BAB II
TINJAUAN PUSTAKA

2.1. Kajian Induktif (Penelitian Terdahulu)

Penelitian tentang keamanan rantai pasok sebelumnya telah dilakukan oleh Park *et al.* (2016) yang menyoroti hubungan antar kecenderungan risiko, praktik keamanan rantai pasok, dan terjadinya gangguan sehingga dapat membantu perusahaan mengetahui apa yang diperlukan untuk mengatasi kerentanan perusahaan terhadap risiko rantai pasok dan kemudian mendapatkan keunggulan kompetitif dari para pesaingnya dengan persiapan yang lebih baik untuk menghadapi gangguan rantai pasok. Hasil dari penelitian tersebut adalah bahwa perusahaan-perusahaan yang menanggapi/mengelola risiko gangguan rantai pasok secara serius lebih mungkin untuk mematuhi inisiatif keamanan dan membangun persediaan pengaman serta dapat mengurangi frekuensi terjadinya gangguan rantai pasok.

Salmela *et al.* (2010) membahas alat manajemen risiko dan proses inovasi pabrik perusahaan seluler sebagai penggerak untuk peningkatan keamanan menggunakan solusi teknologi baru. Salmela et al. (2010) menyebutkan bahwa teknologi baru memberikan peluang untuk meningkatkan keamanan dan keselamatan pengiriman secara keseluruhan dengan manajemen risiko rantai pasokan yang proaktif dan pengenalan solusi keamanan yang kuat. Dengan menggunakan metode pengembangan konsep, alat manajemen risiko dan keahlian teknologi digabungkan ke proses kemudian menghasilkan solusi bisnis yang efektif untuk meningkatkan keamanan rantai pasokan.

Dalam penelitian yang dilakukan Scholliers *et al.* (2016) juga menggunakan teknologi untuk peningkatan keamanan. Teknologi dimanfaatkan untuk peningkatan keamanan kontainer di pelabuhan dan selama aktivitas rantai pasok. Solusi yang diberikan adalah menambahkan peralatan pemantauan, seperti segel elektronik dan alat pelacak, pemantauan lingkungan menggunakan kamera, serta proses gerbang yang ditingkatkan. Penggunaan optimal dari teknologi ini membutuhkan pertukaran informasi antar pemangku kepentingan.

Yang (2011) melakukan penelitian untuk mengevaluasi dampak faktor risiko dari *Container Security Initiative* (CSI) pada rantai pasok maritim di Taiwan

menggunakan matriks kerugian untuk mengidentifikasi tingkat keparahan dan frekuensi risiko keamanan, dan menggunakan diagram bowtie untuk menyelidiki manajemen risiko yang tepat dan strategi untuk menangani risiko keamanan maritim. Hasil dari penelitian tersebut terdiri atas: (1) kategori utama faktor risiko CSI adalah risiko operasional, risiko fisik, dan risiko keuangan; (2) terdapat dua risiko keamanan di level tinggi, sebagian besar risiko berada pada level menengah; strategi manajemen risiko yang diusulkan adalah pencegahan kerugian, pengurangan kerugian, penghindaran, dan transfer non-asuransi; dan (3) semua peraturan dan tindakan keamanan maritim harus mempertimbangkan keseimbangan antara biaya, waktu, keamanan, efisiensi, dan persaingan; jika gagal melakukannya maka dapat menyebabkan beban tambahan bagi penyedia layanan rantai pasokan maritim.

Liu *et al*. (2018) melakukan penelitian untuk menganalisis keamanan sistem rantai pasok SPBU di Cina. Sebanyak 50 kasus kecelakaan di SPBU di China dalam 20 tahun terakhir telah dikumpulkan dari situs web yang berbeda. Kemudian dengan metode FMEA dan bobot entropi digunakan untuk memproses data dan menganalisis seluruh sistem gas stasiun, dicari hasil yang jenis dan kegagalannya paling sering terjadi kecelakaan. Jenis dan penyebab kegagalan dari kecelakaan yang paling sering adalah ledakan statis yang disebabkan oleh listrik. Kemudian diajukan langkah-langkah efektif untuk meringankan dan menangani kecelakaan. Hasil penelitian ini akan membantu manajemen dan staf spbu dalam menangani masalah risiko keselamatan kerja di SPBU di Cina.

Pope (2008) melakukan penelitian tentang dimensi keamanan rantai pasok. Dalam penenlitiannya disebutkan bahwa keamanan rantai pasok memiliki empat dimensi yaitu keamanan produk atau layanan, keamanan arus informasi, keamanan arus uang, dan keamanan sistem logistik. Sedangkan Yang & Wei (2013) mengidentifikasi secara empiris dimensi-dimensi penting dari manajemen keamanan di sektor pengiriman peti kemas di Taiwan dan menilai dampaknya terhadap kinerja keamanan. Data untuk penelitian ini dikumpulkan dengan survei kuesioner. Analisis faktor eksplorasi dilakukan untuk mengidentifikasi dimensi penting manajemen keamanan di sektor pengiriman kontainer. Analisis regresi berganda kemudian dilakukan untuk menguji pengaruh manajemen keamanan pada kinerja keamanan. Penelitian Yang & Wei (2013) menghasilkan empat dimensi

manajemen keamanan yang penting untuk diidentifikasi: fasilitas dan manajemen kargo; pencegahan dan pemrosesan kecelakaan; manajemen informasi; dan manajemen hubungan mitra. Berdasarkan uji Analisis regresi berganda diperoleh bahwa manajemen informasi dan manajemen hubungan kemitraan memiliki efek positif yang signifikan terhadap kinerja keselamatan, sedangkan manajemen hubungan mitra memiliki efek positif yang signifikan terhadap kinerja bea cukai. Dengan begitu diperoleh implikasi praktis bahwa perusahaan pengiriman kontainer dapat meningkatkan keselamatan dan kinerja bea cukai dengan memfokuskan upaya manajemen keamanan pada fasilitas dan manajemen kargo, pencegahan dan pemrosesan kecelakaan, manajemen informasi, dan manajemen hubungan mitra. Penelitian tentang keamanan kargo juga dilakukan oleh Leong (2014) yang menyebutkan bahwa keamanan kargo sangat penting untuk membantu industri transportasi dalam memerangi peningkatan serius terhadap kejahatan kargo.

Lam & Dai (2015) melakukan penelitian untuk mengusulkan metodologi dengan metrik sistematis untuk mengembangkan desain keamanan penyedia jasa logistik (LSP) untuk memenuhi permintaan pelanggan. Penelitian ini menggunakan pendekatan ANP-QFD untuk menerjemahkan kebutuhan pelanggan untuk keamanan rantai pasok yang menjadi metrik sistematis untuk LSP untuk mengembangkan desain keamanan mereka. Hasil dari penelitian tersebut dalam pengembangan kinerja keamanan dapat menguntungkan LSP dalam hal meningkatkan efektivitas dan meningkatkan orientasi pelanggan dari upaya keamanan. Dengan ekstensi, perusahaan lain dapat meningkatkan desain keamanan mereka dengan merujuk pada studi kasus dan metode analitik terintegrasi. Fleksibilitas dari pendekatan ANP-QFD ini menawarkan kelonggaran bagi perusahaan untuk mengubah kebutuhan pelanggan dan kebutuhan desain berdasarkan keadaan mereka masing-masing.

Zailani *et al.* (2015) melakukan penelitian untuk mengeksplorasi hubungan antara praktik keamanan dan kinerja operasional keamanan sehubungan dengan budaya keamanan sebagai moderator. Penelitian ini menggunakan data survei untuk menguji proposisi yang berasal dari literatur keamanan dan analisis *partial least square*. Hasil mengungkapkan bahwa keamanan rantai pasok secara kolektif memengaruhi kinerja operasional keamanan perusahaan di antara penyedia layanan logistik Malaysia. Praktik keamanan rantai pasok berperan penting memberikan

layanan berkualitas tinggi dalam hal kinerja operasional keamanan rantai pasok di negara-negara berkembang. Selain itu, disebutkan bahwa budaya keamanan secara positif memoderasi hubungan antara manajemen fasilitas dan kinerja operasional keamanan perusahaan.

Niekerk *et al.* (2017) melakukan penelitian untuk mengeksplorasi orientasi keamanan rantai pasok perusahaan yang berpartisipasi dalam rantai pasok farmasi Afrika Selatan dengan tujuan mengidentifikasi risiko spesifik dan memahami persepsi keamanan rantai pasok, pendorong orientasi keamanan rantai pasok, dan moderator orientasi keamanan rantai pasok. Data dikumpulkan melalui wawancara semi-terstruktur. Hasil menunjukkan bahwa pembajakan, sindikat dan pencurian adalah risiko utama dalam rantai pasok farmasi Afrika Selatan. Kemitraan terkait keamanan dan cadangan proses bisnis adalah aspek yang paling diabaikan dari orientasi keamanan rantai pasok dalam rantai pasok farmasi. Mengenai orientasi keamanan rantai pasok, asuransi harus dianggap sebagai cara untuk pulih dari pelanggaran keamanan dan bukan hanya cara untuk memulihkan kerugian finansial. Penggerak utama orientasi keamanan rantai pasok diidentifikasi sebagai tata kelola perusahaan, kepatuhan terhadap peraturan dan regulasi, manfaat memperkenalkan proses manajemen risiko, dan terjadinya peristiwa risiko.

Gutta (2012) melakukan penelitian tentang pengukuran keamanan rantai pasok untuk menyelidiki persepsi manajer tentang ancaman dan regulasi keamanan rantai pasok, dan untuk menganalisis kegiatan perusahaan di bidang manajemen keamanan rantai pasok. Penelitian ini didasarkan pada survei yang dilakukan di antara 1.200 eksportir dan importir dari Jerman dan Polandia. Survei mengungkapkan kesadaran yang agak rendah tentang masalah keamanan dan tidak banyak perusahaan menerapkan langkah-langkah keamanan rantai pasok. Jika ada perusahaan yang melakukannya, hal ini biasanya ditentukan oleh pelanggan dan faktor industri. Sebagian besar perusahaan lebih memilih menggunakan tindakan reaktif, seperti membeli asuransi. Tidak banyak perusahaan yang tertarik dengan sertifikasi keamanan. Namun ada beberapa perbedaan dalam persepsi manajer Jerman dan Polandia. Penelitian ini menganalisis perbedaan-perbedaan ini dan mengusulkan beberapa langkah yang dapat diterapkan untuk melindungi rantai pasok.

Speier (2011) melakukan penelitian tentang desain rantai pasok global dengan mempertimbangkan risiko produk dan risiko keamanan. Speier (2011) menyebutkan bahwa gangguan rantai pasok dapat menimbulkan risiko yang semakin signifikan terhadap rantai pasok tersebut. Dalam penelitiannya dilakukan pengembangkan kerangka kerja untuk memeriksa ancaman gangguan potensial pada proses rantai pasok dan berfokus pada strategi mitigasi dan desain rantai pasok potensial yang dapat diimplementasikan untuk mengurangi risiko. Kerangka kerja dikembangkan dengan mengintegrasikan tiga perspektif teoretis teori kecelakaan normal, teori keandalan tinggi, dan pencegahan kejahatan situasional. Penelitian yang dilakukan menggunakan pendekatan multi-metode untuk mengidentifikasi inisiatif keselamatan dan keamanan utama (manajemen proses, berbagi informasi, dan mitra rantai pasok dan manajemen hubungan penyedia layanan) yang dapat diimplementasikan dan kondisi di mana masing-masing inisiatif paling sesuai. Hasil penelitian menunjukkan bahwa keseriusan dan sejauh mana inisiatif keamanan tergantung pada perhatian manajemen puncak, kompleksitas operasional, risiko produk, dan penggabungan.

Soeanu (2015) melakukan penelitian tentang analisis risiko transportasi. Dia berpendapat bahwa jaringan transportasi kompleks dan berpotensi rapuh karena cuaca, bencana alam, atau faktor risiko lainnya. Oleh karena itu, melakukan penilaian risiko transportasi merupakan kemampuan pendukung keputusan utama bersama dengan kemampuan untuk mengevaluasi opsi kontingensi untuk mitigasi risiko. Soeanu (2015) menyajikan pendekatan yang memanfaatkan model probabilistik memeriksa untuk menilai properti terkait risiko untuk tugas-tugas transportasi di hadapan kebijakan pilihan atas berbagai opsi rute yang tersedia dan berbagai tingkat ketidakpastian. Pendekatan yang diusulkan memungkinkan untuk mengevaluasi paparan risiko dan opsi kontingensi untuk mengurangi risiko transportasi.

Vikaliana (2017) melakukan penelitian tentang faktor-faktor risiko dalam perusahaan jasa pengiriman. Vikaliana (2017) menyatakan bahwa perlu dilakukan manajemen terhadap risiko yang seringkali muncul dalam jasa pengiriman barang. Langkah manajemen risiko yang dilakukan di antaranya adalah pengelolaan SDM persaingan bisnis jasa pengiriman barang, kesalahan pengiriman, kerusakan barang yang dikirim, pencurian atau kebakaran gudang. Dengan mengetahui berbagai

risiko yang biasanya dihadapi oleh perusahaan, maka penanganan risiko secara cepat dan tepat dapat meminimalisir risiko yang dihadapi perusahaan, sehingga tidak terlalu menghabiskan dana yang besar.

Jenlina (2013) melakukan penelitian tentang desain manajemen risiko rantai pasok, untuk mengidentifikasi risiko potensial yang ada pada *supply chain* perusahaan manufaktur di Sidoarjo. Hasil dari identifikasi risiko akan dievaluasi berdasarkan tingkat kemungkinan terjadinya risiko dan dampak dari risiko tersebut sehingga akan diketahui apakah risiko tersebut termasuk dalam kategori high risk, medium risk, atau low risk. Metode pengumpulan data adalah dengan wawancara, observasi, dan analisis dokumen. Dengan menerapkan pendekatan ERM, diperoleh hasil yaitu terdapat 2 risiko yang tergolong high risk, 8 risiko yang tergolong medium risk, dan 5 risiko yang tergolong low risk. Rekomendasi yang diberikan sebagian besar adalah untuk mengurangi tingkat kemungkinan terjadinya risiko ataupun dampak dari risiko tersebut. Melalui penerapan Enterprise Risk Management diharapkan pengelolaan terhadap risiko *supply chain* menjadi lebih efektif sehingga dapat mendukung pencapaian tujuan perusahaan.

Berdasarkan penelitian yang telah dilakukan sebelumnya yang berkaitan dengan manajemen risiko keamanan rantai pasok, cakupan kegiatan dalam analisis manajemen risiko rantai pasok seperti identifiaksi risiko, identifikasi penyebab risiko, penilaian risiko, dan penentuan strategi mitigasi risiko belum sepenuhnya lengkap dilakukan oleh setiap peneliti. Oleh karena itu, pada penelitian ini akan dilakukan manajemen risiko keamanan rantai pasok dengan cakupan kegiatan yang lengkap yaitu identifiaksi risiko serta penyebabnya, penilaian risiko, dan penentuan strategi mitigasi risiko pada perusahaan jasa logistik. Selain itu, juga dengan tambahan proses manajemen keamanan rantai pasok yang berdasarkan pada *security supplay chain* ISO 28001. Proses manajemen risiko keamanan rantai pasok dalam ISO 28001 ini dilakukan dengan melakukan penilaian tingkat kesesuaian keamanan terhadap ISO 28001, apabila kesesuaiannya belum tercapai maka harus dilakukan penilaian risiko. Dari penilaian risiko akan diketahui risiko level tinggi yang menjadi dasar untuk diberikan tindakan keamanan. Penilaian kesesuaiann menggunakan analisis gap dan penilaian risiko menggunakan FMEA. Dari penelitian ini diharapakan dapat membantu perusahaan mencapai kesesuaian terhadap *security supply chain* ISO 28001 dengan memberikan usulan strategi mitigasi risiko dan pengembangan rencana keamanan.

Tabel 2.1 Posisi Penelitian

No	Peneliti	Area Studi Kasus		Manajemen Risiko Rantai Pasok			Penyebab Risiko	Hubungan Keterkaitan	Metode/Pendekatan yang digunakan					Fokus Risiko/Fokus Penelitian
		Industri Manufaktur	Industri Jasa	Identifikasi Risiko	Penilaian Risiko	Strategi Mitigasi			FMEA	ANP	QFD	Causal Effect Diagram	Pendekatan Lain	
1	Park (2016)	√						√					SEM (*Structural Equation Model*)	Hubungan antar kecenderungan risiko, praktik keamanan rantai pasokan, dan terjadinya gangguan rantai pasok.
2	Pope (2008)	√	√										Literature review	Dimensi keamanan rantai pasok.
3	Scholliers (2016)												Pemodelan	Peningkatan keamanan kontainer di pelabuhan.
4	Salmela (2010)	√		√	√	√							- Metode MEF (Mobile Enterprise Factory) - LOGRM (Logistics Modelling for Risk Management) - SCSTM (Supply Chain Security and Technology Management)	Peningkatan keamanan rantai pasok.
5	Yang (2011)		√	√	√	√	√						- Analisis deskriptif statistik - Analisis Faktor - Loss exposure matrix	Risiko operasional, risiko fisik, dan risiko keuangan.

No	Peneliti	Area Studi Kasus		Manajemen Risiko Rantai Pasok			Penyebab Risiko	Hubungan Keterkaitan	Metode/Pendekatan yang digunakan					Fokus Risiko/Fokus Penelitian
		Industri Manufaktur	Industri Jasa	Identifikasi Risiko	Penilaian Risiko	Strategi Mitigasi			FMEA	ANP	QFD	Causal Effect Diagram	Pendekatan Lain	
6	Liu (2018)		√	√	√	√	√		√					Risiko kecelakaan kerja.
7	Leong (2014)		√	√									Analisis Statistik	Risiko kejahatan kargo (pencurian).
8	Yang & Wei (2013)		√					√					Analisis Faktor & analisis regresi	- Dimensi keamanan rantai pasok- Pengaruh manajemen keamanan terhadap kinerja keamanan.
9	Lam & Dai (2015)		√							√	√			Mengembangkan desain keamanan penyedia jasa logistik berdasarkan permintaan pelanggan.
10	Zailani (2015)		√					√					Analisis Partial Least Square	Pengaruh keamanan rantai pasok terhadap kinerja operasional keamanan perusahaan.
11	Niekerk (2017)	√		√									Thematic Analysis	Risiko pembajakan, sindikat dan pencurian.
12	Gutta (2012)		√										Analisis deskriptif statistik	Pengukuran keamanan rantai pasok untuk menyelidiki persepsi manajer tentang ancaman

No	Peneliti	Area Studi Kasus		Manajemen Risiko Rantai Pasok			Penyebab Risiko	Hubungan Keterkaitan	Metode/Pendekatan yang digunakan					Fokus Risiko/Fokus Penelitian
		Industri Manufaktur	Industri Jasa	Identifikasi Risiko	Penilaian Risiko	Strategi Mitigasi			FMEA	ANP	QFD	Causal Effect Diagram	Pendekatan Lain	
														dan regulasi keamanan rantai pasok.
13	Speier (2011)			√	√	√							Pendekatan multi-metode untuk mengidentifikasi inisiatif keselamatan dan keamanan utama.	Risiko produk dan risiko keamanan.
14	Soeanu (2015)		√	√	√	√							Model probabilistik: Continuous Stochastic Logic (CSL) & Probabilistic Computation Tree Logic (PCTL)	Risiko transportasi.
15	Vikaliana (2017)		√	√										Risiko pengelolaan SDM, persaingan bisnis, kesalahan pengiriman, kerusakan barang, pencurian, kebakaran gudang.
16	Jenlina (2013)	√		√	√	√							Pendekatan Enterprise Risk Management	Supply risk & demand risk.
17	Hanim (2019)		√	√	√	√	√		√			√	ISO 28001	Risiko Keamanan Rantai Pasok.

2.2. Kajian Deduktif (Tinjauan Pustaka)

2.2.1. Manajemen Risiko

Risiko didefinisikan sebagai suatu keadaan yang tidak pasti yang dihadapi oleh seseorang maupun perusahaan yang dapat menyebabkan kerugian (Kountur, 2004). Menurut Harwood *et al.* (1999), risiko adalah kemungkinan kejadian yang menimbulkan kerugian dimana terdapat berbagai kemungkinan suatu peristiwa seperti kemungkinan menghasilkan pendapatan tidak sesuai dengan yang diharapkan.

Risiko dapat terjadi pada pelayanan, kinerja, dan reputasi dari institusi yang bersangkutan. Risiko yang terjadi dapat disebabkan oleh berbagai faktor antara lain kejadian alam, operasional, manusia, politik, teknologi, pegawai, keuangan, hukum, dan manajemen dari organisasi (Vikaliana, 2017). Risiko berhubungan dengan ketidakpastian ini terjadi oleh karena kurang atau tidak tersedianya cukup informasi tentang apa yang akan terjadi. Sesuatu yang tidak pasti (*uncertain*) dapat berakibat menguntungkan atau merugikan. Ketidakpastian yang menimbulkan kemungkinan menguntungkan dikenal dengan istilah peluang (*Opportunity*, sedangkan ketidakpastian yang menimbulkan akibat yang merugikan dikenal dengan istilah risiko (*Risk*). Secara umum risiko dapat diartikan sebagai suatu hal atau suatu keadaan yang dihadapi seseorang atau perusahaan yang dapat mengakibatkan kerugian. Risiko dapat dikurangi dan bahkan dihilangkan melalui manajemen risiko. Peran dari manajemen risiko diharapkan dapat mengantisipasi lingkungan cepat berubah, mengembangkan *corporate governance*, mengoptimalkan penyusunan *strategic management*, mengamankan sumber daya dan asset yang dimiliki organisasi, dan mengurangi *reactive decision making* dari manajemen puncak.

Manajemen risiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman; suatu rangkaian aktivitas manusia. Manajemen resiko adalah rangkaian langkah-langkah yang membantu suatu perangkat lunak untuk memahami dan mengatur ketidakpastian (Roger S. Pressman, 2002 dalam Vikaliana, 2017). Manajemen risiko pada dasarnya dilakukan melalui proses-proses berikut ini:

Identifikasi risiko, Evaluasi dan pengukuran risiko, serta Pengelolaan risiko Identifikasi Risiko**,** Identifikasi risiko secara akurat dan komplit sangatlah vital dalam manajemen risiko (Roger S. Pressman dalam Hariastuti 2013). Salah satu aspek penting dalam identifikasi risiko adalah mendaftar risiko yang mungkin terjadi sebanyak mungkin. Evaluasi dan Pengukuran Risiko**,** Tujuan dari evaluasi risiko adalah untuk mengetahui karakteristik risiko yang lebih baik tentang risiko yang terjadi dapat memudahkan kita untuk mengelola risiko tersebut (Mallman, 1996 dalam Hariastuti 2013), Pengelolaan Risiko**,** Proses selanjutnya yaitu mengelola risiko. Jika organisasi gagal mengelola risiko, maka konsekuensi yang diterima bisa cukup serius, misalnya kerugian yang besar bahkan bisa bangkrut. Pengelolaan risiko bisa dilakukan dengan berbagai cara, seperti penghindaran, ditahan (retention), diversifikasi, atau ditransfer ke pihak lainnya (Crow, 2002 dalam Hariastuti 2013).

Dalam sistem manajemen keamanan, manajemen risiko digunakan untuk membantu perusahaan dalam membuat suatu rencana keamanan.

2.2.2. Manajemen Risiko Keamanan

Manajemen risiko keamanan merupakan proses identifikasi ancaman, kerentanan, dan dampaknya bagi perusahaan serta identifikasi penanggulangan risiko yang sesuai untuk mengurangi risiko sampai pada batas yang dapat diterima (Zaroni, 2017). Adapun metodologi manajemen keamanan adalah mencakup poin-poin berikut:

1. Mengidentifikasi setiap aktivitas yang berada di dalam sistem manajemen keamanan.
2. Mengidentifikasi pengendalian keamanan dan tindakan penanggulangan saat ini.
3. Mengidentifikasi skenario ancaman keamanan.
4. Menentukan dampak potensial jika skenario ancaman keamanan benar-benar terjadi.
5. Menentukan kemungkinan kejadian yang ditentukan oleh pengendalian keamanan dan tindakan penanggulangan saat ini.

6. Menilai apakah pengendalian keamanan dan tindakan penanggulangan sudah mencukupi.
7. Jika pengendalian keamanan dan tindakan penanggulangan yang ada saat ini belum mencukupi, maka dikembangkan dan diimplementasikan pengendalian keamanan dan penanggulangan tambahan (membuat rencana keamanan).
8. Mengulangi prosesnya.

Dalam mengatasi teknik kejahatan para kriminal yang semakin berevolusi, diperlukan langkah-langkah pencegahan di semua lintasan dalam rantai pasok. Adapun strategi mitigasi risiko keamanan rantai pasok dapat dilakukan dengan langkah-langkah sebagai berikut (Zaroni, 2017).

1. Meningkatkan keamanan rantai pasok

   Menyiapkan protokol keamanan untuk pergerakan kargo, meninjau geografi area yang dilewati, keamanan sistem informasi (*cyber-security*), pemenuhan regulasi-regulasi keamanan.
2. Manajemen kualitas

   Melakukan penilaian dan pemilihan pemasok, membuat perjanjian tertulis untuk *quality activities* serta pengawasan dan peninjauan pemasok secara berkala.
3. Manajemen jasa logistik dan transportasi

   Melakukan seleksi dan penilaian penyedia jasa, peninjauan pengamanan fisik seperti *physical barriers*, gerbang, kendali akses, penggunaan sistem alarm, *loading docks* serta penilaian pengendalian personel baik karyawan maupun pengunjung.
4. Membuat program keamanan spesifik

   Program pencegahan pencurian kargo, program anti teroris, program pencegahan penyelundupan, dan program anti pembajakan.

2.2.3. Manajemen Keamanan Rantai Pasok

Keamanan rantai pasok dapat digambarkan sebagai proses yang melibatkan penerapan program, prosedur, teknologi serta orang-orang untuk mencegah ancaman terhadap informasi. Keamanan juga meningkatkan perlindungan

keadaan ekonomi masyarakat, kesejahteraan sosial dan fisik manusia (Aiguokhian, 2013).

Closs dan Mc Garrell (2004) mendefinisikan keamanan rantai pasok sebagai penerapan kebijakan, prosedur, dan teknologi untuk melindungi aset rantai pasok (produk, fasilitas, peralatan, informasi, dan personel) dari pencurian, kerusakan, atau terorisme dan untuk mencegah masuknya barang selundupan yang tidak sah, orang atau senjata pemusnah massal (WMD) ke dalam rantai pasok.

Berdasarkan ISO 28000:2007 sistem manajemen keamanan untuk suatu rantai pasok meliputi aspek-aspek yang berkaitan dengan keamanan rantai pasok itu sendiri. Aspek-aspek tersebut mencakup finansial, manufaktur, sumberdaya, serta fasilitas dan aktivitas dalam sistem rantai pasok seperti penyimpanan, produksi dan perpindahan barang. Rantai pasok sendiri didefinisikan sebagai seperangkat sumberdaya dan proses-proses yang saling berhubungan, yang diawali dari pemanfaatan bahan mentah sampai pengantaran ke konsumen dengan berbagai tipe transportasi.

2.2.4. Elemen-Elemen Sistem Manajemen Keamanan Rantai Pasok

Di dalam sistem manajemen keamanan rantai pasok terdapat elemen-elemen kunci yaitu (Knight dan Patrice, 2003):

a. Analisis risiko

   Analisis risiko memberikan pondasi dan jastifikasi untuk mengimplementasikan kontrol keamanan yang tepat. Analisis risiko disini adalah manajemen risiko keamanan rantai pasok yang perlu dilakukan perusahaan.

b. Keamanan fisik

   Keamanan fisik meliputi pengukuran keamanan dengan memonitor dan mengontrol fasilitas eksterior dan interior perusahaan.

c. Kontrol akses

   Kontrol akses akan melarang orang tak berkepentingan mengakses fasilitas, kendaraan, kargo, area bongkar-muat barang.

d. Personil keamanan

   Personil yang ditugaskan untuk menjamin keamanan dengan tugasnya.

e. Pendidikan dan pelatihan kepekaan

   Meliputi pendidikan dan pelatihan yang dipberikan kepada personil untuk memahami dan melaksanakan kebijakan keamanan yang telah ditetapkan perusahaan. sehingga setiap personil dapat mengetahui apa yang diperbolehkan, dilarang, dianjurkan, dan apa yang harus dilakukan ketika terjadi insiden.

f. Prosedur Keamanan

   Prosedur yang mengatur aliran barang lintas fungsi dalam perusahaan dan menjamin keamanan suplai barang.

g. Keamanan informasi dan dokumentasi proses keamanan

   Dokuentasi proses keamanan untuk menjamin bahwa informasi dapat dibaca dan dilindungi dari kerusakan, kehilangan dan perubahan.

h. Pelaporan dan investigasi insiden keamanan

   Elemen ini digunakan untuk menjamin kapabilitas *tracking*, dan koordinasi informasi dilakukan secara tepat.

i. Keamanan rekan bisnis

   Elemen ini mengatur manajemen keamanan rantai suplai perusahaan terkait dengan dengan para pemasok dan pelanggannya.

j. Keamanan alat angkut/kendaraan

   Keamanan alat angkut/kendaraan menyediakan proteksi akan orang tak berkepentingan dan kargo asing masuk ke dalam aliran barang perusahaan.

k. Manajemen krisis dan pemulihan keamanan

   Hal ini mencakup perencanaan dan pembentukan proses untuk mempersiapkan, mengkoordinasikan, dan mengoperasikan perusahaan dalam keadaan krisis.

2.2.5. Ancaman Keamanan

Menurut ISO 28000:2007, ancaman keamanan meliputi:

a. Ancaman dan risiko kegagalan fisik, seperti kegagalan fungsional, kerusakan insidental, kerusakan parah atau ancaman teroris atau tindakan kriminal;

b. Ancaman dan risiko operasional, termasuk pengendalian keamanan, faktor manusia dan aktivitas lainnya yang mempengaruhi kinerja, kondisi atau keselamatan organisasi;
c. Kejadian alam (badai, banjir, dsb.) yang mungkin menyebabkan tidak efektifnya peralatan dan tindakan pengamanan;
d. Faktor diluar pengendalian organisasi, seperti kesalahan peralatan dan jasa yang dipasok dari luar;
e. Ancaman dan risiko terhadap pemangku kepentingan seperti kegagalan untuk memenuhi persyaratan perundangan atau rusaknya reputasi atau merk dagang;
f. Disain atau instalasi peralatan keamanan termasuk penggantian, pemeliharaan, dan lain-lain;
g. Manajemen informasi dan data serta komunikasi;
h. Ancaman terhadap kelangsungan operasional;

Dalam ISO 28001:2007, Proses identifikasi ancaman keamanan di setiap fasilitas, proses dan aktivitas dilakukan dengan mempertimbangkan kelangsungan hal-hal berikut:

a. Kontrol Akses
   - Pada lokasi perusahaan dalam rantai pasok dan lingkungan sekitar;
   - Pada alat transportasi (truk, kereta api, pesawat, tongkang, kapal, dan lain-lain.);
   - Pada informasi; dan lain-lain.
b. Alat transportasi (truk, kereta api, pesawat, tongkang, kapal, dan lain-lain.) yang digunakan untuk:
   - Operasi normal;
   - Aktivitas pemeliharaan;
   - Perubahan seperti *break downs*;
   - Perubahan/penggantian alat;
   - *Conveyance* saat tidak digunakan;
   - Penggunaan alat transportasi sebagai senjata; dan lain-lain.

c. Pengelolaan:
   - *Loading*;
   - *Manufacturing*;
   - Penyimpanan (termasuk tempat penyimpanan sementara);
   - Pemindahan;
   - *Unloading*;
   - Pengumpulan/penyebaran; dan lain-lain.

d. Transportasi barang melalui:
   - Udara;
   - Jalan raya;
   - Rel kereta;
   - Sungai;
   - Laut/samudera; dan lain-lain.

e. Deteksi/pencegahan terhadap penyusupan yang diterapkan pada pengapalan

f. Selama inspeksi, seperti inspeksi kendaraan

g. Karyawan
   - Tingkat kompetensi, pelatihan dan kepedulian;
   - Integritas; dan lain-lain.

h. Fungsi rekan bisnis

i. Komunikasi internal dan eksternal
   - Pertukaran informasi;
   - Situasi darurat; dan lain-lain.

j. Pengelolaan atau pemrosesan informasi mengenai kargo atau rute transportasi
   - Perlindungan data;
   - Asuransi data; dan lain-lain.

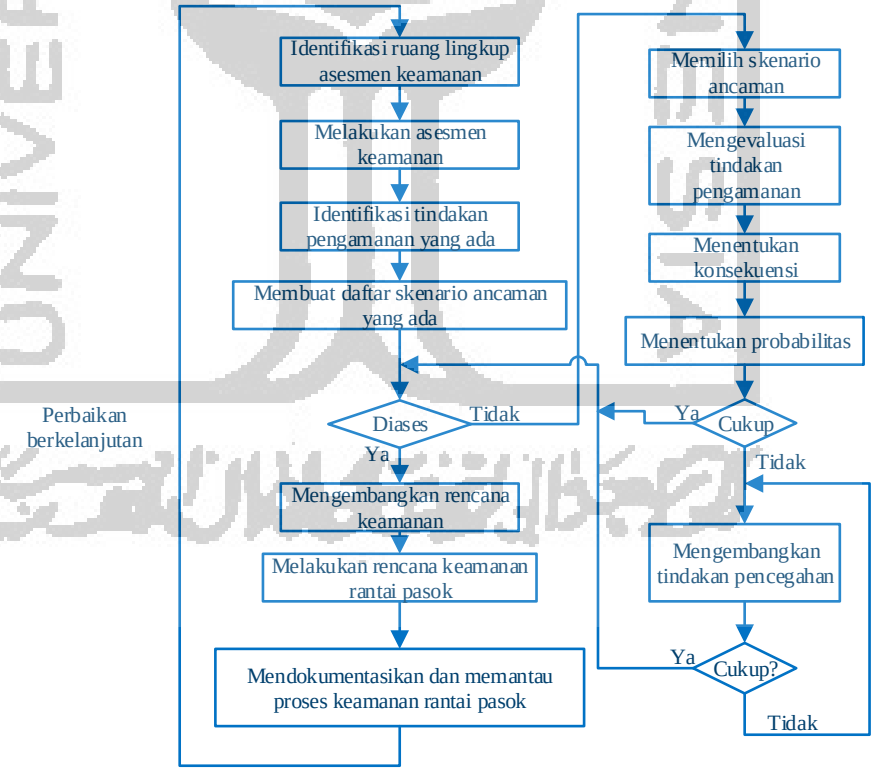
k. Informasi eksternal
   - Hukum;
   - Perintah dari yang berwenang;
   - Praktik industri;
   - Kecelakaan dan insiden;
   - Kapabilitas dan waktu respon pertama; dan lain-lain.

2.2.6. Proses Keamanan Rantai Pasok Berdasarkan ISO 28001

1. Umum

Organisasi dalam rantai pasok yang telah mengadopsi Standar Internasional ini diminta untuk mengelola keamanan di seluruh bagian rantai pasoknya dan memiliki sistem manajemen untuk mendukung pencapaian tujuan tersebut. Standar Internasional ini mensyaratkan praktik dan/atau proses keamanan untuk ditetapkan dan dilaksanakan dengan tujuan untuk mengurangi risiko rantai pasok internasional dari aktifitas-aktifitas yang dapat menyebabkan insiden keamanan.

Organisasi dalam rantai pasok yang menyatakan kesesuaian dengan Standar Internasional ini harus memiliki rencana keamanan berdasarkan hasil dari penilaian keamanan yang didokumentasikan dalam tindakan dan prosedur keamanan yang ada dan memasukkan tindakan pencegahan (*countermeasure*) jika dapat diterapkan untuk bagian rantai pasok internasional yang telah dicakup dalam pernyataan penerapannya.



Gambar 2.1. Diagram Alir Proses Keamanan Rantai Pasok

2. Identifikasi ruang lingkup penilaian keamanan

   Ruang lingkup penilaian keamanan harus mencakup seluruh aktifitas yang dilakukan oleh organisasi. Penilaian harus dilakukan secara berkala dan rencana keamanan harus direvisi secukupnya. Hasil penilaian harus didokumentasikan dan disimpan.

   Penilaian keamanan juga harus mencakup sistem informasi, dokumen dan jaringan informasi yang berkaitan dengan penanganan dan pergerakan barang saat masih berada dalam pengawasan organisasi. Pengaturan keamanan yang berlaku saat ini harus berdasarakn pada persetujuan yang diterima secara internasional dan mitra bisnis, dinilai di semua lokasi dan untuk mitra bisnis apabila terdapat kerentanan keamanan.

3. Pelaksanaan penilaian keamanan

   a. Personil penilaian

      Individu atau tim yang melakukan penilaian keamanan semuanya harus memiliki keterampilan dan pengetahuan termasuk hal-hal berikut:

      – Teknik penilaian risiko yang berlaku untuk semua aspek rantai pasok internasional mulai dari tempat di mana organisasi dalam rantai pasok mengawasi barang hingga di tempat dimana barang tidak berada dalam pengawasan organisasi atau keluar dari rantai pasok;

      – Melakukan tindakan yang dibutuhkan untuk mencegah pengungkapan yang tidak sah atau akses terhadap keamanan materi yang sensitif;

      – Operasional dan prosedur yang terkait dengan proses pabrikasi, penanganan, pemrosesan, pergerakan dan/atau dokumentasi barang secara memadai;

      – Tindakan pengamanan yang berkaitan dengan *consigmnet*, *conveyance*, personel, tempat, dan sistem informasi di bagian rantai pasok yang bersangkutan;

      – Pemahaman mengenai ancaman keamanan dan metodologi mitigasi;

– Memahami Standar Internasional ini.

Nama-nama individu atau anggota tim yang melakukan penilaian serta kualifikasi harus didokumentasikan.

b. Proses penilaian

Organisasi harus menetapkan, menerapkan dan memelihara prosedur untuk mengidentifikasi tindakan pencegahan yang ada untuk memitigasi ancaman keamanan. Organisasi harus membuat daftar mengenai skenario ancaman keamanan yang relevan, termasuk yang dianggap perlu oleh pemerintah terkait. Apabila pemerintah tidak ikut serta, hal ini harus didokumentasikan dalam penilaian keamanan.

Untuk setiap skenario ancaman keamanan, organisasi harus mengevaluasi tindakan pencegahan yang ada serta menentukan peluang kejadian dan konsekuensi yang relevan dengan masing-masing skenario ancaman keamanan dan mengevaluasi kebutuhan tindakan pencegahan tambahan untuk mengurangi risiko keamanan ke tingkat yang dapat diterima.

Organisasi harus mengkaji pernyataan keamanan yang diberikan oleh masing-masing mitra bisnis, menerapkan penilaian professional (*professional judgment*), pengetahuan tentang entitas dan/atau persyaratan yang ditetapkan pemerintah. Organisasi juga dapat memperoleh dan menggunakan informasi lain yang tersedia, dalam menentukan pernyataan penerimaan keamanan.

Organisasi harus mempertimbangkan detail dan validitas setiap pernyataan keamanan ketika melakukan penilaian keamanan dan menentukan seluruh kerentanan rantai pasok sebagaimana yang dijelaskan dalam pernyataan penerapannya.

Informasi berikut harus didokumentasikan:

a) semua skenario ancaman keamanan yang dipertimbangkan;

b) proses yang digunakan dalam mengevaluasi ancaman-ancaman tersebut; dan

c) semua tindakan pencegahan yang diidentifikasi dan diprioritaskan.

Tabel 2.2. Skenario Ancaman Keamanan Pada Rantai Pasok

No	Contoh skenario ancaman keamanan	Contoh Penerapan
1	Menyusup dan/atau mengambil alih pengendalian aset (termasuk *conveyance* dalam rantai pasok)	Merusak/menghancurkan aset.
		Merusak/menghancurkan target luar dengan menggunakan aset atau barang.
		Menyebabkan gangguan sipil atau ekonomi.
		Menyandera/membunuh orang.
2	Menggunakan rantai pasok sebagai sarana penyelundupan	Senjata illegal dibawa masuk atau keluar dari negara/ekonomi.
		Teroris masuk atau keluar negara/ekonomi.
3	Pengacauan (*tampering*) informasi	Mendapatkan akses di lokasi atau dari jauh terhadap sistem informasi/dokumen rantai pasok untuk tujuan mengganggu operasi atau memudahkan kegiatan ilegal.
4	Keutuhan kargo	Pengacauan, sabotase dan/atau pencurian untuk tujuan terorisme.
5	Penggunaan oleh orang yang tidak berwenang	Melakukan operasi dalam rantai pasok dengan tujuan memudahkan insiden teroris termasuk menggunakan sarana transportasi sebagai senjata.
6	Lain-lain	

(Sumber: ISO 28001 Lampiran A)

4. Pengembangan rencana keamanan rantai pasok

   Organisasi harus mengembangkan dan memelihara rencana keamanan pada seluruh bagian dari rantai pasok sebagaimana yang dijelaskan dalam pernyataan penerapannya. Rencana tersebut dapat dipisahkan ke dalam lampiran di mana setiap lampiran menjelaskan mengenai pengamanan yang diberlakukan pada segmen rantai pasok tertentu, termasuk tindakan keamanan organisasi mitra bisnis, akan dipelihara oleh mitra bisnis organisasi sesuai deklarasi keamanannya. Rencana/lampiran juga harus menetapkan bagaimana organisasi akan memantau atau mengkaji deklarasi keamanan tersebut secara berkala.

   Organisasi harus mengkaji dan mempertimbangkan penggunaan panduan yang informatif (dalam Lampiran A dan B) ketika mengembangkan rencana keamanannya.

5. Pelaksanaan rencana keamanan rantai pasok

   Organisasi harus menetapkan sistem manajemen yang memungkinkan proses keamanan rantai pasok yang spesifik untuk diterapkan.

6. Dokumentasi dan pemantauan terhadap proses keamanan rantai pasok

   a. Umum

      Organisasi harus menetapkan dan memelihara prosedur untuk mendokumentasikan, memantau, dan mengukur kinerja sistem manajemen yang diacu diatas. Organisasi harus melakukan audit

sistem manajemen pada interval waktu yang ditetapkan untuk memastikan bahwa sistem manajemen telah dilaksanakan dan dipelihara secara memadai. Hasil audit harus didokumentasikan dan disimpan.

b. Perbaikan berkelanjutan

Organisasi harus melakukan penilaian peluang untuk perbaikan pengaturan keamanannya sebagai sarana untuk meningkatkan keamanan rantai pasok.

7. Tindakan yang disyaratkan setelah terjadinya insiden keamanan

Organisasi harus melakukan kajian terhadap rencana keamanannya setelah terjadinya insiden keamanan yang berkaitan dengan setiap bagian dari rantai pasok internasional yang diawasi organisasi. Kajian tersebut harus:

a. Menentukan penyebab insiden dan tindakan korektif yang dibutuhkan;
b. Menentukan efektivitas tindakan dan prosedur untuk memulihkan keamanan; dan
c. Mempertimbangkan ketentuan tersebut, melakukan penilaian ulang terhadap rantai pasok sesuai ketetapan 5.3.2 (proses penilaian yang telah dijelaskan sebelumnya).

Apabila terjadi pelanggaran keamanan, organisasi harus mengikuti prosedur pelaporan ke Kepabeanan dan/atau lembaga penegak hukum terkait sebagaimana mestinya, sebagaimana ditetapkan dalam rencana keamanan dan kontrak.

Organisasi harus menyimpan data mengenai *consignment* dan data rantai pasok lainnya yang disyaratkan dalam batas waktu sebagaimana dijelaskan undang-undang dan peraturan perundangan yang berlaku.

8. Perlindungan informasi keamanan

Rencana keamanan, tindakan, proses, prosedur, dan rekaman mengenai organisasi harus dianggap sebagai informasi keamanan yang sifatnya sensitif dan harus dilindungi dari akses atau pengungkapan yang tidak sah. Informasi tersebut hanya boleh diungkapkan pada individu yang memiliki "hak untuk mengetahui". Selain petugas dari lembaga atau

wakil yang ditunjuknya, seorang individu dianggap "memiliki hak untuk mengetahui" jika:

a. Individu tersebut membutuhkan akses terhadap informasi keamanan sensitif tertentu untuk menjalankan aktifitas keamanan sebagaimana tercakup dalam rencana keamanan;
b. Individu tersebut sedang dalam pelatihan untuk menjalankan aktifitas yang tercakup dalam rencana keamanan;
c. Informasi dibutuhkan bagi individu yang bersangkutan untuk melakukan supervisi terhadap orang lain yang menjalankan aktifitas keamanan yang tercakup dalam rencana keamanan; atau
d. Individu yang bersangkutan atau yang bertindak atas nama suatu pihak, yang menurut hubungan kontraktual dengan organisasi telah diberikan akses terhadap informasi keamanan yang sensitif yang dikendalikan oleh organisasi sesuai dengan syarat dan aturan yang disepakati.

2.2.7. Gap Analysis

Gap analysis didefinisikan oleh IT *Infrastructure Library* (ITIL) sebagai aktivitas yang mengembangkan dua macam data dan mengidentifikasi perbedaannya. *Gap analysis* biasa digunakan untuk membandingan suatu set persyaratan. *Gap analysis* umumnya terstruktur pada satu set area, topik atau kategori, sehingga membuat *gap analysis* efisien untuk mengetahui *sector* atau bidang mana yang perlu diperbaiki (Picard et al., 2016). Adapun langkah-langkah dalam melakukan *gap analysis* menurut Picard (2016) adalah:

1. Penentuan *score*

   Penentuan *score* yang digunakan adalah skala pengukuran likert dari 1 – 5. Skala pengukuran merupakan kesepakatan yang digunakan sebagai acuan untuk menentukan Panjang pendeknya interval yang ada dalam alat ukur, sehingga alat ukur tersebut jika digunakan dalam pengukuran akan menhasilkan data kuantitatif. Dengan skala likert, maka variabel yang akan diukur dijabarkan menjadi indikator variabel. Kemudian indikator tersebut dijadikan sebagai titik tolak untuk menyusun item-

item instrumen yang dapat berupa pernyataan atau pertanyaan (Sugiyono, 2015). Adapun s*core* dan kriteria penilaian yang digunakan pada *gap analysis* ditunjukkan pada tabel 2.3.

Tabel 2.3. *Score Gap Analysis*

Score	Pengertian
1	- Sistem manajemen keamanan rantai pasok tidak ada - Dokumentasi tidak ada - Penerapan tidak ada
2	- Sistem manajemen keamanan rantai pasok ada - Dokumentasi tidak ada - Penerapan tidak ada
3	- Sistem manajemen keamanan rantai pasok ada - Dokumentasi ada tetapi tidak terorganisir dengan baik - Penerapan tidak dilakukan secara penuh di lapangan, (tidak konsisten, 40-60%)
4	- Sistem manajemen keamanan rantai pasok ada - Dokumentasi ada dan terorganisir dengan baik - Penerapan tidak dilakukan secara penuh di lapangan, (kurang konsisten, 61-80%)
5	- Sistem manajemen keamanan rantai pasok ada - Dokumentasi ada dan terorganisir dengan baik - Penerapan sudah sepenuhnya dilakukan di lapangan, (secara konsisten, 80-100%)

2. Penilaian *checklist*

   Penilaian *checklist* oleh responden berdasarkan kondisi organisasi saat ini. Responden yang dipilih adalah responden yang memiliki kompetensi cukup. Penilaian yang dilakukan berdasarkan ketentuan *scoring* yang dijelaskanpada tabel 2.3.

3. Penilaian gap

   Penilaian gap bertujuan untuk melihat seberapa besar gap yang ada pada perusahaan. Nilai persentase diperoleh dengan menjumlahkan *score* per

variabel dan membaginya dengan nilai maksimal pada *variable* tersebut. Semakin kecil gap yang ada maka semakin baik. Untuk mengukur kesesuaian, nilai persentase yang dihasilkan menunjukkan kesesuaian perusahaan dalam mengimplementasikan ISO 28001. Dalam tabel 2.4. ditunjukkan range dari nilai gap.

Tabel 2.4. ***Range Gap Analysis***

Persentase	Uraian
75% - 100%	Organisasi siap untuk melengkapi persyaratan ISO 28001 dan melakukan sertifikasi.
50% - 74%	Organisasi masih harus memperbaiki sistem manajemen keamanan rantai pasok untuk persiapan ISO 28001.
1% - 49%	Sistem manajemen keamanan rantai pasok organisasi sangat butuh perbaikan karena berbeda jauh dari sistem manajemen keamanan rantai pasok ISO 28001.

(Sumber: Fernando dkk, 2017)

2.2.8. FMEA (*Failure Mode and Effect Analysis*)

Metode FMEA merupakan sebuah metodologi yang digunakan untuk mengevaluasi kegagalan yang terjadi di dalam sebuah sistem, desain, proses, atau pelayanan. Identifikasi kegagalan potensial dilakukan dengan cara pemberian nilai atau skor masing-masing mode kegagalan berdasarkan atas tingkat kejadian (*occurrence*), tingkat keparahan (*severity*), dan tingkat deteksi (*detection*) (Stamatis, 1995). Menurut Gaspersz (2002), *Failure Mode and Effects Analysis* (FMEA) merupakan teknik analisa risiko secara sirkulatif yang digunakan untuk mengidentifikasi bagaimana suatu peralatan, fasilitas/sistem dapat gagal serta akibat yang dapat ditimbulkannya.

Failure Mode and Effect Analysis (FMEA) adalah salah satu metode manajemen risiko yang sistematis dan dapat digunakan untuk mengevaluasi dan mendokumentasikan penyebab serta efek dari kegagalan pada suatu proses (Dyadem Press, 2003). FMEA mampu mengidentifikasi dan mengevaluasi potensi kegagalan suatu produk atau proses dan efek yang

mungkin muncul, serta tindakan yang diperlukan untuk menghilangkan atau mengurangi potensi kegagalan yang mungkin terjadi (Chin et al, 2008).

Metode FMEA dilakukan untuk menganalisa potensi kesalahan/kegagalan dalam sistem dan potensi yang teridentifikasi akan diklasifikasikan menurut besarnya potensi kegagalan dan efeknya terhadap proses. Pada tahap ini dilakukan survei penilaian risiko (RPN) bertujuan untuk mengetahui risiko yang potensial atau tingkat risiko yang paling kritis dengan memperhatikan risiko yang memiliki probabilitas kejadian yang tinggi dan memiliki konsekuensi atau dampak negatif yang besar serta kesempatan untuk memperbaiki dengan mendeteksi modus kegagalan sebelum terjadi dampak yang merugikan. Nilai RPN didapatkan berdasarkan tingkat *probability*, *severity*, dan *detection* dari tiap kejadian variabel risiko yang relevan (Sinaga et al, 2014).

Novanto (2008) melakukan penilaian risiko menggunakan metode FMEA dengan perhitungan nilai RPN berdasarkan tingkat *probability*, *severity*, dan *frequency*. Penilaian terhadap *severity* penilaian yang berhubungan dengan seberapa besar dampak yang ditimbulkan dari risiko yang terjadi. Penilaian terhadap *probability* dilakukan untuk mengetahui seberapa besar kemungkinan terjadinya suatu risiko. Penilaian terhadap *frequency* dilakukan untuk mengetahui seberapa sering risiko itu terjadi. Berikut adalah tabel acuan penentuan nilai *probability*, *severity*, dan *frequency*.

Tabel 2.5. Klasifikasi Kemungkinan (*Probability*) Risiko

	Level	*Descriptor*	Keterangan
Kemungkinan	A	*Most likely*	Sangat mungkin terjadi.
	B	*Possible*	Memiliki kesempatan terjadi dan merupakan kejadian yang tidak biasa
	C	*Conceivable*	Dapat diperkirakan akan terjadi setelah beberapa tahun kemudian setelah kejadian sebelumnya
	D	*Remote*	Tidak diketahui kapan akan terjadi kembali setelah beberapa waktu yang lalu terjadi
	E	*Inconceivable*	Secara praktis tidak mungkin dan belum pernah terjadi

Sumber: Novanto, 2008

Tabel 2.6. Klasifikasi Dampak (*Severity*) Risiko

	Level	*Descriptor*	Keterangan
Dampak:	A	*Catastrophic*	Kerugian finansial yang fatal, kerusakan permanen pada kapabilitas, dan menghancurkan susunan komunitas sosial yang ada
	B	*Major*	Kerugian finansial yang sangat besar, merusak kapabilitas, berdampak besar pada komunitas sosial yang ada
	C	*Moderate*	Kerugian finansial yang besar, merusak sebagian kapabilitas, dan berdampak menengah pada komunitas sosial yang ada
	D	*Minor*	Kerugian finansial menengah, merusak sebagian kecil kapabilitas, dan berdampak kecil pada komunitas sosial yang ada
	E	*Insignificant*	Kerugian finansial yang kecil, tidak ada dampak pada kapabilitas dan komunitas sosial yang ada

Sumber: Novanto, 2008

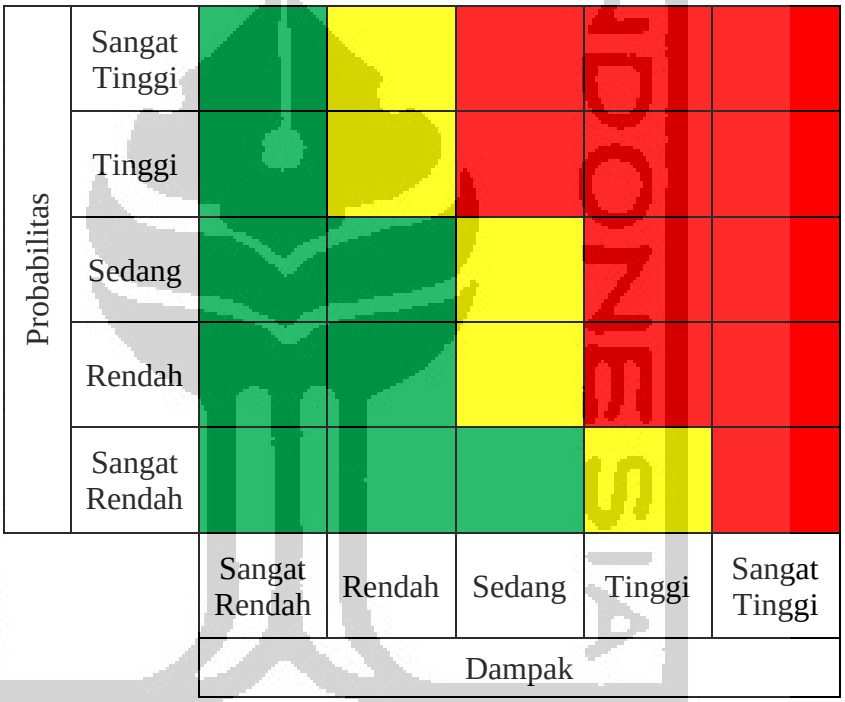
Tabel 2.7. Klasifikasi Frekuensi (*Frequency*) kejadian Risiko

	Level	*Descriptor*	Keterangan
Frekuensi Kejadian	A	*Continuously*	Tarjadi beberapa kali dalam sehari
	B	*Frequently*	1 kali/1 hari
	C	*Occasionally*	1 kali/1 minggu atau bulan
	D	*Infrequently*	1 kali/1 tahun
	E	*Rarely*	2 Tahun sekali atau lebih

Sumber: Novanto, 2008

Setelah diperoleh nilai RPN, kemudian akan ditentukan risiko mana yang akan menjadi prioritas utama untuk diberikan tindakan mitigasi. Menurut Hoseynabadi (2010) dalam Nanda (2014), *probability impact matrix* merupakan salah satu metode pendeteksi risiko pada suatu proses yang bertujuan untuk menentukan daerah prioritas risiko dengan mempertimbangkan nilai *severity* dan nilai *occurrence*. Dasar perhitungan *probability impact matrix* berbeda dengan perhitungan nilai RPN pada metode FMEA. Jika perhitungan RPN menggunakan tiga kriteria utama (*probability*, *severity*, dan *frequency*) untuk mengetahui tingkat risiko, sedangkan *probability impact matrix* hanya menggunakan dua kriteria utama untuk menentukan prioritas risiko, dua *item* utama tersebut yaitu nilai

probability dan *severity*. Dari hasil penilaian *severity* dan *occurrence*, maka dapat dibuat sebuah peta risiko yang dapat menunjukkan posisi masing-masing risiko, apakah risiko berada di level tinggi, sedang, atau rendah. Peta risiko terdiri atas 3 warna yaitu merah, kuning, dan hijau. Daerah warna merah merah merupakan risiko level tinggi (risiko kritis), daerah warna kuning merupakan risiko level sedang, dan daerah warna hijau merupakan risiko level rendah. Berdasarkan level tersebut, maka dapat diambil keputusan risiko mana yang menjadi prioritas utama untuk diberikan tindakan mitigasi.



Gambar 2.2. ***Probability Impact Matrix***