BAB III
METODOLOGI PENELITIAN

3.1. Objek Penelitian

Objek dalam penelitian ini adalah PT. Pos Logistik Indonesia kantor cabang Yogyakarta yang berlokasi di jl. Mayor Suryotomo No. 8, Ngupasan, Gondomanan, Kota Yogyakarta, Daerah Istimewa Yogyakarta 55122. Penelitian dilaksanakan pada bulan Mei 2018 sampai dengan bulan Juli 2018.

3.2. Ruang Lingkup Penelitian

Ruang lingkup penelitian menunjukkan cakupan dan batasan bagian yang diteliti. Adapun ruang lingkup dalam penelitian ini adalah:

1. Penelitian dilakukan pada PT. Pos Logistik Indonesia Kantor Cabang Yogyakarta.
2. Bagian yang diteliti adalah tentang keamanan rantai pasok perusahaan.
3. Daftar kajian kinerja keamanan yang digunakan adalah berdasarkan pada tabel daftar kajian kinerja yang terdapat di ISO 28001 Lampiran A.
4. Metode pengukuran kesesuaian (*compliance*) yang digunakan adalah metode *gap analysis*.
5. Pendekatan yang digunakan untuk penilaian risiko adalah pendekatan FMEA (*Failure Mode and Effects Analysis*).

3.3. Data Penelitian

Data yang digunakan dalam penelitian ini adalah:

1. Data Primer

   Data primer merupakan data yang diperoleh secara langsung melalui observasi lapangan, wawancara dan kuesioner kepada pihak PT. Pos Logistik Indonesia kantor cabang Yogyakarta yang berkaiatan dengan tema penelitian. Data tersebut terdiri atas proses bisnis perusahaan, daftar kajian kinerja keamanan perusahaan, daftar risiko ancaman keamanan beserta penyebab terjadinya risiko, dan tindakan keamanan yang ada.

2. Data sekunder

   Data sekunder berupa data mengenai profil perusahaan, penelitian terdahulu dan studi literatur mengenai keamanan rantai pasok dan teori-teori manajemen risiko serta pendekatan dalam analisis risiko.

3.4. Metode Pengumpulan Data

Pada penelitian ini digunakan beberapa metode dalam pengumpulan data yaitu:

1. Observasi

   Observasi lapangan dilakukan untuk mengidentifikasi serta mempelajari secara langsung permasalahan keamanan rantai pasok di PT. Pos Logistik Indonesia kantor cabang Yogyakarta.

2. Wawancara

   Wawancara dilakukan kepada manager dan staf-staf perusahaan yang terkait untuk mendapatkan data dan informasi mengenai proses bisnis yang terdapat diperusahaan, daftar risiko ancaman keamanan yang mungkin dihadapi perusahaan beserta penyebabnya, dan tindakan keamanan yang ada.

3. Kuesioner

   Kuesioner diberikan kepada staf-staf perusahaan yang terkait untuk mendapatkan data mengenai kesesuaian antara sistem manajemen keamanan rantai pasok di PT. Pos Logistik Indonesia kantor cabang Yogyakarta dengan standar *security supply chain* ISO 28001. Daftar pertanyaan yang digunakan untuk mengidentifikasi kesesuaian perusahaan terhadap ISO 28001 adalah tabel daftar kajian kinerja keamanan yang terdapat di ISO 28001 Lampiran A.

   Kuesioner berikutnya adalah kuesioner untuk mendapatkan nilai probabilitas, dampak, dan frekuensi kejadian serta tindakan pengaman yang ada dari setiap risiko ancaman keamanan.

Tabel 3.1. Daftar Kajian Kinerja Keamanan untuk Penilaian Kesesuaian Perusahaan terhadap Security Supply Chain ISO 28001

No	Faktor	Skor				
		1	2	3	4	5
1	**Manajemen Keamanan Rantai Pasok**					
	Apakah organisasi memiliki sistem manajemen yang menangani keamanan rantai pasok?					
	Apakah organisasi memiliki individu yang ditunjuk sebagai penanggung jawab atas keamanan rantai pasok?					
2	**Rencana Keamanan**					
	Apakah organisasi memiliki rencana keamanan terbaru?					
	Apakah rencana tersebut menjelaskan harapan keamanan organisasi mitra bisnis di hulu dan hilir?					
	Apakah organisasi memiliki rencana manajemen krisis, rencana kelanjutan bisnis, dan rencana pemulihan keamanan?					
3	**Keamanan Aset**					
	Apakah organisasi memiliki perangkat untuk menangani:					
	- 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.					
	Apakah ada prosedur yang diterapkan untuk bisa menghubungi personal keamanan internal atau pihak penegak hukum eksternal jika terjadi pelanggaran keamanan?					
	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?					
	Apakah individu yang menerima atau mengirim kargo sudah diidentifikasi sebelum kargo diterima atau dikeluarkan?					
4	**Keamanan Personel**					
	Apakah organisasi memiliki prosedur untuk mengevaluasi integritas karyawan sebelum mengkaryakannya dan dievaluasi secara periodik dalam melakukan tugas-tugas keamanannya?					
	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?					

No	Faktor	Skor				
		1	2	3	4	5
	Apakah organisasi membuat karyawan peduli terhadap prosedur perusahaan untuk melaporkan insiden yang mencurigakan?					
	Apakah sistem pengendalian akses memuat pemusnahan dengan segera identifikasi dan akses bagi karyawan yang diberhentikan perusahaan ke area yang sensitif dan sistem informasi?					
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?					
	Apakah organisasi yang mengirimkan atau menerima kargo sudah mencocokkan kargo dengan dokumen pengiriman yang sesuai?					
	Apakah organisasi memastikan bahwa informasi kargo yang diterima dari mitra bisnis dilaporkan secara akurat dan diterima tepat waktu?					
	Apakah data relevan dilindungi dalam sistem penyimpanan yang tidak terkait operasional sistem penanganan data utama (apakah ada proses back up data yang diterapkan)?					
	Apakah semua pengguna (user) memiliki ID pengguna untuk penggunaan pribadi, untuk memastikan bahwa kegiatannya dapat terlacak?					
	Apakah ada sistem pengelolaan *password* yang efektif yang diberlakukan untuk memeriksa otentitas *user* dan apakah *user* diminta untuk mengubah *password*-nya minimal setiap tahun?					
	Apakah ada perlindungan terhadap akses yang tidak sah (*unauthorized access*) dan penyalahgunaan informasi?					
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?					
	Apakah ada individu berkualifikasi yang ditunjuk untuk mensupervisi kegiatan kargo?					
	Apakah prosedur diberlakukan untuk memberitahu pihak penegakan hukum dalam kasus kondisi yang tidak normal atau ada kegiatan ilegal yang dideteksi atau dicurigai oleh organisasi?					
	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?					
	Apakah ada proses untuk melacak adanya perubahan tingkat ancaman di sepanjang rute transportasi?					
	Apakah ada peraturan keamanan, prosedur, atau panduan keamanan yang diberikan kepada operator *conveyance* (misalnya, untuk menghindari rute yang berbahaya)?					

No	Faktor	Skor				
		1	2	3	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?					
	Jika digunakan unit pengangkutan kargo tertutup bersegel, apakah ada prosedur terdokumentasi untuk memeriksa adanya tanda-tanda kerusakan segel ketika ada penggantian *conveyance* selama masa 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?					
	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:					
	– Dinding muka					
	– Sisi kiri					
	– Sisi kanan					
	– Lantai					
	– Plafon / Atap					
	– Tutup dalam / luar					
	– Bagian luar/bawah					

(Sumber: ISO 28001 Lampiran A)

3.5. Prosedur Penelitian

Penelitian dilakukan dalam beberapa tahapan yaitu:

1. Identifikasi ruang lingkup asesmen keamanan

   Penelitian dimulai dengan melakukan pemilihan topik dan penentuan perusahaan untuk studi kasus. Kemudian dalam identifikasi ruang lingkup asesmen keamanan dilakukan melalui wawancara dan diskusi dengan staf perusahaan tentang proses bisnis dan aktivitas rantai pasok perusahaan.

2. Melakukan asesmen keamanan

   Asesmen keamanan dilakukan berdasarkan ISO 28001. Daftar kajian kinerja keamanan yang digunakan untuk asesmen keamanan atau mengukur tingkat kesesuaian keamanan perusahaan terhadap sistem manajemen keamanan rantai pasok ISO 28001 terdapat 7 faktor yaitu manajemen keamanan rantai pasok, rencana keamanan, keamanan asset, keamanan personel, keamanan informasi, keamanan barang & *conveyance*, dan unit transportasi kargo tertutup. Responden yang mengisi daftar kajian kinerja adalah manager dan PIC yang bertanggung jawab dalam tiap produk layanan di PT. Pos Logistik Indonesia Kantor Cabang Yogyakarta. Untuk pengisian daftar kajian kinerja digunakan skala likert dari 1-5 seperti pada tabel 2.3.

   Setelah itu dilakukan perhitungan nilai daftar kajian kinerja keamanan yang telah diperoleh. Perhitungan tersebut adalah dalam bentuk persentase. Hasil persentase akan dianalisis dengan metode analisis gap. Persentase yang diperoleh menunjukkan seberapa tingkat kesesuaian sistem manajemen keamanan rantai pasok perusahaan terhadap sistem manajemen keamanan rantai pasok ISO 28001. Apabila tingkat kesesuaian belum tercapai, maka perlu dilakukan pengembangan rencana keamanan. Rencana keamanan yang dikembangkan adalah berdasarkan pada hasil dari penilaian risiko keamanan.

3. Identifikasi risiko keamanan, penyebabnya, dan tindakan pengaman yang ada

   Identifikasi risiko ancaman keamanan serta penyebabnya dan tindakan keamanan yang ada ini diperoleh dengan wawancara dan diskusi dengan manager dan staf perusahaan. Dari hasil wawancara yang didapatkan kemudian dilanjutkan dengan penentuan nilai probabilitas, dampak, dan frekuensi kejadian untuk setiap risiko ancaman keamanan.

4. Menentukan probabilitas, dampak, dan frekuensi kejadian risik

   Untuk mendapatkan nilai probabilitas, dampak, dan frekuensi kejadian risiko dilakukan dengan pengisian kuesioner oleh manajer perusahaan. Penilaian probabilitas, dampak, dan frekuensi kejadian risiko ini sesuai dengan masing-masing kriteria yang telah dibuat berdasarkan diskusi dengan pihak perusahaan. Dalam penilaian probabilitas, dampak, dan frekuensi kejadian risiko digunakan

skala likert dari 1-5. Adapun detail tentang kriteria penilaian yang digunakan adalah sebagaimana terlampir.

5. Menentukan skor risiko

   Dalam menentukan skor risiko digunakan pendekatan FMEA (*Failure Mode and Effects Analysis*) yaitu dengan persamaan berikut:

   $$probabilitas \times dampak \times frekuensi\ kejadian$$

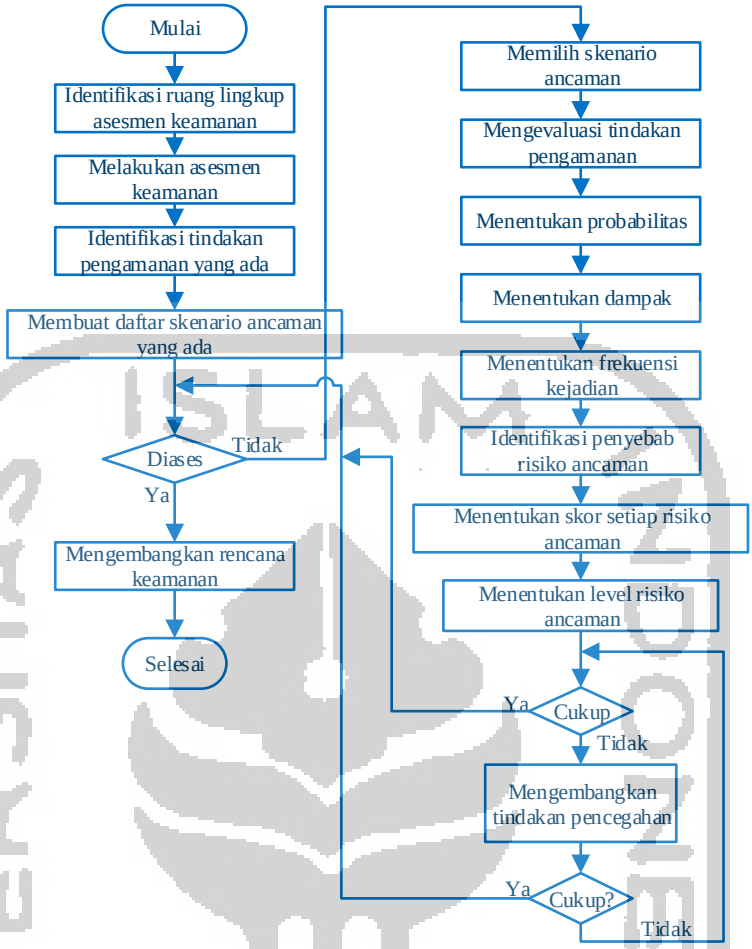
   Perhitungan tersebut dilakukan untuk semua risiko yang teridentifikasi. Dengan persamaan tersebut akan diketahui nilai untuk setiap risiko ancaman keamanan.

6. Menentukan level risiko

   Setelah diperoleh skor risiko kemudian dilakukan pemetaan risiko untuk mengetahui level risiko. Pemetaan risiko ini dilakukan dengan perhitungan (*probability impact matrix*). Level risiko akan menunjukkan seperti apakah tingkatan dari masing-masing risiko yang dihadapi.

7. Menentukan strategi mitigasi dan rencana keamanan

   Berdasarkan hasil dari skor dan level risiko, akan diketahui risiko-risiko yang merupakan risiko kritis yang akan diberikan strategi mitigasi dan rencana keamanan. Dalam menentukan strategi mitigasi dan rencana keamanan dilakukan analisis mengenai penyebab risiko dominan dari risiko kritis yang didapatkan. Penyebab risiko dominan dari risiko kritis inilah yang menjadi prioritas utama dalam penanganan risiko dan penentuan strategi serta rencana keamanan. 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.



Gambar 3.1. Diagram Alir Penelitian