BAB II

LANDASAN TEORI

2.1 Risiko

Risiko adalah kejadian dihubungkan dengan kemungkinan terjadinya akibat buruk (kerugian) yang tidak diinginkan atau tidak terduga. Risiko mempunyai karakteristik :

a. Merupakan ketidakpastian atas terjadinya suatu peristiwa,

b. Merupakan ketidakpastian yang bila terjadi akan menimbulkan kerugian.

Berdasarkan definisi di atas dapat diambil kesimpulan bahwa risiko adalah suatu pontensi kejadian yang dapat merugikan yang disebabkan karena adanya ketidakpastian atas terjadinya suatu peristiwa, dimana ketidakpastian itu merupakan kondisi yang menyebabkan tumbuhnya risiko yang bersumber dari berbagai aktivitas (I W. Wedana Yasa1, 2013)

2.2 Mitigasi Risiko

Berdasarkan UU Nomor 24 Tahun 2007, mitigasi risiko merupakan serangkaian upaya yang digunakan untuk mengurangi risiko bencana baik itu melalui penyadaran dan peningkatan kemampuan dalam menghadapi ancaman atas bencana maupun melalui pembangunan fisik.

2.3 Manajemen Risiko

Manajemen risiko diartikan sebagai kegiatan praktis tentang identifikasi, penilaian, pengontrolan, dan peringanan risiko. Pelaksanaan manajemen risiko merupakan tahapan kegiatan organisasi dalam mengidentifikasi dan memandang

sumber risiko, kerentanan risiko secara menyeluruh dan terkontrol dengan dilaksanakan evaluasi proses secara berkesinambungan.

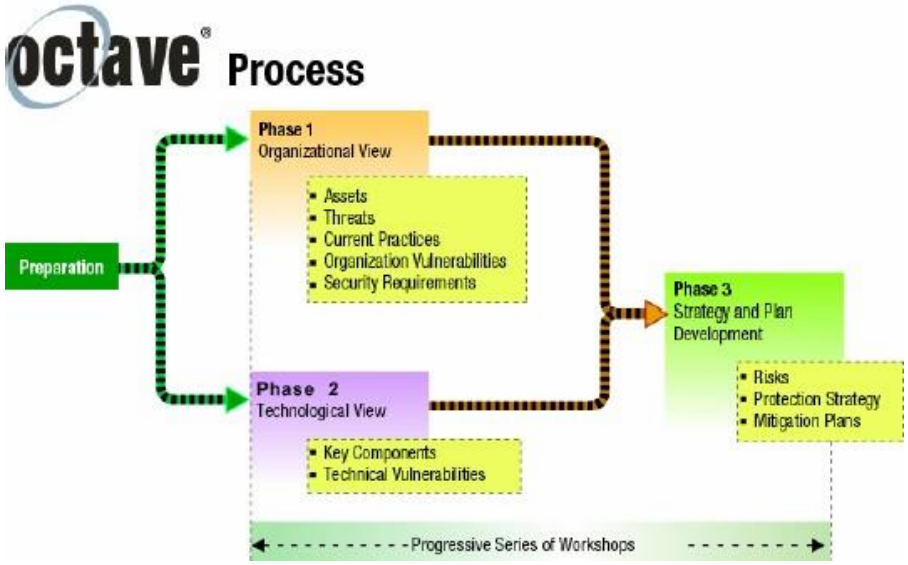
Manajemen risiko merupakan suatu proses yang memungkinkan pemimpin organisasi untuk dapat menyeimbangkan biaya operasional dan ekonomi yang dikeluarkan untuk mengurangi risiko dan mencapai keuntungan dengan melindungi sistem teknologi informasi dan data yang mendukung misi atau tujuan bisnis Menurut (Nugraha, 2016).

Risiko ada di mana-mana, bisa datang kapan saja, dan sulit dihindari. Jika risiko tersebut menimpa suatu organisasi, maka organisasi tersebut bisa mengalami kerugian yang signifikan. Dalam beberapa situasi, risiko tersebut bisa mengakibatkan kehancuran organisasi tersebut. Karena itu risiko penting untuk dikelola. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga kita bisa memperoleh hasil yang paling optimal. Dalam konteks organisasi, organisasi juga akan menghadapi banyak risiko. Jika organisasi tersebut tidak bisa mengelola risiko dengan baik, maka organisasi tersebut bisa mengalami kerugian yang signifikan. Karena itu risiko yang dihadapi oleh organisasi tersebut juga harus dikelola, agar organisasi bisa bertahan, atau barangkali mengoptimalkan risiko. Perusahaan sering kali secara sengaja mengambil risiko tertentu, karena melihat potensi keuntungan dibalik risiko tersebut. Manajemen risiko pada dasarnya dilakukan melalui proses-proses berikut ini.

1. Identifikasi risiko,
2. Evaluasi dan Pengukuran Risiko,
3. Pengelolaan risiko.

2.3.1 Metode Octave S

Menurut Alberts dkk (2005), OCTAVE-S adalah sebuah variasi dari pendekatan OCTAVE yang dikembangkan untuk menemukan kebutuhan-kebutuhan kecil, organisasi-organisasi yang tidak memiliki hirarki. Hal ini memerlukan sebuah analisis tim untuk menguji risiko keamanan di sebuah aset organisasi dalam hubungannya dengan objektif bisnis. Dengan mengimplementasi hasil-hasil dari OCTAVE-S, sebuah organisasi berusaha melindungi semua informasi dengan lebih baik dan meningkatkan keseluruhan bidang keamanan informasi



Gambar 2.1 Alur Octave-S

2.3.2 Fase, Proses dan Aktivitas Metode OCTAVE-S

Menurut Alberts, dkk (2005), OCTAVE-S berdasar pada 3 tahap yang dideskripsikan dalam kriteria OCTAVE, meskipun nomor dan urutan kegiatan berbeda dari metode OCTAVE yang digunakan. Bagian ini memberikan tinjuan

singkat atas tahapan, proses, dan kegiatan OCTAVE-S. Tahapan metode OCTAVE-S adalah sebagai berikut :

Tabel 2.1 Identifikasi Informasi Organisasi

<table>
<tr><td colspan="3">S.1 Proses Membangun asset berdsarkan profil ancaman</td></tr>
<tr><td>Aktifitas</td><td>Langkah</td><td>Deskripsi</td></tr>
<tr><td>S1.1 Membangun Dampak dari kriteria evaluasi</td><td>1.1</td><td>Menentukan ukuran kualitatif (tinggi,sedang, rendah) terhadap efek risiko yang akan dievaluasi dalam misi organisasi dan tujuan bisnis perusahaan.</td></tr>
<tr><td>S1.2 Mengidentifikasi asset organisasi</td><td>2.1</td><td>Mengidentifikasi informasi yang Terkait dengan aset dalam organisasi (informasi, sistem, aplikasi dan orang).</td></tr>
<tr><td rowspan="2">S1.3 Mengevaluasi praktek keamanan organissasi</td><td>3.1</td><td>Menentukan sejauh mana praktek yang di suvei digunakan oleh organisasi</td></tr>
<tr><td>3.2</td><td>Mengevaluasi setiap area praktek keamanan yang menggunakan survei dari angkah 3a, contoh dokumen rincinya:
• Apa yang saat ini organisasi lakukan dengan baik di area ini (praktek keamanan).
• Apa yang saat ini tidak dilakukan dengan baik oleh organisasi di area ini (kerentanan organisasi).</td></tr>
<tr><td></td><td>3.3</td><td>Setelah menyelesaikan langkah 3.1 dan 3.2, tentukan status stoplight (merah, kuning atau hijau) untuk setiap wilayah praktek keamanan. Status stoplightharus menunjukan seberapa baik kepercayaan terhadap kinerja organisasi di tiap area.</td></tr>
</table>

S.2 Proses Membuat profil Ancaman		
Aktivitas	Langkah	Deskripsi
S2 1 Memilih aset kritis	1.1	Meninjau ulang informasi yang Berhubungan dengan asset yang diidentifikasi pada langkah ke 2 dan pilih hingga 5 (lima) yang paling penting untuk dinas Perpustakaan dan kearsipan kota tasikmalaya
	1.2	Catat nama dari aset informasi aset kritis.
	1.3	Catat alasan dari setiap pemilihan asset kritis pada kertas kerja infomasi aset kritis
	1.4	Catat deskripsi dari seriap aset kritis pada kertas kerja informasi aset kritis. Pertimbangkan siapa yang menggunakan aset kritis seperti halnya yang bertanggung jawab untuk itu.
	1.5	Catat aset yang berhubungan dengan setiap aset kritis yang terdapat pada kertas kerja informasi aset kritis. Lihat kertas kerja indetifikasi aset untuk menentukan asset yang terkait dengan aset kritis.

S2.2 Identifikasi kebutuhan keamanan untuk asset kritis	2.1	Catat kebutuhan keamanan untuk setiap aset kritis yang terdapat pada kertas kerja informasi aset kritis
	2.2	Untuk setiap aset kritis catat kebutuhan keamanan yang paling penting yang terdapat pada kertas kerja infomasi asset kritis
S2.3 Identifikasi ancaman pada aset kritis	3.1	Melengkapi semua ancaman yang sesuai dengan aset kritis. Tandai setiap cabang dalam setiap asset

	3.2	Catat contoh spesifik dari pelaku ancaman dalam kertas kerja profil risiko yang berlaku untuk seriap kombinasi motif pelaku
	3.3	Catat kekuatan motif untuk setiap ancaman yang disengaja yang dikarenakan tindakan manusia. Jugamencatat bagaimana kepercayaan terhadap perkiraan kekuatan atas motif pelaku
	3.4	Catat seberapa sering setiap ancaman telah Terjadi di masalalu. Juga mencatat bagaimana keakuratan datayang di percaya.
	3.5	Catat area yang terkait dengan setiap sumber dari ancaman yang sesuai. Sebuah area yang mendefinisikan seberapa spesifik ancaman dapat mempengaruhi asset kritis.

Tabel 2.2 Mengidentifikasi Kerentanan Infrastruktur

Proses S3 Memeriksa Perhitungan Infrastruktur yang Berhubungan dengan asset kritis		
Aktivitas	Langkah	Deskripsi
S3.1 Memeriksa jalur aset	1.1	Pilih sistem yang menarik untuk setiap asset kritis (yakni sistem yang paling berkaitan dengan aset kritis).
	1.2	Tinjau ulang jalur yang digunakan oleh setiap aset kritis dan pilih kelas kunci dari komponen yang berkaitan dengan setiap aset kritis. Tentukan kelas komponen yangnmerupakan bagian dari sistem yang menarik.
	1.3	Menentukan kelas komponen yang bertindak sebagai akses poin lanjut (misalnya komponen yang digunakan untuk mengirimkan informasi dan aplikasi dari sistem yang menarik untuk orang)

	1.4	Menentukan kelas komponen baik internal dan eksternal untuk jaringan organisasi, digunakan oleh orang (misalnya pengguna,penyerang) untuk mengakses system
	1.5	Menentukan dimana informasi yang menarik dari sistem disimpan untuk tujuan back-up.
	1.6	Menentukan mana sistem akses informasi yang lain atau aplikasi dari sistem yang menarik dan kelas komponen mana yang dapat digunakan untuk mengakses informasi kritis atau layanan dari sistem yang menarik
S3.2 Menganalisa proses yang terkait dengan teknologi	2.1	Menentukan kelas komponen yang berhubungan dengan satu atau lebih aset kritis dan yang menyediakan akses kepada aset tersebut. Tandai setiap jalur untuk setiap kelas yang dipilih dalam langkah 18a sampai 18e. Tandai setiap bagian kelas atau contoh spesifik yang berhubungan jika diperlukan.
	2.2	Untuk setiap kelas komponen yang didokumentasi dalam langkah 19a, tandai aset kritis mana yang terkait dengan kelas ersebut.
	2.3	Untuk setiap kelas komponen yang di dokumentasikan dalam langkah 19a, tandai orang atau kelompok yang bertanggung jawab untuk memelihara dan melindungi kelas komponen tersebut.
	2.4	Untuk setiap kelas komponen yang didokumentasikan dalam langkah 2.1, tandai sejauh mana kelas tersebut dapat bertahan terhadap serangan jaringan. Juga catat bagaimana kesimpulan dibuat. Akhirnya, dokumen konteks tambahan berhubungan dengan analisis infrastuktur

Tabel 2.3 Mengembangkan Strategi Keamanan dan Perencanaan

Proses S.4 Identifikasi dan Analisis Risiko		
Aktivitas	Langkah	Deskripsi
S4.1 Mengevaluasi dampak ancaman	1.1	Menggunakan Kriteria evaluasi dampak sebagai panduan, memberi nilai dampak (tinggi, sedang, rendah) untuk setiap ancaman yang aktif bagi aset kritis.
S4.2 Membangun Kemungkinan kriteria evaluasi	2.1	Menentukan Ukuran kualitatif (tinggi, sedang, rendah) terhadap, kemungkinan terjadinya ancaman yang akan di evaluasi.
S4.3 Mengevaluasi Kemungkinan ancaman	3.1	Menggunakan kriteria evaluasi kemungkinan sebagai panduan, menetapkan nilai kemungkinan (tinggi, sedang, rendah) untuk setiap ancaman yangaktifterhadapaset kritis. Dokumenkan tingkat keyakinan dalam memperkirakan kemungkinan

Proses S.5 Mengembangkan Stratgi Perlindungan dan Rencana Mitigasi		
Aktivitas	Langkah	Deskripsi
S5.1 Menggambarkan Strategi perlindungan saat ini	1.1	Mengirim status *stoplight* untuk setiap area praktek keamanan yang sesuai dengan area kertas kerja strategi perlindungan. Untuk setiap area praktek keamanan identifikasikan pendekatan yang dilakukan oleh orga nisasi saat ini yang ditujukan terhadap area tersebut.
S5.2 Memilih pendekatan mitigasi	2.1	Mengirim status stoplight untuk setiap area praktek keamanan dari kertas kerja praktek keamanan ke "area praktek keamanan" (langkah 26) untuk setiap asset kritis dari kertas kerja profil risiko
	2.2	Memilih pendekatan mitigasi (mengurangi, menunda, menerima) untuk setiap risiko aktif. Untuk setiap risiko diputuskan untuk ditangani, lingkari satu atau lebih area praktek keamanan yang hendak dilakukan kegiatan mitigasi
S5.3 Mengembangkan rencana mitigasi risiko	3.1	Mengembangkan rencana mitigasi Untuk setiap area praktek keamanan yang dipilih pada langkah 27. Setelah langkah ini selesai, jika mengalami kesulitan untuk Mendapatkan aktivitas mitigasi yang potensial pada area praktek keamanan, tinjau ulang contoh aktivitas mitigasi dari area tersebut dipanduan aktivitas mitigasi.
S5.4 Identifikasi perubahan untuk strategi perlindungan	4.1	Menentukan apakah rencana mitigasi mempengaruhi strategi perlindungan organisasi. Catat setiap perubahan pada kertas kerja strategi perlindungan. Selanjutan, tinjau tindak ulang strategi perlindungan, diikuti dengan tujuan perubahan. Tentukan apakah ada niat untuk membuat perubahan tambahan pada strategi perlindungan. Catat setiap perubahan tambahan pada kertas kerja strategi perlindungan.
S5.5 Identifikasi langkah selanjutnya	5.1	Menentukan apa yang dibutuhkan organisasi

2.3.3 Metode ISO/IEC 27005

Standar ISO 27005 memberikan pedoman untuk Manajemen Risiko Keamanan Informasi dalam suatu organisasi, mendukung khususnya persyaratan Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan ISO/IEC 27001 dirancang untuk membantu pelaksanaan yang memuaskan dari keamanan informasi berdasarkan pendekatan manajemen risiko. Standar ini berlaku pada semua jenis organisasi (misalnya perusahaan komersial, instansi pemerintah, organisasi nonprofit) yang berniat untuk mengelola risiko yang dapat membahayakan keamanan informasi organisasi (ISO 27005, 2018). Proses MRKI menurut ISO 27005:2018 ditunjukkan pada gambar II.3 dibawah ini meliputi:

1. Penetapan konteks (Context establishment)
2. Penilaian risiko (Risk assessment):
    a. Identifikasi risiko (Risk identification)
    b. Analisis risiko (Risk analysis)
    c. Evaluasi risiko (Risk evaluation)
3. Penanganan risiko (Risk treatment)
4. Penerimaan risiko (Risk acceptance)
5. Komunikasi dan konsultasi risiko (Risk communication and consultation)
6. Pemantauan & kaji ulang risiko (Risk monitoring and review)

Manajemen risiko merupakan proses mengidentifikasi risiko, menilai risiko dan mengambil langkah-langkah untuk mengurangi risiko ke tingkat yang dapat diterima. Tujuan utama manajemen risiko adalah membantu organisasi mengelola risiko dengan misi terkait teknologi informasi dengan lebih baik (Stoneburner et

al., 2002). Sistem teknologi informasi berkaitan dengan masalah keamanan yang merupakan masalah teknis. Pimpinan sebagai manajer terkadang kesulitan dalam menangani masalah kemanan informasi yang tidak mendapatkan perhatian sehingga melihat masalah keamanan sebagai masalah manajemen risiko

2.4 Pemilihan Kerangka Kerja Manajemen Risiko TI

Kerangka kerja untuk manajemen risiko, seperti yang sudah dibahas pada sub-bab sebelutmya tadapat, OCTAVE-S dan ISO 27005 itu masing-masing metodologi dan cakupan nya mempunyai karakteristik yang berbeda. ISO adalah metodologi manajemen risiko yang cakupan nya lebih luas cakupannya perusahaan besar, perusahaan kecil dan pemerintahan, sedangkan untuk implementasi kontrol mengacu pada ISO 27002 karena memang masih dalam satu keluarga. OCTAVE-S ditujukan untuk organisasi kecil yang ingin mengevaluasi organisasinya sendiri oleh dirinya sendiri tidak melibatkan organisasi sasi lain atau poihak lain untuk menilai dan mengevaluasi.

Tabel 2.4 Perbandingan Metode

No	Perspektif	Octave-s	Iso 27005
1		Metode octave banyak di arahkan untuk mengevaluasi organisasi oleh dirinya sendiri, hanya sumberdaya organisasi tersebut saja yang di perbolehkan untuk melaksanakan proses. Artinya bahwa organisasi bertanggung	Cakupannya lebih luas, yakni mencakup SDM, proses bisnis dan teknologi dari organisasi tersebut dan umumnya di arahkan untuk manajemen puncak dan pemangku kepentingan

		jawab untuk menentukan strategi keamanan organisasi	
2	Tim penilai	Tim penilai terdiri dari perwakilan setiap lini bisnis dan departemen ti dari setiap organisasi	Menyebutkan siapa saja yang tepat baik orang teknis maupun non teknis yang terlibat dalam penilaian risiko
3	Teknik pengumpulan informasi	Menggunakan pendekatan dengan melakukan workshop untuk mendapatkan data dan informasi dan juga membuat keputusan	Mealakukan observasi proses bisnis yang ada dalam kebijakan organisasi
4	SDM	Menggunakan SDM sebagai asset jika memang SDN tersebut di golongkan Mission Critical sehubungan dengan masalah TI	Khusus meliputi keamanan sumber daya manusia yang meliputi karyawan, kontraktor dan juga pihak ketiga yang terlibat
5	Target Organisasi	Small Medium Enterprise	Pemerintah, perusahaan besar, small medium enterprise
6	Metodologi risiko	Bergantung kepada katalog sebagai baseline untuk organisasi, katalog tersebut adalah katalog praktek, profil ancaman dan katalog kerentanan	Semua kontrol keamanan dan klausal yang di terapkan dalam standar iso 27002. Setiap klausul berisi sejumlah katagori keamanan utama yang dapat disesuaikan dengan kebutuhan organisasi

Pemilihan metode yang akan di pergunakan adalah Octave-s karena cakupan nya lebih mengerucut di harapkan tidak akan melebar dan dapat di implementasikan langsung. ISO 27005 cakupan nya lebih luas, aset nya termasuk SDM, teknologi dan proses bisnis pentsahaan, dapat di terapkan pada perusahaan besar, pemerintahan dan juga SME, dan memberikan panduan perencanaan manajemen risiko yang secara khusus dan komprehensif dalam melakukan penilaian terkait keamanan infonnasi, juga sesuai dengan panduan penerapan tata kelola keamanan infonnasi. Karena setiap metode mempunyai ke unggulan masing-masing untuk melihat ke efektipan dan implementasi yang mungkin bisa di lakuakan di DIPUSIPDA maka ke dua metode tersebut akan di bandingkan.

2.5 Kajian Penelitian Sebelumnya

Adapun penelitian terkait dari penelitian yang akan dilakukan yaitu:

Tabel 2.5 Penelitian terkait

No	Peneliti	Judul Penelitian	Tahun
1	Kurniawan Eka Putra Mei 2017	Pengukuran Resiko Jaringan Komputer Menggunakan Technical Risk Assessment Pada SMK Muhamma 6bydiyah 2 Pekanbaru	2017
2	Raden Budiarto Juli 2017	Pengelolaan Manajemen Risiko Yang Berisikan Daftar Prioritas Analisis Risiko Yang Disertai Akar Sebab Permasalahan Dan Pengendalian Risiko Sesuai Dengan Standar ISO 27001	2017
3	Gunawan Setyadi, Yupie Kusumawati	Mitigasi Risiko Aset Dan Komponen Teknologi Informasi Berdasarkan Kerangka Kerja Octave Dan Fmea Pada Universitas Dian Nuswantoro	2015
4	Megawati, Mimi Kazmaini 2016	Analisa Manajemen Resiko Sistem Informasi Perpustakaan Menggunakan Cobit 4.1 Pada Domain	2016

5	Ucu Nugraha 28 Mei 2016	Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja Nist Sp 800-300	2016
6	Arif Nurochman 2014	Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus Di Perpustakaati Universitas Gadjah Mada Yogyakarta)	2014
7	Chris Winoto1, Lily Puspa Dewi2, Ibnu Gunawan3	Dentifikasi Risiko Pada Proyek Rfid Di Perpustakaan Perguruan Tinggi Swasta	2015
8	Rini Astuti 2018	Implementasi Manajemen Risiko Sistem Informasi Menggunakan Cobit 5	2018
9	Intan Oktaviani Manik Hapsara Emha Taufiq Luthfi 2014	Analisis Risiko Implementasi Ti Menggunakan Cobit 4.1 (Studi Kasus: Stmik Duta Bangsa Surakarta)	2014

Tabel 2.6 Penelitian yang mendekati

No	Peneliti	Domain Penelitian	Tahun
1	Deni Ahmad Jakaria Hendrik R. Teduh Dirgahayu 2013	Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave	2013
2	Anderes Gui Sanyoto Gondodiyoto Irvan Timotius 2008	Pengukuran Resiko Teknologi Informasi (Ti) Dengan Metode Octave-S	2008
3	Maryani 2014	Pengukuran Manajemen Risiko Teknologi Informasi Dengan Metode Octtave-S	2014
4	Balqis Lembah Mahersmi Feby Artowini Muqtadiroh Bekti Cahyo Hidayanto	Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode Octave Dan Kontrol Iso 27001 Pada Dishubkominfo Kabupaten Tulungagung	2016

5	Rosini Meutia Rachmaniah Badollahi Mustafa	Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro	2013
6	Bambang Supradono	Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, And Vulnerability Evaluation)	2009
7	Angga saputra Nur Widiyasono Alam Rahmatulloh	Implementasi Metode Octave-S Untuk Analisis Keamanan Risiko Informasi Pada Dinas Perpustakaan Dan Kearsipan Kota Tasikmalaya	2019

2.6 Matrik Penelitian Terkait

Adapun ruanglingkup penelitian terkait dari penelitian yang akan dilakukan yaitu:

Tabel 2.7 Matrik penelitian terkait

No	Judul Jurnal	Analisis			Ruanglingkup Penelitian								Penulis
		kualitatif	*Deskriptif*	*implementasi*	Risk Assessment	Iso 27001	Cobit 4.1	FMEA	Cobit 5	Nist Sp 800-300	OCTAVE-S	Octave	
1	Pengukuran Resiko Jaringan Komputer Menggunakan Technical Risk Assessment Pada SMK Muhammadiyah 2 Pekanbaru				✓								Kurniawan Eka Putra
2	Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode					✓		✓					Raden Budiarto

	Fmea Dan Iso 27001 Pada Organisasi Xyz												
3	Mitigasi Asset Yang Dan Mengkalsifikasikan Asset Penting Atau Sedang Di Universitas Dian Sastro		✓									✓	Gunawan Setyadi, Yupie Kusumawati
4	Analisa Manajemen Resiko Sistem Informasi Perpustakaan Menggunakan Cobit 4.1 Pada Domain						✓						Megawati, Mimi Kazmaini
5	Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja Nist Sp 800-300	✓								✓			Ucu Nugraha
6	Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus Di Perpustakaati Universitas Gadjah Mada Yogyakarta)	✓											Arif Nurochman

7	Dentifikasi Risiko Pada Proyek Rfid Di Perpustakaan Perguruan Tinggi Swasta	✓											Chris Winoto1, Lily Puspa Dewi2, Ibnu Gunawan3
8	Implementasi Manajemen Risiko Sistem Informasi Menggunakan Cobit 5			✓					✓				Rini Astuti
9	Analisis Risiko Implementasi Ti Menggunakan Cobit 4.1 (Studi Kasus: Stmik Duta Bangsa Surakarta)			✓			✓						Intan Oktaviani Manik Hapsara Emha Taufiq Luthfi

Tabel 2.8 Matrik penelitian mendekati

No	Judul Jurnal	Analisis			Ruanglingkup Penelitian								Penulis
		kualitatif	*Deskriptif*	*implementasi*	Risk Assessment	Iso 27001	Cobit 4.1	FMEA	Cobit 5	Nist Sp 800-300	OCTAVE-S	Octave	
1	Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave											✓	Kurniawan Eka Putra
2	Pengukuran Resiko Teknologi Informasi (Ti) Dengan Metode Octave-S										✓		Anderes Gui Sanyoto Gondodiyoto Irvan Timotius
3	Pengukuran Manajemen Risiko Teknologi Informasi Dengan Metode Octtave-S										✓		Maryani

4	Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode Octave Dan Kontrol Iso 27001 Pada Dishubkominfo Kabupaten Tulungagung					✓						✓	Megawati, Mimi Kazmaini
5	Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro											✓	Rosini Meutia Rachmaniah Badollahi Mustafa
6	Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, And Vulnerability Evaluation)											✓	Arif Nurochman
7	Implementasi Metode Octave-S Untuk Analisis Keamanan Risiko Informasi Inlislite Pada Dinas Perpustakaan Dan Kearsipan Kota Tasikmalaya			✓							✓		Angga Saputra