International Journal of Excellence
in Public Sector Management

Risk Management in Virtual Organizations

Mohammad Alawamleh
and
Keith Popplewell

Coventry University, UK

ISSN 19938640
VOLUME 4 – Issue 1
January 2011

Abstract

There are many benefits associated with networking, but this novel innovation cannot be considered as being risk free. Both Small and Medium sized enterprises (SMEs) in particular have been at the forefront of significant changes when functioning as a partner within a virtual Organization. These enterprises have been compelled to adjust swiftly and with a great deal of flexibility, due to the pressure imposed by the astonishing speed at which technology has been developing, and by the mounting international competition.

In this paper the literature dealing with the risk to virtual Organizations , beginning with risks in the supply chain, will be discussed, then the risk propagation impact will be addressed before examining the most universally used definitions of risk. In the second part of the paper there will be a discussion of risk management approaches, and the previous model for the identification of risk in supply networks, before proceeding to the essential elements of the risk management process including identification and assessment which is the main core of this research.

Keywords: Risk, Virtual Organization, VO, Networking, SME.

Risk in Networking

In assessing risks within the framework of a VO, it is vitally important that enterprises recognise all types of risks, not only direct risks to their operations but also the risks to all other entities as well as those risks caused by the linkages between them (Jüttner, 2005). To further enhance the understanding of virtual Organization risk, it is worth exploring the existing similarities between this and supply chain risk, and risks in relation to virtual Organization, supply chain and joint venture. This comparison could potentially yield practical proposals resulting from research in this area, and fill in the gap in the study of risk in VOs (Chen and Chen, 2006). Hallikas et al. (2004) argues that although collaboration can be useful as a strategy to manage and to minimize risks, it tends to bring in new risk factors.

Harland et al. (2003) assert that the difficulty is caused by a variety of factors such as globalization, mounting product/service complication, subcontracting, e-business and demanding customers' needs. These factors have led enterprises to depend more and more on their outside resources but these come with risks. In turn, corporate risk management, in terms of its function, has been modified to provide a counter impact to external sources of risk.

Risks and benefits in joint ventures are, as a rule, shared through combined ownership and with official agreement in relation to various aspects, such as obligation contracting, profit distribution and the provision of incentive systems for the

collaboration parties concerned (Harland et al., 2003). Formality is paramount in collaborations as its lack may lead to less understandable risk and disrupt stability and benefit sharing.

Risk management is by no means an easy task due to the nature of its dynamics and the complexity of supply networks. The moment enterprises in the supply networks begin to develop an over reliance on each other, they become highly likely to be affected by the risks and weaknesses of one another. Zsidisin et al. (2000) draw attention to supply risks linked to design, cost, quality, availability, manufacturability, supply, legal and environment, and health and safety. In their assessment of critical risk factors, Sutton et al. (2008) point out that a complete Organization's enterprise risk may be distorted by the ambitious extended enterprise systems in relation to B2B e-commerce. Furthermore, in an attempt to unravel how different factors affect each other and contribute to the overall risk, they investigate the interrelationships between varieties of risk factors in B2B e-commerce.

It appears that the risks connected to collaboration are not purely dependent on a single enterprise's aims and objectives, despite the desire of some parties in these relationships to assume control and also the duty of completely managing the supplier network. The mounting distribution of responsibilities and the very nature of these relationships need to be scrutinized (Hallikas, 2002).

Risk Management Approaches

The Royal society (1992) defines risk management as a sequence of steps and measures created by Organizations to counter any form of risk exposure. This process normally incorporates identification of risk and its measurement as well as control and observation.

The primary aim of risk management, according to Norrman and Jansson (2004), is to comprehend the implications of risks and to reduce their impact by paying attention to elements such as probability and impact. It is also important to note that the phases in relation to the process of risk management may appear to be variable in terms of labeling as in, risk identification, analysis or (estimate), risk assessment or (evaluation), and different strategies for risk management. However, 'labels differ among authors,' but 'the steps are similar' (Norrman and Jansson, 2004).

A number of approaches have been developed in risk management and Supply Chain Management (SCM) to tackle the roots of risk in supply chains. Norrman and Jansson (2004) explain that Ericsson's feedback SCRM approach consists of a set of phases that are simple to understand, beginning with incorporated risk, identification, assessment, remedy and observation and including occurrence management and backup planning in order to diminish risk exposure in supply chains.

Risk Models for Supply Networks

In relation to risk for supply networks, Harland et al. (2003), present a model, as illustrated in the figure (1) below, which adheres to the conventions of a systematic discipline starting with mapping the supply network and ending with implementing network risk strategies.

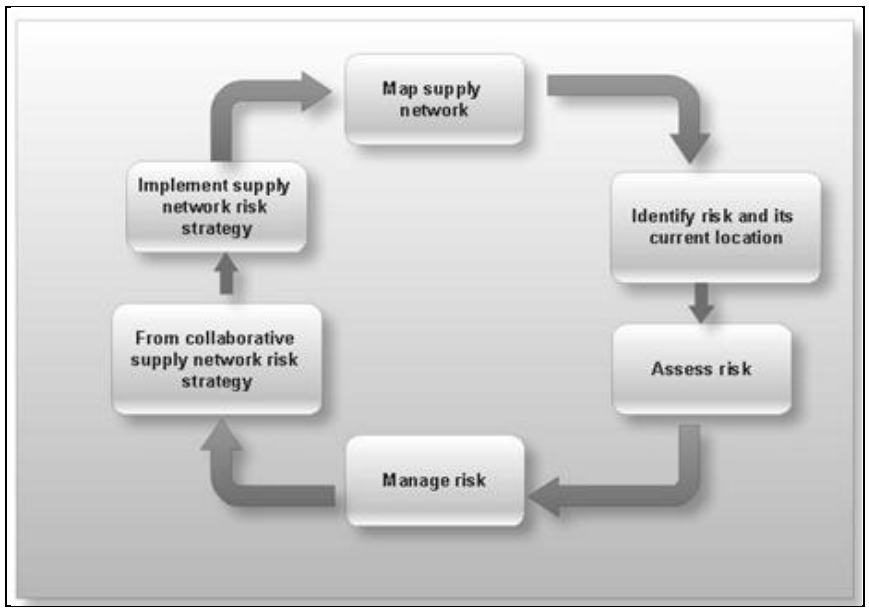

Figure 1: Supply Network Risk Model (Harland et al., 2003).

The steps in the figure clarify the procedure for the model as follows:

1. Map supply network: This may involve identifying who possesses what, and what principal measures are presently put in place as for example transparency in role and responsibility within the network. It is also the start of the risk tool model.
2. Identify risk and its current location: This is step two of the procedure of the tool during which the sources of the risk are located.
3. Assess risks: This is step three and involves scrutinising the selected risks to determine the likelihood of their incidence, exposure in the network, and possible causes.
4. Manage risk: This is the phase where the management of risks is a primary target, and where risks begin to be analyzed within the network and their associated damages are calculated.
5. Form collaborative supply network risk strategy: Here the possibility of selecting more appropriate options for treatment of the risks being examined arises.
6. Implement supply chain risk strategy: This is the final stage where the real option strategy is implemented followed by a remapping of the network.

Zsidisin et al. (2004) propose a process which incorporates the following elements; identification, manager appointment, initiation of score card, criteria review, data collection, assignment of risk scores, impact analysis, document analysis and action, monitoring, and decision to end assessment. The process itself is known as the 'Ten-step SCRM' and consists of eight risk factors.

It appears that the process of risk management applied to the network risk within a virtual Organization and the steps taken are representative of risk management that adheres to risk identification, risk assessment, identification and implementation of risk reduction and risk monitoring.

Pfohl and Buse (2000) are of the view that it is strategic networks and virtual Organizations that should be at centre stage. In regard to virtual Organizations , they suggest they symbolise dynamic networks, and are not based on a hierarchical system. This allows an enterprise to function as a liaison officer in a network including customers, suppliers, services, providers and other specialised services. Conversely, strategic networks tend to be firmer in their nature. There is a division of roles in the network which can make coordination challenging in the sense that responsibilities are to be undertaken by all parties including the first tier supplier and the multi-tier suppliers. The network can also be structurally complex due to the nature of the logistics and service providers linking the first buyer to the first tier supplier.

Supply chain risk management according to Norrman and Lindroth (2004) is the collaboration of partners in applying the risk management process in a supply chain and deploying the appropriate means to tackle 'risks and uncertainties caused by or impacting on logistics related activities or resources'. This description of risk management in a supply chain can fit in with the needs of a single enterprise in the chain when dealing with its risk management concerns. Blackhurst et al. (2004) acknowledge that naturally the activity of every enterprise carries a commercial risk to a certain extent, and taking part in a network enterprise brings with it other risks in relation to collaboration. These risks are evident, for example, in the failure of a particular partner, and may lead to accruing cost to replace a service or a partner. There are also risks associated with loss or exploitation of confidential commercial data. As well as this, the inadequate understanding of technology and uncertainty over the collaboration and commercial abilities of other partners, make risk assessment that is meant to be effective in decision making, more complex and more of an obstacle standing in the way of the need to administer risks presented by various interacting sources.

Both the entwined relationships between risks and their possible impact on the network or the individual enterprise develop within the life span of a network enterprise (Lin and Patterson, 2007). On the same note, in their view of risk management and its strategies in worldwide supply chains, Manuj and Mentzer (2008), assert that global supply chains tend to be less safe than home ones. This is the result of the vast number of connections within an extensive network of establishments. These connections are highly likely to cause a number of negative outcomes such as insolvency, distraction, collapse, global economic and political instability and catastrophes. Therefore, risks levels multiply and their management becomes a daunting task. In describing SCRM as a managerial task, Jüttner et al. (2003) suggests that it is "the identification and management of risks for the supply chain, through a co-ordinated approach amongst supply chain members, to reduce supply chain vulnerability as a whole". This description shares common features with the one put forward by Lindroth and Norrman

(2001) with the exception that the latter adopts a narrow outlook by viewing SCRM as being concerned with 'risks caused by, or impacting on, logistics-related activities or resources'.

Risk Management Process

It is essential that risk management plays a fundamental part in the management and planning of any given Organization. Moreover, for a risk management program to be effective, it has to be a progressive course of assessment, intervention and contingency planning (McGrew and Bilotta, 2000).

Bandyopadhyay et al. (1999) point out four principal constituents of risk management:

1. Risk identification: this involves identifying and measuring the exposures which could jeopardize a company's assets and prosperity.
2. Risk assessment: this entails identifying and evaluating risks imposed on a company and its assets so as to opt for suitable and reasonable defensive measures.
3. Decision and implementation of risk management actions: this involves risk deduction, transfer and response, decreasing or shifting the weight of financial loss, particularly in the case of a crisis, to ensure that a company is able to proceed with its operations without distorting its fiscal steadiness.
4. Risk monitoring: this refers to the continuous assessment of present and possible future exposure.

In general, the risk management process within a network setting consists of the same steps, and every enterprise functions at its own risk as well as bearing the responsibility of managing its own risks. Also, the interdependent nature of enterprises in the network can be helpful in the sense that the risk management process is shared and collaborative strategies are developed to control risks.

White (1995) is of the opinion that most approaches to risk management appear to adhere to the generic process regardless of the various systems that have been proposed, and adds that this process comprises three crucial steps:

1. The risk identification phase which focuses on determining all risk factors that may arise in a project.
2. Risk analysis for the purpose of recognizing the probability and the degree of the most important risks.
3. Risk evaluation focusing on deciding the most suitable management strategy to deal with every risk and the most suitable team to manage the risks identified.

In their study of risk evaluation problems, Li and Liao (2007) reveal that different types of risk factors which influence the operation of partners have been identified, and the measurement of their extent is determined by three elements; the chance of risk incidence, seriousness of consequence and control of the level of risk. These elements are represented by trapezoidal fuzzy numbers.

Figure 2 demonstrates the four stages which constitute the risk management process of dynamic alliances:

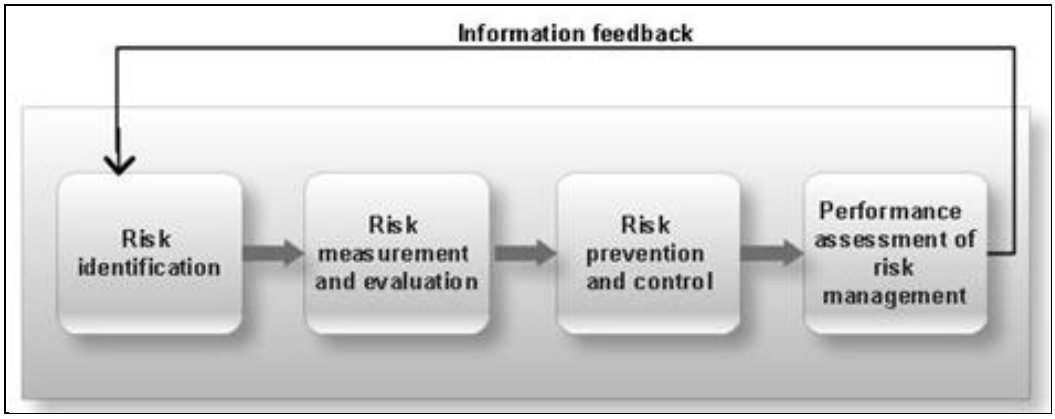

Figure 2: Risk Management Process of Dynamic Alliance (Li and Liao, 2007).

The risk identification phase forms the platform on which the whole process of risk management rests, and focuses mainly on identifying all types of risks factors, be they obvious or potential, by way of analyzing an extensive amount of credible information. The working team bears the responsibility for doing so throughout the business activities of all alliance members.

The risk measurement phase is set to pinpoint the level of risk in each factor based on risk identification, and risk evaluation aims at estimating the overall scale of alliance by way of applying different approaches and technologies such as expert scoring methods, the AHP/ ANP method, and fuzzy inclusive evaluation, among others. This phase is also highly important in the risk management process and should be taken seriously as any incorrect estimation can lead to the alliance missing out on lucrative market opportunities, and any neglect of risks may end in needless losses.

The next phase that follows estimation and evaluation is referred to as risk prevention and control, and it is the part of the process where the focus is on the reduction of both risk incidence likelihood and the level of loss. The final stage of the process is not only put in place to scrutinize and assess risk prevention and control performances, but also to fine-tune risk factors and to alter the means used in risk prevention and control so as to acclimatize to new circumstances.

Risk Sources

Risks can derive from various sources leading to divergent views about what determines them. Manson-Jones and Towill (1998) identify three types of risks in supply chains:

1. Internal risks in operation, such as accidents, non-reliability of equipment, loss of data, individual errors and quality issues; risks occurring as a direct result of managers' decisions such as choosing the size of consignment, safety of supply levels, monetary issues and delivery plans.
2. Risks that occur outside the Organization, but affect the supply chain. These may come to exist amid the interaction between the players in the supply chain, and can be divided into two categories; risks related to suppliers such as reliability, availability of materials, delivery and schedules issues and industrial incidents, and risks related to clients as in for example problems with payments and order processing, changeable demands and tailored requirements.
3. External risks can also be environmentally determined as they can result from factors

such as accidents, severe weather conditions, regulations, crimes and wars.

Dealing with the same problem, Zsidisin et al. (2000) assert that the sources of supply chain risks derive from issues in relation to design, quality, cost, availability of produce and production, supplier, legislative and environmental problems, and health and safety matters.

In classifying risks sources in relation to supply chains, Jüttner et al. (2003) propose three types of sources: external, internal and network related as illustrated in figure (3).

It appears that external risks are influenced by factors such as the social and natural environment, politics and the industry market, whereas internal ones are determined by factors such as actions of the workforce in the case of strikes, production failure related to machine failure, and IT system setbacks. Furthermore, network related risks result from interactions between Organizations inside the supply chain.

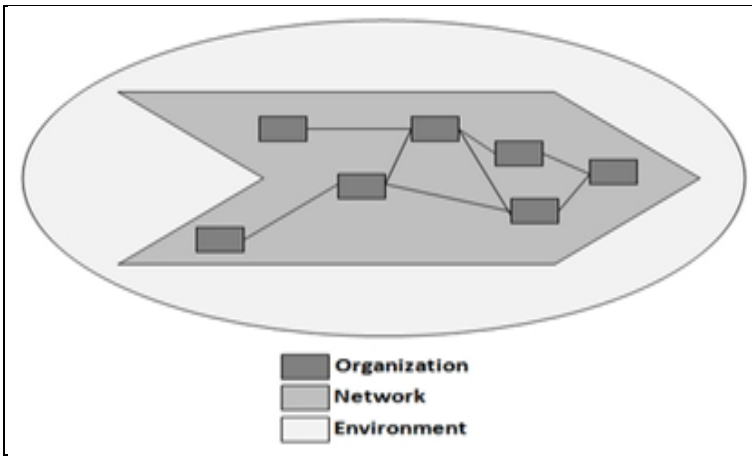

Figure 3 Supply Chain Risk Sources adapted from Jüttner et al. (2003).

In the managerial process set to tackle supply chains risks, Jüttner et al. (2003) put forward four essential sequential steps that are interlinked as described in figure (4) below; risk sources, consequences, risk drivers and mitigation strategies. That is to say risk sources result in unfavorable consequences which are prompted by risk drivers that may be counterbalanced by mitigation strategies.

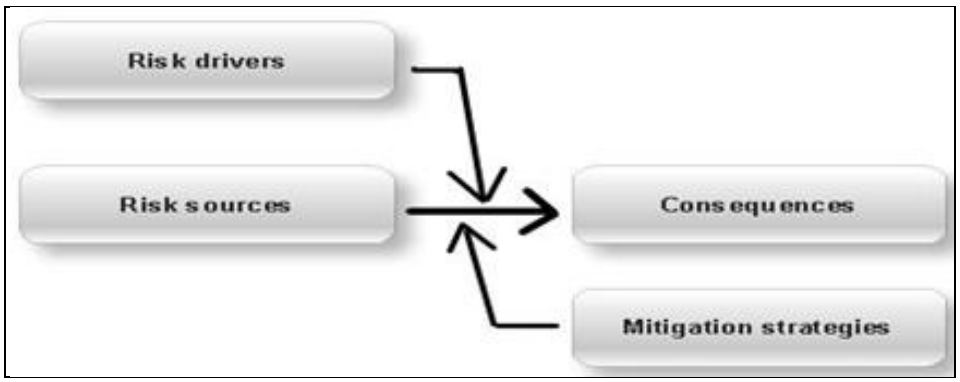

Figure 4: Supply Chain Risk Management adapted from Jüttner et al. (2003).

There are other risks that may occur within supplier networks. These are evident in for example the loss of know-how and the mishandling of data as a result of actions taken by individuals within the network who might be tempted to serve their own personal agenda. As well as this, there may be some cultural differences among partners which in turn may result in an undesirable impact on the nature of trust shared within a network in terms of collaboration. This also may provoke internal antagonism towards cooperation from both staff and management (Zanger, 1997).

Rigby (1996) outlines the risk of project failure which may be attributed to cultural discrepancies or the lack of a unified structure and objectives which would normally connect two parties. Wynstra et al. (2001) suggest another widespread risk source which is defined by the inability to engage in product development collaboration by the chosen suppliers.

In evaluating risk sources and in the light of this literature review and preceding studies, it is safe to state that, as noted in the Jüttner et al. (2003) classification, risk sources in a network are different because of different relations among supply chain partners and virtual Organization partners but internal and external risk sources are similar.

Kent (1992) asserts that supply chain risks can occur at four different levels: Organizational, network, industrial and environmental. The main focus of this study is risk sources in relation to networks, and the risk sources that fit into the second category of risk sources as suggested by Gaonkar and Viswanadham (2007). These risks are divided into two types: the first type suggests that firms are exposed to attacks targeting their assets as well as their suppliers, clients, transportation providers, lines of communication and other aspects in their environment. The second type indicates that firms are equally exposed to unreasonable behavior from their network partners as in for example sharing classified information about product design with an opponent manufacturer.

Jüttner et al. (2003) is of the view that supply chain risks can be directly attributed to the supply chain structure itself. In other words, the sources of supply and demand risks are rooted in supply chains and are likely to impact on the interdependent parties involved in the chain. In addition, demand and supply risks in terms of them being internal supply chain risk sources, suggest that the responsibility for SCRM implementation can be in the hands of any company within the supply chain and that, at the same time, the enterprise itself can be a source of risk to the supply chain.

Bandyopadhyay et al. (1999) assert that the IS environment within an enterprise consists of three levels:

1. The application level: This level focuses on the risks in relation to technical or implementation failure of IT applications. These risks can result from both internal and external sources (Rainer et. al., 1991).
2. The Organizational level: At this level, the focal point is the impact of IT throughout all functional areas of the Organization and not just any isolated application. Noticeably, businesses are increasingly

utilising IT at this level to remain competitive. Lightle and Sprohge (1992) present three types of Organizational risks from the internal auditors' perspectives: sustainability risk, data security risk, and legal risk.

3. The inter-Organizational level: This level involves the IT risks of Organizations which operate in a network environment. The most prominent use of IT nowadays is evident in networks that exceed any Organizational limitations. These are normally automated IS shared by two or more Organizations. The increase in the use of these inter-Organizational systems has helped to increase productivity, flexibility, and competitiveness (Cash et al., 1988).

Das and Teng (1996) argue that risks in strategic alliances can be independently isolated as relational risk and performance risk. They go on to define relational risks as the probability and the consequences of not totally adhering to the cooperation requirements.

These kinds of risks can be triggered by the possibility of opportunistic behavior from any two or more firms. Opportunistic behavior can be tied down to matters such as minimizing information, cheating or otherwise distorting information and so on. This in turn can lead to conflicts as the individual interests of a firm may not be compatible with those of their partners. Khanna et al. (1998) refer to the benefits that ensue to one partner only as 'private benefits' and argue that they are a source of interest conflicts.

Furthermore, there exist several additional factors which may negatively impact on alliance performance. These factors may include new entrants, intensified competition, fluctuations in demand, changed government policies and incompetence of one of the partners. These factors are responsible for performance risk, or the probability and consequences that alliance objectives are not achieved, despite satisfactory cooperation among partner firms (Das and Teng 1996).

Finch (2004) splits risks into three categories including three levels of coverage; application level, Organizational level, and inter-Organizational level. The application level incorporates aspects such as natural disasters, accidents, premeditated acts, data/information security risks, and management issues. The Organizational level refers to risks such as the legal and strategic alterations in decisions that could happen, whereas the inter-Organizational level is where possible uncertainties from the outside of the Organization could pose risks.

Risk Management Strategies and Mitigation Plans

Strategically, risk management aims to identify and assess the probabilities and the aftermath of risks, and to enable the selection of suitable approaches to minimize the probability of losses related to undesirable events. Risk mitigation aims to limit the consequences in the event of undesirable happenings (Norrman and Jansson 2004).

In their view of risk management strategies, Jüttner et al. (2003) and Miller (1992) identify

seven major categories which are avoidance, postponement, speculation, hedging, control, sharing/ transferring and security.

Hallikas et al. (2004) illustrate the structure of the risk management process and put forward their methods in a multifaceted network milieu. Their study is intended to contribute to offering more of a complete understanding of risk management in suppliers' networks. For example in the case of dependency increasing between enterprises, an enterprise may become more susceptible to risks evoked by others within the network and hence become in need of the above proposed process to help with facilitating understanding and managing uncertainties and risks in supplier networks.

On the whole, risks within a network milieu can be managed via the adaptation of a common strategy in addition to appropriate practice modes of actions and contract policies. Notably, it is the identification of risks and their assessment that shed light on what course of actions are to be taken. While some risks can be collectively lessened in the network, others have to be solely managed by each partner. The diversity of objectives of various networks in a multi-network milieu can instigate contradictions for an enterprise, and this is the moment when the actual assessment of risks can assist the enterprise in deciding how to best function in these circumstances.

The nature of network relationships at times increases the need for transferring risks from one company to another, and this may only work if the company receiving the risk can deal with it better than the one who has initially transferred it. Let us consider the risk of investment as an example to better understand the concept of risks transfers. The likelihood of an investment failure may decrease if the supplier can use it in many networks or client relationships. However, at times, the impact of transferred risks may be greater for the risk-taking suppliers than for the original equipment manufacturer.

The main objective of network extended analysis is to find the best possible risk management strategies to share and to weigh up risks at the network level. It is also important to note that the nature of risks is subject to change due to the enterprises and their milieu being changeable, and known risk factors may be monitored to pinpoint the possible trends in their probability or aftermath.

Finch (2004) views supply chain risks management from an inter-Organizational networking angle, and emphasizes the need for enterprises to appropriately plan to ensure continuity in business. This may include matters resulting from processes within or outside the Organization. Christopher and Lee (2004) suggest methods that are controlled within and by the Organization and stress the need for improving supply chains as mechanisms to mitigate risks. Norrman and Lindroth (2001) identify four major techniques in relation to the management of risks: risk sharing, transferring, reduction and avoidance.

Risk sharing is attained via contracts and improved cooperation among members of the supply chain, and risks may be transferred to suppliers by 'just in time

deliveries' and made to order contracts, as well as outsourcing. Risk reduction can be attained via a number of different methods and strategies (Norrman and Jansson, 2004).

Miller (1992) puts forward five elements related to risk management: control, cooperation, imitation, flexibility and risk avoidance. The first four are seen as techniques for the purpose of reducing risks. In order to control uncertainties, companies engage in political lobbying to establish market power and, hence, control competitors via various means. On the other hand, cooperative strategies tend to be less strict than control and incorporate contracts and alliances between various companies where the level of interaction is not as strong as the cooperation at the time of risk sharing. Imitation entails adopting similar approaches used by other companies such as pricing and product development for the purpose of reducing risks. Flexibility is achieved by diversifying product lines and by adequately using various and numerous suppliers.

In so far as avoidance is concerned, if a risk is classed as unacceptable, the company must therefore avoid the product, geographical location, supplier, or the client Organization which instigates the risk as suggested by Norman and Lindroth (2001).

Conclusion

The idea behind this paper is to help with the understanding of risk management in VOs. It has also emerged in this study that most enterprises operate within more than one network and each enterprise sees risks in a different manner. Also, it can be said that where enterprises are dependent on each other, risk transfer and sharing inevitably occur in the VO. It should be remembered that an increase in dependency between enterprises may mean that they are more exposed to risks adhering to other enterprises. Networking also increases the partners' responsibilities and sometimes investment risks may be transferred to partners.

The process of risk identification is a crucial stage of the overall risk management process as, in networks, risk sources may derive from complex chains and can be hard to perceive. It is also important to acknowledge that the dynamics of relationships and their development can cause extra difficulties. Therefore, enterprises should clearly communicate and share their views on risks as this may help enhance their understanding of common opportunities and threats in a more holistic manner. In turn, the enhanced understanding can lead to better decisions and can lessen risks of single Organizations and networks.

References

Bandyopadhyay, K., P. Mykytyn, et al. (1999). "A framework for integrated risk management in information technology." Management Decision 37(5): 437-444.

Blackhurst, J., T. Wu, et al. (2004). "Network-based approach to modeling uncertainty in a supply chain." International journal of production research 42(8): 1639-1658.

Cash, J. I., F. W. McFarlan, et al. (1988). Corporate Information Systems Management,. Homewood, IL., Irwin.

Chen, J. and J. Chen (2006). "Study on revenue sharing contract in virtual enterprises." Journal of Systems Science and Systems Engineering 15(1): 95-113.

Christopher, M. and H. Lee (2004). "Mitigating supply chain risk through improved confidence." International Journal of Physical Distribution and Logistics Management 34(5): 388-396.

Das, T. K. and B.-S. Teng (1996). "Risk types and inter-firm alliance structures." Journal of Management Studies 33: 827-843.

Finch, P. (2004). "Supply chain risk management." Supply Chain Management: An International Journal 9(2): 183-196.

Gaonkar, R. and N. Viswanadham (2007). "Analytical Framework for the Management of Risk in Supply Chain." IEEE Transaction on Automation Science and Engineering 4(2): 265-273.

Hallikas, J., I. Karvonenb, et al. (2004). "Risk management processes in supplier networks" International Journal of Production Economics 90(1): 47-58.

Hallikas, J., V.-M. Virolainen, et al. (2002). "Risk analysis and assessment in network environment: a dyadic case study." International Journal of Production Economics 78: 45-55.

Harland, C., R. Brenchley, et al. (2003). "Risk in supply networks." Journal of purchasing and supply management 9(1): 51-62.

Jüttner, U. (2005). "Supply chain risk management—understanding the business requirements from a practitioner perspective." International Journal of Logistics Management 16(1): 120-141.

Juttner, U., H. Peck, et al. (2003). "Supply chain risk management: Outlining an Agenda for future research." International Journal of Logistics: Research and Applications 6(4): 197-210.

Kent, M. (1992). "A framework for Integrated Risk Management in International Business." Journal of International Business Studies second quarter: 311-331.

Khanna, T., R. Gulatui, et al. (1998). "The dynamics of learning alliances: Competition, cooperation, and relative scope." Strategic Management Journal 19: 193-210.

Li, Y. and X. Liao (2007). "Decision support for risk analysis on dynamic alliance." Decision Support Systems archive 42(4): 2043-2059.

Lightle, S. and H. Sprohge (1992). "Strategic information system risk." Internal Auditing: 31-36.

Lin, A. and D. Patterson (2007). An Investigation into the Barriers to Introducing Virtual Enterprise Networks. Supply Chain Management W. Wang, M. Heng and P. Chau, Idea Group Inc: 23-45.

Lindroth, R. and A. Norrman (2001). Supply chain risk management: purchasers' vs. planners view on sharing capacity investment risks in the telecom industry. Proceedings of the IPSERA 11th International Conference, Enschede.

Manson-Jones, R. and D. R. Towill (1998). "Shrinking the supply chain uncertainty circle." Institute of Operation Management Control Journal 24(7): 17-23.

Manuj, I. and J. T. Mentzer (2008). "Global supply chain risk management strategies." International Journal of Physical Distribution & Logistics Management 38(3): 192-223.

McGrew, J. F. and J. G. Bilotta (2000). "The effectiveness of risk management: measuring what didn't happen." Management Decision 38(4): 293-301.

Miller, K. (1992). "A Framework for Integrated Risk Management in International Business." Second Quarter Journal of International Business Studies 23(2): 311-331.

Norrman, A. and U. Jansson (2004). "Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident." International Journal of Physical Distribution and Logistics Management 34(5): 434-456.

Norrman, A. and R. Lindroth (2004). Categorization of Supply Chain Risk and Risk Management. Supply Chain Risk. C. Brindley: 14-27.

Pfohl, H. and H. Buse (2000). "Inter-organizational logistics systems in flexible production networks." International Journal of Physical Distribution & Logistics Management 30(5): 388-408.

Rainer, R. K., C. A. Snyder, et al. (1991). "Risk analysis for information technology." Journal of Management Information Systems 8(1): 129-147.

Rigby, B. (1996). "Continuous acquisition and life-cycle support: the risks and benefits of early supplier involvement in the development process." Logistics Information Management 9(2): 22-26.

Society, R. (1992). Risk: Analysis, Perception and Management. London, Royal Society

Sutton, S. G., D. Khazanchi, et al. (2008). "Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships." Journal of the Association for Information Systems 3-4(9): 151-174.

White, D. (1995). "Applications of systems thinking to risk management: a review of the literature." Management Decision 33(10).

Wynstra, F., A. v. Weele, et al. (2001). "Managing supplier involvement in product development: Three critical issues " European Management Journal 19(2): 157-167.

Zanger, C. (1997). Opportunities and risks of network arrangements among small and large firms within supply chain. Sixth International Annual Ipsera Conference. Naples, Italy.

Zsidisin, G. A., L. M. Ellram, et al. (2004). "An analysis of supply risk assessment techniques." International Journal of Physical Distribution and Logistics Management 34(5): 397-413.

Zsidisin, G. A., M. Jun, et al. (2000). "The relationship between information technology and service quality in the dual-direction supply chain: A case study approach." International Journal of Service Industry Management 11(4): 312-328.