Chapter 15
Risk Management in Logistics

Hui Ming Wee[1], Mauricio F. Blos[2], and Wen-Hsiung Yang[3]

[1] Industrial and Systems Engineering Department,
Chung Yuan Christian University, Chungli, Taiwan
weehm@cycu.edu.tw
[2] SONY do Brasil Ltda, Supply Chain Solutions, Manaus – AM, Brasil
blos31@yahoo.com.br
[3] Management School, University of Liverpool
Liverpool L69 3BX, UK
jhs.why@gmail.com

Abstract. Due to the complex market and business environment, undesirable disruptions in logistics can affect enterprises and weaken its business strength. Risk Management has become the key in avoiding business losses. Logistics interruption can come from an unforeseen exogenous event such as an earthquake or from an endogenous event, like the Toyota Quality recalls in 2010 that interrupted enterprise logistic operations and degraded its performance (Trkman & McCormack, 2009). In this chapter, the risk management in logistics is studied from the process flow perspective. The topics discussed consist of logistics processes, risk management strategy, risk management process in logistic, and enterprise performance evaluation. Several risk management theories and framework from the literature are presented in the chapter. The aim is to provide valuable insights for enterprises through understanding the essential risk management concepts in logistics.

Keywords: Risk management, Logistics, Risk drivers, Vulnerability, Risk preference, Mitigation, Consequence/probability matrix.

1 Introduction

Due to the complex market and business environment, the increasing globalization resulted in a complex logistics network. To adapt this complexity, logistics has provided more services, such as vendor managed inventory (VMI) and cross-docking warehouse distribution as a business strategy. At the same time, undesirable disruptions in logistics affect enterprises and weaken its business strength. For example, the 2010 Iceland volcano eruption disrupted flight schedules; other factor such as wage increase may force manufacturing plants to relocate.

Logistics is a process linking the activities of product manufacturing from suppliers to customers. The Journal of Logistics Managements (1998) defined logistics as the "process of planning, implementing, and controlling the efficient and effective

J. Lu, L.C. Jain, and G. Zhang: Handbook on Decision Making, ISRL 33, pp. 285–305.
Springerlink.com

flow of storage goods, services, and related information from the point of origin to the point of consumption for the purpose of conforming to customer requirements". From the perspective of the logistics function, logistics is managing the physical delivery and storage in an efficient way to fulfil enterprise business requirements.

According to the Council of Supply Chain Management, logistics management should aim to achieve seven goals: deliver the right product to the right place at the right time with the right quantity and at the right quality and at the right price to the right customer. It is not easy to coordinate all the seven goals for all internal units and external partners. Therefore, to comply with all these goals, a global business must rely upon the collaboration of both the upstream and downstream partners.

Managing logistics in an effective and efficient manner has become a business strategy to sustain enterprise development. Loutenço (2005) stated that "the key to successful logistics management requires heavy emphasis on integration of activities, cooperation, coordination and information sharing throughout the entire supply chain, from suppliers to customers". In terms of information sharing, incessant enhancement of information technology has supported the logistics management on data exchange and communication across the entire process flow, such as the application of bar code and radio-frequency identification (RFID), point of sale (POS); electronic data interchange (EDI), virtual private network (VPN), and the enterprise resource planning (ERP) system. This not only reduces the complexity of physical process flow, but also lowers the uncertainties in the supply chain.

Even so, no logistic system can avoid being affected by the uncertainty of a risk attack. To compete in the low profit margin market, the company must sustain operation performance in all circumstances. The following sections discuss the logistics processes, the risk management strategy, the risk management process in logistics, and the enterprise performance evaluation.

2 Scope

Logistics play an important role in sustaining business competency through process efficiency improvement. Logistics link the internal functions and collaborate with the upstream and downstream partners to achieve synergistic result. Logistics management is adaptive to global networking (Nilsson & Waidringer, 2005) in order to meet market demand, provide prompt services and manage logistics effectively.

Due to the influence of risks in logistics performance, implementing risk management has been a critical issue recently. Risk management strategy can be viewed from the mitigation strategy approach and the contingency strategy. Mitigation strategy means taking pre-actions to avoid or lower the likelihood of a risk, whereas contingency strategy pertains to post-actions taken to handle damage in a quick and short time with minimal expense. This chapter focuses on mitigation strategy to set out risk management processes.

2.1 Logistics Processes

Logistics systems and management are diverse from one industry to another. No single type of logistics management can fit into all types of industries. There are two

kinds of process flows in the logistic chains: the physical flow and the information flow. The physical flow carries the raw materials from the suppliers, transforms it into finished products, and then delivers the products to the customers. Nowadays, information technology helps in the collection of data from each node of logistics in a speedy and timely manner in order to support a complex global delivery network. The logistics network of physical and information flow is illustrated in Figure 1.

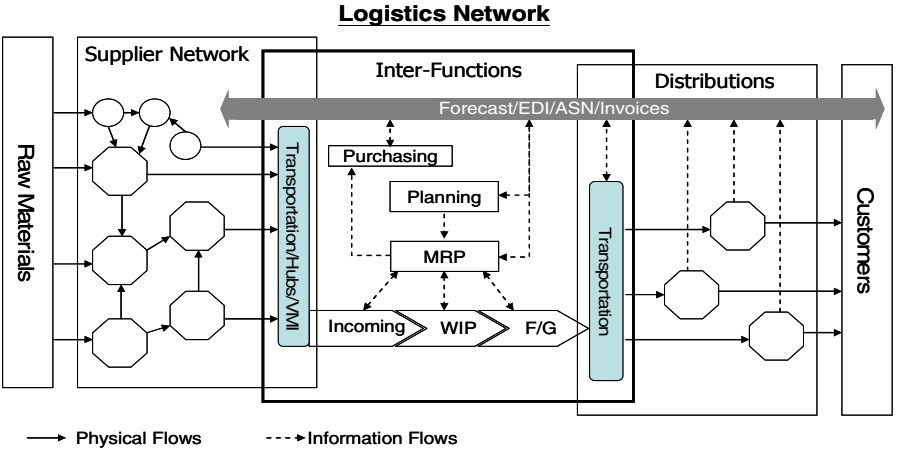

Fig. 1. Physical and information flows in logistics network. (Bowersox et al. 2005).

2.1.1 Physical Flow

Physical flow carries the materials from suppliers and delivers the final products to the customers. Mentzer (2008) classified the physical flow of logistics management functions into seven elements as listed in Table 1. Each function collaborates with other functions in an efficient manner to move products to the customers in accordance with the seven goals.

Table 1. A summary of logistics management functions (Mentzer, et al. 2008)

Transportation management	Network design (inbound and outbound), 3PL/4PL management, commercial tariff/regulation control, vehicle routing
Warehousing management	Location selection, design, management, shelf system and bounded warehouse
Material handling management	Product packing, labeling, picking system, delivery scheduling, dispatching and cross-docking management
Inventory management	FIFO, strategic inventory control, JIT, VMI, consignment and total inventory cost control
Order management and fulfillment	Ordering system, data mining and documents exchange
Procurement	Supplier management, cost negotiation and sourcing
Customer Service	Customer satisfaction, delivery scheduling and data mining

The logistics chains include many activities and involve different partners in the chain. Autry et al. (2008) defined the activities in the pipeline of logistics, including the material moving processes and management control network. Currently, the global business environment and the diversity of market demand on product design encourage enterprises to provide more services at local markets that result in a complex logistics network as well as adding more processes in the chains. There are three complexities- product, network, and process - which result in the difficulty of controlling logistic activities (Hofer & Knemeyer, 2009). In addition, the information flow consists of all the activities from the business plan to the front-end data collection. Many advanced information technologies have been developed to reduce the complexities in logistics flows.

2.1.2 Information Flow

Information is important in every business and organization, and it can be generated from any form of data such as market survey, production figures and shipment details. However, the contribution of information is in its value to the enterprise, and not in the volume of information. Each enterprise uses information technology at different levels, such as the EDI system which is implemented to reduce order cycle time and inventory (Willersdorf, 2007) or collaborative planning, forecasting and replenishment (CPFR) is used to improve forecast accuracy and to enhance collaboration with partners.

In logistics flow, besides involving many functions and activities, it also exchanges numerous data that need to be collected systematically and compiled in order to obtain valuable information for management decision-making. From the logistics process flow perspective, data are exchanged in three levels: daily operational processes, managerial control, and business planning.

- **Daily Operation:** the data collection starts from receiving the customer PO up to the delivery of products to the customers.
- **Managerial Control:** includes inventory stock monitoring, material In/Out, transportation scheduling and document exchange.
- **Planning:** integrates data from operation and processes based on business strategy and market status for planning.

In addition to information consolidation, information sharing among each node in the chain has been identified as a support to inventory control and to reduce the bullwhip effect. Nevertheless, both physical flow and information flow should move from one node to another efficiently. Any disruption may break the process flow or lower the performance of the logistics system.

2.2 Risk Management

Recently, risk management has been widely discussed. Many disturbances have been found in daily operations. Examples of disturbances are earthquakes, Iceland's volcano eruption, labour wage increase in China, BP oil leakage, and so on. Each disturbance may affect business operations and result in the adjustment of the logistics system.

The impact of accidental events can be controlled if the enterprise has a plan already in place. In general, risk management can be classified into two approaches. One is mitigation strategy and another is contingency strategy. Husdal (2008) illustrated the relationship of mitigation and contingency strategy in Figure 2. Mitigation action manages the risk sources while contingency action handles the consequences of a risk.

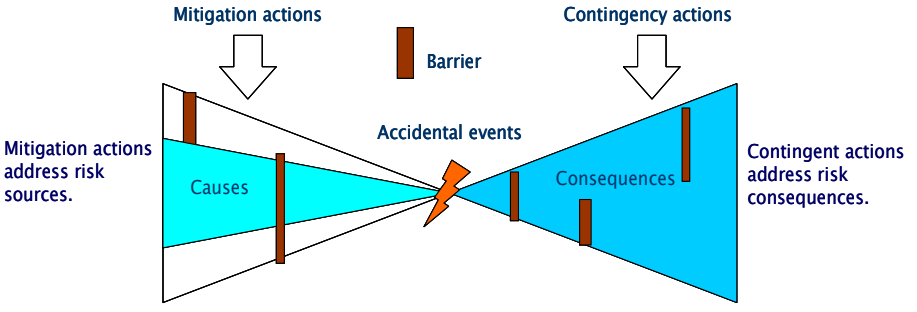

Fig. 2. Risk Mitigation and Contingency strategies. (Husdal, 2008).

In order to minimize the impact of uncertain events, enterprises should be prepared in responding to potential risks, and to take action to decrease the likelihood of disruption or reduce the level of impact when risk is unavoidable. When an enterprise is being attacked by a risk, how well the enterprise can resume its normal operation quickly and minimize its losses relies on a well designed contingency strategy.

2.2.1 Mitigation Strategy

Mitigation strategy is a set of plans to act against uncertain events prior to its occurrence. The purpose is either to prevent disturbance or to reduce the impact when it occurs. A mitigation strategy should tailor specific disturbances or threats, and it is expected that certain costs would be incurred in order to avoid disruption or lower losses. In addition, the costs and benefits of a mitigation strategy should be assessed before any decision is made. Moreover, the trade-off between strategies is another factor that needs to be assessed during the decision processes.

In enterprise risk management (ERM), there are some principle approaches that have been adopted in mitigation strategy which can also be applied in logistics management processes. The Committee of Sponsoring Organizations (COSC) provides guidance in response to a risk attack; it encompasses four approaches as shown below:

- **Accept** => monitor
- **Avoid** => eliminate (get out of situation)
- **Reduce** => institute controls
- **Share** => partner with someone

The above four approaches are set in a general direction, but the right mitigation strategy should be tailored to a specific risk. Chopra and Sodhi (2004) identified the source of threats in the supply chain, assessed the vulnerabilities by a stress test, and then defined the seven mitigation approaches and the tailored strategies. Other mitigation strategies have been identified by Tang (2006) and Faisal (2006) and so on.

A clear and comprehensive risk identification plan should be considered in developing an appropriate mitigation strategy that minimizes the impact of a risk. Another factor that could affect the mitigation strategy is the enterprise business strategy decision. Companies set forth their business competition strategy to win the market by selecting the best mitigation strategy.

Identifying and mitigating risks is a pre-requisite for an enterprise to reduce the impacts of risk. Pettit et al. (2010) demonstrated a zone of resilience composed of

supply chain capability and vulnerability (see Figure 3). A company should aim to balance its portfolio of capabilities to match the pattern of vulnerabilities. The less vulnerable the system is, the lower the likelihood of being attacked by risk.

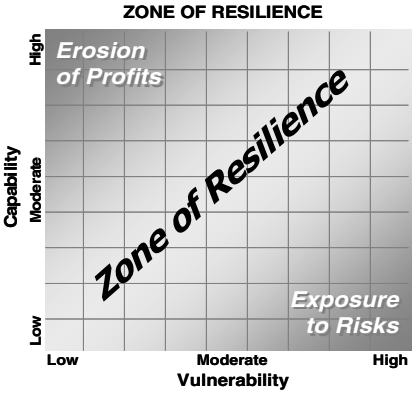

Fig. 3. Zone of Resilience (Pettit et al., 2010)

Table 2. Definition of Contingency plan (Department of Health and Human Services-US)

The National Institute of Standards and Technology (NIST)	As management policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergency, system failure, or disaster.	-Business Continuity Plan, -Business Recovery Plan, -Continuity of Operations Plan, -Continuity of Support Plan, -Crisis Communications Plan, -Cyber Incident Response Plan, -Disaster Recovery Plan, -Occupant Emergency Plan,
The Information Technology Infrastructure Library (ITIL)	As a series of processes that focus only upon the recovery processes, principally in response to physical disaster, that are contained within business continuity management (BCM).	
The Department of Health and Human Services (HHS) Enterprise Performance Life Cycle (EPLC)	As the strategy and organized course of action that is to be taken if things don't go as planned or if there is a loss in the established business product or system due to disasters such as a flood, fire, computer virus, or major failure.	

2.2.2 Contingency Strategy

Contingency strategy aims to respond to disruption rapidly and also to conduct recovery quickly with minimum expenses. Setting up a contingency plan is an essential

policy to manage natural disasters in government institutions. Many organizations have defined its contingency plan for multiple purposes, and use different terms for the recovery processes (see Table 2).

The contingency strategy can be an extension of the mitigation strategy plan. A good mitigation strategy plan should be able to either reduce the likelihood of an event or to reduce the costs of contingency actions. This chapter focuses on mitigation strategy, and the processes of risk mitigation management are discussed in the following sections.

3 Risk Management Process in Logistic

Risk management should be led by enterprise high level management and be set as a strategic process across all hierarchy levels. The risk assessment framework of each functional department should be in accordance with the enterprise risk management strategy and in line with the customer and stakeholder value. Some risk management standards have been established such as the Committee of Sponsoring Organization (COSO) ERM, International organization for standardization ISO-31000:2009, or Australian standard AS/NZS-4630.

In Information Technology (IT) system, there are more standard procedures that have been applied to manage the risks in daily system operations. Such as Basel II +IT control objective, OCTAVE, ISO-2700n, CRAMM, CERT SNAP, ISF, and ISO/IEC TR13335. The distribution of the risk management standard is shown in Figure 4.

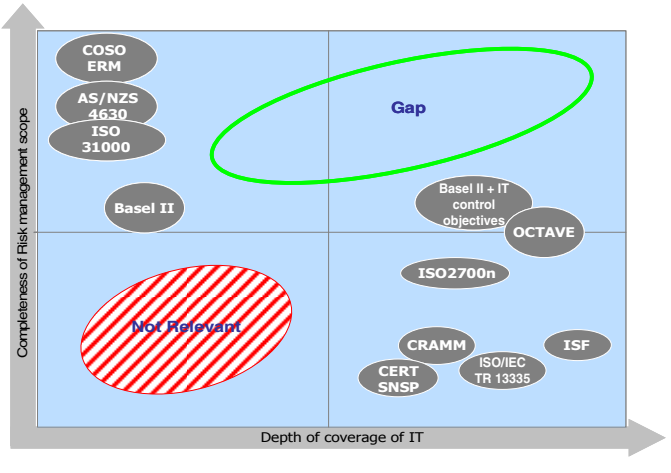

Fig. 4. Risk management system distribution ISACA/ITGI (2009)

The risk management of the logistics department should be adopted from the enterprise risk management strategy. In accordance with the organization functions, Nadler & Slywotzky (2008) classified risks in five categories (Strategic, Financial, Operational, Human Capital, and Hazard). The sources of risks are diverse in different business environments as well as in the company's internal systems. From a broad application, COSO (2004) provided a three dimension cubic to manage risks and built management processes across the entire enterprise (see Figure 5).

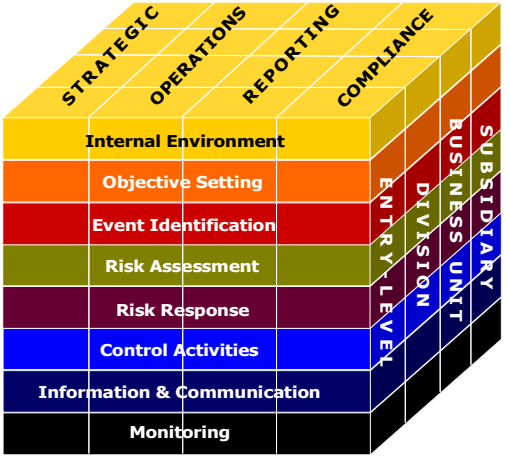

Fig. 5. A cubic of enterprise risk management (COSO, 2004)

The COSO model defined four risk categories in a firm (Strategic, Operations, Reporting, and Compliance), and applied it to every hierarchy level of an enterprise. Logistics department is a risk owner who assesses potential risks in these four categories in accordance with the enterprise's risk management strategy.

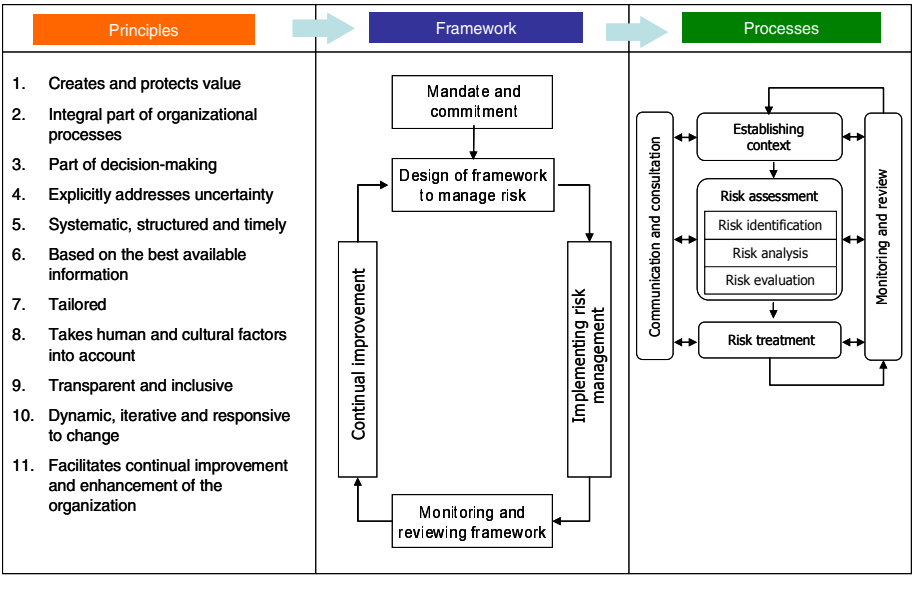

Fig. 6. ISO-31000 risk management standard (ISO)

Another international risk management standard (ISO-31000:2009) is issued by the International Organization for standardization (ISO). This is a continuous improvement process based on the PDCA (Plan-Do-Check-Act) continuous improvement cycle (see Figure 6). The COSO's framework organizes all the different units into one direction. The ISO's risk management standard is more practical and explicitly defines each process step.

An information system links all the departments of a firm. As mentioned above, there are many risk management procedures for a developed IT system. According to the Information Systems Audit and Control Association (ISACA), an IT risk management framework includes three aspects that correspond to business objectives.

- **Risk governance** => Integrated with ERM, risk awareness.
- **Risk evaluation** => Risk analysis, collect data, and maintain risk profile.
- **Risk response** => Manage risks; react to events, and articulate risk.

In this chapter, the COSO-ERM, ISO-31000, and ISACA risk IT framework are used to discuss risk management in logistics. An assessment framework is shown in Figure 7. For managing the risks in the logistics chains, this chapter assesses the risks from the process flow perspective, both the physical and the information flow. In accordance with the process steps of ISO31000, the following section discusses risk identification, evaluation, mitigation strategies, implementation, and monitoring.

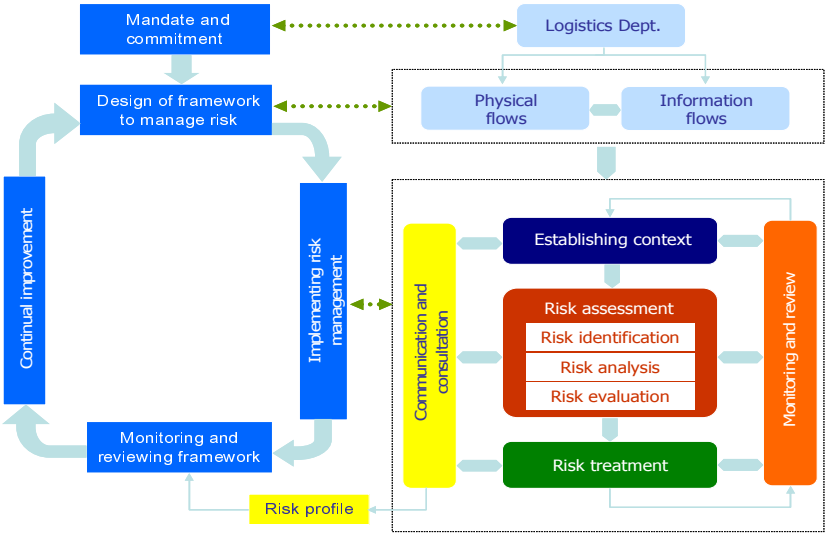

Fig. 7. Risk management framework of logistics (COSO, ISO, and ISACA)

3.1 Risks Identification

The first step of risk management is to identify the sources or drivers of risks. The disturbances can happen in any way at any time. Enterprises need to collect all

possible disruptions or threats systematically. The risks can be found in different aspects, either from external environment or internal operations. In logistics chains, the chance of exposure to risk is higher than other departments. The disruption not only happens in the process flows but also at the suppliers and customers site.

The losses resulted from risk occurrence are determined not only by its source (driver) but also by the vulnerability of a system. The vulnerability is the weakness of an enterprise operation. It can be a process, function, or a certain condition, and it may not harm the system until it is attacked by risk. For example, having a lean production can reduce the inventory holding cost, but may increase the risk of material shortage due to volcano eruption or earthquake. In addition, the results of every company facing risk may vary due to their different vulnerabilities.

3.1.1 Sources or Drivers of Risk

The sources or drivers of risks are defined differently. Besides the OCSC definition of risk, many other studies assess risks from different points of view. Blos, et al. (2009) studied the supply chain of the automotive industries in Brazil, and classified risks into four categories such as strategic, financial, operational, and hazard. Cavinato (2004) identified risk from the physical flow, financial flow, information flow, relational, and innovation perspectives. In order to collect all possible sources of risks in logistics chains, the process flow and its functions for identifying the risk source in each node of logistics flows are used. A framework for risk identification is illustrated in Figure 8.

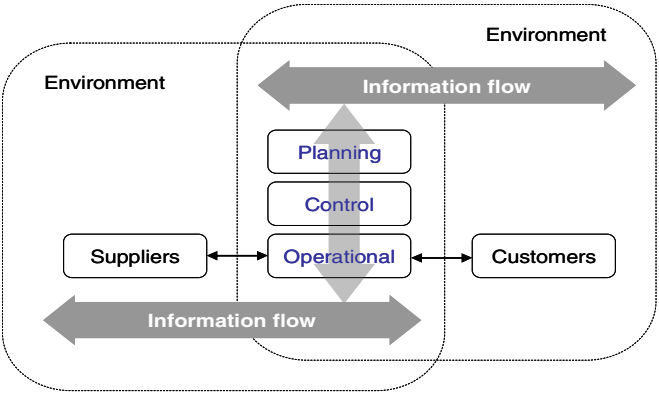

Fig. 8. Risk framework- process flow perspective

Following this framework to assess the potential risk might affect the performances of each logistics management function. As each enterprise has different risk awareness and vulnerability, a matrix (Table 3) can help to describe most of the sources of risk and assess its vulnerability against each identified risk. Departments may focus on the risks that may have a direct impact on their department's operations.

Table 3. A matrix of risks in each of logistics management function

Functions / Risk categories	Transportation management	Warehouse management	Material Handling	Inventory Management	Order management	Purchasing management	Customer Services	Information management
Environment	✓	✓	✓	✓				✓
Suppliers				✓	✓	✓		✓
Operational	✓		✓			✓	✓	✓
Control		✓		✓	✓			✓
Planning				✓	✓	✓	✓	✓
Customers					✓		✓	✓
Information	✓	✓	✓	✓	✓	✓	✓	✓

3.1.2 Vulnerabilities

Depending on their vulnerability to risks, enterprises may not be able to avoid disruptions, but they can control the effects of risk. For example, when an earthquake occurs, an enterprise located in that area would be affected. Though another enterprise is not located in the disaster zone, yet its suppliers in that area could not deliver the materials. Therefore, the vulnerability of the two enterprises is not the same. The way they manage the disaster will be different as well.

As a consequence, the way of handling risks is varied. Since there is no standard vulnerability among companies, finding the vulnerability of each risk is a challenge. Chopra and Sodhi (2004) have taken a stress test to assess the vulnerability of each given risk (see Table 4) where each department can evaluate its own vulnerabilities.

Table 4. Stress test on production disruption (Chopra & Sodhi, 2004)

Risk source		Stress testing
Production disruption	Supplier	A supplier capacity dropped by 20% overnight
	Internal- operation	Key plant shut down unexpectedly for one month
	Customer	Demand goes up by 20% for a key product; Demand goes down by 20% for a key product.

As mentioned above, each department might have different risk awareness. It would be necessary to collect and review all the vulnerabilities of each department. This can be used to assess the overall risks and vulnerabilities of a firm; and evaluate the level of risk so as to set the strategy priority as well as resource allocation.

3.2 Risk Analysis and Evaluation

After identifying the risk's source and vulnerability, the next step is to identify the loss severity and the likelihood of risk. However, learning the impact of a risk depends on the nature of the risks such as earthquake, or foreign exchange rate fluctuation. The diversity of risks requires different techniques for risk evaluation, a general calculation of risk can be illustrated by the likelihood of risk and its severity level.

3.2.1 Assessment Techniques

The type of risks varies and requires different techniques for decision-making. The ISO-31010:2009 has summarized a set of risk assessment techniques in Table 5. The application can be classified and applied to each step of the risk assessment process. Moreover, the technique should be applied in accordance with the nature of risks. It not only selects the right technique but also identifies the risk level for decision-making. As many methods can be used for risk assessment, the discussion in this chapter is based on a common application across three stages, the consequence/probability matrix, to evaluate the likelihood and severity of risks.

3.2.2 Risk Evaluation

In general, risk naturally exists in a daily business operation. The risk information is collected from historical data and the assumption is that the disruption would happen in the future in the same way. The enterprise should be able to reduce or avoid either the possibility of risk or its impact. In addition, some risks may not be repeating threats to an enterprise, for example, the transfer of a production plant to new locations away from a danger zone can avoid the same danger happening. Hence, the risks should be evaluated for a period of time and be profiled for further actions.

Table 5. Assessment techniques in each stage (ISO-31010/FDIS IEC)

Stage	Assessment technique (Strong applicable)
Identification	Brainstorming, Structure or Semi-Structure Interview, Delphi, Check-list, Primary hazard analysis, HAZOP, HACCP, *Environment risk assessment*, *Structure-What if-SWIFT*, Scenario analysis, *FMEA*, Cause-and-effect analysis, *Human reliability analysis*, *Reliability centered maintenance*, *Consequence/probability matrix*.
Analysis	HAZOP, HACCP, *Environment risk assessment*, *Structure-What if-SWIFT*, Scenario analysis, Business impact analysis, Root cause analysis, *FMEA*, Fault tree analysis, Event tree analysis, Cause and consequence analysis, Cause-and-effect analysis, LOPA, Decision tree, *Human reliability analysis*, Bow tie analysis, *Reliability centered maintenance*, Markov analysis, Bayesian statistics and Bayes Nets, FN curves, Risk indices, *Consequence/probability matrix*, Cost/Benefit analysis, Multi-criteria decision analysis.
Evaluation	HACCP, *Environment risk assessment*, *Structure-What if-SWIFT*, Root cause analysis, *FMEA*, *Reliability centered maintenance*, Mento Carlo simulation, Bayesian statistics and Bayes Nets, FN curves, Risk indices.

Risks could be assessed according to the possibility of risk occurrence and its severity level. As discussed in the previous sections, the enterprise vulnerability is a key factor that leads to its losses. For example, a computer hacker may succeed particularly when the system is vulnerable to such attacks. Therefore, the likely solution should include the frequency of hacker attacks and the possibility of the system's vulnerability. In addition, the severity should not only solve the physical losses but also the concealed expenses such as the production downtime and the expenditure for recovery. The consequence/probability matrix method collects the information in accordance with each identified risk source/driver, and assesses the likelihood as well as the level of severity. An example of data collection is shown in Table 6. In arriving at the score of each risk, the management team can then set the priority for each risk and develop a tailored mitigation strategy accordingly. (The higher the score, the higher the risk level)

Table 6. Risk level calculation table (Asbjornslett & Rausand, 1999)

Scenario		Likelihood (5-1)		Consequences of Scenario (5-1)								Resources to mitigate, rebuild, restore, etc.		
No.	Dsecription	Source (frequency)	Vulnerability (possibility)	Transportation management	Warehouse management	Material Handling	Inventory Management	Order management	Purchasing management	Customer services	Information management	Internal (5-1)	External (5-1)	Total Score
1	Economic Recession	Demand dropped 20% (2)	Product % over 50% (5)				5		3	3		5	2	180
2	Production line down	Supplier failed delivery (5)	Single source (1)				3	3	2	5		2	3	90

Afterwards, by using a grid which is composed of the possibility and the severity level of each risk, the grid classifies risk into nine levels. The priority of each risk could be identified based on the nine levels in the evaluation results. For example, the risk score in C2, C3, and B3 are the first priority that needs actions. If the risk score in A1 is of less priority and enterprise can either ignore it or handle it evenly.

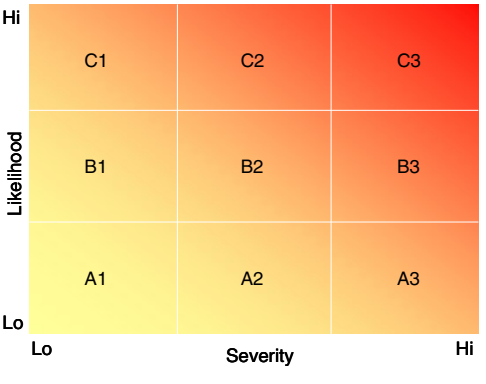

Fig. 9. Risk level grid

3.3 Risk Treatment-Mitigation Strategy

Prevention is better than the cure. The mitigation strategy is designed to manage the risks prior to its occurrence and to minimize the losses. Meanwhile, there are two

factors, risk preference and trade-offs, that should be considered when selecting a mitigation strategy. Also, there are two kinds of tradeoffs in selecting strategies: the cost-benefit and the tradeoff strategy.

3.3.1 Preference

The preference on risks means that companies would choose the risk which they are willing to deal with. This is highly associated with the enterprise's capability and its business strategy. When an economic recession happens, some enterprises would try to cut expenses; others would invest more on new technologies or new markets in order to boost when economy upturn. There are no standard criteria to follow in selecting the preference suitable for an enterprise. It would be a challenge for the enterprise to set a proper risk management policy and to achieve logistic performance requirements. In order to lower the impact of risk, a tailored mitigation strategy is needed, but it may not be able to comply with all the needs of each department or worst against others' benefit because the preference of each department is not the same. Therefore, it should be a collective risk mitigation strategy against both long-term and short-term performance requirements.

3.3.2 Trade-Off

It is not possible to use a single strategy for all the risks. In other words, it will have more strategies or actions to deal a specific risk. While deciding a tailored risk mitigation strategy for an identified risk, two factors should be assessed and answered. One is the cost and benefit trade-off of the strategy. Another is the trade-off between strategy options.

3.3.2.1 Costs/Rewards. A certain investment for mitigation strategy is needed in order to lower the likelihood of risk or reduce losses. In general, the value of investment should surpass the potential losses when no actions are taken to reduce the risks.

According to Chopra and Sodhi (2004), managers should "move to a higher level of efficiency by reducing risk while increasing rewards". For example, in order to reduce the material shortage risk, whether having more suppliers (from location x to B), or investing in suppliers as a joint venture (from location x to A), the investment can lower the risk of the material shortage, and at the same time, a supplier's early involvement can help to launch the products to the market in a timely manner (see Figure 10).

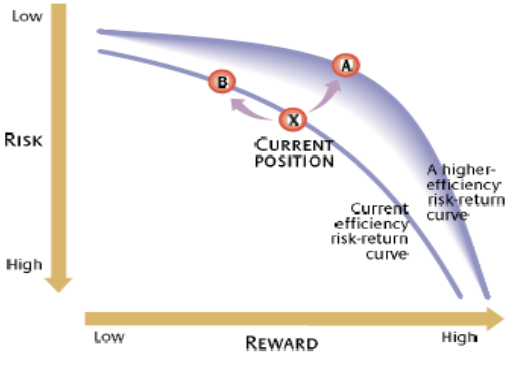

Fig. 10. Relation between reward and risk (Chopra and Sodhi, 2004)

3.3.2.2 Selecting Strategies. There could be more than one mitigation strategy needed to manage the risks. Selecting only one strategy may lead to other risks or may benefit one department but not other departments. Hence, the costs/rewards analysis is used to evaluate the impact of all decisions to each function of the logistics flow so as to decide which strategy is most beneficial to the entire enterprise.

3.3.3 Tailored Mitigation Strategies

To select a correct mitigation strategy is not easy especially when the risk is characterized by uncertainty. The risk mitigation strategy should be tailored to a specific risk, and most of the time, no single action can solve all the risks. Therefore, collective strategies to mitigate the risks are needed. The relationship between mitigation strategies is not in a linear cause-and-effect chain but in a complex interaction among the strategies.

Causal loop diagrams are used to explain the tailored mitigation strategy development and the relationships between strategies. For example, consider the risk of demand uncertainty, there could be a number of uncertainties (internal as well as external factors) that affect demand. Moreover, it is difficult to predict if the demand would change. Besides the uncertain characteristic of risk, the interaction of risk strategies also increases the risk uncertainty and affects the result of risk management. For example, in order to meet customer demand on time, keeping extra inventory could be a strategy but this may lead to the risk of material devaluation or obsolescence, not to mention the cost of holding inventory. Therefore, a collective risk mitigation strategy would be needed in order to achieve a comprehensive synergic result. A causal loop diagram example is illustrated in Figure 11.

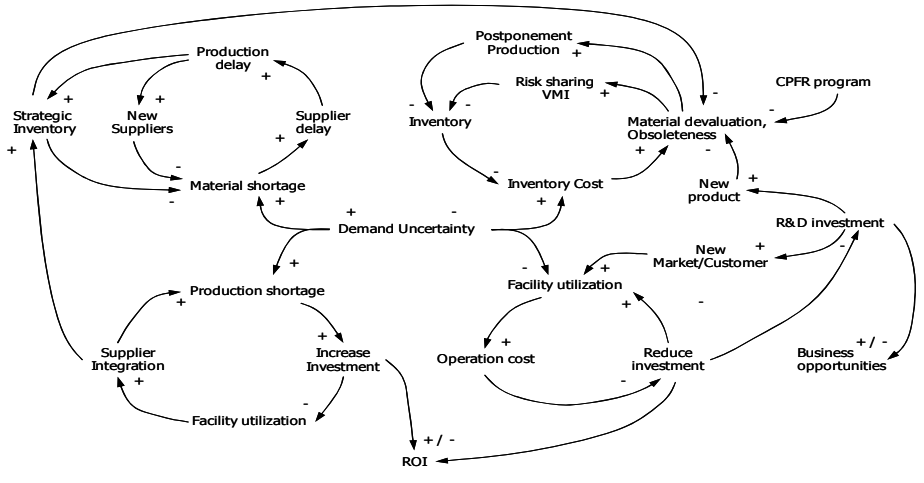

Fig. 11. Risk mitigation strategies interaction (Yang, 2010)

3.4 Implementation

Risk management can be successful if the policy protects the enterprise from potential losses effectively. An efficient risk management relies on the management involvement

to control as well as to monitor all the processes. Therefore, the implementation process could become another vulnerability to the success of risk management.

3.4.1 Governance

Governance is built on an effective management process. The primary objective of logistics management is to serve the customer effectively and efficiently. At the same time, logistics management should aim to reduce the cost in each node of the chain. Therefore, balancing the cost and service levels are a synergy performance result of the logistics management. In addition, the processes in the logistics chain are linked with one another, and any failure in the chain flow can lead to a serious impact on the entire logistics chain performance.

With this, a robust governance mechanism is necessary for an enterprise to link up all factors. Besides integrating the processes from suppliers to customers, it also ensures that risk management sustains the logistics performance targets. The risk management in logistics is a part of the enterprise risk management system. From the functional perspective, the governance of risk management should be taken from the enterprise's policy and strategy to set and evaluate logistics performance in accordance to its objectives.

From a process perspective, the governance is "a process by which the board sets the objectives for an organization and oversees progress toward those objectives" (Zoelick & Frank 2005), and the governance should provide "a base foundation for facilitating the effective communication and collaboration needed to achieve success on complex process projects" (Richardson, 2006).

There is no standard governance procedure for all enterprises or logistics firm. Zoellick & Frank (2005) provided a guideline of Governance, Risk management, and Compliance (GRC) that can be used as a reference for risk management in logistics function. The procedure is shown in Figure 12.

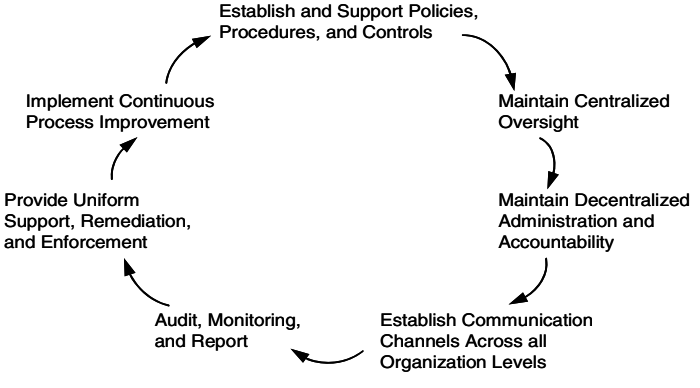

Fig. 12. Governance procedure (Zoellick & Frank, 2005)

The governance cannot be successfully executed without a solid control, monitoring mechanism and continuous improvement process. The control, monitoring, and continuous improvement processes are aim to sustain the logistics management performance so as to satisfy customer needs.

3.4.2 Control and Monitoring

Once the risk management governance has been set and implemented down to the front-end employees, the next action is to control the risks and to monitor the results. In general, a mitigation strategy can be categorized into five approaches such as accept, reduce, alliance, insure, and avoid. The control is based on mitigation strategies tailored to the identified risk, and the actions should be put in place prior to the risks occurrence. The results of mitigation strategies are seen after the risk occurs. There is a need to monitor as well as to periodically collect the data from the logistics activities in order to ensure that risk management is performed. The result should be recorded and also profiled if new risks are identified during the process.

3.4.3 Continuous Improvement

The risk status is subject to environment, business competition, and/or a company's decision. When there is an emerging market that needs local deliveries, the enterprise needs to set up a warehouse near this market. In this condition, the risk of shipment delay would be lower, but the inventory holding cost and risk of inventory obsolesce would increase. Business competition is changing all the time. Having a continuous improvement mechanism can help companies to adjust the strategies in a timely manner so as to become an adaptive organization which controls the changes or enhances the enterprise's resilience. The continuous improvement in risk management also maintains the risk profile and reviews the mitigation strategies in line with the enterprise's strategies.

Managing a change or strategy is not easy, especially in collaborating with different functional departments. Since each department has its own interest, strong and authorized governance mechanisms are needed to conduct and align all of the activities in the same direction. Therefore, an enterprise performance level index would be the basis for all departments in setting risk management strategy.

4 Performance Evaluation

Up to this point, the processes of risk management and its mitigation strategies have been discussed. However, the benefit of these actions to the business operations should be evaluated effectively. Fugate et al. (2008) provided the role of logistics in three aspects, including efficiency, effectiveness, and differentiation to evaluate the performance of logistics management. Other specific performance measurement indexes can be different for each company. Moreover, the key logistics performance index would be affected by the enterprise's strategy. Some performance indexes have been identified in the studies listed in Table 7. The enterprise should choose the key performance index in accordance with their business strategy. For example, to have a lean system, the inventory turnover rate should be higher and the stock-keeping unit (SKU) should be less. However, this may not fulfill the increasing customer demand in a timely manner.

Table 7. Logistics performance indexes

World Bank LPI	Griffis, S.E., et al.,(2007)	Fawcett, & Copper, (1998)
• Efficiency of the clearance process • Quality of trade and transport related infrastructure • Ease of arranging competitively priced shipments • Competence and quality of logistics services • Ability to track and trace consignments • Timeliness of shipments in reaching destination within the scheduled or expected delivery time	• On-time delivery % • Logistics costs / sales • Days order late • Inventory turnover ratio • Complete order fill rate • Average order cycle time • Order cycle time variability • Items picked per person per hrs • Average line item fill rate • Weeks of supply • Average backorder fill time • Sales lost due to stockout • Percent error pick rate • Logistics cost per unit	• Total logistics cost • On-time delivery • Cost trend analysis • Customer satisfaction • Actual versus budget • Stock out • Customer complaints • Inventory levels • Inventory turns • Cost per unit • Delivery consistency

Regarding the risk management performance setting, the first priority should be to sustain the logistics performance. Similar to risk preference, companies need to choose the risk that they are willing to accept. For example, in comparing company #1 and #2 as shown in Figure 13, both company's risk preference are not the same, when the risk #4 moves to the first quadrant, it is accepted by company #1 but is not good enough for company #2.

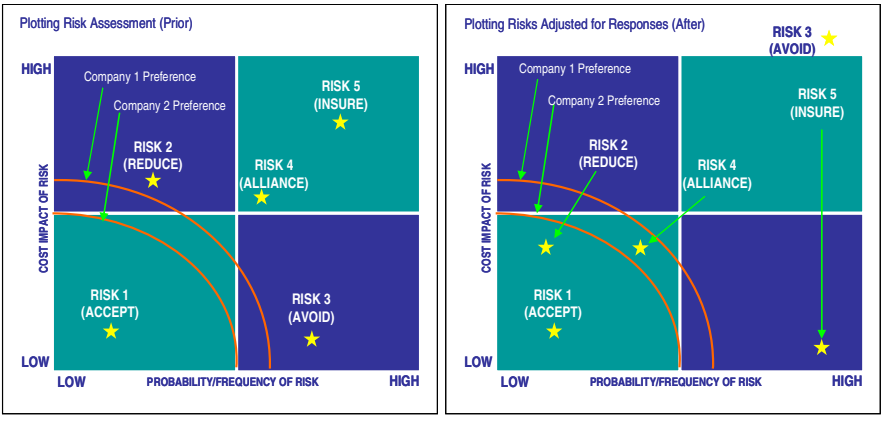

Fig. 13. Plotting risk mitigation strategies (Ballou & Heitger, 2005)

In addition, individual risk should be assessed and reported. Based on the five approaches, observe if the likelihood or losses are reduced or controlled (see Table 8). Finally, identify whether there are any risks that have not been found.

Table 8. Risk management assessment

Strategies	Likelihood	Losses
Accept	--	--
Reduce	🡻	🡻
Alliance	🡻	🡻
Insure	--	🡻
Avoid	✖	✖

🡻 Decreasing; ✖ Will not happen; -- Unchanged

5 Conclusions

Risks resulting in logistic disruptions are inevitable. Therefore, it is important to understand the applications of risk management in an enterprise. Besides risk awareness, the vulnerability of the system and preference on managing risks affect the results of logistic risk management. The company business strategy plays a key role in deciding logistic management operations as well as the risk management implementation. Nevertheless, how to decide the right mitigation varied between companies. This chapter studies the risk management in logistics by discussing the logistics processes, the risk management strategy, the risk management process in logistic, and the enterprise performance evaluation. This gives an understanding on the important risk management principles in dealing with logistics disruption.

References

1. Asbjornslett, B.E., Rausand, M.: Assess the vulnerability of your production system. Production Planning & Control 10(3), 219–229 (1999)
2. ASSE. TECH 482/535 Class Notes: Industrial Safety Engineering Analysis, http://www.ceet.niu.edu/depts/tech/sse/tech482/index.html (retrieved June 20, 2010)
3. Autry, C.W., Zacharia, Z.G., Lamb, C.W.: A logistics strategy taxonomy. Journal of Business Logistics 29(2), 27–51 (2008)
4. Ballou, B., Heitger, D.L.: A Building-Block Approach for Implementing COSO's: Enterprise Risk Management-Integrated Framework. Management Accounting Quarterly 6(2), 1–10 (2005)
5. Blos, M.F., et al.: Supply chain risk management (SCRM): a case study on the automotive and electronic industries in Brazil. Supply Chain Management: An International Journal 144(4), 247–252 (2009)
6. Bowersox, D.J., Closs, D.J., Drayer, R.W.: The digital transforma-tion: Technology and beyond. Supply Chain Management Review 9(1), 22–29 (2005)
7. Cavinato, J.L.: Supply chain Logistics Risks: From the back room to the board room. International Journal of Physical Distribution & Logistic Management 34(5), 383–387 (2004)
8. Chopra, S., Sodhi, M.S.: Managing Risk to Avoid Supply-Chain Breakdown. MIT Sloan Management Review 46(1), 53–62 (2004)

9. Department of Health and Human Services-US. Enterprise performance life cycle framework: Practice guide- Contingency Plan, http://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/36-Contingency-Disaster%20Recovery%20Plan/eplc_contingency_plan_practices_guide.pdf (retrieved June 21, 2010)
10. Faisal, M.N., Banwet, D.K., Shankar, R.: Supply chain risk mitiga-tion: modeling the enablers. Business Process Management Journal 12(4), 535–552 (2006)
11. Faisal, M.N., Banwet, D.K., Shankar, R.: Information risks man-agement in supply chains: an assessment and mitigation framework. Journal of Enterprise Information Management 20(6), 677–699 (2007)
12. Fugate, B.S., Mentzer, J.T., Flint, D.J.: The role of logistics in ket orientation. Journal of Business Logistics 29(2), 1–26 (2008)
13. Griffis, S.E., et al.: Aligning logistics performance measures to the in-formation needs of the firm. Journal of Business Logistics 28(2), 35–56 (2007)
14. Hofer, A.R., Knemeyer, A.M.: Controlling for logistics complexity: scale development and validation. The International Journal of Logistics Management 20(2), 187–200 (2009)
15. Husdal, J.: The dark side of supply chain, http://www.husdal.com/2008/11/12/supply-chain-risk/ (retrieved January 5, 2008)
16. ISACA/ITGI. Risk-IT-Overview, http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx (retrieved June 22, 2010)
17. Logistics world. What is Logistics?, http://www.logisticsworld.com/logistics.htm (retrieved June 1, 2010)
18. Lourenço, H.R.: Logistics Management: an opportunity for Metaheuristics. In: Rego, C., Alidaee, B. (eds.) Metaheuristics Optimization via Memory and Evolution, pp. 329–356. Kluwer Academic Publishers (2005)
19. Mentzer, J.T., Stank, T.P., Esper, T.L.: Supply chain management and its relationship to logistics, marketing, production, and operations management. Journal of Business Logistics 29(1), 31–46 (2008)
20. Nadler, Slywotzky: Risk and the Enterprise. MMC Journal Viewpoint 1, 1–11 (2008)
21. Nilsson, F., Waidringer, J.: Toward adaptive logistics management. In: Proceedings of the 38th Hawaii International Conference on System Science. IEEE (2005), http://www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2005.629 (retrieved June 20, 2010)
22. Pettit, T.J., et al.: Ensuring supply chain resilience: development of a conceptual framework. Journal of Business Logistics 31(1), 1–21 (2010)
23. Richardson, C.: Project Performance Corporation. Process governance best practices: building a BPM center of excellence (2006), http://www.ppc.com/Documents/ProcessGovernanceBestPractices.pdf (retrieved June 20, 2010)
24. Spekman, R.E., Davis, E.W.: Risky business: expanding the discus-sion on risk and the extended enterprise. International Journal of Physical Distribution & Logistics Management 34(5), 414–433 (2004)
25. Tang, C.S.: Robust Strategies for Mitigating Supply Chain Disruptions. International Journal of Logistics: Research and Applications 9(1), 33–45 (2009)
26. The institute of internal auditors, COSO. Applying COSO's Enterprise Risk Management — Integrated Framework (2004), http://www.coso.org/documents/COSO_ERM.ppt (retrieved June 23, 2010)

27. Trkman, P., McCormack, K.: Supply chain risk in turbulent environ-ments—A conceptual model for managing supply chain network risk. International Journal of Production Economics 119(2), 247–258 (2009)
28. Willersdorf, R.G.: Adding Value through Logistics Management. Logistics Information Management 3(4), 6–8 (1993)
29. World Bank. Logistics Performance Index, http://info.worldbank.org/etools/tradesurvey/Mode2a.asp (retrieved June 25, 2010)
30. Yang, W.H.: Identification of risk mitigation strategies in supply chains of electronics manufacturing services companies, Master Thesis: University of Liverpool (2010)
31. Zoellick, B., Frank, T.: Compliance Consortium Whitepaper. Governance, Risk Management, and Compliance: An Operational Approach (2005), http://www.securitymanagement.com/archive/library/compliance_consortium0805.pdf (retrieved June 20, 2010)