BAB II
TINJAUAN PUSTAKA

2.1 Kajian Pustaka

Kajian pustaka merupakan suatu penjelasan atau uraian berupa kajian literatur yang dijadikan acuan atau dasar pemikiran atau gagasan dalam penyelesaian masalah dalam sebuah penelitian. Kajian pustaka juga mendukung dalam proses pencarian teori.

Tabel 2. 1 Hasil Kajian Pustaka

No	Nama Peneliti	Judul	Hasil Penelitian
1	Stefan Agustinusa, Adi Nugrohob, Ariya Dwika Cahyono	Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS	Dari hasil penelitian yang telah dilakukan, ditemukan terdapat 26 kemungkinan risiko yang berada di sekitar dari aset-aset yang terkait dengan program HRMS. Dari ke-26 kemungkinan risiko tersebut diketahui jika 2 kemungkinan risiko memiliki level of risk dengan tingkatan high, 18 kemungkinan risiko yang memiliki level of risk dengan tingkatan medium, serta 6 kemungkinan risiko yang memiliki level of risk dengan tingkatan low. [2]
2	Andi Novia Rilyani, Yanuar Firdaus A W ST., MT, Dawam Dwi Jatmiko ST., MT	Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University)	Berdasarkan hasil penelitian tersebut database server down memiliki nilai risiko yang paling tinggi dan diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem i-Gracias membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik. [3]
3	Jakaria, Rini Fitriani, Joy Nashar Utamajaya	Evaluasi Manajemen Risiko Teknologi Informasi Berbasis ISO 31000:2018	Berdasarkan proses analisis risiko ISO 31000:2018, didapatkan 3 jenis variabel risiko, yaitu risiko dari alam atau lingkungan, risiko dari kesalahan

No	Nama Peneliti	Judul	Hasil Penelitian
			manusia, serta risiko dari sistem dan infrastruktur. Selanjutnya melakukan penilaian risiko dan menggunakan FMEA (failure Mode dan Efek). Analisis metode. ISO 31010:2009 menunjukkan bahwa dengan adanya RPN 100, Pareto 6%, dan kesalahan pada sistem dengan data yang rusak, nilai RPN tertinggi menghasilkan tingkat keparahan, insiden, dan tingkat deteksi kritis. RPN 72., Pareto 4% akan melakukan risk aversion (untuk menghindari terjadinya risiko). Diikuti oleh risiko lain dengan tingkat keparahan dan perlakuan risiko yang berbeda [4].
4	Joshua Ecleas, Augie David Manuputty	Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000	Dari penelitian tersebut didapatkan 19 kemungkinan risiko yang ada di sekitar asset yang terkait dengan sistem PEGA yang ada di PT. Asuransi Sinar Mas. Hasil tersebut kemudian dikelompokan menjadi 2 kategori level yang diidentifikasikan menggunakan matriks kemungkinan (likelihood) dan dampak (impact). Dari matrik tersebut didapatkan hasil kemungkinan risiko yang dikategorikan memiliki level risiko medium, yaitu: kebakaran, gempa bumi, server down, listrik padam, terputusnya koneksi jaringan, sistem error, bug pada sistem, error saat input data di sistem, kinerja sistem yang lambat, kurangnya pengetahuan tentang penggunaan aplikasi, kesalahan input data pada sistem, dan diketahui ada risiko yang dikategorikan dalam level risiko low yaitu : banjir, badai, petir, serangan virus, kerusakan pada hardware, sistem log out secara otomatis, kurang memahami alur kerja sistem, double input data di sistem. Dari hasil yang didapat dapat dilihat bahwa dalam mengatasi kemungkinan risiko yang ada

No	Nama Peneliti	Judul	Hasil Penelitian
			Perusahaan sudah menerapkan langkah untuk meminimalisir dampak dari kemungkinan risiko yang mungkin terjadi, namun untuk masalah sistem error dari pihak perusahaan dapat lebih memantau dan melakukan maintenance secara berkala pada sistem agar masalah sistem error dapat di minimalisir dan proses bisnis dapat berjalan dengan baik [5].
5	Reski Mai Candra, Yuli Novita Sari, Iwan Iskandar, Febi Yanto	Sistem Manajamen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018	Berdasarkan penelitian yang dilakukan didapatkan kesimpulan sebagai berikut : 1. Sistem manajamen risiko keamanan aset teknologi informasi telah berhasil dirancang dan dibangun sesuai proses penilaian manajemen risiko pada ISO 31000. 2. Setelah dilakukan penilaian di DISKOMINFOPS Kab. INHIL, teridentifikasi 45 risiko secara keseluruhan untuk aset, terdapat 14 risiko level rendah, 16 risiko level menengah, dan 15 risiko level tinggi. Maka DISKOMIFOPS Kab. INHIL dapat dikategorikan memerlukan perhatian khusus terutama untuk 15 risiko tinggi yang termasuk menjadi prioritas risiko didalamnya yaitu risiko koneksi jaringan putus yang sangat sering terjadi. 3. Berdasarkan pengujian UAT untuk sistem manajemen risiko keamanan aset teknologi informasi pada DISKOMINFOPS Kab. INHIL telah berjalan sesuai fungsinya dengan hasil UAT yaitu sangat bagus (82.11%) [6].

2.2 Teknologi Informasi

Definisi teknologi informasi secara umum adalah suatu studi perancangan, implementasi, pengembangan, dukungan atau manajemen sistem informasi berbasis komputer terutama pada aplikasi *hardware* atau perangkat keras dan *software* atau perangkat lunak komputer. Secara sederhana, pengertian dari teknologi informasi, yaitu sebuah fasilitas yang terdiri dari perangkat keras dan perangkat lunak yang mendukung dan meningkatkan kualitas informasi untuk setiap kalangan masyarakat secara cepat dan berkualitas [7].

2.3 Kategori Risiko Teknologi Informasi

Menurut Hughes, Dalam penggunaannya teknologi informasi berisiko terhadap kehilangan informasi dan pemulihannya antara lain :

1. Keamanan

   Risiko yang informasinya diubah atau digunakan oleh orang yang tidak berwenang. Sebagai contoh kejahatan komputer, kebocoran data, dan terorisme yang bersifat *cyber*.

2. Ketersediaan

   Risiko yang datanya tidak dapat diakses setelah kegagalan sistem, karena adanya kesalahan manusia (*human error*), perubahan konfigurasi, dan kurangnya pengurangan arsitektur.

3. Daya pulih

   Risiko dimana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup, setelah terjadinya kegagalan dalam perangkat lunak atau keras, ancaman eksternal, atau bencana alam.

4. Performa

   Risiko dimana informasi tidak tersedia saat diperlukan, yang diakibatkan oleh arsitektur terdistribusi, permintaan yang tinggi dan topografi informasi teknologi yang beragam.

.

5. Daya skala

   Risiko yang perkembangan bisnis, pengaturan *bottleneck*, dan bentuk arsitekturnya membuatnya tidak mungkin menangani banyak aplikasi baru dan biaya bisnis secara efektif.

6. Ketaatan

   Risiko yang manajemen atau penggunaan informasinya melanggar keperluan dari pihak pengatur. Yang dipersalahkan dalam hal ini mencakup aturan pemerintah, panduan pengaturan perusahaan dan kebijakan internal.

2.4 Sistem Informasi

Sistem informasi adalah sistem didalam suatu organisasi, yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi bersifat menejerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan.

2.5 Risiko

Risiko dapat diartikan sebagai peluang terjadinya hasil yang tidak diharapkan. Sehingga risiko hanya terkait dengan situasi yang memungkinkan munculnya hasil buruk serta berkaitan dengan kemampuan memperkirakan terjadinya.

Risiko merupakan sebuah hal yang melekat dan tidak pernah lepas dari segala aspek kehidupan serta hal yang dilakukan. Risiko adalah kejadian yang merupakan efek ketidakpastian. Risiko berkaitan dengan sesuatu hal yang negatif atau tidak menyenangkan yang dapat menimbulkan kerugian, tetapi dapat juga berkaitan dengan sesuatu yang positif [1]. Risiko yang harus ditanggulangi adalah risiko yang bersifat negatif karena dapat menjadi hambatan untuk mencapai sebuah sasaran atau tujuan dan dapat mengakibatkan kerugian [2].

Menurut Kamus Besar Bahasa Indonesia (KBBI), risiko adalah akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan [8].

Pengertian risiko menurut Soemarno adalah suatu kondisi yang timbul karena ketidakpastian dengan seluruh konsekuensi tidak menguntungkan yang mungkin terjadi disebut resiko. Sedangkan definisi risiko menurut Voughan, yaitu :

1. *Risk is the chance of loss*

   Risiko merupakan kesempatan terjadinya kerugian. *Chance of loss* berkaitan dengan sebuah *exposure* (keterbukaan) terhadap kemungkinan kerugian. Pada ilmu statistik, *chance* berguna untuk menunjukkan tingkat probabilitas terhadap situasi tertentu.

2. *Risk is the possibility of loss*

   Risiko adalah kemungkinan kerugian. Istilah *possibility* mengartikan bahwa probabilitas merupakan sebuah kejadian yang berada di antara nol dan satu. Tetapi, pengertian ini kurang tepat bila digunakan dalam analisis secara kuantitatif.

3. *Risk is uncertainly*

   Risiko adalah ketidakpastian. *Uncertainly* dapat bersifat subjektif ataupun objektif. *Subjective uncertainly* merupakan penilaian individu pada situasi risiko berdasarkan pengetahuan serta sikap individu yang bersangkutan. Sedangkan *objective uncertainly* memiliki dua definisi risiko sebagai berikut :

   a. *Risk is the dispersion of actual from expected results*

      Risiko adalah penyebaran hasil aktual dari hasil yang diharapkan. Ahli statistik mengemukakan risiko sebagai derajat penyimpangan sesuatu nilai di sekitar suatu posisi sentral atau di sekitar titik rata-rata.

   b. *Risk is the probability of any outcome different from the one expected*

      Risiko adalah probabilitas sesuatu keluaran berbeda dengan keluaran yang diharapkan. Menurut pengertian tersebut, risiko bukan probabilitas dari suatu kejadian tunggal, tetapi probabilitas dari beberapa keluaran yang berbeda dari yang diharapkan.

Risiko pada umumnya berkaitan dengan kemungkinan atau *probability* yang mengarah kepada kerugian terutama yang menimbulkan masalah. Jika kerugian lebih dahulu diketahui, kemungkinan dapat direncanakan terlebih dahulu cara

untuk mengatasinya. Risiko menjadi masalah penting jika kerugian yang ditimbulkannya tidak diketahui secara pasti [9].

2.6 Manajemen Risiko

Semua orang menyadari bahwa di dunia ini penuh dengan ketidakpastian. Ketidakpastian itu mengakibatkan risiko yang dapat merugikan. Ketidakpastian beserta risikonya toidak dapat diabaikan, tetapi dapat diminimalisirkan dengan manajemen risiko [10]. Implementasi manajemen risiko dirasakan semakin dibutuhkan, tidak hanya untuk memenuhi ketentuan, namun juga untuk kebutuhan dalam mengelola risiko yang dihadapi [11]. Manajemen risiko yang baik akan dapat meminimalisir kerugian yang akan dihadapi, sehingga bisa tetap menjaga kelangsungan kegiatan yang terjadi [12]. Menurut standar Australia Standard/New Zealand Standard (AS/NZS) 4360 manajemen risiko menyangkut budaya, proses dan struktur dalam mengelola suaturisiko secara efektif dan terencana dalam suatu sistem manajemen yang baik. Manajemen merupakan sebuah kegiatan yang terarah serta terkoordinasi yang terkait dengan pengelolaan sebuah risiko [13].

Manajemen risiko merupakan sebuah proses dalam mengidentifikasi risiko, mengukur risiko, serta membentuk sebuah strategi guna mengelolanya melalui sumber daya yang tersedia. Manajemen risiko berguna dalam mengelola risiko agar risiko tersebut dapat teratasi sehingga dapat memperoleh hasil yang optimal.

2.7 Manfaat Manajemen Risiko

Terdapat manfaat dalam manajemen risiko antara lain :

1. Keyakinan yang lebih besar atas pasokan yang tepat pada waktu yang tepat, untuk tujuan aktivitas spesifik lebih lanjut.
2. Pengendalian ketidakpastian yang lebih baik.
3. Mengurangi dampak risiko.
4. Meningkatkan pengambilan keputusan yang realistis.
5. Komunikasi yang lebih kuat.
6. Kemungkinan terkena risiko akan lebih rendah.

2.8 ISO 31000

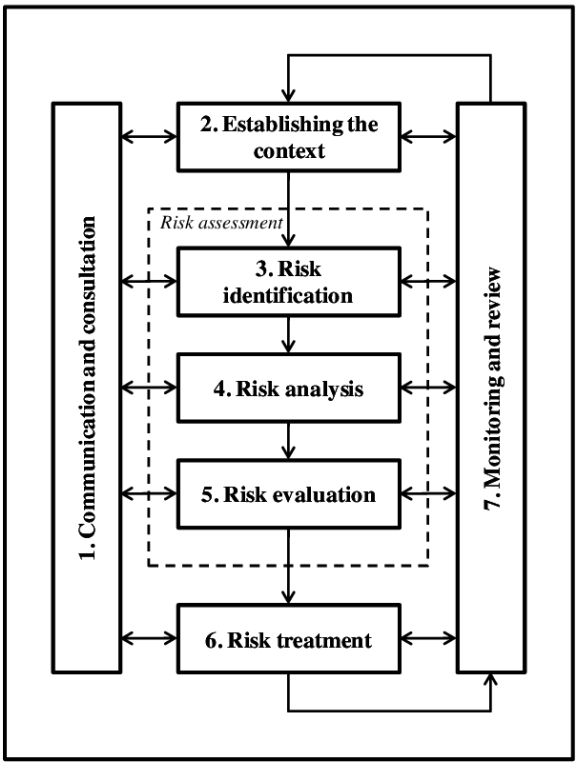
ISO 31000 merupakan sebuah standar internasional yang dibuat oleh ISO (*International Organization for Standardization*) untuk menangani manajemen risiko. ISO 31000 merupakan pengembangan dari standar AS/NZS 4360:2004 yang dikeluarkan oleh *Standards Australia*. ISO 31000 dikembangkan oleh komite teknis ISO bidang manajemen risiko, ISO/TC 262. Standar lain dalam portofolionya, yang mendukung ISO 31000, antara lain laporan teknis ISO/TR 31004, Manajemen Risiko - Panduan penerapan ISO 31000, dan Standar Internasional ISO/IEC 31010, Manajemen risiko-Teknik penilaian risiko, dikembangkan bersama dengan *International Electrotechnical Commission* ((ISO), 2018). ISO 31000 dapat digunakan oleh industri dan organisasi manapun dan pada seluruh level organisai tidak terbatas pada organisasi tertentu, karena menjelaskan apa yang dimaksud dengan risiko dan bagaimana penanganannya. ISO 31000 berisikan tentang prinsip-prinsip serta panduan untuk pengelolaan risiko organisasi. Penerapan ISO 31000 dapat membantu sebuah organisasi untuk memperbaiki dan mengidentifikasi peluang serta ancaman risiko yang mungkin terjadi [14].

Kelebihan ISO 31000 dibandingkan *framework* lain adalah ISO 31000 merupakan dasar penataan yang mencakup seluruh kegiatan manajemen risiko disemua tingkatan organisasi. ISO 31000 dapat membantu organisasi mengelola risiko secara efektif melalui penerapan proses manajemen risiko, memastikan informasi risiko yang lengkap dan memadai yang digunakan sebagai landasan untuk pengambilan keputusan dalam melakukan proses manajemen risiko [15].

ISO 31000 mensyaratkan bahwa penerapan manajemen risiko yang efektif haruslah mengikuti 11 prinsip sebagai berikut :

1. Pengelolaan risiko menciptakan dan melindungi nilai yang berkontribusi untuk pencapaian objektif dan perbaikan organisasi.
2. Manajemen risiko merupakan bagian yang terintegrasi dengan keseluruhan proses dalam organisasi dan menjadi bagian dari tanggung jawab manajemen.
3. Manajemen risiko merupakan bagian dari proses pengambilan keputusan melalui peranannya dalam memberikan pilihan kepada pengambil keputusan.

4. Manajemen risiko secara eksplisit memperhitungkan ketidakpastian dan sifat ketidakpastian itu, serta berusaha mengurangi ketidakpastian dalam setiap aktivitasnya dalam memastikan pencapaian objektif organisasi.
5. Manajemen risiko adalah suatu yang sistematis, terstruktur, dan tepat waktu agar dapat berkontribusi secara efisien dan secara konsisten menghasilkan sesuatu yang dapat diperbandingkan dan diandalkan.
6. Manajemen risiko berdasarkan ketersediaan informasi yang terbaik seperti data historis, pengalaman, umpan balik pemangku kepentingan, observasi, perkiraan ke depan dan pertimbangan para ahli.
7. Manajemen risiko memerlukan penyesuaian sesuai dengan konteks eksternal dan internal organisasi dan profil risiko organisasi.
8. Manajemen risiko memperhitungkan faktor manusia dan budayanya yang merupakan kemampuan, persepsi dan kemauan individu eksternal maupun internal dari suatu organisasi yang dapat mendukung pencapaian objektif.
9. Manajemen risiko adalah transparan dan inklusif melibatkan semua pemangku kepentingan terutama pengambil keputusan dalam menentukan kriteria risiko.
10. Manajemen risiko adalah dinamis, iteratif, dan responsif terhadap perubahan, eksternal dan internal.
11. Manajemen risiko memfasilitasi perbaikan berkelanjutan organisasi yang diukur dari tingkat kematangan manajemen risikonya [16].



Gambar 2. 1 Kerangka Kerja ISO 31000

2.8.1 *Communication and Consultation* (Komunikasi dan Konsultasi)

Komunikasi dan konsultasi merupakan hal yang penting dalam proses manajemen risiko karena menurut prinsip manajemen risiko dalam melakukan diharuskan transparan dan inklusif, dimana manajemen risiko harus dilakukan oleh seluruh bagian organisasi dan memperhitungkan kepentingan dari seluruh *stakeholders* organisasi [17]. Dengan adanya komunikasi dan konsultasi diharapkan dapat membangun dukungan yang memadai dalam kegiatan manajemen risiko dan membuat kegiatan manajemen risiko menjadi tepat sasaran.

2.8.2 *Establishing the Context* (Menentukan Konteks)

Menentukan konteks atau establishing the context bertujuan untuk mengidentifikasi dan mengungkapkan sasaran organisasi, lingkungan dimana sasaran hendak dicapai, *stakeholders* yang berkepentingan, dan keberagaman

kriteria risiko, dimana hal-hal ini akan membantu mengungkapkan dan menilai sifat dan kompleksitas dari risiko [18].

Terdapat empat konteks yang perlu ditentukan dalam penetapan konteks, yaitu :

1. Konteks internal

   Konteks internal memperhatikan sisi internal organisasi yaitu struktur organisasi, kultur dalam organisasi, dan hal-hal lain yang dapat mempengaruhi pencapaian sasaran organisasi.
2. Konteks eksternal

   Konteks eksternal mendefinisikan sisi eksternal organisasi yaitu pesaing, otoritas, perkembangan teknologi, dan hal lain yang dapat mempengaruhi pencapaian sasaran organisasi.
3. Konteks manajemen risiko

   Konteks manajemen risiko memperhatikan bagaimana manajemen risiko diberlakukan dan bagaimana hal tersebut akan diterapkan di masa yang akan datang.
4. Kriteria risiko

   Dalam pembentukan manajemen risiko, organisasi perlu mendefinisikan parameter yang disepakati bersama untuk digunakan sebagai kriteria risiko.

2.8.3 *Risk Identification* (Identifikasi Risiko)

Risk identification atau Identifikasi risiko merupakan proses dalam menemukan, mengenali, dan mencatat risiko. Dalam proses manajemen risiko, identifikasi risiko merupakan tahap yang dilakukan paling awal pada proses penilaian risiko. Tujuan dalam melakukan identifikasi risiko adalah untuk mengidentifikasi sebuah kejadian atau situasi yang memungkinkan terjadi yang dapat mempengaruhi pencapaian dari tujuan sebuah organisasi. Setelah melakukan identifikasi risiko, tahap selanjutnya yang dilakukan adalah mengidentifikasi pengendalian yang telah dilkukan terhadap risiko tersebut [19].

2.8.4 *Risk Analysis* (Analisis Risiko)

Analisis risiko adalah proses mengembangkan pemahaman terhadap suatu risiko. Analisis risiko memberikan masukkan untuk proses evaluasi risiko dan dalam mengambil keputusan apakah suatu risiko risiko perlu dikendalikan dan memilih strategi dan metode pengendalian yang tepat. Penilaian risiko digunakan untuk menghasilkan peringkat yang dipakai sebagai bahan pertimbangan untuk pengambilan keputusan prioritas risiko untuk melakukan pencegahan yang akan dilakukan [3]. Analisis risiko merupakan bagian dari tahap assessmen risiko dalam proses manajemen risiko dan dilakukan terhadap risiko-risiko yang telah diidentifikasi dalam proses identifikasi risiko.

Analisis risiko mencakup analisis terhadap penyebab dan sumber risiko, dampak positif atau negatif dari suatu risiko, dan kemungkinan suatu risiko dapat terjadi. Faktor-faktor yang mempengaruhi dampak dan kemungkinan kejadian risiko harus diidentifikasi. Efisiensi dan efektifitas pengendalian risiko yang telah diterapkan sebelumnya juga harus dipertimbangkan. Keterkaitan yang mungkin terjadi di antara risiko-risiko yang telah diidentifikasi juga perlu dipertimbangkan.

2.8.5 *Risk Evaluation* (Evaluasi Risiko)

Risk Evaluation atau evaluasi risiko merupakan proses melakukan evaluasi terhadap tingkat kegawatan masing-masing risiko menggunakan kriteria yang telah ditentukan. Tujuan evaluasi adalah untuk membantu dalam pengambilan keputusan. Hasil evaluasinya adalah daftar risiko yang memerlukan penanganan yang berada dalam *risk appetite* untuk diterima. Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut [20, 21]. Tahap evaluasi risikopun meliputi proses membandingkan hasil analisis dari masing-masing risiko terhadap kriteria risiko yang telah ditetapkan dan selanjutnya untuk menetapkan apakah suatu tindakan lebih lanjut diperlukan atau tidak [22].

2.8.6 *Risk Treatment* (Perlakuan Risiko)

Tahapan ini meliputi upaya untuk menyeleksi pilihan-pilihan yang dapat mengurangi atau bahkan meniadakan dampak serta kemungkinan terjadinya risiko kemudian menerapkan pilihan-pilihan tersebut. Pada dasarnya upaya perlakuan risiko dilakukan melalui pengurangan kemungkinan terjadinya risiko dan/atau mengurangi dampak risiko, bila risiko tersebut terjadi. Perlakuan terhadap risiko meliputi identifikasi opsi-opsi untuk memperlakukan risiko, menilai opsi tersebut, persiapan dan implementasi rencana perlakuannya.

Beberapa opsi tersebut antara lain:

1. Penerimaan Risiko (*Accept*)

   Menerima risiko adalah strategi menerima risiko dan terus menggunakan sistem dan teknologi informasi, sambil berusaha mengendalikan risiko yang ada dalam kisaran yang dapat diterima.

2. Menghindari Risiko (*Avoid*)

   Penghindaran risiko adalah strategi untuk mencegah terjadinya risiko dengan tidak melakukan aktivitas yang dianggap memiliki risiko yang tidak dapat diterima. Risiko juga dapat dihindari dengan menghilangkan sumber ancaman yang dapat menimbulkan risiko.

3. Berbagi Risiko (*Sharing/Transfer*)

   Pembagian risiko adalah strategi yang digunakan untuk mengalihkan risiko tertentu kepada individu, badan usaha, atau organisasi lain. Mentransfer risiko bukan berarti mengurangi tingkat keparahan risiko, tetapi hanya mengalihkannya ke pihak lain. Harus diakui bahwa dampak risiko pada akhirnya tetap pada pemangku kepentingan risiko utama (*principal risk owner*).

4. Mitigasi Risiko (*Mitigation*)

   Mitigasi risiko adalah perlakuan risiko yang dirancang untuk mengurangi risiko. Pengurangan risiko ini dapat berupa pengurangan kemungkinan terjadinya risiko dan pengurangan risiko.

Di tahap inipun, dilakukan pemberian saran mengenai perlakuan untuk semua kemungkinan risiko yang mungkin terjadi. Saran perlakuan diharapkan

dapat mengurangi atau dapat meminimaisir kemungkinan risiko yang terjadi. serta dapat juga digunakan sebagai bentuk pencegahan terhadap kemungkinan risiko yang ada [23].

2.8.7 *Monitoring and Review* (Pemantauan dan Riviu)

Tahap ini diperlukan untuk memastikan bahwa implementasi manajemen risiko telah berjalan sesuai dengan rencana yang diinginkan dan dilakukan. Hasil dari tahap ini juga dapat digunakan sebagai bahan pertimbangan untuk melakukan perbaikan terhadap proses manajemen risiko.