PART 2.
LOGISTICS MANAGEMENT IN THE SUPPLY CHAIN

CHAPTER 1
SUPPLY CHAIN RISK MANAGEMENT STRATEGIES

Sylwia Konecka[1]

[1] Poznan School of Logistics, Estkowskiego 6, 61-755 Poznan, Poland
sylwia.konecka@wsl.com.pl

Abstract

The article presents the fundamental risk management strategies: avoidance, reduction, sharing and retention. Then, reference is made to the risk management strategies in the context of the supply chain. Pointed to the vulnerability, agility, resilience and transparency of supply chains. The author also presents the main ways to deal with the risk in the supply chain. Finally, briefly describes the basic concepts of risk management in the supply chain, such as: Supply Chain Risk Management (SCRM), Supply Chain Event Management (SCEM), Supply Chain Security Management (SCSM), Enterprise Risk Management (ERM) and Business Continuity Management (BCM), presents the results of its own research in the field of their use in Polish companies.
Keywords: risk management strategies, supply chain risk management strategies, supply chain risk management concepts

1.1. Introduction

Risk management has been known for a long time, but no less under the influence of globalization and integration of enterprises has become critically important to consider the basic risk management strategies in a broader context − the context of the supply chain. Besides the notion of SCRM, there are functioning types or strategies for supply chain management taking into account the risk as well as a number of concepts that have similar assumptions with regard to risk.

Kolinski A. (ed.), Logistics Management - modern development trends, Poznan School of Logistics Press, Poznan 2016; DOI: 10.17270/B.M.978-83-62285-25-9.2.1

This article has been taken to systematize risk management strategies in the supply chain and indicated the scope of their use in enterprises.

1.2. Risk management strategies

All strategies of the risk management fall into one or more of these four major categories:

- avoidance (eliminate, withdraw from or not become involved),
- reduction (optimize – mitigate) − reducing the negative effect or probability of the threat,
- sharing (transfer – outsource or insure) − transferring the threat to another party (e.g. an insurance company),
- retention (accept and budget) accepting some or all of the potential or actual consequences of a particular threat, and the opposites for opportunities (uncertain future states with benefits).

Ideal use of these strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions.

Risk avoidance

The elimination of the risk, is undoubtedly the most radical and the most effective way to deal with the risk. This includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the legal liability that comes with it. Another would be not flying in order not to take the risk that the airplane were to be hijacked. However, it is not always the most favorable way e.g. because of the cost, and above all, very rarely realistically possible to apply. It is possible to eliminate the risk e.g. for external threats like earthquakes or natural disasters by changing the location of the company − to the seismic-free area or the area that is not threatened by flooding. More difficult is to eliminate the risk in relations to business processes. For example the resignation of entering on a new market because of occurring there difficulty of hindering trade theft protection Also, the cost of implementing solutions for eliminating the risk generally argue against their use. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

Risk reduction

Risk reduction or ‘optimization’ involves reducing the severity of the loss or the likelihood of occurrence of adverse events. For example, sprinklers are designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy. Risk reduction is the most common method of dealing with risk.

This is the way almost always possible, its concrete shape, we can also to some extent adapted to available resources, and achieved effect to our expectations. In relation to the risk of an accident at work reducing the level of risk can be achieved by the introduction of personal security employee (as helmets and protective clothing) or by the use of technical and organizational solutions (barriers and guards, reducing the speed of movement of internal transport, etc.). In a similar way the risks associated with the introduction of a new product could be reduced by appropriate market research, the risk of a drop in sales by using effective methods of marketing and promotion, and the risk of theft through the use of technology (cameras, security of goods, magnetic, etc.) or the employment of security personnel. Restrictions on the use of solutions to reduce risk − in addition to those resulting from the nature of business processes − are generally only costs and inventiveness of people. Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a call center.

Risk sharing (transfer)

Risk sharing briefly defined as ‘sharing with another party the burden of loss or the benefit of gain, from a risk, and the measures to reduce a risk’. The term of ‘risk transfer’ is often used in place of risk sharing in the mistaken belief that you can transfer a risk to a third party through insurance, outsourcing or legal solutions.

Insurance is the oldest form of risk management by moving its effects, relatively simple and easy to use, though not necessarily the cheapest and not always the most rational. Risk transfer (actually only the financial consequences) for the insurance company gives you a little false sense of security (risk

elimination) and the release of their own responsibility for the threats. This may lead to a situation where any indirect effects of the risk of becoming deeper and more onerous.

In practice if the insurance company or contractor go bankrupt or end up in court, the original risk is likely to still revert to the first party. As such in the terminology of practitioners and scholars alike, the purchase of an insurance contract is often described as a 'transfer of risk'. However, technically speaking, the buyer of the contract generally retains legal responsibility for the losses 'transferred', meaning that insurance may be described more accurately as a post-event compensatory mechanism. For example, a personal injuries insurance policy does not transfer the risk of a car accident to the insurance company. The risk still lies with the policy holder namely the person who has been in the accident. The insurance policy simply provides that if an accident (the event) occurs involving the policy holder then some compensation may be payable to the policy holder that is commensurate with the suffering/damage.

By outsourcing, we can significantly reduce the risks associated for example with the transport of goods, by commissioning of these activities to an external carrier. Then, as compared to using their own means of transport, we avoid the risk of a type of a road traffic accident or car breakdown − they will be directly affected by leased transport company. Nowadays very popular are 3PL − third party logistics services, by its nature, the contractor carrying the risk of logistics.

Legal solutions as a form of risk transfer are relatively youngest solution practiced in the risk management, although it seems that they have a relatively large development potential. As a typical example can be given quite often used in the practice of transferring risks arising from warranty obligations, for large retail chains and service companies by way of appropriate contractual clauses. Gains on the manufacturer because it reduces their risk and counterparty, because doing so can get better trading conditions.

The major drawbacks − restrictions on the use of risk transfer include (Machowiak, 2014, p. 85):

- with regard to outsourcing − partial (sometimes very significant) loss of control of the business processes and the more difficult the introduction of changes in them
- insurance − not everything can be insured (eg. the image of the company),
- the legal solutions − rarely being a de facto equality of the parties.

Risk retention

Risk retention involves accepting the loss, or benefit of gain, from a risk when it occurs. True self-insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much. Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

1.3. Supply chain risk management strategies

Present nature of the business causes that a risk management becomes increasingly important, as well as supply chains, which have a higher degree of complexity than individual companies. In such a situation, the risk and risk management need of incorporating its associated tasks in the management of the entire supply chain. The issue of risk management began to be considered in the context of the supply chain. This indicates a greater difficulty in the analysis. Thus, the risk and risk management can be discussed at different levels of complexity: individual activities of logistics, the logistics company, supplier-consumer relationships, supply chain, supply network.

Insofar as risk management outside can be regarded as a kind of extrapolation activities, methods and techniques known to the enterprise risk management. On the whole undertakings in the SCRM will be made up so the two areas of activity: effective risk management in the (possible) of all companies that are partners in the supply chain and parallel co-ordinated conduct aimed at reducing the level of risks that require joint actions, including against the risks specific to the supply chain. Threats that require collective actions − in addition to the risks specific to the

supply chain − will consist of the risk of 'external' − risks arising from the interaction between supply chain and its environment, the external environment.

In the first case we will therefore implement a 'classic' risk management process (risk identification, analysis and evaluation, selection and implementation of actions). With regard to the risks specific to the supply chain, because of their source of which is the relationship and interaction between partners, the need for more sophisticated methods. There is quite a large compliance authors about the fact that the most effective action will be here to give supply chain characteristics such as agility and flexibility, the ability to respond quickly to emerging threats to the continuity of supply and customer service.

Particular relevance as conditionality in the functioning of supply chains is limited in scale of supply chain applicability, of knowledge in the field of risk management gained in the enterprise. Very interesting issues leads extending the discussion about the relationship of risk management strategy at the level of supply chains. Operational management and supply chain management are equally a matter of business philosophy and a set of tools and techniques (Bozarth and Handfiled, 2006, p. 273). However, while the same risk management − a holistic − is more and more widely in the practice of corporate governance, so much the scale of the supply chain of its location, role and expected effects are still more academic discipline than practically used instrument management strategy (Machowiak, 2012, p. 277-285).

Somehow in the handling of supply chains in the context of uncertainty and risk in the literature there are also 'new types' or 'new strategies' of supply chains using risk management. There is talk of the already mentioned SCRM and in this context vulnerable, resilient, resistant or fragile supply chains, as well as the need to maintain transparency/visibility or agility of supply chains.

Resilience

The term 'resilience' is used, as it relates to the supply chains in the context of the network, and it was easy to take the dictionary definition, which is rooted in the science of ecosystems. Resilience refers to the physical feature of a property that helps it to return to the original formation after a deformation that is not beyond its elasticity. In a business perspective, it is the responsibility of an organization to react to business disruptions (Valverde and Talla, 2012). Christopher and Peck (2004, p. 2) state that the resilience is 'the ability of the system to return after the disturbance to its original or desired form.'

Resilience can be either proactive or reactive risk management strategy, because some of disruptions are not expected to happen, for example disruptions caused by natural disaster. Consequently, it refers to the ability of any system to return to the desired or original state. On the other hand, to restore once a disruption has occurred, plans are put in place on the supply chain to its original design and structure. The implication of resilience is included in the concept of flexibility of the network, given that the desired state may be different from the original. Resilience can be achieved either through flexibility or redundancy. Flexibility in this context is possible for a business to switch to other suppliers in case of disruptions while redundancy is reassignments to other industries due to underutilization. It can be achieved through infrastructure and resources investment, for example, multi-skilled work force, which is a system that can be able to accommodate multiple products, which has the capacity of a real change and number of suppliers (Wolden, Valverde, Talla, 2015, p.1847).

Transparency

Transparency of the chain is the ability of all members of the supply chain to track flows across the board supply chain. Transparency allows for example an insight into the conditions (demand and supply-side, production schedules and procurement, inventory levels maintained in the supply chain representing supply network, as well as in the supply chain representing the distribution network) using clear communication channels and agreements on one of the existing set of measures. The most popular tool to achive transparency in supply chains is track&trace system and traceability which is obligatory in food and pharmaceutical industry. Lack of transparency in the supply chain, forcing managers to make decisions based on forecasts, maintaining a relationship the stocks (i.e. buffers) which do not correspond to the actual demand. These are usually created independently of each other, as a result of decisions made by individual members of the supply chains and distribution networks, who do not have detailed knowledge about what is happening in the rest of the network. This often leads to popular Forrester effect. In this type of supply chain overconcentration of operations exists, resulting from the desire to take advantage economies of scale, quantitative rebates and lowering transaction costs, the trend excessive concentration of activity in a particular chain link. Excessive concentration reduces the flexibility of the supply chain to respond to changes in the environment and leads to greater vulnerability to sudden noise, which is sometimes called the fragility of the supply chain (Hendricks, Singhal, 2005, p. 695–711).

Vulnerability

Thus, the vulnerability of the supply chain can be defined as exposure serious disruption resulting from the risks in the supply chain, as well as external threats to the supply chain.

Vulnerability in the supply chain is potential susceptibility to sources of risk. The interaction of structures and measures determines the potentials of vulnerabilities. Vulnerabilities can be dealt with by the design and structure of the supply chain; alternatively, higher dependencies have resulted from changing trends in supply chain management. These vulnerabilities can be dealt with by security measures that can be created via structure and design. It is important to note that, the better the balance between supply chain and the security tools the lower the vulnerability. Another important aspect to note is that the business disruption cannot be fully eliminated as some risk sources cannot be eliminated. The following are some of the underlying reasons for vulnerability, reduction in inventory, reducing the number of subcontractors, research, and development of new materials. Research has shown that current principles used in supply chains have resulted in very vulnerable chains (Stephens, Valverde, 2013, p. 1). For example, the drive towards efficient supply networks has amounted into those networks becoming more vulnerable to business disruptions. Some supply chains aim at reducing vulnerability, but there remain chances that can result into disruption escalation. Therefore, it is easy to deal with the internal sources more than the external ones (Wolden, Valverde, Talla, 2015, p. 1847)

Agility

Agility refers to the ability to react to short-term changes that takes place in a supply chain as well as the ability to respond to external disruptions smoothly. It also means the ability to respond to short-term changes in demand or supply quickly (Grittner, Valverde 2012, p. 246-270). In this case there are back-ups that are set aside to deal with disruptions and other suppliers can be selected as solutions to a disruption. This is a proactive measure. In agility, aspects such as visibility, velocity, and acceleration are important. Agility can be important in dealing with demand and supply fluctuations although it is an important remedy in increasing the supply chain. Agility can be increased by promotion of information flow between suppliers and customers. The collaborative relationship within suppliers, postponing design, coming up with inventory buffers, and having a dependable logistic system are all-important factors to consider. As mentioned in

the redundancy context, working with known suppliers is emphasized (Valverde, Saade, 2015).

For the most frequently taken action aiming at lowering the level of risk in the supply chain for example are:

- diversification of sources of supply and avoid the principle of 'single sourcing',
- parallel processes and / or alternative,
- buffer inventory, maintaining reasonable reserves production,
- storage and transportation, and of course
- insurance (in relation to external threats),
- early warning describes activities that identify and inform about critical developments as early as possible. On the basis of early warning information, appropriate measures can be initiated in sufficient time in order to minimize the impacts of unforeseen events. In this context an EWS is a specific information system that informs decision makers in companies about developments and events with significance.

The supply chain risk treatments involve many possibilities. An exhaustive list of possible approaches presented Wildgoose (2016, p. 82):

- avoiding the risk by not engaging in an activity that gives rise to the risk in the context of a supply chain − e.g., by not sourcing from a particular country,
- changing the likelihood or the consequences of a supply chain event, or both: aim to prevent an event from happening − e.g., ensuring that a key supplier site has not been built in a flood zone; aim to detect the event if it happens and thus reduce the consequences − e.g., a number of leading companies have mapped out critical supplier locations and the status of their business continuity plans; aim to react to an event if it happens and thus reduce consequences − e.g., a company that has mapped out its key supplier sites, because it gets regular status reports on whether they have been affected, is more quickly able to bring in alternatives,
- improvements in the risk controls through increased of IT tools enabling supply chain transparency and the use of data analytics, such as financial health indicators: There are various financial measures, including the use of Z scores (which measure the likelihood of financial failure), payment records, and credit scores from a variety of third-party providers. These are now even able to start to look at the financial exposure of the whole chain,

- exposure to natural catastrophe risk: Many map-based incident dashboards and real-time data services can be used to monitor events in real time and identify exposure and risk concentrations,
- supplier databases can indicate whether suppliers have been the subject of legal action − for example, over intellectual property, employee or environmental issues. This is also a useful risk treatment in respect of brand risk,
- supplier and subtier risk management: A supplier and subtier risk management tool starts by mapping production site locations for an organization's suppliers and suppliers' supply chains ('subtiers'). It then, through risk assessment of each site, enables risk prioritization of treatment actions, such as changing to another supplier or a new production location,
- supplier and subtier crisis response: A supplier and subtier crisis response tool starts by alerting customers that a crisis event has taken place in the customer's supply chain − in other words, near the customer's supplier production sites or the sites of the suppliers' supply chains. It then contacts the emergency contacts in the supply chain to determine which supplier and subtier sites are affected by the crisis event,
- improve critical supplier/customer relationships: A number of metrics and assessment best practices frameworks can quantify the dependencies and relationships that exist between a customer and the supplier staff to understand and improve the approach at an individual level,
- supplier performance: There are many tools to record and measure the quality, delivery capability, and capacity of suppliers, and these can provide key insights into potential disruptions.

It is obvious that some of the presented ways of dealing with risk − especially involving the creation of reserves and inventories − have a direction opposite to some extent, e.g. to the principles of 'lean management' and other similar. It is not possible to completely avoid such a situation, safety is always the costs − to maintain suitable proportions must be subject to the relevant provisions in the formulation of policy risk.

When developing a risk management strategy in the supply chain should take into account the following elements (Machowiak, 2014, p. 83):

- how to look like a common policy against the risk at the supply chain,
- what should be the main objectives and ways of their implementation,
- which will be the most important tasks on the way to achieving in goals,

- who will be responsible for strategic risk management in the supply chain to be its competence,
- whether and what structures will be established within the framework of risk management in the supply chain, what will be the rules of participation.
- how you want monitoring and controling the flow of information.

1.4. Major concepts of supply chain risk management

These ways of dealing with risk in the supply chain business practice may be used in the form of several concepts. The most important among them are: ERM, SCRM, BCM, SCEM and SCSM.

ERM − Enterprise Risk Management

ERM is 'integrated management of business risk, financial risk, operational risk, as well as the transfer of risk, aimed at maximizing the value of the company.' It may be regarded as 'a systematic process of identifying, analyzing and responding to risk.' This means that companies first identify risk, then analyze them, using for example a matrix of probability and effect, to ultimately predict how they respond to specific risks − preventing him, avoiding it or reduce its effects. Generally, risk management refers to the situation before the execution of the threat or actual occurrence of the noise, because it is based on the estimation of the probability of occurrence of a specific event and its possible consequences. This is confirmed by the authors of the publication in which the emphasis is on value flowing to risk management:

- early switching suppliers as a risk mitigation strategy,
- preparation companies a danger by creating plans of risk,
- prepare scenarios for the reorganization of the network in the event of a fault,
- strategies to mitigate or minimize the effects of inter.

SCRM − Supply Chain Risk Management

SCRM can be defined as 'the integration and management of organizations within the supply chain − in order to minimize risk and reduce the likelihood of interference through cooperative relationships between organizations, effective business processes and a high level of information exchange.' The fundamental idea is to ensure profits and business continuity. This can be achieved through cooperation and coordination along the supply chain.

BCM − Business Continuity Management

BCM is a holistic management process that aims to determine the potential impact of disruption on the organization and creating conditions to build resistance to them and the ability to respond effectively to the protection of the vital interests of the owners, reputation and brand organizations, as well as the value achieved in the previous activity. Business continuity management according to the standard BS 25999 consists primarily of:

- identifying the critical states of interfering maintain business continuity and identify key resources necessary for their liquidation (human resources, infrastructure, the most important supplier, documented operating procedures, information systems, budget, etc.),
- risk management (hazard analysis, risk assessment and the introduction of risk mitigation methods) for critical processes,
- preparation of plans operating procedures (in case of the incident and crisis) and communicated them to all interested parties.

For each critical operation organization should identify appropriate methods of dealing with the risk of being recommended are the following three:

- reduction of the probability of occurrence,
- shortening the duration of the interference,
- reduce the impact of noise on business.

In the context of supply chain management and on the basis of those ways of understanding the risk of disruptions in the supply chain should be assumed that business continuity is the overriding objective functioning of the supply chain at a strategic level and ensure its operational tasks are executed. The concept of BCM traditionally been recognized for the individual companies, but also includes the latest standard supply chains. In the literature, there are statements like 'the concept of business continuity in the supply chain' (Business Continuity Management for Supply Chain). Zsidisin (2005, p. 47-55) writes about the planning stages of 'the continuity of the supply chain' (The Supply Chain Business Continuity Planning).

SCEM − Supply Chain Event Management

Another concept associated with the risk in the supply chain − SCEM − defined as 'a business process, in which event destructive are timely detected and launch appropriate action, such as notifying key staff and adjusting the flow of materials and information to new conditions.' The purpose is to allow to react SCEM chain of adverse events by minimizing their impact, thereby avoiding the need to change the plan. This means estimation, monitoring and evaluation of disruptive events

within individual companies and consistent initiating action. The idea of SCEM cooperation partners in the supply chain in order to identify critical nodes and links through which goods flow in the supply chain. The designated nodes and connections are agreed control limits and permissible variations in the levels of activity. If for some reason the level of activity beyond the set limit, an alarm is automatically generated to allow for corrective action.

Currently SCEM is considered primarily from the point of view of information systems. Firms supplying systems SCEM offer the following functionality: management of alerts and incidents, tracking and reporting in the opportunity, to review the status of orders and inbound and outbound supply warehouse and their links to the purchase and sales orders, production, quality control, and financial processes. They also offer support exceptions, such as delayed delivery, exceeding the permitted time shipment rejected by the carrier, inconsistencies in the advanced notifications of shipments, damaged goods held in order to declare. However, academia indicates that SCEM systems should be based on active and systematic methods to anticipate and react to situations that differ significantly from the typical reports of the exceptions generated by the enterprise resource planning systems. As part of SCEM it does not optimize all the processes from beginning to end, and instead considered the risk of events that may affect the continuation of the activity within the desired value chain structures and networks.

SCSM − Supply Chain Security Management

Terminology concerning both safety and risks, are used interchangeably. However, more often they are identified as different. Supply chain security is defined as the prevention of pollution, damage or destruction of assets or products in the supply chain. On the other hand, supply chain risk is defined as the probability, the chance of harmful effects of noise on the company and the results of the supply chain. Some processes involve both security management and risk in the supply chain, with the concept of business continuity. However, ensuring continuity of operation is based on the analysis of weaknesses in the system of the organization and relates primarily to the existing internal factors. Designing security solutions is, above all, prevention, and design solutions to business continuity concerns the diagnosis and treatment and to continue operations during the repair work. Security management of the supply chain is an approach based primarily on the cooperation of enterprises with economic partners, public entities. It aims to protect relationships with suppliers and customers, productivity, efficiency and resistance to interference and assets of the supply chain, including against theft, terrorism, illegal trafficking of people and weapons of mass

destruction. It stresses that the more complex and extensive structure of the supply chain, the more attention the company should pay to safety. SCSM is focused on the physical security of infrastructure, people, information, business partners and supplies. It also includes aspects such as education, training, safety procedures, incident reporting and incident response. Initiatives security management of the supply chain has also partnered companies with government departments, for example: a partnership companies trade and customs against terrorism (Customs-Trade Partnership Against Terrorism, C-TPAT) initiative, secure containers (Container Security Initiative, CSI), an institution authorized entrepreneurs (Authorized Economic operator, AEO). As part of the combination of risk management and security management of the supply chain operating concept of the supply chain-oriented security (Supply Chain Security Orientation, SCSO).

It has already been mentioned that many of the risk management strategies in the context of the supply chain remains academic considerations. That is why the author decided to check how the involvement of Polish enterprises in the use of these concepts. Table 1 shows the results of tests carried out on a sample of 192 enterprises, mainly from the logistics sector, the research was conducted in 2014. Respondents were asked to answer whether their company uses appropriate management concepts. Answers were presented in the table 1.1.

Tab. 1.1 Range of usage of supply chain risk management concepts in Polish enterprises

Conception	YES		NO		I DO NOT KNOW	
	% of responses	No. of responses	% of responses	No. of responses	% of responses	No. of responses
SCRM − Supply Chain Risk Management	16,15%	31	39,58%	76	44,27%	85
SCEM − Supply Chain Event Management	21,35%	41	42,19%	81	36,46%	70
BCM − Business Continuity Management	41,67%	80	25,52%	49	32,81%	63
ERM − Enterprise Risk Management	6,25%	12	41,15%	79	52,60%	101
SCSM − Supply Chain Security Management	31,25%	60	27,08%	52	41,67%	80

Source: results of own studies

It should be emphasized that the study sample could not be considered as representative. But it can be see that a small percentage of enterprises use concepts

of risk management in the supply chain. The most popular is BCM concept, and what is strange the least known is ERM. It is surprising because the concepts like SCEM or SCRM are a kind of extension of ERM. Undoubtedly aware of these concepts is low, in each case, nearly half of respondents do not know is it even exist.

1.5. Conclusions

To conclude, the ways of dealing with risk in the supply chain are derived from the four basic risk management strategies. In the context of the supply chain are described in many types of passwords, strategies or concepts of risk management in the supply chain, however, come down to very similar areas: integration of partners in the supply chain, information sharing on potential internal and external threats, appropriate inventory management. Taking into account the practical use of the concept of risk management in the supply chain it remains included up to 30% of enterprises, while maintaining the continuity of action in 40% of companies.

References

1. Bozarth, C., Handfield, R.B., (2006), Introduction to operations and supply chain management, Upper Saddle River, Pearson Prentice Hall, New Jersey.
2. Christopher M., Peck H., (2004), Building the Resilient Supply Chain. The International Journal of Logistics Management, 15, 2, p. 1-14.
3. Detlef G., Raul V., (2012), An object oriented supply chain simulation for products with high service level requirements in the embedded devices industry, International Journal of Business Performance and Supply Chain Modelling, Vol.4, No.3/4, pp. 246-270.
4. Hendricks, K.B., Singhal, V.R., (2005), Association between supply chain glitches and operating performance, Management Science, vol. 51, iss. 5, p. 695–711.
5. Machowiak W., (2012), Risk management − unappreciated instrument of supply chain management strategy, LogForum, 8 (4), p. 277-285.
6. Machowiak W., (2014), Podstawy zarządzania ryzykiem w ujeciu ERM [Fundamentals of Risk Management in ERM], Wyższa Szkoła Logistyki, Poznań.
7. Stephens J., Valverde R., (2013), Security of E-Procurement Transactions in Supply Chain Reengineering, Computer and Information Science, Vol. 6, No. 3.
8. Valverde R., Talla M., (2012), Risk Reduction of the Supply Chain Through Pooling Losses in Case of Bankruptcy of Suppliers Using the Black–Scholes–Merton Pricing Model, in: Chaubey P. Yogendra (ed) Some Recent Advances in Mathematics and Statistics, World Scientific.
9. Valverde R., Saade R., (2015), The Effect of E-Supply Chain Management Systems in the North American Electronic Manufacturing Services Industry, Journal of Theoretical and Applied Electronic Commerce Research, Vol. 9, No. 3.

10. Wildgoose N., (2016), Supply Chain Risk Management, in: Green P. E. J., Enterprise Risk Management. A Common Framework for the Entire Organization, Elsevier, Oxford.
11. Wolden M., Valverde R., Talla M., (2015), The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System, IFAC-PapersOnLine 48-3, p. 1846–1852.
12. Zsidisin G.A., Smith M.E., (2005), Managing Supply Risk with Early Supplier Involvement: A Case Study and Research Propositions, 'Journal of Supply Chain Management', Vol. 41, No. 4, s. 44-57, in: Macdonald J.R., (2008), Supply Chain Disruption Management: A Conceptual Framework and Theoretical Model (doctoral dissertation), The University of Maryland, College Park