BAB IV

PENGUMPULAN DAN PENGOLAHAN DATA

4.1. Pengumpulan Data

4.1.1. Profil Perusahaan

Sejarah

Berawal dari sebuah proyek bisnis logistik di 2004, dan berkembang menjadi Strategic Business Unit di 2007, kemudian berdasarkan Akta Notaris yang disahkan oleh Menteri Hukum dan Hak Asasi Manusia dalam Surat Keputusan No: AHU-08351.AH.0101 pada 17 Februari 2012, Pos Logistik Indonesia resmi terlahir sebagai anak perusahaan dari PT Pos Indonesia (Persero).

Dengan posisi sebagai anak perusahaan dari perusahaan milik pemerintah, serta didukung dengan pekerja dan tim profesional dalam merumuskan strategi dan positioning bisnis, maka PT Pos Logistik Indonesia diharapkan dapat beroperasi secara independen untuk dapat memaksimalkan peluang bisnis logistik di Indonesia sekaligus memanfaatkan jaringan dari Pos Indonesia yang sudah terbangun di seluruh Indonesia, dengan 4.367 kantor cabang dan 33.000 titik penjualan.

Visi

Menjadi penyedia solusi logistik terpadu yang terpercaya, terluas, dan terkemuka di Indonesia.

Misi

- Memberikan solusi logistic yang efisien dan terintegrasi bagi pelanggan serta mendukung daya saing logistic nasional.
- Memberikan kontribusi laba yang maksimal dan membangun sinergi usaha dengan PT. POS Indonesia.
- Membangun kemitraan usaha dengan mitra kerja strategis yang saling menguntungkan.
- Terus berupaya mengembangkan kompetensi karyawan dan organisasi agar memiliki daya saing nasional.

Struktur Organisasi

Gambar 4.1. Struktur Organisasi PT. Pos Logistik Kantor Cabang Yogyakarta

Produk/Layanan PT. Pos Logistik Indonesia Kantor Cabang Yogyakarta

1. Layanan postal & KDR

   Layanan postal logistics memberikan solusi penerusan kiriman pos baik domestik maupun internasional. Layanan ini meliputi penerusan kiriman pos jalur primer dan sekunder, penyeberangan, pengelolaan proses distribusi (*indoor process*), kiriman khusus ritel, serta kargo ritel domestik.

2. Contract Logistics

   Poslog Kantor Cabang Yogyakarta memberikan layanan Contract Logistics berupa solusi transportasi dan distribusi. Dengan berbagai armada transportasi, pengiriman multi moda, dan berbagai jaringan, Poslog menyediakan solusi untuk proses distribusi konsumennya mulai dari pengelompokan area pengiriman, cross-docking, dan bahkan solusi logistic terbaik.

   Poslog sebagai partner logistic yang cukup besar untuk mengakomodasi freight apapun macamnya ke semua tempat melalui udara, laut, darat ataupun kereta api namun tetap mampu memberikan perhatian khusus dan personal yang dibutuhkan pelanggan. Poslog membantu para pelanggan dalam meningkatkan jaringan transportasi mereka secara konstan untuk memperoleh keuntungan yang kompetitif dengan menyediakan semua yang dibutuhkan supaya pengadaan produk mereka lebih cepat dan lebih efisien di pasar. Solusi transportasi Poslog mencakup layanan: *in-land trucking*, a*ir freight*, *sea freight*, dan multimoda.

3. Project Logistics

   Memberikan solusi untuk mengendalikan arus distribusi barang dengan mode transportasi multi Laut, Udara, dan Darat. Kami mengoperasikan logistik proyek dengan penanganan khusus dan kerangka waktu tertentu untuk mengontrol konsumsi waktu pada proses logistik agar efektif, efisien, dan informatif.

4.1.2. Proses Bisnis Perusahaan

Proses bisnis untuk masing-masing produk layanan yang terdapat di PT. Pos Logisik Indonesia Kantor Cabang Yogyakarta adalah berbeda-beda. Adapun proses bisnisnya adalah sebagai berikut:

1. Layanan Postal & KDR

   Layanan postal merupakan produk layanan PT. Pos Logistik yang dikhususkan untuk melayani PT. Pos Indonesia. Jadi PT. Pos Indonesia adalah customernya. Untuk layanan ini sudah terjadwal setiap harinya dan jadwalnya adalah dari PT. Pos Indonesia. Jadi setiap hari armada disiapkan untuk menuju Gudang PT. Pos Indonesia yang terdapat di jl. Monjali untuk mengambil barang kemudian berangkat untuk pengiriman ke masing-masing kota tujuan.

   Layanan cargo retail (KDR) merupakan produk layanan milik PT. Pos Logistik sendiri. Jadi yang menangani semua prosesnya adalah staf PT. Pos Logistik (dari barang datang, barang diperiksa, barang di-*packing* kembali, barang dimuat di alat transportasi, barang dibongkar, sampai barang diantar ke tujuan). Terdapat dua macam pelayanan dalam layanan cargo retail yaitu regular (jalur darat dan laut) dan ekspres (jalur udara). Adapun dokumen pengiriman yang digunakan adalah resi dan surat jalan.

   Pada layanan cargo retail, untuk pengiriman barang berbentuk cairan disediakan armada sendiri/khusus untuk barang itu saja tidak dicampur dengan barang lainnya dengan tujuan untuk menghindari kontaminasi terhadap barang yang lain.

   Proses penerimaan pengiriman pada layanan cargo retail

   Customer datang membawa barang → ke loket → barang diperiksa → kalau ok (lolos pemeriksaan) → barang diproses → repacking barang → barang dimuat → barang diangkut untuk dikirimkan ke tempat tujuan.

   Proses penolakan pengiriman pada layanan cargo retail

   Customer datang membawa barang → ke loket → barang diperiksa → kalau tidak ok (tidak lolos pemeriksaan) → barang dikembalikan kepada customer

2. Contract logistics

   Layanan contract logistic merupakan produk layanan milik PT. Pos Logistik sendiri yang aktivitasnya adalah menyediakan jasa logistic. Customer dari produk layanan ini adalah PT. Sandang Lea Mashindo, PT. Market Tama, PT. Orang Tua, PT. Otezen, dan PT. Bina Para Nusantara.

   Moda transprotasi yang digunakan pada layanan ini adalah FUSO, Tronton, dan CDD. Moda transportasi yang digunakan ada yang milik sendiri ada juga yang menggunakan mitra. Untuk menjaga kualitas armada, PT. Pos Logistik mempunyai kriteria untuk armada yang digunakan yaitu bersih, tidak bocor, kering, dan tertutup. Adapun proses bisnis untuk layanan contract logistic adalah sebagai berikut:

   - PIC perusahaan (pelanggan) mengajukan PO lewat email H-2 sebelum tgl pengiriman (dalam email terdapat penjelasan tentang tonase barang yang akan diangkut, hal ini sebagai acuan PT. Poslog dalam menentukan armada yang dibutuhkan).
   - PIC CL PT. Poslog meng-*arrange* armada yang dibutuhkan.
   - Armada berangkat ke perusahaan (pelanggan) untuk mengambil barang.
   - Armada berangkat mengirimkan barang ke perusahaan tujuan (dokumen yang dibawa adalah surat jalan dan PO).
   - Armada sampai di perusahaan tujuan, surat jalan mendapatkan tanda tangan dari pihak perusahaan penerima barang (perusahaan diusahakan sampai perusahaan sebelum jam 4 agar barang dapat langsung dibongkar pada hari itu juga).
   - Armada pulang kembali.
   - Surat jalan yang telah mendapatkan tanda tangan dari perusahaan penerima akan dijadikan sebagai bukti penagihan ke perusahaan pelanggan.

3. Project Logistics

   Produk layanan Project Logistic mempunyai proses yang berbeda-beda berdasarkan pada masing-masing proyek. Project logistic sendiri biasanya diperoleh dengan mengikuti lelang atau dengan penunjukan langsung. Penunjukan langsung ini untuk proyek dengan nilai dibawah 200juta. Sedangkan untuk lelang biasanya dengan mendapatkan informasi lelang dari LSPE. Apabila

dalam proses lelang PT. Pos Logistik menang, maka akan menjalankan proyek tersebut. Moda transportasi yang digunakan dalam kegiatan project logistic adalah menggunakan vendor. Moda transportasi tersebut berupa CDD dan FUSO.

Contoh proyek yang telah selesai ditangani adalah distribusi kotak surat suara. Untuk kotak surat suara (wilayah Sleman dan Bantul): mengambil barang di gudang kemudian dikirimkan sampai ke tempat tujuan kemudian mengambil lagi (setelah selesai pemungutan suara) dari masing-masing tempat pemungutan suara untuk dikembalikan lagi ke gudang.

4.1.3. Daftar Kajian Kinerja Keamanan Perusahaan

Daftar kajian kinerja keamanan perusahaan digunakan untuk mengukur tingkat kesesuaian keamanan perusahaan terhadap sistem manajemen keamanan rantai pasok ISO 28001. Dalam pengisian daftar kajian kinerja digunakan skala likert 1-5 untuk masing-masing poin dari masing-masing faktor. Kriteria penilaian yang digunakan untuk mengisi daftar kajian kinerja keamanan adalah berdasarkan pada tabel 2.3. Responden yang melakukan pengisian daftar kajian kinerja adalah manager dan PIC masing-masing produk layanan PT. Pos Logistik Indonesia Kantor Cabang Yogyakarta. Pemilihan responden tersebut karena responden dianggap telah mengetahui dan memahami proses bisnis dan kegiatan operasional perusahaan dengan baik, selain itu juga terlibat langsung dalam kegiatan di perusahaan. Data rata-rata skor untuk daftar kajian kinerja perusahaan ditunjukkan pada tabel 4.1.

Tabel 4.1. Data Daftar Kajian Kinerja Keamanan untuk Penilaian Kesesuaian Perusahaan terhadap Security Supply Chain ISO 28001

No	Faktor	Skor Rata-Rata
1	**Manajemen Keamanan Rantai Pasok**	
	Apakah organisasi memiliki sistem manajemen yang menangani keamanan rantai pasok?	4.75
	Apakah organisasi memiliki individu yang ditunjuk sebagai penanggung jawab atas keamanan rantai pasok?	4.5
2	**Rencana Keamanan**	
	Apakah organisasi memiliki rencana keamanan terbaru?	4.25
	Apakah rencana tersebut menjelaskan harapan keamanan organisasi mitra bisnis di hulu dan hilir?	4

No	Faktor	Skor Rata-Rata
	Apakah organisasi memiliki rencana manajemen krisis, rencana kelanjutan bisnis, dan rencana pemulihan keamanan?	4.25
3	**Keamanan Aset**	
	Apakah organisasi memiliki perangkat untuk menangani:	4.5
	- keamanan fisik bangunan	
	- Pemantauan dan pengendalian perimeter eksterior dan interior,	
	- Penerapan pengendalian akses yang tidak sah orang yang tidak berwenang memasuki fasilitas, *conveyance*, dermaga muat dan area kargo, dan pengendalian managerial untuk penerbitan identifikasi (karyawan, pengunjung, vendor, dsb) dan akses lainnya?	
	Apakah ada teknologi keamanan operasional yang bisa meningkatkan perlindungan aset secara signifikan? Sebagai contoh, deteksi terhadap adanya gangguan, atau kamera rekam CCTV/DVS yang mencakup area yang penting dalam aktifitas rantai pasok, dengan rekaman disimpan untuk periode waktu yang cukup lama untuk digunakan dalam investigasi insiden.	4
	Apakah ada prosedur yang diterapkan untuk bisa menghubungi personal keamanan internal atau pihak penegak hukum eksternal jika terjadi pelanggaran keamanan?	4.5
	Apakah ada protokol yang diterapkan untuk melarang, mendeteksi, dan melaporkan akses oleh orang yang tidak berwenang untuk semua area kargo dan area penyimpanan barang kiriman?	4.25
	Apakah individu yang menerima atau mengirim kargo sudah diidentifikasi sebelum kargo diterima atau dikeluarkan?	4.5
4	**Keamanan Personel**	
	Apakah organisasi memiliki prosedur untuk mengevaluasi integritas karyawan sebelum mengkaryakannya dan dievaluasi secara periodik dalam melakukan tugas-tugas keamanannya?	4.5
	Apakah organisasi melakukan pelatihan pekerjaan secara khusus untuk membantu karyawan menjelaskan tugas keamanannya, sebagai contoh: menjaga keutuhan kargo, mengenali potensi ancaman internal yang mengancam keamanan internal dan melindungi akses yang diawasi?	4.5
	Apakah organisasi membuat karyawan peduli terhadap prosedur perusahaan untuk melaporkan insiden yang mencurigakan?	4.5
	Apakah sistem pengendalian akses memuat pemusnahan dengan segera identifikasi dan akses bagi karyawan yang diberhentikan perusahaan ke area yang sensitif dan sistem informasi?	4.5
5	**Keamanan Informasi**	
	Apakah prosedur diberlakukan untuk memastikan bahwa semua informasi yang digunakan untuk pemrosesan kargo, baik elektronik maupun manual, sudah jelas, tepat waktu, akurat, dan terlindungi dari risiko diubah, hilang, atau memuat data yang salah?	4.75
	Apakah organisasi yang mengirimkan atau menerima kargo sudah mencocokkan kargo dengan dokumen pengiriman yang sesuai?	4.5

No	Faktor	Skor Rata-Rata
	Apakah organisasi memastikan bahwa informasi kargo yang diterima dari mitra bisnis dilaporkan secara akurat dan diterima tepat waktu?	4.5
	Apakah data relevan dilindungi dalam sistem penyimpanan yang tidak terkait operasional sistem penanganan data utama (apakah ada proses back up data yang diterapkan)?	4
	Apakah semua pengguna (user) memiliki ID pengguna untuk penggunaan pribadi, untuk memastikan bahwa kegiatannya dapat terlacak?	4.25
	Apakah ada sistem pengelolaan *password* yang efektif yang diberlakukan untuk memeriksa otentitas *user* dan apakah *user* diminta untuk mengubah *password*-nya minimal setiap tahun?	4
	Apakah ada perlindungan terhadap akses yang tidak sah (*unauthorized access*) dan penyalahgunaan informasi?	4.25
6	**Keamanan Barang dan *Conveyance***	
	Apakah prosedur diberlakukan untuk membatasi, mendeteksi, dan melaporkan akses yang tidak sah untuk memasuki semua area pengiriman, area dermaga muat dan unit penyimpanan transportasi kargo tertutup?	4.5
	Apakah ada individu berkualifikasi yang ditunjuk untuk mensupervisi kegiatan kargo?	4.5
	Apakah prosedur diberlakukan untuk memberitahu pihak penegakan hukum dalam kasus kondisi yang tidak normal atau ada kegiatan ilegal yang dideteksi atau dicurigai oleh organisasi?	4.75
	Apakah prosedur diberlakukan untuk menjamin keutuhan barang/kargo ketika barang/kargo dikirimkan ke organisasi lain (penyedia jasa transportasi, pusat pengumpulan barang, fasilitas intermodal, dsb) dalam rantai pasok?	4.5
	Apakah ada proses untuk melacak adanya perubahan tingkat ancaman di sepanjang rute transportasi?	4.75
	Apakah ada peraturan keamanan, prosedur, atau panduan keamanan yang diberikan kepada operator *conveyance* (misalnya, untuk menghindari rute yang berbahaya)?	4.5
7	**Unit Transportasi Kargo Tertutup**	
	(WCO SAFE *framework* mencakup "*Seal Integrity Program*" sebagaimana yang dijelaskan dalam Lampiran pada Lampiran 1 yang menjelaskan prosedur yang berkaitan dengan pemasangan dan verifikasi atas segel pengaman dan/atau alat deteksi kerusakan lain. Personil yang mengisi formulir ini sebaiknya mengkaji bab dalam *framework* tersebut).	
	Jika digunakan unit pengangkutan kargo tertutup, apakah ada prosedur terdokumentasi untuk pemasangan dan pencatatan segel pengaman mekanis yang memenuhi ISO / PAS 17712 dan / atau perangkat deteksi kerusakan lainnya oleh pihak yang menyusun unit kargo?	4.25
	Jika digunakan unit pengangkutan kargo tertutup bersegel, apakah ada prosedur terdokumentasi untuk memeriksa adanya tanda-tanda kerusakan segel ketika ada penggantian *conveyance* selama masa	4.25

No	Faktor	Skor Rata-Rata
	pengapalan dan untuk menangani adanya ketidaksesuaian yang terdeteksi?	
	Jika digunakan unit pengangkutan kargo tertutup, apakah ada inspeksi dengan segera terhadap kontaminasi oleh pihak yang menyusun kargo sebelum penyusunan dilakukan?	4.5
	Jika digunakan unit pengangkutan kargo tertutup, apakah ada prosedur terdokumentasi untuk inspeksi dengan segera oleh pihak yang menyusun sebelum penyususnan untuk memverifikasi keutuhan fisiknya, termasuk kehandalan mekanisme penguncian unit? 7 proses inspeksi yang dianjurkan:	4.68
	– Dinding muka	
	– Sisi kiri	
	– Sisi kanan	
	– Lantai	
	– Plafon / Atap	
	– Tutupdalam / luar	
	– Bagian luar/bawah	

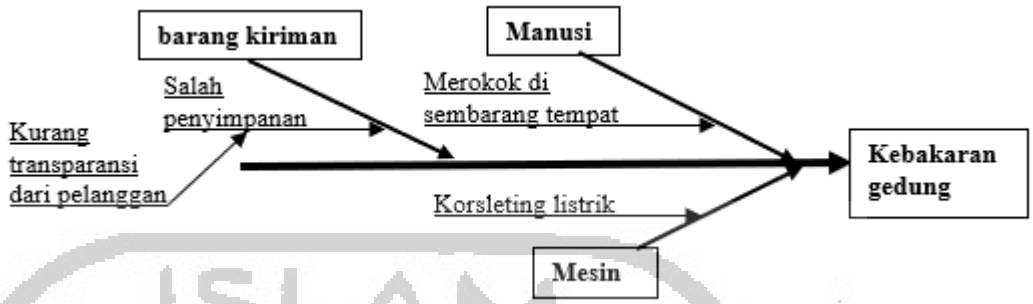
(Sumber: penilaian oleh perwakilan perusahaan)

4.1.4. Daftar Risiko Ancaman Keamanan yang Mungkin Dihadapi Perusahaan

Risiko ancaman keamanan diperoleh dengan wawancara dan diskusi dengan manager perusahaan, dimana dalam menentukan risiko ancaman keamanan yang mungkin dihadapi perusahaan adalah berdasarkan pada sistem manajemen keamanan rantai pasok ISO 28000 (terdapat dalam klausa 4.3.1 penilaian risiko keamanan) dan ISO 28001 (terdapat dalam lampiran B poin B.2 tahap pertama - pertimbangan skenario ancaman keamanan). Risiko ancaman keamanan yang diidentifikasi merupakan risiko ancaman yang berkaitan dengan aktifitas rantai pasok perusahaan.

Selain daftar risiko ancaman keamanan, melalui wawancara juga dilakukan identifikasi penyebab atau sumber terjadinya risiko dan tindakan kontrol yang telah dilakukan perusahaan terhadap masing-masing risiko ancaman keamanan. Data penyebab atau sumber terjadinya risiko sangat penting untuk diketahui karena digunakan untuk menentukan/menyusun tindakan mitigasi yang tepat. Penyebab atau sumber terjadinya risiko ditampilkan dalam diagram sebab akibat seperti pada gambar 4.2. Pada bagian ini hanya ditampilkan diagram sebab akibat satu risiko yaitu pada risiko terhadap fisik asset gedung berupa risiko

kebakaran. Untuk risiko-risiko yang lain, data selengkapnya sebagaimana terlampir.



Gambar 4.2. Diagram Sebab Akibat Risiko Kebakaran

Berdasarkan wawancara yang telah dilakukan, tindakan kontrol belum dilakukan secara menyeluruh artinya masih banyak risiko ancaman keamanan yang belum ada tindakan kontrolnya. Untuk risiko yang telah ada tindakan kontrolnya maka dituliskan "Ya" pada kolom "Ada" dan dituliskan "Tidak" pada kolom "Tidak" untuk risiko yang belum ada tindakan kontrolnya. Kemudian untuk risiko yang telah ada tindakan kontrolnya dituliskan penjelasan tindakan kontrol yang telah dilakukan seperti apa di kolom "Penjelasan".

Setiap risiko ancaman keamanan kemudian dilakukan penilaian terhadap kemungkinan terjadinya, dampak, dan frekuensi kejadian risiko dengan menggunakan skala likert 1-5 oleh manager perusahaan. Penilaian dilakukan berdasarkan kriteria penilaian terhadap masing-masing risiko. Kriteria penilaian tersebut didasarkan pada studi literatur dan diskusi dengan pihak perusahaan. Contoh penilaian risiko kebakaran yang merupakan risiko terhadap fisik asset, dalam menentukan nilai kemungkinan terjadinya risiko terdapat nilai 1-5 dengan masing-masing kriteria seperti dalam tabel 4.2. Manager perusahaan akan memilih salah satu nilai yang paling sesuai dengan keadaan di perusahaan. Pada risiko kebakaran ini nilai kemungkinan terjadinya adalah 1 yang artinya adalah kejadian risiko hanya akan terjadi dalam kondisi yang sangat spesifik dan hanya memiliki peluang kejadian maksimal 5%.

Tabel 4.2. Kriteria Penilaian Kemungkinan Terjadinya Risiko Kebakaran

Skala	Detesis	Besarnya Peluang	Keterangan
5	Most likely	peluang>80%	Kejadian risiko yang kemungkinan terjadinya lebih dari 80%.
4	possible	60%<peluang<=80%	Kejadian risiko yang kemungkinan kejadiannya sering, dengan kemungkinan kejadian diatas 60% sampai dengan 80%
3	conceivable	20%<peluang<=60%	Kejadian risiko yang mungkin terjadi sewaktu-waktu, dengan kemungkinan kejadian diatas 20% sampai dengan 60%.
2	remote	5%<peluang<=20%	Kejadian risiko yang bisa saja terjadi sewaktu-waktu, dengan kemungkinan kejadian diatas 5% sampai dengan 20%.
1	inconceivable	peluang<=5%	Kejadian risiko yang diperkirakan hanya akan terjadi dalam kondisi yang sangat spesifik. Biasanya hanya memiliki peluang kejadian maksimal sama dengan 5%.

Nilai dampak terjadinya risiko juga terdapat nilai 1-5 dengan masing-masing kriteria seperti dalam tabel 4.3. Nilai dampak untuk masing-masing kategori yang dihasilkan oleh sebuah risiko bisa berbeda-beda. Dengan perbedaan nilai dampak yang dihasilkan, maka untuk menentukan besarnya nilai dampak adalah dengan memilih nilai dampak yang paling besar. Misalnya dalam menentukan nilai dampak dari risiko kebakaran. Nilai dari dampak yang dihasilkan untuk masing-masing kategori adalah berbeda-beda yaitu dampak untuk kategori reputasi bernilai 2, finansial bernilai 5, operasional bernilai 5, pelayanan bernilai 5, dan human resources bernilai 2. Berdasarkan nilai tersebut, maka nilai yang diambil untuk dampak risiko kebakaran adalah 5.

Tabel 4.3. Kriteria Penilaian Dampak Terjadinya Risiko Kebakaran

Skala	Detesis	Reputasi	Finansial	Operasional	Pelayanan	Human Resources
5	Catastrophic/ sangat tinggi	Kehilangna reputasi atau publisitas jelek media nasional dan tuntutan hukum	Kerugian/biaya yang harus dikeluarkan lebih dari Rp500juta	Menimbulkan kegagalan diatas 75% proses operasional atau berdampak pada sebagian besar unit bisnis	Mengganggu pelayanan lebih dari 2minggu	Kematian massal
4	Major/Besar	Kemunduran/hilang kepercayaan stakeholders	Kerugian/biaya yang harus dikeluarkan antara Rp250juta-Rp500juta	Menimbulkan kegagalan antara 50-75% proses operasional atau berdampak pada sebagian besar unit bisnis	Mengganggu pelayanan lebih dari 1minggu sampai 2minggu	Kematian tunggal
3	Moderate/ Menengah	Pemberitaan negatif yang menurunkan kepercayaan stakeholders	Kerugian/biaya yang harus dikeluarkan sebesar Rp100.000.001	Menimbulkan gangguan antara 30-50% proses operasional atau	Mengganggu pelayanan sampai 1 minggu	Rawat inap/cacat

Skala	Detesis	Reputasi	Finansial	Operasional	Pelayanan	Human Resources
			hingga Rp250juta	berdampak pada 2 unit bisnis terkait		
2	Minor/Kecil	Terdapat pemberitaan negatif yang dapat mempengaruhi kinerja	Kerugian/biaya yang harus dikeluarkan sebesar Rp25.000.001 hingga Rp100juta	Menimbulkan gangguan antara 10-30% fungsi operasional atau hanya berdampak pada 1 unit bisnis	Mengganggu pelayanan sampai 2hari	Luka/perawatan ringan
1	Insignificant/ sangat rendah	Terdapat pemberitaan negatif namun tidak mengakibatkan penurunan kepercayaan	Kerugian/biaya yang harus dikeluarkan hingga Rp25.000.000	Menimbulkan gangguan kecil pada fungsi sistem terhadap proses bisnis namun tidak signifikan	Cukup mengganggu pelayanan	Kasus P3K (cedera sangat ringan)

Nilai frekuensi kejadian risiko juga terdapat nilai 1-5 dengan masing-masing kriteria seperti dalam tabel 4.4. Untuk menentukan nilai frekuens, Manager perusahaan akan memilih salah satu nilai dengan range frekuensi yang paling sesuai dengan keadaan di perusahaan. Pada risiko kebakaran ini nilai frekuensi kejadiannya adalah 1 yang artinya maksimal terjadinya risiko adalah sekali dalam setahun. Karena berdasarkan informasi dari pihak perusahaan untuk risiko ini belum pernah terjadi dan semoga tidak akan terjadi.

Tabel 4.4. Kriteria Penilaian Frekuensi Terjadinya Risiko Kebakaran

Skala	Detesis	Keterangan
5	Continuously	lebih dari 15 kejadian akan terjadi dalam 1 tahun
4	Frequently	maksimal 15 kejadian dalam waktu 1 tahun
3	Occasionally	maksimal 10 kejadian dalam waktu 1 tahun
2	Infrequently	maksimal 5 kejadian dalam waktu 1 tahun
1	Rarely	maksimal 1kejadian dalam 1 tahun

Keterangan lebih detail mengenai kriteria penilaian kemungkinan terjadinya, dampak, dan frekuensi kejadian risiko untuk masing-masing risiko yang diidentifikasi adalah sebagaimana terlampir. Data yang diperoleh dari penilaian kemungkinan terjadinya, dampak, dan frekuensi kejadian risiko ini akan digunakan untuk mengukur tingkatan risiko keamanan perusahaan berdasarkan kondisi saat ini. Hasil olah data pengukuran risiko nantinya akan dijadikan sebagai dasar untuk membuat rencana keamanan. Tabel 4.5. menampilkan data mengenai daftar risiko ancaman keamanan yang mungkin dihadapi perusahaan.

Tabel 4.5. Daftar Risiko Ancaman Keamanan Perusahaan

No	Ancaman yang mungkin dihadapi	Kontrol yang sudah ada			Kemungkinan Terjadinya					Dampak					Frekuensi Kejadian				
					1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
		Ada	Tidak	Penjelasan, bila ada															
1	**Ancaman terhadap Fisik Aset**																		
	a. Gedung																		
	- Kebakaran		Tidak		1									5	1				
	- Kebocoran	Ya		- Bagian Staf Umum		2				1					1				
	- Aksi Kriminal Pencurian		Tidak		1							3			1				
	- Aksi Pengerusakan		Tidak		1							3			1				
	b. Peralatan Kantor																		
	- Kehilangan peralatan		Tidak		1							3			1				
	- Kerusakan peralatan	Ya		- Bagian Staf Umum		2					2					2			
	c. Unit Transportasi																		
	- Kehilangan *spare part* armada	Ya		- Bagian Staf Bisnis - Prosedur keamanan		2						3			1				
	- Kerusakan armada	Ya		- Bagian Staf Bisnis - *Maintenance* rutin armada			3					3			1				
2	**Ancaman Personel**																		
	- Karyawan bekerja tidak sesuai SOP		Tidak					4				3			1				
	- Karyawan menyalahgunakan wewenangnya		Tidak					4				3			1				
3	**Ancaman terhadap Data/Informasi**																		
	- Penyalahgunaan informasi oleh siapapun		Tidak		1						2				1				
	- Kebocoran rahasia perusahaan		Tidak		1							3			1				
	- Salah informasi ketika komunikasi		Tidak					4				3			1				
4	**Ancaman terhadap Proses Muat Barang**																		
	- Kerusakan barang	Ya		- Adanya *checker* - Mengetahui karakterisitik barang (koordinasi dengan pemilik barang) untuk memberikan perlakukan yang tepat terhadap barang				4			2							4	

No	Ancaman yang mungkin dihadapi	Kontrol yang sudah ada			Kemungkinan Terjadinya					Dampak					Frekuensi Kejadian				
					1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
		Ada	Tidak	Penjelasan, bila ada															
	- Ketidaktepatan kuantiti/jumlah barang	Ya		- Adanya *checker* - Ketelitian petugas				4			2								5
5	**Ancaman terhadap Proses Bongkar Barang**																		
	- Kerusakan barang	Ya		- Adanya *checker* - Mengetahui karakterisitik barang (koordinasi dengan pemilik barang) untuk memberikan perlakukan yang tepat terhadap barang				4			2							4	
	- Ketidaktepatan kuantiti/jumlah barang	Ya		- Adanya *checker* - Ketelitian petugas				4			2								5
6	**Ancaman terhadap Proses Dekonsolidasi/Konsolidasi Barang**																		
	- Kerusakan barang	Ya		- Petugas mengetahui karakterisitik barang untuk memberikan perlakukan yang tepat terhadap barang				4			2							4	
7	**Ancaman terhadap Proses Penyimpanan Barang**																		
	- Kerusakan barang		Tidak		1						2							4	
	- Kehilangan barang		Tidak		1						2				1				
8	**Ancaman terhadap Proses Pengiriman/Pengangkutan Barang**																		
	- Kerusakan barang	Ya		- Penyusunan barang yang baik dan benar				4				3						4	
	- Adanya tindakan kriminal	Ya		- Pemilihan tempat istirahat yang aman - Tidak mudah terpengaruh terhadap ketidakjelasan orang selama perjalanan (kehati-hatian)				4				3						4	
	- Kecelakaan di jalan selama pengiriman	Ya		- *Check* kelayakan armada - Kesiapan *driver*				4				3						4	

No	Ancaman yang mungkin dihadapi	Kontrol yang sudah ada			Kemungkinan Terjadinya					Dampak					Frekuensi Kejadian				
					1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
		Ada	Tidak	Penjelasan, bila ada															
	- Kerusakan armada saat pengiriman	Ya		- *Check* kelayakan armada				4				3					3		
	Ancaman terhadap Bencana Alam/Lingkungan																		
	- Gunung Meletus		Tidak		1							3			1				
	- Gempa	Ya		- *Update* BMKG		2							4		1				
10	**Ancaman Mitra Bisnis**																		
	- Ketidakpatuhan mitra bisnis terhadap aturan perusahaan	Ya		- Adanya *checker* - Penolakan armada yang tidak sesuai				4		1							3		
	- Keterlambatan kedatangan armada	Ya		- Komunikasi yang baik		2				1							3		
	- Armada tidak sesuai spesifikasi	Ya		- Adanya *checker* - Penolakan armada vendor		2					2						3		
	- Vendor perusahaan mengambil alih customer perusahaan tanpa sepengetahuan perusahaan	Ya		- Komunikasi yang baik terhadap vendor - Mengutamakan *quality* dan professionalisme kerja				4			2						3		
	- Customer perusahaan mengontak langsung vendor perusahaan tanpa sepengetahuan perusahaan	Ya		- komunikasi yang baik terhadap vendor - mengutamakan quality dan professionalisme kerja				4			2						3		
11	**Ancaman terhadap reputasi dan nama baik**																		
	- Komplain dari pelanggan	Ya		- *Monitoring* terhadap pergerakan barang - Komunikasi yang baik terhadap pelanggan, contoh ketika terdapat kendala dalam pengiriman					5			3					3		

(Sumber: diskusi dengan manager PT. Poslog Jogja)

4.2. Pengolahan Data

4.2.1. Daftar Kajian Kinerja Keamanan Perusahaan Menggunakan Analisis Gap

Pada daftar kajian kinerja keamanan perusahaan, faktor serta poin pertanyaan yang digunakan adalah berdasarkan daftar kajian kinerja yang terdapat di ISO 28001 Lampiran A. Dalam pengisian daftar kajian kinerja digunakan skala likert 1-5 untuk masing-masing poin dari masing-masing faktor, kemudian hasil perhitungan nilai tiap faktor akan dianalisis menggunakan analisis gap dimana hasil yang diperoleh akan dibandingkan dengan nilai yang seharusnya. Berikut adalah hasil perhitungan nilai masing-masing faktor.

Tabel 4.6. Nilai Daftar Kajian Kinerja Keamanan Perusahaan

Faktor	Jumlah Poin	Skor Tertinggi	Nilai Tertinggi	Nilai Aktual	Persentase Kesesuaian terhadap ISO 28001
1. Manajemen Keamanan Rantai Pasok	2	5	10	9.25	92.50%
2. Rencana Keamanan	3	5	15	12.50	83.33%
3. Keamanan Aset	5	5	25	21.75	87.00%
4. Keamanan Personel	4	5	20	18.00	90.00%
5. Keamanan Informasi	7	5	35	30.25	86.43%
6. Keamanan Barang & *Conveyance*	6	5	30	27.50	91.67%
7. Unit Transportasi Cargo Tertutup	4	5	20	17.68	88.39%

Berdasarkan pengolahan data, nilai yang diperoleh perusahaan untuk masing-masing faktor dalam kajian kinerja keamanan perusahaan adalah antara 83% - 92.5%. Nilai yang diperoleh adalah diatas 75% yang menunjukkan bahwa perusahaan siap untuk melengkapi sistem manajemen keamanan rantai pasok ISO 28001 dan melakukan sertifikasi.

4.2.2. Penilaian Risiko Ancaman Keamanan yang Mungkin Dihadapi Perusahaan Menggunakan FMEA

Rencana keamanan perusahaan dapat dibuat setelah dilakukan identifikasi performa keamanan perusahaan. Output dari proses ini adalah daftar ancmaman keamanan yang memiliki skor risiko tinggi yang perlu untuk diberikan tindakan kontrol yang tepat.

Data yang telah diperoleh mengenai nilai kemungkinan terjadinya, dampak, dan frekuensi kejadian untuk setiap risiko ancaman keamanan kemudian digunakan untuk menghitung nilai RPN (*Risk Priority Number*) untuk mengetahui nilai prioritas risiko yang harus segera ditangani. Nilai RPN merupakan perkalian antara *probability*, *severity*, dan *frequency*. Tabel 4.7. menunjukkan hasil perhitungan nilai RPN.

Berdasarkan olah data nilai RPN terdapat 12 risiko kritis atau nilai RPN-nya lebih tinggi dari nilai RPN kritis. 12 risiko tersebut adalah kerusakan barang dalam proses muat barang (14), ketidaktepatan jumlah barang dalam proses muat barang (15), kerusakan barang dalam proses bongkar barang (16), ketidaktepatan jumlah barang dalam proses bongkar barang (17), kerusakan barang dalam proses dekonsolidasi/konsolidasi barang (18), kerusakan barang dalam proses pengiriman barang (21), adanya tindakan kriminal dalam proses pengiriman barang (22), kecelakaan di jalan selama pengiriman (23), kerusakan armada saat pengiriman (24), vendor perusahaan mengambil alih *customer* perusahaan tanpa sepengetahuan perusahaan (30), *Customer* perusahaan mengontak langsung vendor perusahaan tanpa sepengetahuan perusahaan (31), dan komplain dari pelanggan (32).

Tabel 4.7. Hasil Perhitungan RPN (*Risk Priority Number*)

No	Faktor	Risiko Ancaman Keamanan	Probability	Severity	Frequency	RPN
1	Ancaman terhadap Fisik Aset Gedung	- Kebakaran	1	5	1	5
2		- Kebocoran	2	1	1	2
3		- Aksi Kriminal Pencurian	1	3	1	3
4		- Aksi Pengerusakan	1	3	1	3
5	Ancaman terhadap Fisik Aset Peralatan Kantor	- Kehilangan peralatan	1	3	1	3
6		- Kerusakan peralatan	2	2	2	8
7		- Kehilangan *spare part* armada	2	3	1	6

No	Faktor	Risiko Ancaman Keamanan	Probability	Severity	Frequency	RPN
8	Ancaman terhadap Fisik Aset Unit Transportasi	- Kerusakan armada	3	3	1	9
9	Ancaman Personel	- Karyawan bekerja tidak sesuai SOP	4	3	1	12
10		- Karyawan menyalahgunakan wewenangnya	4	3	1	12
11	Ancaman terhadap Data/Informasi	- Penyalahgunaan informasi oleh siapapun	1	2	1	2
12		- Kebocoran rahasia perusahaan	1	3	1	3
13		- Salah informasi ketika komunikasi	4	3	1	12
14	Ancaman terhadap Proses Muat Barang	- Kerusakan barang	4	2	4	32
15		- Ketidaktepatan kuantiti/jumlah barang	4	2	5	40
16	Ancaman terhadap Proses Bongkar Barang	- Kerusakan barang	4	2	4	32
17		- Ketidaktepatan kuantiti/jumlah barang	4	2	5	40
18	Ancaman terhadap Proses Dekonsolidasi/ Konsolidasi Barang	- Kerusakan barang	4	2	4	32
19	Ancaman terhadap Proses Penyimpanan Barang	- Kerusakan barang	1	2	4	8
20		- Kehilangan barang	1	2	1	2
21	Ancaman terhadap Proses Pengiriman/ Pengangkutan Barang	- Kerusakan barang	4	3	4	48
22		- Adanya tindakan kriminal	4	3	4	48
23		- Kecelakaan di jalan selama pengiriman	4	3	4	48
24		- Kerusakan armada saat pengiriman	4	3	3	36
25	Ancaman terhadap Bencana Alam/Lingkungan	- Gunung meletus	1	3	1	3
26		- Gempa	2	4	1	8
27	Ancaman Mitra Bisnis	- Ketidakpatuhan mitra bisnis terhadap aturan perusahaan	4	1	3	12
28		- Keterlambatan kedatangan armada	2	1	3	6
29		- Armada tidak sesuai spesifikasi	2	2	3	12
30		- Vendor perusahaan mengambil alih customer perusahaan tanpa sepengetahuan perusahaan	4	2	3	24
31		- Customer perusahaan mengontak langsung vendor	4	2	3	24

No	Faktor	Risiko Ancaman Keamanan	Probability	Severity	Frequency	RPN
		perusahaan tanpa sepengetahuan perusahaan				
32	Ancaman terhadap reputasi dan nama baik	- Komplain dari pelanggan	5	3	3	45
Total RPN						613
Nilai Kritis RPN						19.156

Probability impact matrix merupakan salah satu metode pendekatan risiko yang dapat digunakan untuk menentukan daerah prioritas risiko yang mempertimbangkan nilai *probability* dan *severity* (Hoseynabadi **(**2010) dalam Nanda (2014)). Hal ini menunjukkan adanya perbedaan antara nilai RPN dan *probability impact matrix* dalam menentukan prioritas risiko. Pada RPN yang digunakan adalah tiga kriteria utama yaitu *probability*, *severity*, dan *frequency* sedangkan pada *probability impact matrix* kriteria yang digunakan hanya *probability* dan *severity*.

Gambar 4.3. merupakan hasil pemetaan berdasarkan nilai *probability* dan *severity*. Hasil pemetaan menunjukkan bahwa terdapat 10 risiko yang berada pada level tinggi atau pada daerah yang berwarna merah dalam peta risiko. 10 risiko pada level tinggi ini merupakan risiko kritis yang menjadi prioritas utama untuk diberikan tindakan mitigasi. Yang termasuk dalam 10 risiko kritis adalah komplain dari pelanggan (32), Karyawan bekerja tidak sesuai SOP (9), karyawan menyalahgunakan wewenangnya (10), salah informasi ketika komunikasi (13), kerusakan barang dalam proses pengiriman barang (21), adanya tindakan kriminal dalam proses pengiriman barang (22), kecelakaan di jalan selama pengiriman (23), kerusakan armada saat pengiriman (24), gempa (26), dan kebakaran (1).

Risiko yang berada pada level sedang atau pada daerah yang berwarna kuning dalam peta risiko terdapat 9 risiko yaitu kerusakan barang dalam proses muat barang (14), ketidaktepatan jumlah barang dalam proses muat barang (15), kerusakan barang dalam proses bongkar barang (16), ketidaktepatan jumlah barang dalam proses bongkar barang (17), kerusakan barang dalam proses dekonsolidasi/konsolidasi barang (18), vendor perusahaan mengambil alih *customer* perusahaan tanpa sepengetahuan perusahaan (30), *customer*

perusahaan mengontak langsung vendor perusahaan tanpa sepengetahuan perusahaan (31), kehilangan *spare part* armada (7), dan Kerusakan armada (8). Risiko yang berada di level rendah atau pada daerah yang berwarna hijau dalam peta risiko terdapat 13 risiko yaitu kebocoran (2), keterlambatan kedatangan armada (28), penyalahgunaan informasi oleh siapapun (11), kerusakan peralatan (6), kerusakan barang dalam proses penyimpanan barang (19), kehilangan barang dalam proses penyimpanan barang (20), armada tidak sesuai spesifikasi (29), aksi kriminal pencurian (3), aksi pengerusakan (4), kehilangan peralatan (5), kebocoran rahasia perusahaan (12), gunung meletus (25), dan ketidakpatuhan mitra bisnis terhadap aturan perusahaan (27).

Probability (Kemungkinan Terjadinya)							
	5	Most likely			32		
	4	Possible	27	14, 15, 16, 17, 18, 30, 31	9, 10, 13, 21, 22, 23, 24		
	3	Conceivable			8		
	2	Remote	2, 28	6, 19, 20, 29	7	26	
	1	Inconceivable		11	3, 4, 5, 12, 25		1
			Severity (Dampak)				
			1	2	3	4	5
			Sangat kecil	Kecil	Sedang	Besar	Sangat besar

Gambar 4.3. Hasil Perhitungan *Probability Impact Matrix*

Risiko ancaman keamanan yang telah diidentifikasi ada yang telah diberikan/dilakukan tindakan kontrol oleh perusahaan dan ada yang belum. Dari hasil pemetaan risiko, sebagian besar risiko yang berada di level tinggi merupakan risiko yang telah ada tindakan kontrolnya. Namun karena posisinya berada di level tinggi maka perlu dikaji ulang mengenai tindakan kontrol tambahan yang perlu dilakukan sehingga dapat mengurangi salah satu dari nilai probabilitas dan dampak atau kedunya. Untuk risiko-risiko yang berada di level sedang sudah ada tindakan kontrolnya dari perusahaan. Untuk risiko-risiko yang berada di level rendah ada yang sudah diberikan tindakan kontrol ada yang belum.

Meskipun levelnya rendah, karena belum ada tindakan kontrolnya maka perlu dibuat tindakan kontrol agar risiko yang berada di level rendah ini posisinya tetap berada di level rendah. Namun, pada penelitian ini tindakan kontrol/tindakan mitigasi yang diusulkan dikhususkan untuk risiko-risiko yang berada pada level tinggi. Jadi, untuk risiko yang berada di level sedang dan rendah tidak diberikan usulan tindakan mitigasi atau tindakan kontrol tambahan.

Setelah dilakukan penilaian risiko, selanjutnya adalah menentukan respon risiko atau strategi mitigasi yang tepat untuk mengurangi dari segi probabilitas atau dampak yang ditimbulkan oleh risiko yang ada. Menurut Flanagan dan Norman (1993), *risk response* adalah tanggapan atau reaksi terhadap risiko yang dilakukan oleh setiap orang atau perusahaan dalam pengambilan keputusan, yang dipengaruhi oleh pendekatan risiko (*risk attitude*) dari pengambil keputusan. Lembaga Sertifikasi Profesi Manajemen Risiko menyatakan 4 tindakan strategi mitigasi yang dapat dilakukan untuk respon risiko adalah: menghindari risiko (*avoid*) yaitu dengan menghentikan aktivitas atau pelayanan yang meningkatkan risiko, mengurangi risiko (*reduce*) yaitu mengambil tindakan untuk mengurangi probabilitas dan/atau dampak dari suatu risiko, membagi risiko (*share*) yaitu membagi risiko yang dihadapi dengan pihak lain, dan menerima risiko (*accept*) yaitu menerima tingkat risiko yang terjadi (risiko masih berada dalam batas toleransi) dan mempertahankan/mengelola risiko agar tidak meningkat ke level yang lebih tinggi.

Dari hasil perhitungan RPN dan *probability impact matrix* terdapat 5 risiko kritis yang sama yaitu komplain dari pelanggan (32), kerusakan barang dalam proses pengiriman barang (21), adanya tindakan kriminal dalam proses pengiriman barang (22), kecelakaan di jalan selama pengiriman (23), kerusakan armada saat pengiriman (24).

Jadi melalui hasil perhitungan RPN dan *probability impact matrix* diperoleh 17 risiko kritis yaitu kebakaran (1), karyawan bekerja tidak sesuai SOP (9), karyawan menyalahgunakan wewenangnya (10), salah informasi ketika komunikasi (13), kerusakan barang dalam proses muat barang (14), ketidaktepatan jumlah barang dalam proses muat barang (15), kerusakan barang dalam proses bongkar barang (16), ketidaktepatan jumlah barang dalam proses bongkar barang (17), kerusakan barang dalam proses dekonsolidasi/konsolidasi barang (18), kerusakan barang dalam proses pengiriman barang (21), adanya tindakan kriminal dalam proses pengiriman barang (22), kecelakaan di jalan selama pengiriman (23), kerusakan armada saat pengiriman (24), gempa (26), vendor perusahaan mengambil alih *customer* perusahaan tanpa sepengetahuan

perusahaan (30), *Customer* perusahaan mengontak langsung vendor perusahaan tanpa sepengetahuan perusahaan (31), dan komplain dari pelanggan (32).

Dalam menentukan strategi mitigasi dan rencana keamanan dilakukan analisis mengenai penyebab risiko dominan dari risiko kritis yang telah diperoleh dari hasil perhitungan RPN dan pelevelan risiko. Penyebab risiko dominan merupakan penyebab risiko yang mempunyai skor/nilai paling tinggi. Skor tersebut diperoleh dari hasil perkalian frekuensi kejaidan risiko karena penyebab tersebut dengan dampak risiko karena penyebab tersebut. Tabel 4.8. menunjukkan perhitungan skor/nilai penyebab risiko untuk masing-masing risiko kritis yang berdasarkan pada frekuensi dan dampak risiko.

Penyebab risiko dominan dari risiko kritis inilah yang menjadi prioritas utama dalam penanganan risiko dan penentuan strategi serta rencana keamanan. Berdasarkan perhitungan skor/nilai penyebab risiko tersebut diperoleh 9 faktor penyebab yang berdampak besar terhadap perusahaan apabila tidak dikelola dengan baik yaitu kurangnya kehati-hatian karyawan dalam meng-*handle* barang, lokasi gudang yang berada di lantai 2 dan tidak ada lift yang membuat karyawan harus memindahkan barang secara manual melalui tangga, kurangnya transparansi barang dari pelanggan, kurangnya mengoptimalkan fungsi *checker* dengan baik mengakibatkan ketidaktepatan jumlah barang dalam proses bongkar dan muat barang, tempat istirahat yang kurang aman membuat *driver* mengalami tindakan kriminal selama proses pengiriman barang, *driver* mengantuk/kelelahan karena waktu keberangkatan pengiriman malam hari dan *driver* hanya sendiri menyebabkan kecelakaan dalam proses pengiriman barang, masa pakai armada yang dapat menyebabkan kerusakan armada selama pengiriman barang, penggunaan vendor baru (vendor kurang memahami kode etik) membuat perusahaan kehilangan konsumen karena vendor biasanya akan langsung mengambil alih konsumen perusahaan, dan harga yang kurang bersaing membuat konsumen berpindah menggunakan jasa lain yang seringnya konsumen langsung menggunakan mitra perusahaan, hal ini membuat perusahaan kehilangan pelanggan. Tabel 4.9. menunjukkan strategi mitigasi dan tindakan rencana keamanan untuk menangani 9 faktor penyebab risiko dominan terjadinya risiko kritis.

Rencana keamanan yang disusun diharapkan dapat menurunkan probabilitas, dampak, atau frekuensi kejadian risiko keamanan di perusahaan sehingga dapat membantu perusahaan dalam mencapai tingkat kesesuaian keamanannya dengan ISO 28001.

Tabel 4.8. Perhitungan Skor Penyebab Risiko untuk Risiko Kritis

No	Risk Number	Risiko	Penyebab	Frekuensi	Dampak (Rp)	Nilai
1	(1)	Kebakaran	Karyawan merokok di sembarang tempat	-	-	-
			Korsleting listrik	-	-	-
			Barang kiriman (barang kiriman yang disimpan, karena kurangnya transparansi konsumen kepada perusahaan terhadap barang yang akan dikirim, misalnya: barang yang dikirim ternyata mudah terbakar), perlakuan yang kurang tepat dalam menyimpan barang kiriman tersebut	-	-	-
2	(9)	Karyawan bekerja tidak sesuai SOP	Kurangnya kesadaran karyawan terhadap pentingnya mematuhi SOP	-	-	-
			Kurangnya pengetahuan karyawan terhadap pentingnya mematuhi SOP	-	-	-
			Kurangnya pengetahuan karyawan terhadap SOP perusahaan	-	-	-
			Kurangnya pengawasan internal perusahaan	2	-	-
3	(10)	Karyawan menyalahgunakan wewenangnya	Kurangnya kesadaran karyawan terhadap pentingnya memegang wewenang	-	-	-
			Kurangnya pengetahuan karyawan terhadap pentingnya memegang wewenang	-	-	-
			Kurangnya pengetahuan karyawan terhadap batasan wewenang yang dimiliki	-	-	-
			Kurangnya pengawasan internal perusahaan	2	-	-
4	(13)	Salah informasi ketika komunikasi	Karyawan kurang memahami perintah atasan	4	-	-
			Karyawan bingung dengan perintah yang ada di internal perusahaan dengan perintah dari perusahaan pusat	7	-	-
5	(14)	Kerusakan barang dalam proses muat barang	Karyawan kurang hati-hati	3	5juta	15 juta
			Karyawan kurang hati-hati	10	-	-
			Karyawan tidak memahami bagaimana cara memperlakukan barang/ cara handling barang	-	-	-
			Kurang pengawasan dari atasan	3	1juta	3 juta

No	Risk Number	Risiko	Penyebab	Frekuensi	Dampak (Rp)	Nilai
6	(15)	Ketidaktepatan jumlah barang dalam proses muat barang	Kesalahan karyawan dalam menyortir barang	12	100ribu	1.2 juta
			Kesalahan karyawan dalam membaca packing list barang	5	100ribu	500ribu
			Barang tercampur dengan barang lain	1	200ribu	200ribu
			Checker tidak berfungsi dengan baik	2	20juta	40 juta
7	(16)	Kerusakan barang dalam proses bongkar barang	Karyawan kurang hati-hati	10	1juta	10juta
			Karyawan tidak memahami bagaimana cara memperlakukan barang/ cara handling barang	-	-	-
			Kurang pengawasan dari atasan	5	1juta	5juta
			Lokasi warehouse: gudang berada di lantai 2 dan tidak ada lift (menaikkan barang ke lantai 2 melalui tangga)	2	3juta	6juta
			Waktu yang terbatas	3	2juta	6juta
8	(17)	Ketidaktepatan jumlah barang dalam proses bongkar barang	Kesalahan karyawan dalam menyortir barang	10	100ribu	1juta
			Kesalahan karyawan dalam membaca packing list barang	6	100ribu	600ribu
			Checker tidak berfungsi dengan baik	5	5juta	25 juta
9	(18)	Kerusakan barang dalam proses dekonsolidasi/konsolidasi barang	Karyawan kurang hati-hati	5	1juta	5 juta
			Karyawan tidak memahami bagaimana cara memperlakukan barang/ cara handling barang yang benar	-	-	-
			Kurang pengawasan dari atasan	4	1juta	4 juta
			Lokasi warehouse: gudang berada di lantai 2 dan tidak ada lift (menaikkan barang ke lantai 2 melalui tangga)	2	3juta	6juta
			Waktu yang terbatas	4	1juta	4 juta
10	(21)	Kerusakan barang dalam proses pengiriman barang	Cara penyusunan barang kurang tepat	11	500ribu	5.5. juta
			Cara packing barang kurang tepat	1	300juta	300 juta
			Salah perlakuan barang karena kurangnya transparansi barang dari pelanggan	1	500juta	500 juta

No	Risk Number	Risiko	Penyebab	Frekuensi	Dampak (Rp)	Nilai
11	(22)	Adanya tindakan kriminal dalam proses pengiriman barang	Tempat istirahat yang kurang aman	12	2juta	24 juta
			Jalan yang kurang aman	-	-	-
			Pemilihan waktu pengiriman	-	-	-
12	(23)	Kecelakaan di jalan selama pengiriman	Driver mengantuk/kelelahan karena waktu keberangkatan pengiriman malam hari dan driver hanya sendiri	11	7juta	77 juta
13	(24)	Kerusakan armada saat pengiriman	Skill driver	-	-	-
			Muatan yang berlebihan	-	-	-
			Masa pakai armada	5	1.7juta	8.5 juta
			Masa pakai armada	2	10juta	20 juta
14	(26)	Gempa	Faktor alam	-	-	-
			Lokasi perusahaan di daerah yang rawan terhadap gempa	-	-	-
15	(30)	Vendor perusahaan mengambil alih customer perusahaan tanpa sepengetahuan perusahaan	Penggunaan vendor baru (Vendor kurang memahami kode etik)	4	300juta	1.2 M
			Vendor masih mencari konsumen yang sesuai	-	-	-
			Vendor menginginkan keuntungan yang lebih	2	100juta	200 juta
16	(31)	Customer perusahaan mengontak langsung vendor perusahaan tanpa sepengetahuan perusahaan	Konsumen ingin mendapatkan harga lebih murah	10	100juta	1 M
			Konsumen menginginkan efisiensi	-	-	-
17	(32)	Komplain dari pelanggan	Waktu pengiriman yang lama karena melibatkan banyak stakeholder karena belum adanya jaringan poslog di wilayah timur	3	3.2juta	9.6 juta
			Barang rusak karena karyawan kurang hati-hati	2	9juta	18 juta
			Barang rusak karena karyawan kurang hati-hati	4	500ribu	2 juta

Tabel 4.9. Strategi Mitigasi dan Rencana Keamanan

No	Penyebab Dominan	Strategi Mitigasi	Tindakan Rencana Keamanan	PIC
1	Karyawan kurang hati-hati dalam meng-*handle* barang	- *Reduce* - *Share*	- Memberikan pelatihan kepada karyawan tentang cara packing, handling, dan penyusunan barang yang baik dan benar sesuai dengan SOP. - Menerapkan asuransi terhadap barang.	Manager BO & Supervisor
2	*Checker* tidak berfungsi dengan baik	*Reduce*	- Meningkatkan fungsi dan kinerja *checker* dalam proses penyusunan barang.	Supervisor
3	Lokasi warehouse: gudang berada di lantai 2 dan tidak ada lift (menaikkan barang ke lantai 2 melalui tangga)	*Reduce*	- Karyawan harus lebih hati-hati dalam memindahkan barang. - Meningkatkan pengawasan.	Supervisor
4	Salah perlakuan barang karena kurangnya transparansi barang dari pelanggan	- *Reduce* - *Share*	- Menambahkan alat pendeteksi barang	Manager BO & Supervisor
5	Tempat istirahat yang kurang aman	- *Avoid* - *Reduce*	- Memberikan edukasi kepada karyawan/*driver* tentang tempat-tempat peristirahatan yang aman. - *Driver* menghindari tempat istirahat yang tidak aman/pemilihan tempat istirahat yang aman - Melakukan pengawasan terhadap proses pengiriman.	Manager BO & Supervisor
6	Driver mengantuk/kelelahan karena waktu keberangkatan pengiriman malam hari dan driver hanya sendiri	- *Reduce* - *Share*	- Memilih *driver* yang tepat (sehat kondisi fisik dan psikis) - Memberikan sosialisasi kepada driver tentang pengetahuan manajemen waktu dan manajemen pengendaraan. - Memastikan driver melakukan istirahat yang cukup dan berkualitas. - Menerapkan asuransi terhadap karyawan, barang, dan kendaraan.	Manager BO & Supervisor
7	Masa pakai armada	*Reduce*	- Menggunakan armada sesuai dengan batas usianya - Melakukan penilaian dan pemilihan mitra bisnis yang sesuai kemudian membuat peraturan dan perjanjian tertulis tentang pengecekan kelayakan armada dan usia pemakaian armada pada rekan bisnis serta pengawasan	Manager BO & Supervisor
8	Penggunaan vendor baru (Vendor kurang memahami kode etik)	- *Avoid* - *Reduce*	- Menghindari penggunaan vendor baru - Lebih hati-hati dalam pemilihan vendor - Memilih vendor dengan kredibilitas yang baik	Manager BO & Supervisor
9	Konsumen ingin mendapatkan harga lebih murah	*Reduce*	- Penentuan harga yang dapat bersaing dengan kompetitor dengan tetap memberikan pelayanan terbaik kepada pelanggan.	Manager BO & Supervisor