

Perancangan Sistem Manajemen Keamanan Pada Rantai Pasok ISO 28000:2007 Di PT X

Jerim Renai Rumalutur¹, Jani Raharjo²

Abstract: This research is meant to explain the program of security supply chain management in order to get the certification of ISO 28000:2007 at PT. X. Security supply chain management system is used to assure the secure of the supply chain. The research at the PT. X is done by analysing the Gap Analysis between the company and the terms of the ISO 28000:2007. The research result shows us at 9.35% of compatibility with the ISO 28000:2007 terms and condition. The thesis result is going to be used to fix and develop the security supply chain management at PT. X. The development is going to be used to arrange the document to be suitable with the ISO 28000:2007 terms and condition. The systems are. The result of the final Gap Analysis shows at 69,16% of suitability with the ISO 28000:2007.

Keywords: Security supply chain management system, ISO 28000:2007.

Pendahuluan

Setelah kejadian terorisme pada tanggal 11 September 2001 yang terjadi di Amerika Serikat, isu mengenai keamanan rantai pasok menjadi topik yang banyak dibicarakan di kalangan pengusaha, peneliti dan pemerintah. Keamanan pada rantai pasok merupakan hal yang penting bagi perusahaan karena jika terjadi gangguan pada rantai pasok, maka akan mengakibatkan penerunan nilai saham dengan rata-rata 40% (Ditteaman [1]). Besarnya dampak kerugian dari gangguan rantai pasok mendorong negara-negara dan organisasi internasional untuk membuat kebijakan mengenai keamanan rantai pasok. International Standard Organization (ISO) sebagai salah satu organisasi internasional yang juga ikut serta dalam membuat kebijakan dengan menerbitkan ISO 28000 sebagai standar bagi perusahaan untuk menerapkan sistem manajemen keamanan rantai pasok.

PT. X adalah perusahaan manufaktur yang bergerak di bidang *consumer goods* khususnya pembuatan tisu. PT. X yang didirikan pada tahun 2017 di Jawa Timur memproduksi tisu jenis Napkin yang dinamakan sebagai Napkin A dan Napkin B. Dalam proses bisnis yang dijalankan oleh PT. X, keamanan rantai pasok adalah salah satu faktor utama yang perlu dijaga, namun sistem manajemen keamanan rantai pasok yang berdasarkan ISO 28000:2007 masih belum diterapkan oleh PT. X.

Dengan banyaknya manfaat dari penerapan ISO 28000 dan adanya permintaan dari *customer*, tuntutan dari manajemen dan pengontrolan risiko yang masih kurang, maka pihak top manajemen memutuskan untuk menerapkan ISO 28000:2007.

Permasalahan yang dihadapi oleh PT. X adalah untuk memastikan keamanan pada rantai pasok. Hasil perancangan ini diharapkan dapat bermanfaat bagi PT. X untuk mendapatkan sertifikasi ISO 28000:2007. Sertifikasi ISO 28000:2007 dapat membantu PT. X untuk terhindar dari ancaman keamanan pada rantai pasok yang dapat merugikan perusahaan.

Metode Penelitian

Pada bagian ini akan dibahas mengenai metode metode yang digunakan untuk membantu memberikan rancangan perbaikan terhadap permasalahan yang ada.

Manajemen Keamanan Rantai Pasok

Manajemen keamanan rantai pasok adalah penerapan kebijakan, prosedur, dan teknologi untuk melindungi aset rantai pasokan dari pencurian, kerusakan, atau terorisme, dan untuk mencegah masuknya barang selundupan, orang dan senjata ilegal ke dalam rantai pasokan (Ekwall [2]).

Ancaman Keamanan

Ancaman keamanan menurut ISO 28000:2007 diantaranya adalah:

- Ancaman kerusakan fisik dan risiko seperti

^{1,2} Fakultas Teknologi Industri, Jurusan Teknik Industri, Universitas Kristen Petra. Jl. Siwalankerto 121-131, Surabaya 60236. Email: jerimrenai@gmail.com, jani@petra.ac.id

kerusakan fungsi, kerusakan insidensial, ancaman kerusakan karena terror atau aksi kriminal.

- Gangguan operasional dan risiko mencakup kontrol keamanan, faktor manusia dan aktivitas lainnya yang berdampak pada performa, kondisi atau keamanan perusahaan.
- Fenomena alam yang dapat membawa perangkat dan kontrol keamanan bekerja tidak efektif.
- Faktor diluar kontrol perusahaan, seperti kesalahan peralatan atau pemasok.
- Gangguan stakeholder dan risiko seperti gagal memenuhi peraturan yang berlaku atau rusaknya nama baik atau reputasi perusahaan.
- Disain dan instalasi perlengkapan keamanan seperti penggantian alat, pemeliharaan, dan lain-lain.
- Informasi dan manajemen data serta komunikasi.
- Masalah rutinitas operasional.

Manajemen Risiko

Manajemen risiko adalah seperangkat kebijakan, prosedur yang lengkap, yang dipunyai organisasi, untuk mengelola, memonitor, dan mengendalikan eksposur organisasi terhadap risiko (Lee dan Whang [3]). Dalam manajemen risiko terdiri dari beberapa tahapan, dimulai dari identifikasi ancaman keamanan, penilaian risiko, penyusunan kontrol dan implementasi respon risiko. Berikut adalah penjelasan mengenai setiap tahapan dalam manajemen risiko.

Identifikasi Ancaman Keamanan

Identifikasi ancaman keamanan yang mungkin terjadi merupakan proses pertama dalam manajemen risiko. Hasil dari proses ini adalah daftar mengenai ancaman yang mungkin terjadi di perusahaan.

Penilaian Risiko

Proses selanjutnya adalah penilaian risiko. Setiap risiko yang mungkin terjadi dilakukan penilaian masing-masing dengan menggunakan metode *Failure Mode and Effects Analysis* (FMEA). Output dari penilaian risiko adalah tingkat risiko yang didapatkan melalui persamaan berikut ini:

$$\text{Tingkat Risiko} = \text{Severity} \times \text{Occurance} \quad (1)$$

Severity merupakan tingkat keparahan dampak dari suatu risiko. Penilaian *severity* terdiri dari lima tingkat keparahan. Kriteria penilaian *severity* dapat dilihat pada Tabel 1.

Tabel 1. Kriteria Penilaian *Severity*

<i>Rating</i>	<i>Description</i>	<i>Keterangan</i>
1	Tidak Diketahui	Sebelum prioritas ditetapkan, kehilangan telah digantikan bersamaan dengan pergantian keempat prioritas lainnya.
2	Relatif Tidak Penting	Kehilangan yang akan dianggarkan pada pengeluaran operasional normal selama periode yang masih berlangsung.
3	Serius	Kehilangan yang sangat berdampak pada pendapatan dan memerlukan perhatian manajemen senior eksekutif.
4	Sangat Serious	Kehilangan yang dapat mengakibatkan perubahan besar dalam kebijakan investasi dan berdampak besar pada keseimbangan aset.
5	Fatal	Kehilangan yang dapat mengakibatkan rekapitalisasi atau ketidakberlangsungan jangka panjang.

Kriteria penilaian *severity* terbagi menjadi lima tingkat, dimana dari tingkat satu yang tidak diketahui hingga tingkat lima yang memberi dampak fatal. Penilaian berikut adalah *occurance*. *Occurance* merupakan frekuensi terjadinya suatu risiko, kriteria penilaian *occurance* dapat dilihat pada Tabel 2.

Tabel 2. Kriteria Penilaian *Occurance*

<i>Rating</i>	<i>Description</i>	<i>Keterangan</i>
1	Sangat Jarang	Suatu insiden mungkin dapat terjadi pada suatu kondisi yang khusus/luar biasa/setelah bertahun-tahun.
2	Jarang	Suatu kejadian mungkin terjadi pada beberapa kondisi tertentu, namun kecil kemungkinan terjadinya.
3	Sedang	Suatu kejadian akan terjadi pada beberapa kondisi tertentu.
4	Sering	Suatu kejadian mungkin akan terjadi pada hamper semua kondisi.
5	Sangat Sering	Suatu kejadian akan terjadi pada semua kondisi/setiap kegiatan yang dilakukan.

Kriteria penilaian *occurance* terbagi menjadi lima tingkatan, dari tingkat satu yang menunjukkan bahwa kejadian sangat jarang terjadi sampai tingkat lima yang menunjukkan bahwa kejadian sangat sering terjadi.

Penyusunan Kontrol

Setelah Setelah pengelompokkan risiko, tahap selanjutnya adalah menyusun kontrol risiko sesuai dengan daftar risiko keamanan yang terukur. Tabel 3 adalah tindakan kontrol untuk risiko keamanan dan deskripsinya.

Tabel 3. Tindakan Kontrol Ancaman Keamanan

Tindakan	Deskripsi
Eliminasi	Apakah bahaya dapat dieliminasi?
Substitusi	Apakah proses/bahan baku/alat dapat di ganti dengan yang lebih aman?
Kontrol Teknis	Apakah bahaya dapat dilakukan dengan: <i>Isolation/enclosure, Machine guards, Ventilation, Mechanical Aids?</i>
Kontrol Administrasi	Apakah prosedur dapat dikembangkan?
<i>Personal Protective Clothing and Equipment</i>	Melengkapi personil dengan <i>safety tools</i>

Implementasi Respon Risiko

Tahap terakhir dalam melaksanakan manajemen risiko adalah implementasi respon risiko yang dilakukan untuk mengendalikan risiko dengan menerapkan strategi respon risiko yang sudah dirancang. Implementasi juga meliputi monitoring perkembangan risiko dan pengawasan terhadap risiko baru.

Hasil dan Pembahasan

Tinjauan Awal

Tinjauan keamanan rantai pasok PT. X untuk meninjau pemenuhan klausul ISO 28000:2007 yang telah dilaksanakan oleh perusahaan dilakukan dengan menggunakan metode *gap analysis*. *Gap analysis* PT. X dilaksanakan dengan dibagi menjadi dua fase yaitu tinjauan awal dan tinjauan akhir. Tinjauan keamanan rantai pasok awal berupa *gap analysis* dimana dilakukan sebelum pemenuhan klausul ISO 28000:2007 dilaksanakan. *Gap analysis* meninjau klausul ISO 28000:2007 pada klausul 4.1,

4.2, 4.3, 4.4, 4.5, dan 4.6. Hasil dari tinjauan keamanan rantai pasok awal menggunakan metode *gap analysis* dapat dilihat pada tabel 4.

Tabel 4. Hasil Tinjauan Awal

Klausul	Status Kesesuaian Awal		Persentase Kesesuaian
	Ya	Tidak	
	4.1 Umum	0	4
4.2 Kebijakan Manajemen Keamanan	0	12	0%
4.3 Rencana dan Penilaian Risiko Keamanan	2	36	5.26%
4.4 Implementasi dan Operasi	8	22	26.67%
4.5 Pemeriksaan dan Tindakan Perbaikan	0	22	0%
4.6 Tinjauan Manajemen dan Perbaikan Berkelanjutan	0	1	0%
Rata-Rata Persentase Kesesuaian			9.35%

Total persentase tinjauan keamanan rantai pasok awal dengan menggunakan metode *gap analysis* sebesar 9.35%. Angka 9,35% ini menunjukkan bahwa penerapan sistem manajemen keamanan rantai pasok di PT.X masih sangat kurang. Dimana dasar-dasar sistem manajemen keamanan rantai pasok seperti kebijakan keamanan, tujuan dan sasaran keamanan serta penilaian risiko masih belum diterapkan.

Identifikasi dan Penilaian Risiko

Identifikasi dan penilaian terhadap risiko yang mungkin terjadi di perusahaan perlu dilakukan oleh manajemen untuk dapat mengetahui risiko apa saja yang memiliki nilai tingkat risiko yang tinggi ataupun sedang dan masih belum memiliki kontrol/penanganan yang tepat. Identifikasi risiko pada sistem manajemen keamanan rantai pasok dilakukan dengan mendaftarkan rincian setiap kegiatan rantai pasokan yang ada pada perusahaan.

Penetapan nilai *severity* dan *occurance* dilakukan sesuai dengan kondisi di PT.X dimana nilai *severity* didapatkan dari besaran kerugian ekonomi yang ditimbulkan oleh risiko sesuai dengan kondisi perusahaan. Sedangkan nilai *occurance* didapatkan dengan melihat histori kejadian risiko perusahaan. Data ini diambil untuk mengukur performa keamanan perusahaan saat ini, hasil olahan data ini akan dijadikan dasar untuk membuat rencana keamanan. Pengambilan data ini merupakan pelaksanaan salah satu proses manajemen keamanan yaitu penilaian risiko keamanan. Data ini

diambil dengan cara berdiskusi dengan departemen sertifikasi perusahaan.

Perancangan Sistem Manajemen Keamanan Rantai Pasok

Perancangan pada sistem manajemen keamanan rantai pasok dibuat berdasarkan hasil *gap analysis*, dimana klausul-klausul pada ISO 28000:2007 yang masih belum terpenuhi akan dibuatkan rancangannya. Klausul yang tidak dibuatkan perancangannya karena sudah memenuhi saat *gap analysis* awal adalah klausul 4.3.2 tentang hukum, undang-undang dan persyaratan peraturan keamanan lainnya, klausul 4.4.5 tentang dokumen dan pengendalian data. Selain kedua klausul tersebut klausul lainnya akan dibuatkan perancangannya.

Kebijakan Manajemen Keamanan

Kebijakan manajemen keamanan merupakan suatu komitmen perusahaan yang dibuat oleh top management. Kebijakan manajemen keamanan menjadi salah satu persyaratan wajib dari sistem manajemen keamanan rantai pasok ISO 28000:2007 dimana tercantum aspek-aspek komitmen untuk menjaga keamanan rantai pasok. Kebijakan manajemen keamanan PT. X yang mencakup komitmen dari top management terdiri dari tiga aspek sebagai berikut:

- Selalu berkomitmen untuk melindungi karyawan, *property*, informasi, reputasi, dan asset pelanggan perusahaan dari potensi resiko dan ancaman dalam rantai pasokan melalui analisa risiko sesuai dengan ISO 28000:2007.
- Peningkatan berkelanjutan dalam kaitannya dengan keamanan rantai pasok melalui prosedur yang terintegrasi, pencegahan, dan kesiapsiagaan insiden; serta komitmen terhadap ketaatan ketentuan hukum, peraturan perundangan, serta persyaratan lain yang relevan dengan perusahaan.
- Senantiasa meningkatkan kompetensi karyawan agar menyadari dan bertanggung jawab atas aspek keamanan dari kegiatan bisnis perusahaan dan berkontribusi untuk kemajuan perusahaan demi tercapainya visi & misi perusahaan.

Kebijakan keamanan rantai pasok yang dibuat oleh PT. X sudah memenuhi persyaratan ISO 28000:2007 mengenai kebijakan keamanan dimana harus konsisten dengan kebijakan bisnis perusahaan, memberi kerangka kerja dan menggambarkan komitmen perusahaan untuk melakukan perbaikan berkelanjutan pada sistem manajemen rantai pasok.

Tujuan dan Sasaran Manajemen Keamanan

Tujuan dan sasaran manajemen keamanan merupakan pelaksanaan dari kebijakan manajemen keamanan rantai pasokan, yang adalah implementasi konkret dari perusahaan untuk mengurangi risiko, meningkatkan kemampuan bisnis dan meningkatkan reputasi, yang konsisten dengan kebijakan dari unit keamanan rantai pasokan (termasuk komitmen untuk perbaikan berkelanjutan).

Tujuan dan sasaran dibuat berdasarkan inputan dari kebijakan keamanan, penilaian risiko, hukum dan persyaratan keamanan dan tinjauan manajemen. Dari hasil penilaian risiko diketahui bahwa ada satu risiko yang masuk kategori *extreme risk*, tiga risiko yang masuk kategori *high risk*, dan 13 risiko yang masuk kategori *moderate risk*. Dengan hasil ini maka tujuan dan sasaran keamanan PT. X akan dibuat berdasarkan hasil penilaian risiko ini. Tujuan dan sasaran manajemen keamanan rantai pasok PT. X dapat dilihat pada tabel 5 dibawah ini.

Tabel 5. Tujuan dan Sasaran Keamanan PT.X

No	Tujuan	Sasaran
1	Melengkapi persyaratan keamanan rantai pasok	Seluruh area pabrik terpasang CCTV (Area Gudang, Bongkar Muat, Converting, Kantor) Seluruh karyawan memiliki dan menggunakan kartu identitas kerja Downtime akibat dari kerusakan mesin/emboss dibawah atau sama dengan 10% (batas downtime maksimal)
2	Mengurangi kerugian ekonomi yang diakibatkan oleh risiko	dari downtime keseluruhan Persentase kerusakan pengiriman <i>finished goods</i> kurang dari 1% Kejadian pencurian dalam gudang 0
3	Meningkatkan kesadaran karyawan terhadap keamanan rantai pasok	Seluruh karyawan mendapatkan pelatihan keamanan rantai pasok Kejadian kecelakaan kerja 0

Tujuan keamanan PT.X ada tiga bagian yang pertama adalah melengkapi persyaratan keamanan rantai pasok dimana ada dua sasaran yang ingin

dicapai yaitu seluruh area pabrik terpasang CCTV, area yang dimaksud ialah area gudang, area bongkar muat barang, area *converting* dan area kantor. Dengan adanya pemasangan CCTV, PT.X dapat menerima manfaat sebagai berikut.

- CCTV yang berada dilokasi pos *security* dapat memberi informasi pemantauan mengenai kendaraan atau orang yang keluar masuk pabrik, sehingga saat terjadi gangguan keamanan pihak terkait yang menangani dapat menelusuri penyebabnya melalui CCTV.
- CCTV yang berada di area bongkar muat dapat memberi informasi kepada *manager/supervisor* untuk mengetahui kinerja karyawan dan dapat dijadikan bahan bukti saat terjadi gangguan keamanan pada proses bongkar muat.
- CCTV yang berada di area *converting* dapat memberikan informasi kepada *manager/supervisor* produksi untuk mengetahui penyebab gangguan keamanan yang terjadi pada mesin maupun operator di area *converting*.

Sasaran yang kedua untuk mencapai tujuan pertama adalah seluruh karyawan memiliki dan menggunakan kartu identitas kerja.

Tujuan keamanan PT.X yang kedua adalah mengurangi kerugian ekonomi yang diakibatkan oleh risiko dimana ada tiga sasaran yang ingin dicapai yaitu yang pertama *downtime* akibat dari kerusakan mesin/*emboss* berkurang 50%, yang kedua persentase kerusakan pengiriman *finished goods* kurang dari 1%, dan yang ketiga kejadian pencurian dalam gudang nol kejadian.

Tujuan keamanan PT.X yang ketiga adalah meningkatkan kesadaran karyawan terhadap keamanan rantai pasok dimana ada dua sasaran yang ingin dicapai yaitu seluruh karyawan mendapatkan pelatihan keamanan rantai pasok dan kejadian kecelakaan kerja nol kejadian.

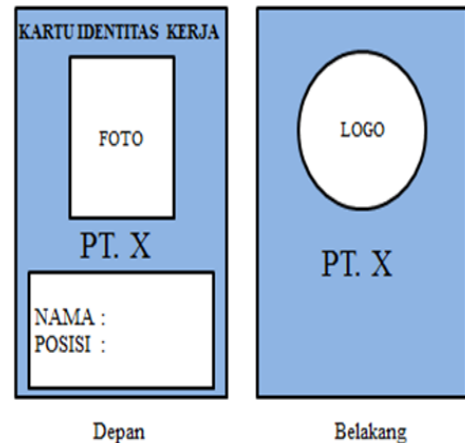
Pengendalian Operasi

Perancangan pada klausul 4.4.6 mengenai pengendalian operasi memiliki tujuan untuk dapat mengontrol dan mengelola risiko dan ancaman keamanan rantai pasokan perusahaan dengan efektif, dan memastikan bahwa proses logistik, arus informasi dan arus modal terkendali dengan efektif sesuai dengan persyaratan yang sudah ditentukan.

Ruang lingkup perancangan pada prosedur ini adalah prosedur berlaku untuk seluruh proses rantai pasokan perusahaan dan untuk pengelolaan dan pengontrolan proses rantai pasokan yang melibatkan pihak-pihak terkait.

Hasil perancangan prosedur kerja untuk pengendalian operasi seperti penjelasan dibawah ini.

- 1) Untuk semua karyawan tetap maupun tidak tetap, perusahaan harus ada kontrak kerja maupun pemutusan kontrak kerja yang tertulis. Karyawan perusahaan wajib memiliki dan menggunakan kartu identitas kerja yang ada foto dan kartu akses untuk keadaan tertentu. Desain kartu identitas kerja seperti gambar berikut ini.



Gambar 1. Kartu Identitas Kerja

- 2) Adanya data kriminal dalam kurung waktu 5 tahun untuk karyawan perusahaan yang bekerja di bagian keuangan, manajemen informasi/data penting, dan barang. Pengunjung wajib mendapatkan persetujuan masuk dan menggunakan lencana visitor dengan ditemani personil yang relevan.
- 3) Personil yang tidak berwenang dilarang memasuki area forklift dan penyimpanan produk.
- 4) Jika ada personil yang tidak berwenang memasuki area truk, *forklift* dan penyimpanan produk dan tidak mendengar teguran, maka segera melapor kepada *security* atau kepolisian setempat.
- 5) Perusahaan dapat memberikan instruksi kerja dan pelatihan yang rinci dan benar kepada operator yang melakukan proses bongkar muat, pemindahan, penumpukan dan penyimpanan produk.
- 6) Adanya catatan tertulis mengenai partisipasi karyawan dalam pelatihan kesadaran keamanan dan simulasi keamanan.
- 7) Perusahaan harus menyediakan program pelatihan tentang respon untuk mencegah perampokan, dan menentukan metode penyelamatan saat personil mengalami ancaman keselamatan.
- 8) Bila diperlukan saat karyawan atau pekerja subkontrak selesai bekerja, lakukan penarikan kartu kerja, kartu akses, kunci atau informasi sensitif lainnya.

Tinjauan Akhir

Tinjauan keamanan rantai pasok akhir PT. X menggunakan metode *gap analysis* untuk membandingkan pemenuhan persyaratan yang telah dipenuhi setelah melakukan perancangan terhadap dokumen-dokumen yang diperlukan ISO 28000:2007. Tinjauan akhir menunjukkan sub klausul yang telah dipenuhi melalui perancangan sistem manajemen keamanan rantai pasok ISO 28000:2007. Tinjauan akhir digunakan untuk sebagai pembanding dengan hasil tinjauan awal saat sebelum dilakukan perancangan sistem manajemen keamanan rantai pasok ISO 28000:2007. Hasil tinjauan keamanan rantai pasok akhir dapat dilihat pada tabel 6.

Tabel 6. Hasil Tinjauan Akhir

Klausul	Status		Persentase Kesesuaian
	Kesesuaian Awal		
	Ya	Tidak	
4.1 Umum	4	0	100%
4.2 Kebijakan Manajemen Keamanan	12	0	100%
4.3 Rencana dan Penilaian Risiko Keamanan	32	6	84.21%
4.4 Implementasi dan Operasi	21	9	70%
4.5 Pemeriksaan dan Tindakan Perbaikan	5	17	22.73%
4.6 Tinjauan Manajemen dan Perbaikan Berkelanjutan	0	1	0%
Rata-Rata Persentase Kesesuaian			69.16%

Total persentase tinjauan keamanan rantai pasok akhir dengan menggunakan metode *gap analysis* sebesar 69,16%. Angka 69,16% ini menunjukkan bahwa penerapan sistem manajemen keamanan rantai pasok di PT.X sudah mengalami peningkatan yang besar dibandingkan saat tinjauan awal. Dimana dasar-dasar sistem manajemen keamanan rantai pasok seperti kebijakan keamanan, tujuan dan sasaran keamanana serta penilaian risiko sudah diterapkan. Namun masih ada beberapa klausul yang belum diterapkan sepenuhnya seperti program keamanan, pengendalian operasi pemantauan dan pengukuran kinerja keamanan, evaluasi sistem, keamanan terkait kegagalan, insiden,

ketidaksesuaian, dan tindakan perbaikan dan pencegahan dan tinjauan manajemen dan perbaikan berkelanjutan.

Simpulan

Tinjauan *Gap Analysis* dilakukan pada PT.X menggunakan checklist dari persyaratan pada setiap klausul sistem manajemen keamanan rantai pasok ISO 28000:2007. Tinjauan *Gap Analysis* awal sebesar 9.35% yang telah dipenuhi oleh PT. X yang menunjukkan bahwa masih banyak temuan dari klausul-klausul yang belum dipenuhi. Perancangan dokumen sistem manajemen keamanan rantai pasok ISO 28000:2007 akan dibuat untuk memenuhi persyaratan yang belum terpenuhi oleh PT. X. Perancangan dokumen meliputi kebijakan manajemen keamanan, penilaian risiko keamanan rantai pasok, tujuan dan sasaran keamanan, tanggung jawab departemen untuk setiap klausul dan prosedurnya.

Perancangan sistem manajemen keamanan rantai pasok ISO 28000:2007 pada PT. X menunjukkan peningkatan, hingga persentase kesesuaian dengan persyaratan klausul-klausul ISO 28000:2007 sebesar 69,16%. Hasil ini menunjukkan rancangan dokumen telah memenuhi persyaratan pada klausul ISO 28000:2007. Persyaratan yang belum terpenuhi adalah program keamanan, pengendalian operasi, pemantauan dan pengukuran kinerja keamanan, evaluasi sistem, keamanan terkait kegagalan, insiden, ketidaksesuaian, dan tindakan perbaikan dan pencegahan dan tinjauan manajemen dan perbaikan berkelanjutan.

Daftar Pustaka

1. Ditteman., *Supply Chain Risk: It's Time to Measure It*, 2010, retrieved from <https://hbr.org/2010/02/is-your-supply-chain-at-risk-1> on 02 February 2019.
2. Ekwall, D., Supply Chain Security – Threats and Solutions. In N. Banaitiene (Eds.), *Risk Management – Current Issues and Challenges*, Rijeka: InTech, 2012, pp. 157-184.
3. Lee, H.L., and Whang, S., *Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management*, Elsevier B.V, Standford, 2004.