International Journal of Safety and Security Engineering
Vol. 11, No. 2, April, 2021, pp. 135-142
Journal homepage: http://iieta.org/journals/ijsse

Analysis of Compliance and Supply Chain Security Risks Based on ISO 28001 in a Logistic Service Provider in Indonesia

Elisa Kusrini*, Kholida Hanim

Department of Industrial Engineering, Faculty of Industrial Technology, Islamic University of Indonesia, Jl Kaliurang Km 14.5 Yogyakarta, Indonesia

Corresponding Author Email: elisakusrini@uii.ac.id

https://doi.org/10.18280/ijsse.110202

Received: 6 March 2021
Accepted: 15 April 2021

Keywords:
safety supply chain, security risk, ISO 28001, logistic service provider

ABSTRACT

Risk of goods and security incidents, such as theft, boycott, smuggling and terrorism are likely to occur in a shipping process, therefore risk controls are needed to reduce the adverse effects. A research on the supply chain security risk management based on ISO 28001 security supply chain is conducted to overcome such problems. The purpose of this research is to analyse compliance & supply chain security risks and propose a mitigation based on ISO 28001 in a logistic service provider in Indonesia. A gap analysis is conducted to assess the compliance of security performance in seven areas, i.e. supply chain security management, security plans, asset security, personnel security, information security, security of goods & conveyance and transportation units closed cargo. The result of the assessment showed that a compliance level of above 75% indicates that the company is ready to implement an ISO 28001. The risk mitigation plan is proposed based on Failure mode effect analysis (FMEA) which calculates the Risk Priority Number (RPN). The RPN value indicates the level of risk where the higher the value, the more critical the risk and become the priority to handle. The mitigation proposed for managing risk are reducing, sharing and avoiding.

1. INTRODUCTION

Supply chain management involves many actors to ensure that the distribution of goods is carried out in the right quantity, quality and on time. The more parties involved make the supply chain vulnerable to uncertainty events. One of the risks that arise in supply chain activities is the supply chain security risk. Closs and McGarrell [1] defined the supply chain security as the application of policies, procedures, and technology, to protect the supply chain assets (products, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the entry of contraband illegitimate, people, or weapons of mass destruction, into the supply chain. Zailani et al. [2] revealed that the supply chain security can collectively affect the operational performance of corporate security among the Malaysian logistics service providers. The supply chain security practices play an important role in providing high quality services in terms of operational performance of supply chain security in developing countries. Security also increases the protection of people's economic conditions, social and physical well-being of humans [3]. Companies that manage the risk of supply chain disruption seriously are more likely to adhere to security initiatives and build safety supplies and can reduce the frequency of supply chain disruptions [4].

One of the initiatives carried out to overcome supply chain security issues is to apply the ISO 28001. In this study, the selection of a security system using the ISO 28001 standard because only ISO 28001 in ISO series standard that specifies the supply chain security management system for the protection of people, property, information and infrastructure in companies and or organizations that participate in local, national and international supply chain [3]. ISO 28001 is a series of International Standard Management Systems that sets the requirements and aspects of a supply chain security management system. This standard can be applied by all organizations involved in supply chain activities namely manufacturing, services, warehousing, or transportation (air, train, road and sea) [5]. By implementing the ISO 28001 in a company, it is expected to improve supply chain security, to increase customer satisfaction, and to raise company competitiveness.

The purpose of this research is to analyse compliance & supply chain security risks and propose a risk mitigation based on ISO 28001 in a logistic service provider (LSP) which is a state-owned company in Indonesia. Risk mitigation based on ISO 28001 is preceded by assessing the level of compliance using a gap analysis to assess the company's security performance, subsequently proceed with a risk evaluation using Failure Mode and Effects Analysis (FMEA) and mitigation plan with a reduce, avoid or share strategy.

This paper is organised as follows. First, it discusses literature review on supply chain security management followed by research methodology, results and discussion and finally, conclusions, managerial implications and potential future research are explained.

2. LITERATURE REVIEW

According to Pressman (2002) [6], risk management is a structured approach/methodology in managing uncertainty related to threats; a series of human activities. In a security

management system, risk management is used to assist companies in making a security plan. Closs and Mc Garrell [1] defined supply chain security as the application of policies, procedures, and technology to protect supply chain assets (products, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the entry of contraband illegitimate, people, or weapons of mass destruction, into the supply chain.

Table 1. Related research on supply chain security management

No	Researcher	Case study area		Supply chain risk management					Approach used					Research focus
		Manufacture industry	Service industry	Risk identification	Risk assessment	Mitigation strategy	Risk agent	Relationship	FMEA	ANP	QFD	Causal Effect Diagram	Other Approach	
1	Park (2016)	√						√					SEM (*Structural Equation Model*)	Relationship between risk trends, supply chain security practices, and supply chain disruptions.
2	Pope (2008)	√	√										Literature review	Dimensions of supply chain security.
3	Scholliers (2016)												Modeling	Improved container safety at the port.
4	Salmela (2010)	√		√	√	√							MEF Method (Mobile Enterprise Factory) LOGRM (Logistics Modelling for Risk Management) SCSTM (Supply Chain Security and Technology Management)	Increased supply chain security.
5	Yang (2011)		√	√	√	√	√						Statistical descriptive analysis Factors analysis Loss exposure matrix	Operational risk, physical risk, and financial risk.
6	Liu (2018)		√	√	√	√	√		√					Risk of work accident.
7	Leong (2014)		√	√									Statistical analysis	Risk of cargo crime (theft).
8	Yang & Wei (2013)		√					√					Factors analysis & regression analysis	Dimensions of supply chain security & effect of security management on security performance.
9	Lam & Dai (2015)		√							√	√			Develop a security service provider logistics design based on customer demand.
10	Zailani (2015)		√					√					Partial Least Square Analysis	The effect of supply chain security on the operational performance of a company's security.
11	Niekerk (2017)	√		√									Thematic Analysis	Risk of piracy, syndicate and theft.
12	Gutta (2012)		√										Statistical descriptive analysis	Supply chain security measures to investigate the perceptions of manager on supply chain security threats and regulations.
13	Speier (2011)			√	√	√							Multi-method approach to identify key safety and security initiatives	Product safety and security risks.
14	Soeanu (2015)		√	√	√	√							Probabilistic model: Continuous Stochastic	Transportation risk.

											Logic (CSL) & Probabilistic Computation Tree Logic (PCTL)	
15	Vikaliana (2017)		√	√							Risk Management	Risk of human resources management, business competition, shipping errors, damage to goods, theft, warehouse fire.
16	Jenlina (2013)	√		√	√	√					Enterprise Risk Management	Supply risk & demand risk.
17	Kusrini & Hanim (2019)		√	√	√	√	√	√	√		ISO 28001	Supply chain security risk.

Based on Ref. [5], the security management system for a supply chain covers aspects including finance, manufacturing, resources, and facilities and activities in the supply chain system such as storage, production, and movement of goods. The supply chain itself is defined as a set of interrelated resources and processes, which started from the use of raw materials to the delivery for consumers with various types of transportation.

Research on the supply chain security management has been carried out by many researchers. The focus of previous studies addresses several issues such as the linkages between supply chain security and supply chain disruptions [4] and the effect of security management on the security performance [2, 7], the supply chain security risk management [6, 8-15]. Other studies include the dimensions of supply chain security [4], the development of models to improve the container security at port [16], the development of security design for logistics service providers [17], and the supply chain security measurement [18]. Various case studies are researched, for both the manufacturing and service industries. Case studies on risk security system in manufactures are conducted by [4, 8, 12, 15], while case study in service industries conducted by [2, 6, 7, 9-11, 14, 17-19] conducted in both. Various methods are employed to analyze security risk management, among others, such as FMEA [10], statistical analysis [9, 11, 14], modelling [8], literature review [6], Analytical Network Process (ANP), Quality Function Deployment (QFD), thematic analysis [12], Enterprise Risk Management [15], and multi-method approaches [13] as shown on Table 1.

Based on the literature review, it can be concluded that supply chain risk management research has different focuses, scope, activities and approaches. The scope of activities in risk management analysis such as risk identification, risk causes, risk assessment, and determination of risk mitigation strategies have not been fully carried out by each researcher. Therefore, this study will conduct supply chain security risk management with a complete series of activities, namely identification of risks and their causes, risk assessment, and determination of risk mitigation strategies. Furthermore, research focused on assessing the readiness to implement system security standards such as ISO 28001 has not been widely discussed. Therefore, this research will complement the shortcomings of the previous research by conducting a risk assessment to assess the readiness of the organization in implementing a supply chain security management system. The security plan is developed based on the results of the risk assessment obtained by identifying the risks, the causes of risks, the existing safeguards, determining the probabilities, severities, and the frequency of risk events. By discovering the causes of risk, hopefully a more appropriate security plan can be developed.

3. RESEARCH METHODS

3.1 Security assessment

This research begins by conducting a security assessment based on the list of performance studies contained in the ISO 28001. There are seven factors in the list of performance studies, namely supply chain security management, security plans, asset security, personnel security, information security, security of goods & conveyance, and transportation units closed cargo [20]. These factors are listed in a questionnaire to assess the compliance score ranging from 1-5 (1= not ready and very low conformance to security standard, 5 = ready and high conformity to security standard). The level of conformity is state in percentage that would be analysed using gap analysis method. The percentages obtained indicated the level of conformity of the company's supply chain security management system to the ISO 28001 supply chain security management system. After discovering the level of conformity, then the development of a security plan which was based on the results of the security risk assessment is conducted.

3.2 Risk assessment

The risk assessment begins with a series of interview and questionnaire to managers and staffs to identify risk and the cause. The information obtained from the interview consist of business process, list of risk, and security risk that may be encountered by the company and analysing the root causes. The participants are required to fill in questionnaire to determine probability, severity, and frequency of the risk event with a scale of 1-5 (1 = low, 5 = very high), subsequently the result from the interview and questionnaire will be used to measure risk score. In calculating the risk score, the FMEA (Failure Mode and Effects Analysis) approach is used to obtain the RPN (Risk Priority Number) value by the following formula:

$$probability \times severity \times frequency$$

The RPN value indicates the level of risk where the higher the value the more critical the risk and become the priority to handle.

3.3 Security plan and mitigation

The results of the risk level is used to determine the mitigation strategy and the security action plan for critical risks. The mitigation strategies and the security action plan is composed based on the causes of each critical risk. The mitigation plan is expected to reduce the probability, severity, or frequency of the risk event therefore it can help the company to maintain its risk in to an acceptable level.

4. RESULTS AND DISCUSSION

4.1 Security assessment results

The security assessment carried out based on the performance studies list of the ISO 28001 security supply chain included 7 factors, namely the supply chain security management, the security plans, the asset security, the personnel security, the information security, the security of goods and conveyance, and the closed cargo transportation units. The gap analysis was conducted to assess the differences of safety condition between existing and standard in the ISO 28001 security supply chain [21]. A Likert scale of value 1-5 was used to score degree of compliance. The result value was in the form of a percentage. The greater the percentage indicates the level of compliance of the company with ISO 28001 [21].

The results of the assessment showed that the level of conformity of each factor as follows: supply chain security management factor is 92.5%, the security plan is 83.33%, the asset security is 87%, the personnel security is 90%, the information security is 86.43%, the security of goods safety and conveyance is 91.67%, and the closed cargo transportation units is 88.39% as shown in Table 2. These results, which in range of percentage values of 75%-100% indicated that the organization was ready to implement the ISO 28001 and conducted certification [22]. In order to increase the company's readiness to complete the supply chain security management system and conduct the ISO 28001 certification, it is necessary to develop a security management based on the results of a security risk assessment.

4.2 Risk assessment results

The risk assessment was carried out by the FMEA method which started with the identification of risks, the existing safeguards, the causes of risks, probabilities, severities, and the frequency of risk events through interviews and discussions with managers and company staff. The determination of the value of the probability, severity, and frequency of risk, was obtained by filling out the questionnaire with the Likert scale of 1-5.

In the risk assessment, the calculation of the RPN (Risk Priority Number) value was obtained from the multiplication of the probability, severity, and frequency of risk event [23]. The RPN value calculation aims to determine the potential risk or the most critical level of risk by taking into account the risks that have a high probability of occurrence and have a large severity, as well as opportunities to improve by detecting failure modes before adverse severity occur [24].

Based on the interviews and discussions, 32 security risks in the supply chain were obtained. Then the critical RPN value or the average RPN value was calculated. This critical RPN value was used to determine the critical risk. Critical risk is the risk that has a higher RPN value than the critical RPN value. [25]. Out of 32 risks, there were 12 critical risks, or the RPN values which were higher than the critical RPN values. The 12 risks included the damage to the goods in the process of loading the goods (14), the inaccuracy in the number of goods in the process of loading the goods (15), the damage to the goods in the process of unloading the goods (16), the inaccuracy in the number of goods in the process of unloading the goods (17), the damage to the goods in the process of deconsolidation/consolidation of the goods (18), the damage to the goods in the process of shipping the goods (21), the presence of criminal acts in the process of shipping the goods (22), road accidents during the shipping (23), vehicle damage when shipping (24), vendors took over the company's customers under-the-table (30), the company's customers contacted the company's vendors directly under-the-table (31), complaints from the customers due to the longer lead time of the shipment (32).Value of RPN is shown in Table 3.

After obtaining the results of the risk analysis using FMEA and RPN, then risks are mapped with probability impact matrix to determine mitigation priorities. The probability impact matrix is one method of risk detection that aims to determine the priority area of risk by considering severity and probability [26]. The calculation of the probability impact matrix only uses two criteria to determine risk priority, namely the probability value and the severity value; which is different from the RPN calculation which uses three criteria (probability, severity, and frequency). Based on the probability impact matrix as shown in Figure 1, there are 10 critical risks, namely the high level risks, including the customers' complaint due to the shipment's longer lead time (32), the employees do not work according to the SOP (9), the employees abuse their authority (10), misinformation happens during communication (13), damage to the goods in the process of shipping the goods (21), criminal acts in the process of shipping the goods (22), road accidents during the shipping (23), vehicle damage when shipping (24), earthquake (26), and fire (1).

Table 2. Level of compliance

Factors	Total Point	Highest Score	The Highest Score	Actual Score	Percentage of Compliance to ISO 28001
Management of Supply Chain Security	2	5	10	9.25	92.50%
Security Plan	3	5	15	12.5	83.33%
Asset Security	5	5	25	21.75	87.00%
Personnel Security	4	5	20	18	90.00%
Information Security	7	5	35	30.25	86.43%
Goods and Conveyance Security	6	5	30	27.5	91.67%
Closed Cargo Transport Units	4	5	20	17.68	88.39%

Table 3. Risk Priority Number (RPN) calculation

Factors	Risk Number	Risk of Security Threats	Probability	Severity	Frequency	RPN
Threats to Physical Asset Building	1	Fire	1	5	1	5
	2	Leakage	2	1	1	2
	3	Criminal Theft	1	3	1	3
	4	Destructive Action	1	3	1	3
Threats to Physical Asset Office Equipment	5	Lost equipment	1	3	1	3
	6	Equipment Damage	2	2	2	8
Threats to Physical Asset Transportation Unit	7	Lost vehicle spare parts	2	3	1	6
	8	Vehicle damage	3	3	1	9
Personnel Threats	9	The employees do not work according to the SOP	4	3	1	12
	10	The employees abuse their authority	4	3	1	12
Threats to Data / Information	11	Misuse of information by anyone	1	2	1	2
	12	Leakage of company secrets	1	3	1	3
	13	Misinformation happens during communication	4	3	1	12
Threats to the Process of Loading Goods	14	Damage to the goods	4	2	4	32
	15	Inaccuracy in the number of goods	4	2	5	40
Threats to the Process of Unloading Goods	16	Damage to the goods	4	2	4	32
	17	Inaccuracy in the number of goods	4	2	5	40
Threats to the Deconsolidation / Consolidation of Goods	18	Damage to the goods	4	2	4	32
Threats to the Goods Storage Process	19	Damage to the goods	1	2	4	8
	20	Lost goods	1	2	1	2
Threats to the Process of Goods Shipment	21	Damage to the goods	4	3	4	48
	22	A criminal act	4	3	4	48
	23	Road accidents during shipping	4	3	4	48
	24	Damage to the vehicle when shipping	4	3	3	36
Threats to Natural / Environmental Disasters	25	Volcanic eruption	1	3	1	3
	26	The earthquake	2	4	1	8
Business Partner Threats	27	Non-compliance of business partners with company rules	4	1	3	12
	28	Delay in arrival of the vehicle	2	1	3	6
	29	The vehicle does not meet specifications	2	2	3	12
	30	Vendors took over the company's customers under-the-table	4	2	3	24
	31	The company's customers contacted the company's vendors directly under-the-table	4	2	3	24
Threats to reputation	32	Customers complaints due to the shipment's longer lead time	5	3	3	45
		RPN Total				613
		Critical Value of RPN				19.16

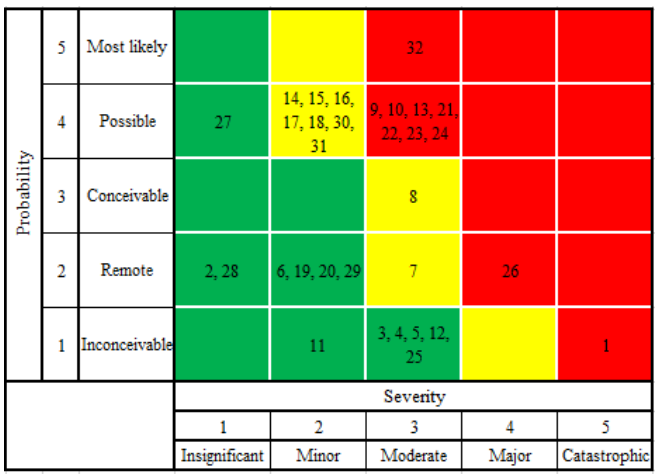

Figure 1. Probability impact matrix

4.3 Risk assessment results

Based on the probability impact matrix, there were 10 critical risks out of 32 supply chain security risks. In this research, the mitigation strategy was focused on 10 critical risks obtained from the probability impact matrix. The Risk Management Professional Certification Agency states that there are 4 mitigation strategies that can be implemented to respond to risks, namely: avoiding risks, which is by stopping activities or services that increase risks; reducing risks with taking action to reduce the probability and/or severity of risks; sharing the risks which are faced with other parties; and accepting the risks, which is accepting the level of risks that occurs (the risks are still within tolerance); and maintaining/managing risks so as not to increase to higher level. In order to develop a mitigation strategy and an appropriate security plan, the causes of the critical risks must be considered. Table 4 shows Security plans & risk mitigation strategies.

The risk of complaints from customers is due to the longer delivery lead time caused by lack of a logistics network in eastern Indonesia. This led to the use of other logistics partners which caused difficulties in controlling the movement of goods. To reduce this risk, a reduction strategy is carried out by making new policies related to regulations and agreements with logistics services, as well as monitoring and evaluation for partners.

The risk of employees working improperly and abusing their authority is due to their lack of knowledge of Standard Operating Procedures (SOP) and lack of supervision. This risk is reduced by conducting training to increase their understanding of the importance of working according to SOPs, and complying with company regulations. This is in line with the results of research by Pradipta et al. [27] which states that employees who understand the importance of working according to SOPs are less likely to violate them. To improve the supervision system for each job, the regulations related to punishment for workers who do not obey the SOPs can be proposed [27-30]. Pradipta et al. [27] and Dyanita [30] also state that a good communication between workers can also influence them to obey the SOPs.

The risk of misinformation during communication was caused by inaccurate employees and lack of supervision. To reduce this risk, a mitigation strategy was provided through training about the effective communication, working in concentration, conscientious working, working in accordance with the SOPs and improving the supervision as well as inserting the culture of orderliness, discipline, and precision in working. Mistakes can be avoided by increasing the job training and the staff education in working accordance with the SOPs [9].

The risk of damage goods during the process of the goods shipment was due to the improper arrangement and packing of the goods. To reduce this risk, a mitigation strategy was provided by increasing the training for the employees. [17] state that a culture of security and training can increase employees' knowledge about how to deal with security risks. Prasetyo [31] also states that by increasing the training for the employees, it can overcome employees' carelessness at work.

The risk of criminal acts in the process of shipping goods usually occurs due to unsafe routes and unsafe resting places. To reduce this risk, an avoidance strategy is given by avoiding less safe routes or rest areas, this is in line with studies [14, 17] which stated to choose a route with a lower risk. Furthermore, the reduction strategy is to provide education to employees about precautions [15], safe routes and rest areas, as well as overseeing the safety of the delivery process.

The risk of accidents on the road during shipping was caused by the sleepy drivers. To reduce the risk, the strategy of reducing was provided by giving the drivers a socialization about safety in driving and by applying the pre-drive nap for them, which was by taking a nap before driving/traveling, in order to help their body's readiness for night driving or long-distance driving. This is in line with the research [15, 32], which recommends adequate rest for drivers, while Sari et al. [32], also recommends that drivers should drink enough mineral water during the trip to overcome drowsiness while driving which is also in accordance with the statement from the National Sleep Foundation. The second strategy was to share by applying insurance for both the drivers and the vehicles.

Risk of damage to the vehicles during the shipment was caused by overloaded vehicles, the vehicles' lifetime, and the drivers' skills. To reduce the risk, the strategy of reducing was provided with by the maintenance for the vehicles, the vehicles' usage according to their capacities and ages, and the selection of the right drivers. Sari et al. [32] also reveals that a vehicle inspection should be done first before driving, and never force to drive a vehicle which is not roadworthy.

This earthquake risk was caused by natural factors because the company, as the case study, was located in an area prone to earthquakes. To reduce the risk, the strategy of reducing was provided by forming a disaster preparedness organization, making SOPs on disaster management and disaster response procedures, making inventories of emergency support resources, organizing disaster management simulation trainings [33, 34]. To secure the owned value of assets, the company has implemented the strategy of sharing, namely applying insurance.

The risk of fire was caused by smoking in any place, and electrical short circuit. To reduce the risk, the strategy reducing was provided by putting up stickers/posters about smoking bans in places which were vulnerable to fires [27]. The socialization of fire hazards and fire simulation training, planning fire emergency preparedness, and completing facilities and fire extinguishers [35-37]. To secure the owned value of assets, the company has implemented the strategy of sharing, namely applying insurance.

Table 4. Security plans & risk mitigation strategies

Risk Number	Risk Event	Mitigation Strategies	Security Plan Actions	PIC	Planning Time
32	Customers complaints due to the shipment's longer lead time	*Reduce*	Making new policies	Manager BO & Supervisor	6-12 months
9	The employees do not work according to the SOP	*Reduce*	Increasing trainings Improve the supervision system for each job & communication	Supervisor	3 months
10	The employees abuse their authority	*Reduce*	Increasing trainings The regulations related to punishment for workers who do not obey the SOPs	Supervisor	3 months
13	Misinformation happens during communication	*Reduce*	Increasing trainings Improving the culture of orderliness, discipline, and precision in working	Supervisor	3 months
21	Damage to the goods	*Reduce*	Increasing trainings Improve the performance checker	Manager BO & Supervisor	6-9 months
		Share	Applying insurance		Already implemented

Risk Number	Risk Event	Mitigation Strategies	Security Plan Actions	PIC	Planning Time
22	A criminal act	*Avoid*	Providing education to the employees	Manager BO & Supervisor	3-6 months
		Reduce	Supervising the shipping process		
			Avoiding the less safe routes or rest areas		
23	Road accidents during shipping	*Reduce*	Select the right driver	Manager BO & Supervisor	3 months
			Ensure adequate rest for drivers		
		Share	Applying insurance		Already implemented
24	Damage to the vehicle when shipping	*Reduce*	Routine maintenance for the vehicles	Manager BO & Supervisor	6-9 months
			Improve the supervision of quality management in business partners		
			Selection of the right drivers		
26	The earthquake	*Reduce*	Provide a disaster preparedness organization	Manager BO & Supervisor	6-12 months
			Making SOPs on disaster response procedures		
			Making inventories of emergency support resources		
			Organizing disaster management simulation trainings	Manager BO & Supervisor	3 months
		Share	Applying insurance		Already implemented
1	Fire	*Reduce*	Planning fire emergency preparedness	Manager BO & Supervisor	3-9 months
			Completing facilities and fire extinguishers		
			Organizing simulation trainings	Manager BO & Supervisor	3 months
		Share	Applying insurance		Already implemented

5. CONCLUSIONS

Analysis of compliance & supply chain security risks based on ISO 28001 is conducted by assessing the level of conformity using a gap analysis, subsequently proceed with a risk evaluation and mitigation plan. Based on this study, the results of security assessment show that the company is ready to complete the Supply Chain Security Management System based on ISO 28001 and carry out certification with the value above 75% for all factor of assessment. The results of risk assessment based on risk levelling using probability impact matrix show that 10 out of 32 risks are critical risks that need to be managed. Based on the analysis on causes of risk, mitigation strategies to manage 10 critical risks are 'reduce, share, and avoid'.

The managerial implication of this research is that the application of a security management system needs to get the focus of the company because it gives an organization the ability to plan, evaluate and mitigate risks along its supply chain. security management can help avoid all kinds of risks, threats that disrupt business, and for recover faster if something goes wrong thereby increasing supply chain resilience.

In order to implement compliance & supply chain security risks based on ISO 28001, organizational readiness and investment in various aspects ranging from preparation of people (awareness, training), infrastructure, organization and governance are required. This provides an opportunity for further research to analyse how much investment is needed and the benefits to be obtained and how to manage communication and coordination with business partners to implement the security system effectively.

This study has a limited number of samples used, so further research is needed on a larger number of logistics service providers to find out the security systems and risks faced on a wider industrial scale.

REFERENCES

[1] Closs, D.J., McGarrell, E.F. (2004). Enhancing security throughout the supply chain. Special Report Series IBM Center for The Business of Government. Washington, USA.

[2] Zailani, S.H., Subaramaniam, K.S., Iranmanesh, M., Shaharudin, M.R. (2015). The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy: Security culture as moderator. International Journal of Physical Distribution & Logistics Management, 45(7): 652-673. https://doi.org/10.1108/IJPDLM-12-2013-0286

[3] Aiguokhian, E. (2013). Supply Chain Security Using RSA Algorithm (A Theoretical Frame Work). Thesis. Master's Degree Programme in Industrial Management, Savonia University, Savonia, Finland.

[4] Park, K., Min, H., Min, S. (2016). Inter-relationship among risk taking propensity, supply chain security practices, and supply chain disruption occurrence. Journal of Purchasing & Supply Management, 22(2): 120-130. https://doi.org/10.1016/j.pursup.2015.12.001

[5] ISO 28000:2007 Specification for Security Management Systems for The Supply Chain—Requirements.

[6] Vikaliana, R. (2017). Faktor-faktor risiko risiko dalam perusahaan jasa pengiriman. Jurnal Logistik Indonesia, 01: 68-76. https://doi.org/10.31334/jli.v1i1.128

[7] Yang, C., Wei, H. (2013). The effect of supply chain security management on security performance in container shipping operations. Supply Chain

Management: An International Journal, 18(1): 74-85. https://doi.org/10.1108/13598541311293195
[8] Salmela, H., Toivonen, S., Scholliers, J. (2010). Enhancing supply chain security with vulnerability management and new technology. IET Intelligent Transport Systems, 4(14): 307-317. https://doi.org/10.1049/iet-its.2009.0124
[9] Yang, Y. (2011). Risk management of Taiwan's maritime supply chain security. Safety Science, 49(3): 382-393. https://doi.org/10.1016/j.ssci.2010.09.019
[10] Liu, Y., Kong, Z., Zhang, Q. (2018). Failure modes and effects analysis (FMEA) for the security of the supply chain system of the gas station in China. Ecotoxicology and Environmental Safety, 164: 325-330. https://doi.org/10.1016/j.ecoenv.2018.08.028
[11] Leong, C.E. (2014). A research on supply chain security in Malaysia. International Journal of Supply Chain Management, 3: 85-93.
[12] Niekerk, S.V., Niemann, W., Kotze, T., Mocke, K. (2017). Supply chain security orientation in the pharmaceutical industry. Southern African Business Review, 21: 446-479.
[13] Speier, C., Whipple, J.M., Closs, D.J., Voss, M.D. (2011). Global supply chain design considerations: Mitigating product safety and security risks. Journal of Operations Management, 29(7): 721-736. https://doi.org/10.1016/j.jom.2011.06.003
[14] Soeanu, A., Debbabi, M., Alhadidi, D., Makkawi, M., Allouche, M., Belanger, M., Lechevin, N. (2015). Transportation risk analysis using probabilistic model checking. Expert Systems with Applications, 42(9): 4410-4421. https://doi.org/10.1016/j.eswa.2014.12.052
[15] Jenlina. (2013). Desain risk management untuk rantai pasok PT. X. Jurnal Ilmiah Mahasiswa Universitas Surabaya, 2: 1-19.
[16] Scholliers, J., Permala, A., Toivonen, S., Salmela, H. (2016). Improving the security of containers in port related supply chains. Transportation Research Procedia, 14: 1374-1383. https://doi.org/10.1016/j.trpro.2016.05.210
[17] Lam, J.S.L., Dai, J. (2015). Developing supply chain security design of logistics service providers: An analytical network process-quality function deployment approach. Supply Chain Management: An International Journal, 45(7): 674-690. https://doi.org/10.1108/IJPDLM-12-2013-0293
[18] Gutta, M.J. (2012). Supply chain security measures – the business perspective. The Research Project of The National Science Centre Poland. 227-250.
[19] Pope, J.A. (2008). Dimensions of Supply Chain Security. Southern Business Review, 21-27.
[20] ISO 28001 Security Management Systems for The Supply Chain — Best Practices for Implementing Supply Chain Security — Assessments and Plans.
[21] Picard, M., Renault, A., Barafort, B., Cortina, S. (2016). Measuring readiness for compliance: a gap analysis tool to complete the TIPA process assessment framework. Springer International Publishing Switzerland, 633: 106-116.
[22] Fernando, J.M., Purwanggono, B., Adi, P. (2017). Analisis Kesiapan Sertifikasi ISO 9001:2015 Pada PT. Wijaya Nagatsupazki dengan Menggunakan Metode Gap Analysis. eJurnal Teknik Industri Universitas Diponegoro, 6: 1-10.
[23] Novanto, M.H. (2008). Perancangan Sistem Manajemen Keamanan Rantai Suplai Perusahaan S Berdasarkan ISO 28000:2007. Skripsi. Program Studi Teknik Industri, Universitas Indonesia, Depok, Indonesia.
[24] Sinaga, Y.Y., Bintang, C., Adi, T.W. (2014). Identifikasi dan Analisa risiko kecelakaan kerja dengan metode FMEA (Failure Mode dan Effect Analysis) dan FTA (Fault Tree Analysis) di proyek jalan tol Surabaya-Mojokerto. Jurnal Teknik POMITS, 1: 1-5.
[25] Suryani, F. (2018). Penerapan metode diagram sebab akibat (fish bone diagram) dan FMEA (Failure Mode and Effect Analysis) dalam menganalisa risiko kecelakaan kerja di PT. Pertamina Talisman Jambi Merang. Journal Industrial Servicess, 3: 63-69.
[26] Nanda, L., Hartanti, L.P.S., Runtuk, J.K. (2014). Analisis risiko kualitas produksi miniatur bus dengan metode failure mode and effect analysis pada usaha kecil menengah niki kayoe. Jurnal GEMA AKTUALITA, 3: 71-82.
[27] Pradipta, N.R., Kurniawan, B., Jayanti, S. (2016). Analisis kepatuhan pelaksanaan Standard Operational Procedure (SOP) pada pekerja kelistrikan di PT. Angkasa Pura I Semarang Tahun 2016. Jurnal Kesehatan Masyarakat, 4: 537-548.
[28] Agushinta, L., Wijaya, R.A.K. (2016). Pengaruh penerapan kesehatan dan keselamatan kerja terhadap kecelakaan kerja karyawan. Jurnal Manajemen Bisnis Transportasi dan Logistik, 2: 287-295.
[29] Putri, F.A., Suroto, S., Wahyuni, I. (2017). Hubungan antara pengetahuan, praktik penerapan SOP, praktik penggunaan APD dan komitmen pekerja dengan risiko kecelakaan kerja di PT. X Tangerang. Jurnal Kesehatan Masyarakat, 5: 269-277.
[30] Dyanita, F. (2017). Kepatuhan terhadap SOP ketinggian pada pekerja konstruksi. The Indonesian Journal of Occupational Safety and Health, 6(2): 225-234. https://doi.org/10.20473/ijosh.v6i2.2017.225-234
[31] Prasetyo, G. (2018). Analisis kualitas layanan pengiriman barang menggunakan pendekatan six sigma di PT. TIKI JNE Kota Bandar Lampung. Skripsi. Program Studi Manajemen Fakultas Ekonomi dan Bisnis, Universitas Lampung, Lampung, Indonesia.
[32] Sari, W.P., Mahyuni, E.L., Salmah, U. (2015). Faktor-faktor yang mempengaruhi potensi kecelakaan kerja pada pengemudi truk di PT. Berkatnugraha Sinarlestari Bela Wan tahun 2015, 4: 1-12.
[33] BNPB. (2017). Buku Pedoman Latihan Kesiapsiagaan Bencana: Membangun Kesadaran, Kewaspadaan dan Kesiapsiagaan dalam Menghadapi Bencana. BNPB.
[34] Morib, M. A. (2013). Mitigasi bencana dan analisis risiko gempa pada bangunan gedung di Yogyakarta. Majalah Ilmiah UKRIM, 63-72.
[35] International Labour Office. (2018). Manajemen Risiko Kebakaran.
[36] Putra, B.K. (2010). Pencegahan dan penanggulangan kebakaran di PT. INKA (persero) Madiun Jawa Timur. Laporan Khusus Program D3 Hiperkes dan keselamatan Kerja Universitas Negeri Sebelas Maret, Surakarta, Indonesia.
[37] Hastutik, F.Y. (2010). Upaya pencegahan dan penanggulangan bahaya kebakaran di PT. Semen Gresik (persero) Tbk pabrik Tuban Jawa Timur. Laporan Khusus Program D3 Hiperkes dan keselamatan Kerja Universitas Negeri Sebelas Maret, Surakarta, Indonesia.