TAMPERE UNIVERSITY OF TECHNOLOGY

RISK MANAGEMENT IN NETWORKS

9.8.2011

Pasi Kuparinen

EXECUTIVE SUMMARY

Generally risk is considered as a possibility of loss / injury or other harmful consequences. Thus, risk is considered mainly as a possibility of a negative outcome. Positive outcomes are in the minority. Moreover, because risk is considered as a possibility, phenomena that are known to lead to a negative outcome are not risk events. Basically risk has two characteristics: losses and uncertainty about their occurrence and amount.

There are three sources of risks in a network or in a supply chain. First, there are risks related to organization itself. Second, a supply chain requires cooperation with other organizations and thus this cooperation has risks also. The third source of risks is the corporate environment where all the remaining risks are located. Essentially all the stakeholders and interest groups generate risks and those risks can be considered as environmental risks. Only half of the risks affecting the focal company are visible to them without a network wide inspection. Moreover, this visibility level is likely to decrease as the environment becomes fuzzier. That is why a systematic network risk management method and ultimately culture is needed.

Risks can be managed by avoiding or eliminating the risk, mitigating the risk, sharing or transferring the risk, accepting or taking the risk, or further analyzing individual risks. These are the main strategies also in the network risk management. Essentially there is no difference between network risk management and general risk management. Though, there are some aspects that differ as seen from the two processes introduced in this paper. Thus, also in networks risk management process has four main phases: risk identification, risk assessment, risk management actions and risk monitoring.

When companies are collaborating, they are exposed to several risks. First, they surrender their decision-making sovereignty in the field of activity in which the cooperation takes place. Thus, every risk is not in their hands. Second, the risk of conflicts over objectives arising can result if companies are made to place their own aims in second position to those of the network. Third, depending on the intensity of the links among the network partners, there is a risk of individual partners losing their flexibility. Fourth, there is a risk of a loss of know-how advantages and misuse of information. Finally, strong differences between the partners' cooperation cultures create risks and prevent cooperation.

Risk mitigation is the basic strategy to respond to a risk. In networks collaborative relationship, information sharing and trust among supply chain partners create the basis for risk mitigation. These enablers have high driving power and low dependence of other enablers. Thus, those three factors require maximum attention and their strategic importance is essential. There are also four strategies to mitigate risks: risk controlling, risk avoiding, cooperating with someone, and creating flexibility around the risk object.

All in all, a collective risk management is especially important in network relationships. Without a systematic collaborative process, the underlying risks are not exposed and managed. Thus, companies need cooperation also when identifying risks. Moreover, proactive risk management should be used to manage risks. It means that risks are identified well before they occur and materialize.

TABLE OF CONTENTS

1. INTRODUCTION

This paper was written for a part of Smart Grids and Energy Markets – research program. It is a follow-up paper for the earlier two reviews considering "Incentives and revenue sharing in networks" (Kuparinen 2011a) and "Profit sharing in collaborative networks" (Kuparinen 2011b). This review is related to the two mentioned review by widening the network and collaboration theme into risk management. Kuparinen 2011a tackled networks in general and the challenges in coordination of a network. Thus this review is based on that and its specification of networks and network coordination.

The purpose of this paper is to shed some light for the concept of network risk management. This review covers recent scholar papers and thus this is a literature review. The main challenge of this review is the term supply chain. That is because most of the literature deals with a product supply chain and its risks, whereas the main focus of this review and therefore SGEM-project focus is on collaborative service networks. The SGEM network structure can be considered as national companies cooperating to deliver services to local customers. Moreover, supply risk is derived from purchasing risk because in a supply chain the main principle is essentially purchasing a good. This viewpoint, which is considered in some reviews, goes even further from collaboration. Despite that, the term 'supply chain' is widely used in this review because it still describes the collaborative nature of organizations.

Collaborative risk management research is mainly concentrated on vertically arranged networks. Hence, the main terms used in this review are supply risk and supply risk management. Only few papers touch horizontally cooperating companies and their risk management. Thus this kind of risk management is not covered in this context, although some or most of the risk management concepts are valid in horizontal cooperation as well. First, this paper defines risks and its features in the chapter 2. Then different sources of network risks are introduced in the chapter 3. Finally in the chapter 4 the whole risk management process is described with a special focus on risk sharing and risk mitigation.

2. CONCEPT OF RISK

Generally risk is considered as a possibility of loss / injury or other harmful consequences. Though there is a wide range of aspects in defining the concept of risk (see Zsidisin 2003, p. 218; Harland et al. 2003, p. 53). Despite that, risk is considered mainly as a possibility of a negative outcome. Positive outcomes are in the minority. Moreover, because risk is considered as a possibility, phenomena that are known to lead to a negative outcome are not risk events. Basically risk has two characteristics: losses and uncertainty about their occurrence and amount. (Hallikas et al. 2004)

For a more specific inspection of risk, Yates and Stone (1992) remark that a risk has three elements: (1) the elements of loss, (2) the significance of loss and (3) the uncertainty associated with loss. First, one has to note that risk is not limited to one specific loss. Instead, the incident can result in various outcomes. For instance, a fire can have a wide range of consequences. In addition, incidents can intersect multiple categories of consequences, such as financial, performance and so on. Second, the more significance (usually valued by funds) the risk has, the greater is the implied risk. Thus, the significance of loss is directly proportional to the amount of loss. Third, uncertainty is related to the degree of confidence a decision maker has.

One classification of risks is to divide them into pure and speculative risks. Pure risks consist of factors that can prevent either directly or indirectly a company from pursuing its goals. Hence, pure risks have no beneficial result, only possible outcome is loss. For example wrong choice of personnel and lack of skilful employees are pure risks. Speculative risks are related to investments. Hence, speculative risks may result either in gain or loss. These types of risks are made consciously and therefore they are not a result of uncontrollable circumstances. For instance an investment decision to build a new factory includes speculative risk. (Hallikas & Virolainen 2004; Investopedia.com)

The actions the risk carrier depend upon whether it is a risk taker, a risk averse or a risk neutral actor. A risk taker is ready to accept the risk and all the consequences and is therefore not afraid of uncertainty. A risk-averse actor is instead avoiding risks. A risk neutral actor is located between avert and taking actors and it tries purposely to overlook risk when deciding investments. (Investopedia.com.) Hence, all the risk related decisions comes to the question of whether the actor is ready to take the risk or not.

3. RISKS RELATED TO NETWORKS

Jüttner et al. (2003, p. 201) note that risks in a supply chain have three sources. First, there are risks related to organization itself. Second, a supply chain requires cooperation with other organizations and thus this cooperation has risks also. The third source of risks is the corporate environment where all the remaining risks are located. Essentially all the stakeholders and interest groups generate risks and those risks can be considered as environmental risks. All the three sources are depicted in the Figure 1.

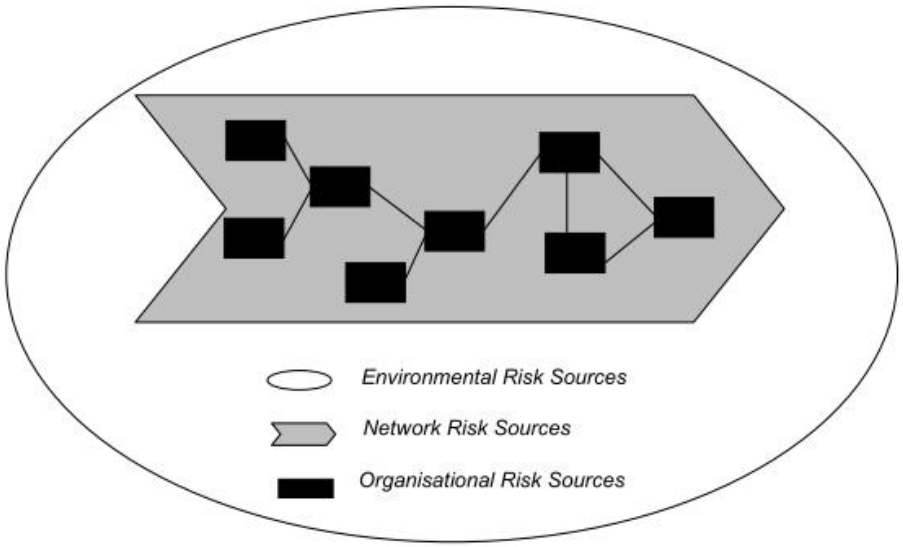

Figure 1. Risk sources. (Jüttner et al. 2003, p. 202)

Identification of risk sources is becoming more and more challenging because of increased complexity of business processes, decentralized decision making policies, and asymmetric information flows (Hallikas 2003). Moreover, there is no common risk in a supply chain. Instead, tighter relationships require that risks should be studied from different perspectives. Thus, risks are dependent on the viewpoint and risks affect differently the partnering companies. (Hallikas et al. 2004, p. 50) That is why every member of a supply chain is essentially responsible for their individual risks, but also company-wide holistic and systemic risk evaluation is needed in order to recognize network-related risks (Hallikas 2003).

Harland et al. (2003) studied that less than 50 % of the risks affecting the focal company were visible to them. Moreover, they argue that this visibility level is likely to decrease as the virtual organizations and supply chains increase and as they become more complex. (Harland et al. 2003, p. 59) Thus, the collaboration within risk management is extremely important.

Zsidisin (2003, p. 222) define supply risk as

> *"the probability of an incident associated with inbound supply from individual supplier failures or the supply market occurring, in which its outcomes result in*

the inability of the purchasing firm to meet customer demand or cause threats to customer life and safety."

This definition emphasizes the nature of a supply chain as uninterrupted flow of goods. But still that definition has two important elements considering networks. The first element is that a risk source is associated to a partnering company. The second element is that if a supply risks materializes, then the principal is unable to meet customer demand.

3.1. Types of supply chain and network risks

Most of the scholars have classified supply chain risks, while only some have concentrated on network risk typing. One fundamental classification of risks is presented by Norrmann & Lindroth (2004). They divide supply chain risks into three separate categories: operational accidents, operational catastrophes and strategic uncertainty. Operational accidents affect the operational process or resources related to the supply chain. Operational catastrophes are rare and difficult to predict and once they occur they have a severe impact like natural disasters. Strategic uncertainties are affecting at the strategy level. An example of strategic uncertainty is a supplier default or bankruptcy.

Tang and Tomlin (2008) categorize supply chain risks into six categories. Their classification is more detailed and thus more specific that the one introduced in the previous paragraph. The six categories are: supply risks, process risks, demand risks, intellectual property risks, behavioral risks and political/social risks.

An even more specific typing is presented by Chopra and Sodhi (2004). They categorized supply chain risks into disruptions, delays, systems, forecast, intellectual property, procurement, receivables, inventory and capacity. This kind of classification is useful when managers want to know the universe of supply chain risk categories. The classification lists basically every aspect of a supply chain.

The only classification considering network related risks, which is introduced in this review, is presented by Hallikas et al. (2004). They group risks into four categories based on their study of two example networks. These four categories are: (1) Too low or inappropriate demand, (2) Problems in fulfilling customer demand, (3) Cost management and pricing, (4) Weaknesses in resources, development and flexibility. Essentially there is no difference between network and supply risk chain typing. The only difference is that risks are grouped based on different level of viewpoint; some are grouped on the process level and some on the whole system level.

Das and Teng (1996) classify risks in strategic alliances into two categories, namely relational and performance risks. They consider relational risk as the probability and consequences of not having satisfactory cooperation due to lack of commitment. Performance risk is related to alliance performance so that the alliance objectives and goals are not achieved. The cooperation may be satisfactory but it still may not achieve the targets. Sources of performance risks are among others intensified rivalry, new entrants, demand fluctuations, changing policies, a lack of competence and sheer bad luck. Performance risk is present in all strategies.

3.2. General network and collaboration risks

Zanger (1997, p. 13–14 according to Hallikas & Virolainen 2004) has studied small and medium sized enterprises (SME) and risks that may arise in a network of suppliers. She found fife typical network risk:

1. Network partners **surrender their decision-making sovereignty** in the field of activity in which the cooperation takes place.
2. The risk of **conflicts over objectives arising** can result if SMEs are made to place their own aims in second position to those of the network, in which case economically second-best behavior has to be consciously accepted.
3. Depending on the **intensity of the links** among the network partners, there is a risk of individual partners **losing their flexibility**.
4. In the case of individual network partners' opportunistic behavior, there is a risk of a **loss of know-how advantages and misuse of information**.
5. Strong **differences between the partners' cooperation cultures** have an adverse effect on the trustful atmosphere of partnership within network. They can lead to inner opposition to the cooperation from management and employees.

These fife risk types are typical of collaboration. That is because when companies are collaborating they may have conflicts, which generates disputes and therefore risks of collaboration.

Christopher and Lee (2001) have also depicted risks related to networks. They found three sources of general network risks: lack of ownership, chaos and inertia. First, lack of ownership means that due to complex network of business relationships there is often confusion about responsibilities. By chaos they mean the complex forces of a supply chain. Chaos can result among others from over-reactions, unnecessary intervention, distorted information and mistrust. Inertia is the general lack of responsiveness to changing environment. In a supply chain or in a network flexibility is often sacrificed for cost reduction which increases inertia and therefore the supply chain is unable to respond quickly to competitors moves. (Christopher & Lee 2001)

Future trends and other major disruptions in the near or far future pose a threat to a network. If a company or a network is not prepared to future trends or it is not prepared to change its policies to correspond future trends, it may not succeed in the future. Therefore orientation, knowledge and resources have to be maintained and modified all the time. (Hallikas et al. 2004, pp. 51–52)

3.3. Demand and supply risks

In a supply chain the main risks along with operational risks, which were briefly discussed in the previous chapter, are in supply and demand. Supply risks, which were also discussed earlier, are related to supply partners. Tang (2006) presents a comprehensive review for supply and demand risk management in a supply. Essentially supply risks include supplier selection, supply yields, supply lead times, supply capacity, supply cost and supply contracts in general. Manuj and Mentzer (2008) add that in supply risks include also supply quality, supplier opportunisms and transit uncertainties. Demand risks are associated with customers and markets generally. Demand risks include forecasting errors, demand variability, and competitor moves. (Manuj & Mentzer 2008)

4. RISK MANAGEMENT IN NETWORKS

Risk management is a process which aims to find and control risks. Risk management activities are important on all organizational levels, because only by managing, risks can be identified and controlled. Majority of the risks are not managed without appropriate tools. Risk management strategies include: (Hallikas et al. 2001, p. 53)

- Avoiding or eliminating the risk
- Mitigating the risk
- Sharing or transferring the risk
- Accepting or taking the risk
- Further analysis of individual risks

Moreover, there are two ways to influence a risk: (Hallikas et al. 2001, p. 53)

- Mitigating the possibility of unwanted occurrences
- Diminishing the severity of outcomes

Avoiding the risk means that one strives for not to materialize the risk. It can be done by adjusting the probability to zero or by developing a protection mechanism that prevents possible outcomes. Generally the best way to avoid a risk is to renounce the activity. Although, note that by renouncing the activity new risks may come up. Risk mitigating can be done by mitigating the possibility or severity as mentioned earlier. See more about risk mitigation in the chapter 4.5. Risk can be shared or transferred to a partner or to an insurance company. (Hallikas et al. 2001, p. 53–54.) See more about risk sharing and transferring in the chapter 4.4.

If there is nothing that can be done to the risk or every possible action is done to mitigate the risk, then one has to accept it. Taking the risk is a more intentional action than accepting the risk. It means that one is ready to gamble. In other words the possibility of the risk is recognized, but it would be too costly, in time or money, to reduce, share or eliminate the risk. (Hallikas et al. 2001, p. 53–54.) If the possibilities of occurrence or severity of outcomes are not exactly clear, it is feasible to further analyze the risk and make actions after the inspection. (Hallikas et al. 2004, p. 54)

4.1. General risk management process

Generally risk management process does not differ between a supply chain and a single company (Hallikas et al 2004, p. 52; Zsidisin & Ritchie 2009, p. 4). According to Hallikas et al. (2004) a typical risk management process consists of:

- Risk identification
- Risk assessment
- Decision and implementation of risk management actions
- Risk monitoring

Risk identification is a phase where a decision-maker becomes aware of phenomena that cause uncertainty to be able to tackle them proactively. Thus, risks are identified by strong signals or by weak signals. Strong signals are easy to recognizer whereas weak signals require multiple feedback loops and chains of dependent events before one can tackle them. Information gathering, transmission and filtering are essential features when risks are identified. In a network, the dependences on other companies must be taken into account. (Hallikas et al. 2004, p. 52)

Risks are assessed by giving them an impact and a probability. Usually impact and probability are both ranked on a scale one to fife (or four), where fife is the most severe impact or a very probable risk. Impacts and consequences should be assessed from the viewpoint of an individual company, not network widely, whereas probabilities should be assessed from both viewpoints. That is because impacts vary from company to company. Some impacts may have negative effect, some positive when a risk materializes. On the contrary, the whole network affects the probability of a risk, because the probability is dependent on activities of a network. (Hallikas et al. 2004, p. 53). More about risk assessment can be read in Zsidisin et al's paper "An analysis of supply risk assessment techniques" (2004) and in Hallikas et al.'s paper "Risk analysis and assessment in network environments a dyadic case study" (2002).

The third phase is the actual risk management. Once the risk has been identified and assessed it can managed. The risk management action strategies (mitigate, eliminate, share, transfer, accept…) were already introduced earlier in the chapter 4 and that is why they are not discussed in this context. In a network, risks can be managed by a common network strategy, best practices and contract policies. Therefore collaboration and information exchange are important features of risk management in networks. (Hallikas et al. 2004, p. 54)

As actions are implemented, a constant monitoring is the next phase. Monitoring is done because risk status may change or new significant risk factors may arise as the environment is not static. Thus, changes in the network, customer needs, technology, competitors and partner strategies are monitored in order to identify risks. Hence, risk management is an iterative process. (Hallikas et al. 2004, p. 54)

In addition to these four phases, Zsidisin and Ritchie (2009, p. 5) add a fifth phase for supply chain risk management process. They call it as "organizational and personal learning including knowledge transfer". In this phase the experiences of the management process are shared within the organization as well as within associated supply chain members. The aim is to learn from the experiences and to share information.

4.2. Risk management tools for a supply chain

In this section tools for risk management in networks and supply chains are introduced. The first tool is based on the general risk management process that was discussed in the previous chapter. See Figure 2 for Hallikas et al's proposed tool.

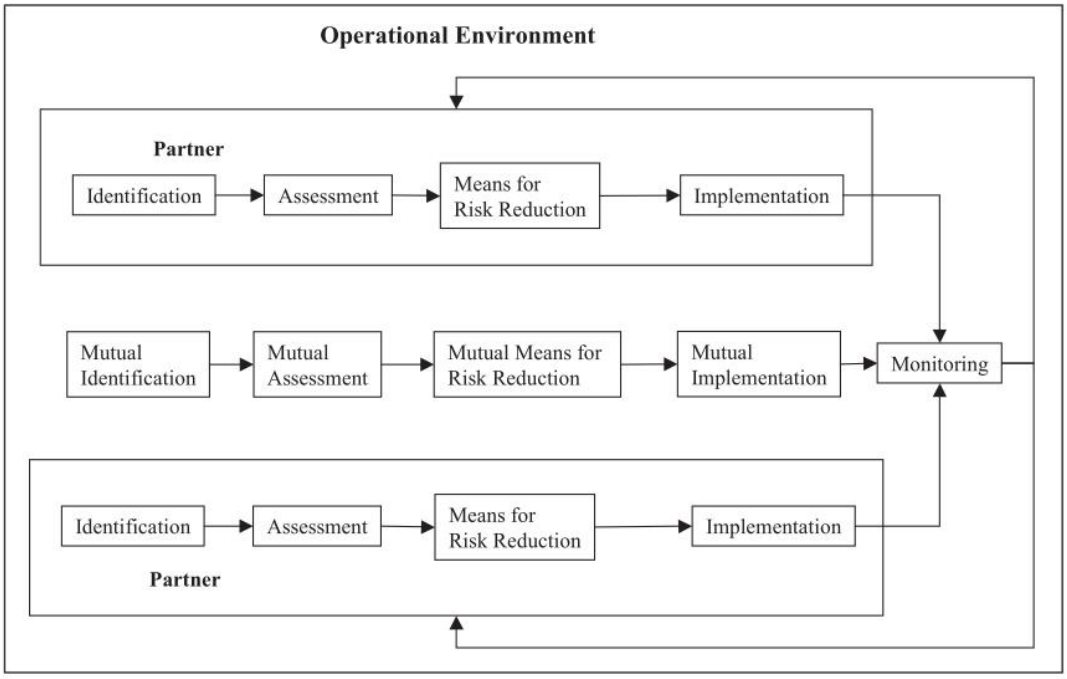

Figure 2. Risk management process in network environment. (Hallikas et al. 2004, p. 55)

Hallikas et al.'s process has the same phases as the earlier introduced general process, but in addition to the general risk management process it has a phase where companies manage risks collaboratively. So, each company is of course responsible for its own risks, but there is an extra round of mutual risk investigation. Hallikas et al. (2004) note that the risk management should be a continuous process.

Another tool was introduced by Harland et al. (2003). Their proposed model is a supply network risk tool by which one can assess and manage supply risks. It consists of six phases, which are iterated. The phases are similar to the earlier introduced general process. See the whole process in the Figure 3.

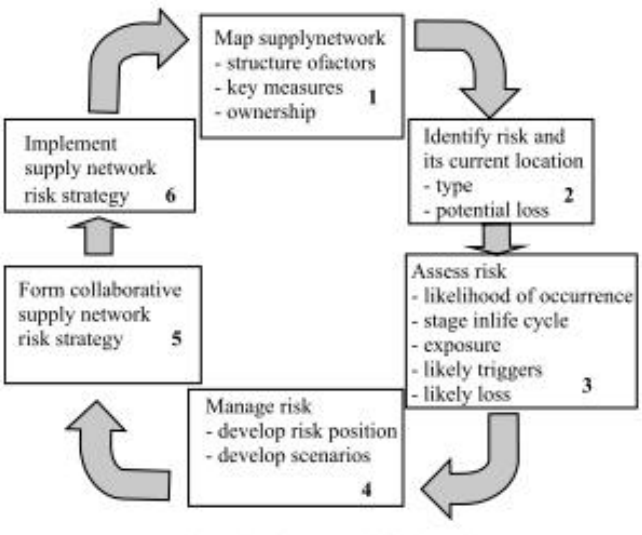

Figure 3. Supply network risk tool. (Harland et al. 2003, p. 56)

The first phase is to map the supply network. Mapping clarifies the roles and responsibilities of the actors and it defines the problem. The second box is related to identifying the risks by specifying them with the type of risk and its location. At this stage only those risks that can have a significant loss should be considered. The third box considers risk assessment. In this phase the likelihood of the risk occurrence, potential triggers and the likelihood of the amount of the losses are assessed. Moreover, one should evaluate at what stage in the life cycle the risk is likely to be materialized. (Harland et al. 2003, p. 56)

In the fourth box the assessment of information is analyzed and a risk position is determined. For a certain risk a risk position can be reactive, defensive, prospective or analytical. Depending upon the risk position, different scenarios are developed to realign the risk among the actors. The emphasis is on the network structures and relationship strategies. In the last phases 5 and 6, the chosen redesign is used to form a collaborative supply network risk strategy and the strategy is implemented. After implementation the network should be remapped. In other words a new iteration round begins. (Harland et al. 2003, p. 56)

The third tool introduced in this chapter is presented by Das and Teng (1999). Their work is based on strategic alliances and it is not a short-term process like the two earlier tools. Instead, their model depicts different phases of collaboration and risks included in those phases. Thus, they have a somewhat different perspective of how to manage risks in collaboration. The following Figure 4 depicts the risks.

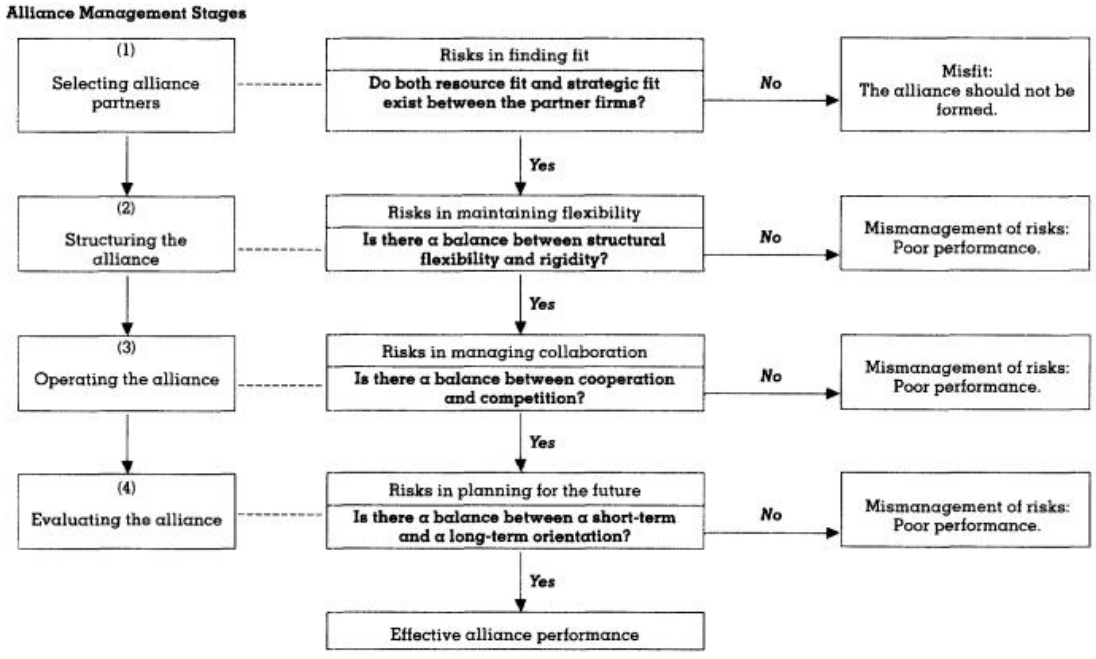

Figure 4. Risk management tool in strategic alliances. (Das & Teng 1999, p. 53)

As seen in the Figure 4, there are four stages of collaboration. In each of them the collaborating firms have to make an evaluation, whether the collaboration is efficient enough to advance to the next level. So, the companies are comparing risks and gains of collaboration.

4.3. Proactive supply chain risk management

Proactive supply risk management means that potential risks are identified at the supply chain design stage. Reactive management, instead, would mean that risks are mitigated when they materialize. Therefore proactive risk management is preferable, but it requires a lot of investments and people. Moreover, it becomes difficult to justify the time and money spent if risks never materialize. (Dani 2009, p. 58)

Normann and Jansson (2004) have discussed proactive supply risk management in case of leading telephone company Ericsson. They proposed a model that combines risk management, current logistics and three supply chain principles. The three principles are responsiveness, leanness and agility. Increasing agility, responsiveness and leanness may lead to increased outsourcing and reduced buffers and lead times, which indeed increase vulnerability and risks. On the other hand these principles also expose risks that are hidden and thus if these risks are managed properly, these techniques make supply chain risk management more efficient. (Normann & Jansson 2004)

4.4. Risk sharing and transferring

A risk can be transferred completely or shared with a partner. Moreover, a risk can be insured by an insurance company. Risk sharing or transferring does not generally diminish the overall risk, but instead it will share responsibilities of the risk. A partner, who accepts to take a share of the risk, will want some utility from the action. Therefore usually risk sharing includes some kind of fund transfer as of an insurance fee. (Hallikas 2001, p. 54.) Furthermore, when risk sharing is applied to network collaboration, the means varies according to the type of collaboration. (Harland et al. 2003, p. 55)

On the other hand, the total risk may be reduced by sharing the risk, if an insurer can cope with it better than the company sharing or transferring it. In other words, the risk may be too heavy to carry for a company and thus it may create a threat to the company's existence or other major problems. Therefore, risk sharing balances the situation and the overall risk (risk with all the consequences) will diminish. (Hallikas 2004, p. 54.) Also risks and profits go hand in hand and thus profit sharing is a way to share risks as well. This topic is dealt in Kuparinen's (2011) paper "Profit sharing in collaborative networks".

4.5. Risk mitigation

Risk mitigation is one of the main strategies for risk management. Faisal et al. (2006) have studied supply chain risk mitigation and determined 11 mitigation enablers. Those enablers are listed in the Table 1.

Table 1. Enablers of supply chain risk mitigation (Faisal et al. 2006)

Enabler	Comment
Information sharing	Effective communication and coordination are essential to success
Agility in the supply chain	Ability to thrive in a continuously changing, unpredictable business environment
Trust among supply chain partners	Mutual trust reduces opportunism
Collaborative relationships among supply chain partners	Support the development of flexibility and responsiveness. Require trust and commitment
Information security	Leaking sensitive information creates a major threat to a supply chain
Corporate social responsibility	Disclosing social responsibility information to public reduces threats of lawsuits and boycotts
Aligning incentives and revenue sharing policies	Aligning reduces opportunistic behavior
Strategic risk planning	Successful companies identify and develop contingency plans for various risks
Risk sharing in a supply chain	Focusing on the risks of others, not only on own risks, helps to understand the entity
Knowledge about risks in a supply chain	Improved knowledge of risks helps to make better decisions
Continual risk analysis and assessment	Dynamic environment may change risks

In their study Faisal et al, found that **collaborative relationship, information sharing** and **trust among supply chain partners** create the basis for risk mitigation. These enablers have high driving power and low dependence of other enablers. Thus, those three factors require maximum attention and their strategic importance is essential. Other variables are resultant actions of these bolded enablers. Hence, other variables have lower driving power and their dependence is higher. None of the variables have both low driving power and dependence and therefore all of them are connected to the system and managers have to pay attention to them. (Faisal et al. 2006)

Also Jüttner et al. have studied different risk mitigation strategies in supply chains. They adapted Miller's (1992) proposed strategies to fit to supply chains. Thus, they had four strategies, which are listed in the Table 2.

Table 2. Risk mitigating strategies in supply chains (Jüttner et al. 2003, p. 206 originally Miller 1992)

Mitigation strategy	Examples
Avoidance	• Dropping specific products/markets/supplier/customer organizations
Control	• Vertical integration • Buffer inventory • Maintaining excess capacity • Imposing contractual obligations to suppliers
Cooperation	• Joint efforts to improve supply chain visibility • Joint efforts to share risk-related information • Joint efforts to prepare supply chain continuity plans
Flexibility	• Postponement • Multiple sourcing • Localized sourcing

Avoidance means that a certain product, market, supplier or customer is dropped because it generates unacceptable risks. By controlling contingencies from the risk sources, companies can better mitigate risks. In other words it is sensible to control rather than passively treat uncertainties as constraints. With cooperation companies can jointly resolve problems related to the supply chain. Jointly made agreements improve supply chain visibility and understanding. Flexibility increases responsiveness in a supply chain. Thus, risks are mitigated with a fast responsiveness to the problem. (Jüttner et al. 2003, pp. 205–207)

REFERENCES

Chopra, S. & Sodhi, M. S. 2004. Managing Risk To Avoid Supply-Chain Breakdown. MIT Sloan Management Review. Vol. 46, No. 1, pp. 53-62.

Dani, S. 2009. Predicting and Managing Supply Chain Risks. Supply Chain Risk: a handbook of assessment, management and performance. Springer US. pp. 53-66.

Das, T. & Teng, B. S. 1999. Managing risks in strategic alliances. The Academy of Management Executive. Vol. 13, No. 4, pp. 50-62.

Faisal, M. N., Banwet, D. K. & Shankar, R. 2006. Supply chain risk mitigation: modeling the enablers. Business Process Management Journal. Vol. 12, No. 4, pp. 535-552.

Hallikas, J., Virolainen, V. & Tuominen, M. 2002. Risk analysis and assessment in network environments: A dyadic case study. Int J Prod Econ. Vol. 78, No. 1, pp. 45-55.

Hallikas, J., Ojala, M. and Metalliteollisuuden keskusliitto. 2001. Riskienhallinta yhteistyöverkostossa, Metalliteollisuuden kustannus.

Hallikas, J. 2003. Managing risk in supplier networks: case studies in inter-firm collaboration. Doctor of Science thesis, Lappeenranta University of Technology.

Hallikas, J. & Virolainen, V. 2004. Risk management in supplier relationships and networks. Supply Chain Risk: a handbook of assessment, management and performance. pp. 43-65.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V. & Tuominen, M. 2004. Risk management processes in supplier networks. Int J Prod Econ. Vol. 90, No. 1, pp. 47-58.

Harland, C., Brenchley, R. & Walker, H. 2003. Risk in supply networks. Journal of Purchasing and Supply Management. Vol. 9, No. 2, pp. 51-62.

Investopedia.com. 2011. [WWW] http://www.investopedia.com. Cited 20.7.2011.

Jüttner, U., Peck, H. & Christopher, M. 2003. Supply chain risk management: outlining an agenda for future research. International Journal of Logistics: Research & Applications. Vol. 6, No. 4, pp. 197-210.

Kearney, A. 1999. Insight to impact: results of the fourth quinquennial European logistics study. European Logistics Association, Brussels.

Kuparinen, P. 2011a. Profit sharing in collaborativenetworks. Tampereen teknillinen yliopisto.

Kuparinen, P. 2011b. Incentives and revenue sharing in networks. Tampereen teknillinen yliopisto.

Manuj, I. & Mentzer, J. T. 2008. Global supply chain risk management strategies. International Journal of Physical Distribution & Logistics Management. Vol. 38, No. 3, pp. 192-223.

Miller, K. D. 1992. A Framework for Integrated Risk Management in International Business. J.Int.Bus.Stud. Vol. 23, No. 2, pp. 311-331.

Norrman, A. & Jansson, U. 2004. Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. International Journal of Physical Distribution & Logistics Management. Vol. 34, No. 5, pp. 434-456.

Tang, C. & Tomlin, B. 2008. The power of flexibility for mitigating supply chain risks. Int J Prod Econ. Vol. 116, No. 1, pp. 12-27.

Yates, J. F. & Stone, E. R. 1992. The risk construct.

Zanger, C. 1997. Opportunities and risks of network arrangements among small and large firms within supply chain. Vol. 24, pp. 26.

Zsidisin, G. A. and Ritchie, B. 2009. Supply Chain Risk Management – Developments, Issues and Challenges. Supply Chain Risk: a handbook of assessment, management and performance. Springer US. pp. 1-12.

Zsidisin, G. A., Ellram, L. M., Carter, J. R. & Cavinato, J. L. 2004. An analysis of supply risk assessment techniques. International Journal of Physical Distribution & Logistics Management. Vol. 34, No. 5, pp. 397-413.

Zsidisin, G. A. 2003. A grounded definition of supply risk. Journal of Purchasing and Supply Management. Vol. 9, No. 5-6, pp. 217-224.