7 April 1995. Pendidikan dasar saya diselesaikan pada tahun 2007 di SD Negeri 189 Palembang. Pendidikan Menengah Peryama saya diselesaikan pada tahun 2010 di SMP Karya Ibu Palembang. Pada tahun 2013, saya menyelesaikan Sekolah Menengah Atas di MAN 2 Palembang. Pada tahun itu juga, saya melanjutkan kuliah pada program studi Sistem Informasi di Universitas Islam Negeri Raden Fatah Palembang yang saya selesaikan pada tahun 2018.