Research note

Assessing and managing risks using the Supply Chain Risk Management Process (SCRMP)

Rao Tummala
Computer Information Systems Department, College of Business, Eastern Michigan University, Ypsilanti, Michigan, USA, and

Tobias Schoenherr
Department of Supply Chain Management, The Eli Broad Graduate School of Management, Michigan State University, East Lansing, Michigan, USA

Abstract

Purpose – The purpose of this paper is to propose a comprehensive and coherent approach for managing risks in supply chains.

Design/methodology/approach – Building on Tummala *et al.*'s Risk Management Process (RMP), this paper develops a structured and ready-to-use approach for managers to assess and manage risks in supply chains.

Findings – Supply chain risks can be managed more effectively when applying the Supply Chain Risk Management Process (SCRMP). The structured approach can be divided into the phases of risk identification, risk measurement and risk assessment; risk evaluation, and risk mitigation and contingency plans; and risk control and monitoring via data management systems. Specific techniques for conducting this process are suggested.

Originality/value – While supply chain risk management is an emerging and important topic in our dynamic and interconnected world, conceptual frameworks providing a clear meaning and normative guidance are scarce (Manuj and Mentzer, 2008). This paper presents such a framework, offering structure and decision support for managers.

Keywords Supply chain management, Risk management process, Supply chain risk, Risk management

Paper type Research paper

1. Supply chain risk management

At a time when global competition is intensifying and supply chains are becoming longer and more complex, the likelihood of not achieving the desired supply chain (SC) performance increases, mainly due to the risk of SC failures. It is therefore essential that companies plan for disruptions and develop contingency plans as they design or redesign their supply chains. Firms need to understand supply chain interdependencies, identify potential risk factors, their likelihood, consequences and severities. Risk management action plans can then be developed to preferably avoid the identified risks, or if not possible, at least mitigate, contain and control them. The risk involved in supply chains, as well as the impact severity of supply chain failures, has been demonstrated recently by the recalls and subsequent lawsuits for toy cars (Story, 2007) and pet food (FDA, 2008). While risk may be associated with unacceptable products delivered from upstream, it can also involve risks associated with the environment, such as the impact of hurricanes Katrina and Rita (Devlin, 2005), or the current hijackings and robberies of vessels by pirates off the coast of Somalia (Peats, 2008).

The purpose of this paper is to introduce a structured and systematic approach to enumerate SC risks, and to assess their severity and likelihood, so that risk mitigation plans can be developed and implemented. As such, this paper makes an important contribution to the area of supply chain risk management, and highlights an approach to manage these risks. It continues the tradition of recent academic research and industry reports, which have stressed the importance of supply chain risk management, as well as the development of approaches for its management (e.g. Blos *et al.*, 2009; Manuj and Mentzer, 2008; Shaer and Goedhart, 2009).

Risk can be defined as a "combination of probability or frequency of occurrence of a defined hazard and magnitude of the occurrence" (BS 4778, 1991). Building on several authors that have defined supply chain risk (e.g. Choi and Krause, 2006; Zsidisin *et al.*, 2000, 2004), we conceptualize supply chain risk as an event that adversely affects supply chain operations and hence its desired performance measures, such as chain-wide service levels and responsiveness, as well as cost. Regardless of the area of interest, risk is associated with an undesirable loss, i.e. an unwanted negative consequence, and uncertainty. Table I presents an illustrative list of supply

The current issue and full text archive of this journal is available at **www.emeraldinsight.com/1359-8546.htm**

Supply Chain Management: An International Journal
16/6 (2011) 474–483

[DOI 10.1108/13598541111171165]

The authors are grateful to Guest Editor Dr Charlene Xie and two anonymous reviewers for the valuable feedback and comments received on earlier versions of this paper.

Table I Supply chain risk categories and their triggers

Risk category	Risk triggers
Demand risks	Order fulfillment errors Inaccurate forecasts due to longer lead times, product variety, swing demands, seasonality, short life cycles, and small customer base Information distortion due to sales promotions and incentives, lack of SC visibility, and exaggeration of demand during product shortage
Delay risks	Excessive handling due to border crossings or change in transportation mode Port capacity and congestion Custom clearances at ports Transportation breakdowns
Disruption risks	Natural disasters Terrorism and wars Labor disputes Single source of supply Capacity and responsiveness of alternate suppliers
Inventory risks	Costs of holding inventories Demand and supply uncertainty Rate of product obsolescence Supplier fulfillment
Manufacturing (process) breakdown risks	Poor quality (ANSI or other compliance standards) Lower process yields Higher product cost Design changes
Physical plant (capacity) risks	Lack of capacity flexibility Cost of capacity
Supply (procurement) risks	Quality of service, including responsiveness and delivery performance Supplier fulfillment errors Selection of wrong partners High capacity utilization supply source Inflexibility of supply source Poor quality or process yield at supply source Supplier bankruptcy Rate of exchange Percentage of a key component or raw material procured from a single source
System risks	Information infrastructure breakdowns Lack of effective system integration or extensive system networking Lack of compatibility in IT platforms among SC partners
Sovereign risks	Regional instability Communication difficulties Government regulations Loss of control Intellectual property breaches
Transportation risks	Paperwork and scheduling Port strikes Delay at ports due to port capacity Late deliveries Higher costs of transportation Depends on transportation mode chosen

chain risks, compiled from various prior studies, most notably Chopra and Sodhi (2004) and Schoenherr *et al.* (2008).

Even though the assessment and management of risk in supply chains is more of a recent phenomenon, studies exist that explored risk management approaches from a variety of angles (e.g. Charette, 1989; Hayes *et al.*, 1986; Lowrance, 1976; Rowe, 1977; Starr and Whipple, 1980). Building on these studies, Tummala *et al.* (1994), by following Raiffa (1982) and Hertz and Thomas (1983), developed a structured Risk Management Process (RMP) consisting of the five phases risk identification, risk measurement, risk assessment, risk evaluation, and risk control and monitoring. This RMP framework has been successfully applied to identify potential risk factors and to assess their likelihood of occurrence. In addition, the seriousness of associated consequences can be identified, and appropriate risk mitigating strategies can be developed (Burchett and Tummala, 1998). While the RMP has proven to be useful when applied to such individual project decisions, for example the risk involved in an extra high voltage transmission line project (Tummala and Burchett, 1999), it has yet to be applied to the much broader context of the supply chain. Additional risk management approaches are included in the works of, Blos *et al.* (2009), De Waart (2006), Kilgore (2004), Kleindorfer and Saad (2005), Kleindorfer and Van Wassenhove (2004), Manuj and Mentzer (2008), Sinha *et al.* (2004) and Zsidisin and Ellram (2003).

However the process may look like, techniques need to be in place for assessing the likelihood of occurrence of identified risk factors, as well as the seriousness of associated consequences. The present paper is based on and extends above studies, primarily the work by Tummala and colleagues (Tummala *et al.*, 1994; Tummala and Mak, 2001), but also research conducted by Ellegaard (2008), Finch (2004), Manuj and Mentzer (2008), Schoenherr *et al.* (2008), and proposes an approach consisting of a modified RMP to identify, assess and manage supply chain risks. This modified approach is referred to as the supply chain risk management process (SCRMP). Techniques mentioned by Tummala and colleagues (Tummala *et al.*, 1994; Tummala and Mak, 2001), as well as others, will be highlighted in subsequent sections within the context of supply chain risk assessment. Overall, the paper presents a conceptual framework and approach for effective and efficient management of risks in supply chains, and attempts to reduce to the current lack of conceptual frameworks in SC risk management (Manuj and Mentzer, 2008). While this work is a primary extension of Tummala and colleagues' (Tummala *et al.*, 1994; Tummala and Mak, 2001) RMP, its application to supply chain management and supply chain risks is novel and provides significant insight into the management of such risks. The paper follows the tradition of risk management within the supply chain (e.g. Harland *et al.*, 2003; Hauser, 2003; Paulsson, 2004).

2. The Supply Chain Risk Management Process (SCRMP)

The complete SCRMP is depicted in Figure 1. While the focus of this paper is on a detailed description of the three phases, the other components, such as drivers, risk categories, supplier/logistics evaluation criteria and performance measures should not be neglected. Risk identification, risk measurement and risk assessment comprise Phase I of the

SCRMP, which will be described in the next section. Input to this first phase are internal and external drivers, such as those illustrated in Figure 1.

2.1 Phase I of SCRMP

2.1.1 Risk identification

The first step of the first phase of the SCRMP is risk identification (Figure 1). Risk identification involves a comprehensive and structured determination of potential SC risks associated with the given problem. Understanding risks, related to such categories as highlighted in Table I, is critical. These risk categories have also been included in our overall framework (Figure 1). Rather than attempting to be exhaustive, this list is illustrative of the multitude of risks that may be present. Affected areas need to be clearly identified and consequences need to be understood so that risk mitigation strategies can be implemented. Care should be taken since some strategies may adversely affect other risks (Chopra and Sodhi, 2004). Understanding the variety and interrelationships of SC risks is therefore important as well. Such an understanding can be achieved by considering threats and resources (Crockford, 1986). While threats refer to the broad range of forces, which could produce adverse results, resources refer to assets, people or earnings, which could be affected by the threats. One can start by first enumerating all possible threats that could produce adverse results for the performance of the supply chain. Then, for each threat, one needs to determine the resources of the organization that could be affected. The following approaches can help in the identification of potential SC risks: supply chain mapping, checklists or checksheets, event tree analysis, fault tree analysis, failure mode and effect analysis (FMEA) and Ishikawa cause and effect analysis (CEA) (see Tummala *et al.*, 1994).

While it is beyond the scope of this paper to provide a thorough overview of each of these suggested approaches, they will be briefly defined and described in the following. Illustrative references are provided to which the interested reader is referred. First, supply chain mapping is an approach in which the SC and its flow of goods, information and money is visually depicted, from upstream suppliers, throughout the focal firm, to downstream customers. A strategic supply chain map is a tool to align supply chain strategy with corporate strategy, and to help firms manage and modify the supply chain (Gardner and Cooper, 2003). Once every detail of the supply chain has been mapped, potential risks can be identified better. Second, checklists or checksheets are forms to record how often a failure was attributed to a specific event. These forms are used to standardize data collection and to create histograms (Chase *et al.*, 2006). Checklists could for example be used to record late deliveries from suppliers, which can serve as information to rate their reliability, i.e. the risk for not delivering on time. Third, event tree or fault tree analyses are graphical representations of all possible and subsequent outcomes triggered by an event (Pate-Cornell, 1984), such as a supply chain failure. While both types of trees may appear to look the same, there are important differences, such as the presence of single or multiple event paths in the diagram (Hollnagel, 2004). One may for example map out the potential events and responses that may be triggered by a supply chain failure to then plan for alternatives. Fourth, failure mode and effect analysis (FMEA) is a tool to identify "at the design stages potential risks during the manufacture of a product and during its use by the end customer" (Karim *et al.*, 2008, p. 3,601). For an introduction to FMEA please see McDermott *et al.* (1996). Before committing to a supply chain one could conduct such an analysis with this SC to analyze and assess what could go wrong, as well as how severe the consequences would be. And fifth, Ishikawa cause and effect analysis involves the brainstorming and exploration of all possible relationships between potential causes and failure events. Due to its structure, CEA diagrams are also sometimes called fishbone diagrams (Chase *et al.*, 2006). Once a supply chain failure has been identified, these diagrams could be used to discover the true root cause of the incident.

2.1.2 Risk measurement

Risk measurement, the second step of the first phase (Figure 1), involves the determination of the consequences of all potential SC risks, together with their magnitudes of impact. Consequences are defined as the manner in which or the extent to which the threat manifests its effects upon the resources (Crockford, 1986). Manifestations may include loss of or damage to assets, loss of income, interruption of service levels, cost overruns, schedule delays, poor process performance, liabilities incurred, damage repair costs, or injuries. Once a checklist, an event tree, a fault tree, an FMEA, or even an Ishikawa CEA analysis is applied to identify SC risks, corresponding consequences and their severity levels can be assessed.

Risks can be classified in terms of four types of undesirable consequences, with differing characteristics of frequency, severity and predictability. A popular classification is provided by Crockford (1986), who characterized consequences into trivial, small, medium and large. As such, trivial consequences occur with a very high frequency, have a very low severity, and a very high predictability. Small consequences have a high frequency, a low severity, and a reasonable predictability, with however their occurrence being infrequent. Medium consequences have a low frequency, a medium severity, and also a reasonable predictability, with their occurrence being frequent. Finally, large consequences can be characterized by a very low frequency, a high severity, and a minimal predictability. This framework can also be applied to our context. "Trivial losses" are losses that are expected to occur in any organization and can be met by normal operating budgets (Crockford, 1986). "Small losses" may present little problems, unless their frequency becomes so high that their aggregate effect approaches that of a single "medium loss".

Although not preferred, "medium losses" would not cause the firm serious concern if they happened at regular intervals, for then their cost could be expressed as an annual amount, and provisions could be made. A "large loss" presents the most serious problem. A loss of this kind happens very rarely, but if it did occur, it could be catastrophic for the firm.

US Military Standard 882C can be used to assess consequence severities qualitatively as described in Table II below (Grose, 1987; Military Standard, MIL-STD-882C, 1993). This type of severity assessment is useful when objective information is not available. Although the descriptions of consequence severity categories in the Military Standard are explained in terms of losses to buildings, environment, people, illness, etc, they can be adapted to our SC context, as illustrated in the example in Table II in terms of delivery risk. Risk consequence indices

Figure 1 Supply Chain Risk Management Process (SCRMP)

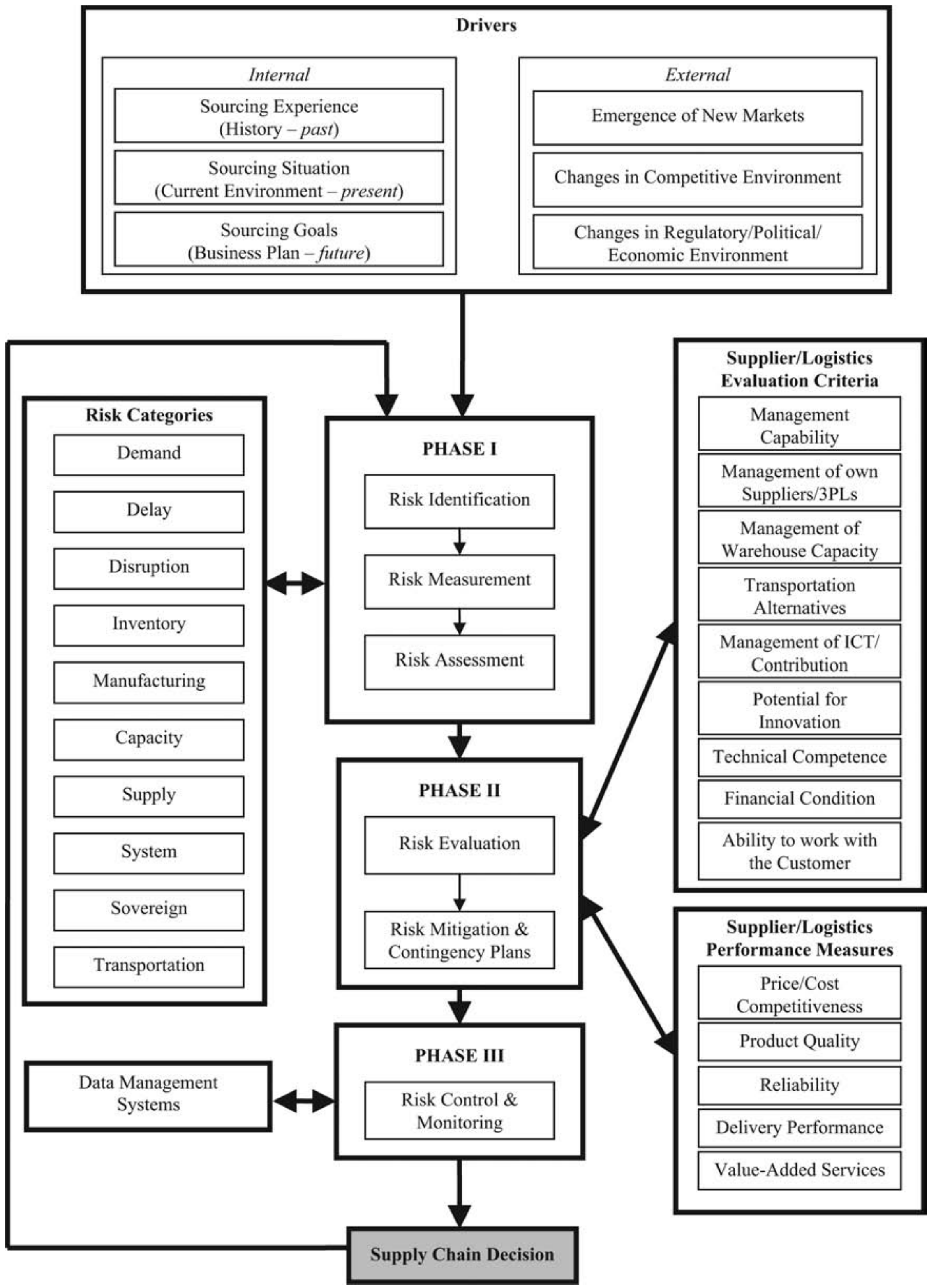


Table II Consequence severities and indexes

Consequence severity level	Qualitative description	Risk Consequence Index	HTP Code
Catastrophic	Plant shut down for more than a month due to lack of components with zero safety stock levels	4	A
Critical	Slow down of process or plant shut down for one week due to lack of components with zero safety stock levels	3	B
Marginal	Decreased service levels with depleting safety stocks	2	C
Negligible	Service levels not impacted due to sufficient safety stock levels	1	D

can then describe the severities, with their descriptions changed to suit a particular situation. We will use these index numbers to derive the risk exposure values. Table II also includes the corresponding HTP codes, which will be used in a later section to integrate consequence severities with other risk assessment aspects.

2.1.3 Risk assessment

Risk assessment, the third step of the first phase (Figure 1), is synonymous with the assessment of uncertainties (Raiffa, 1982), and is concerned with the determination of the likelihood of each risk factor. Uncertainties can be assessed by objective information, and probability distributions for relevant SC risks or consequences can be derived. If, however, objective information is not available, subjective information, beliefs and judgment can be used to approximate distributions. Techniques such as the Delphi method or expert focus groups can aid in the derivation of probabilities. Other approaches include parameter estimation, five point estimation, probability encoding, or Monte Carlo simulation (see Tummala *et al.*, 1994). Alternatively, probability categories, as suggested in the US Military Standard 882C (Grose, 1987; Military Standard, MIL-STD-882C, 1993) can be applied (Table III). The adapted qualitative descriptions can be changed to suit a given situation and supply chain environment; we have adapted them in our instance to the delivery risk example used above. The occurrence probability of an event such as hurricane Katrina could for example be classified as "rare" to "extremely rare", whereas the occurrence of a later delivery could be classified as "often" to "infrequent". Each risk probability category is assigned a risk probability index, which will help in finding the risk exposure values, as explained in a later section. Table III also includes the corresponding HTP codes, which will be used in a subsequent section to construct the Hazard Totem Pole, a tool to integrate various risk characteristics.

2.2 Phase II of SCRMP

Phase II of the SCRMP includes the steps of risk evaluation and risk mitigation and contingency plans. Both of these steps drawn on evaluation criteria and performance measures for suppliers and logistics, as indicated by the boxes on the right hand side of Figure 1. While it is beyond the scope of the present paper to discuss these criteria and measures, they are an important input for the two steps described in the following.

2.2.1 Risk evaluation

Risk evaluation is the first step in Phase II of the SCRMP (Figure 1), and involves the sub-steps of risk ranking and risk acceptance. These two sub-steps are practical particularly when objective probability assessment is difficult or sufficient data are not available to derive probabilities. These components are discussed in the following.

2.2.1.1 Risk ranking. Risk ranking is based on the determination of risk exposure values for each identified SC risk, and is defined as

$$\text{Risk Exposure Value of Risk Factor} = \text{Risk Consequence Index} \times \text{Risk Probability Index}$$

This equation uses the indices defined in Tables II-III above (see Tummala and Mak, 2001; Ng *et al.*, 2003). For example, if the consequence severity of a SC risk is critical and the corresponding probability category is often, then the risk exposure value is $3 \times 4 = 12$. In this fashion we can find the risk exposure values for each identified risk factor as illustrated in Table IV.

For simplicity and parsimony, these risk exposure values can be grouped into classes representing similar ranges of exposure. For example, risks with values between 16 and 11 could be grouped in the most critical class. These could for instance include the risk of the shipment being stolen or lost during transfer, the risk of the only qualified supplier going out of business, or the risk of the company's warehouse burning down. Risks between 10 and 6 could be categorized in the next-most critical class. Risks in this category could include the risk of temporary strikes at a supply chain or logistics partner, delays at customs, or the breakdown of a

Table III Probability categories and indexes

Risk probability categories	Qualitative description The identified risk factor could occur on an average of …	Probability Index	HTP Code
Often	… once per week	4	J
Infrequent	… once per month	3	K
Rare	… once per year	2	L
Extremely rare	… once per decade	1	M

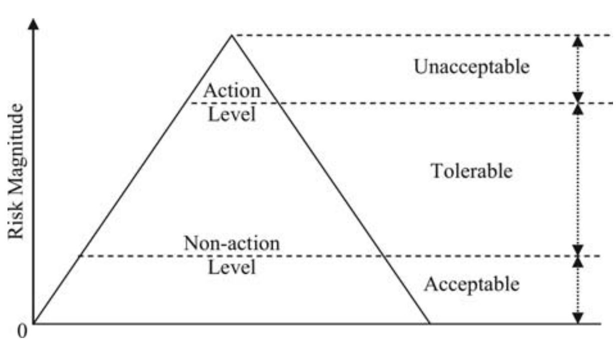
Table IV Risk exposure values

	Probability			
Severity	**Often (Index = 4)**	**Infrequent (Index = 3)**	**Rare (Index = 2)**	**Extremely rare (Index = 1)**
Catastrophic (Index = 4)	16	12	8	4
Critical (Index = 3)	12	9	6	3
Marginal (Index = 2)	8	6	4	2
Negligible (Index = 1)	4	3	2	1

machine used by a supplier to provide products to the focal company. Risks between 5 and 1 could then be classified in the negligible class. These risks could involve late, incomplete or defective deliveries of suppliers that do not necessarily threaten the operations of the focal company, due to for example sufficient safety stock of the supplies or the non-critical nature of the items. Alternatively, the risk exposure values may also be used to classify risks based on an 80-20 approach (Pareto analysis), i.e. the 20 percent of the risks could be identified that are likely responsible for 80 percent of the supply chain failures, and then these critical risks could be mitigated.

2.2.1.2 Risk acceptance. Once the SC risks are classified, acceptable levels of risk must be established. This is the second sub-step of risk evaluation in Phase II (Figure 1). The ALARP (as low as reasonably practicable) principle can be used to classify SC risk as unacceptable, tolerable or acceptable (Engineering Council, 1994). Cross-functional teams, including senior management, must be involved, and all available relevant information should be used in establishing these criteria. Based on these guidelines the demarcation between acceptable and unacceptable SC risks can be defined, as illustrated in Figure 2 (Tummala and Mak, 2001; Ng *et al.*, 2003). As risk-exposure values increase, they are initially at a value below some level; at this stage risks are considered to be so small that it is not advisable to spend time and resources for their control. An example may include late delivery of pencils to a manufacturing facility – pencils are not necessarily critical for the proper operation of the plant, and therefore expending resources to reduce the risk of late delivery from office products suppliers may not be warranted. As risks become elevated and their risk-exposure values increase to unacceptable levels, appropriate response actions must be taken for their containment. Unacceptable risks usually have adverse effects on the proper operation of the firm and can result in the shutdown of the assembly line, when for example deliveries from an upstream supplier are

Figure 2 Acceptable, tolerable, and unacceptable risks



not received. The risks for which the risk-exposure values fall between these two levels may be considered tolerable with no immediate action required. However, they should be monitored continuously and further improvement should be sought if resources are available. Continuing with the example from above, tolerable risks could be tardy deliveries from suppliers that do not shut down the assembly line. While certainly not desired, these late deliveries do not interrupt the flow of products, but the potential for doing so may be increased. Contracts developed between customers, suppliers, logistics providers and manufacturers may aid in the determination of these acceptability levels. Overall, mapping risks along their magnitudes, as illustrated in Figure 2, can provide a useful overview of all risks involved in a particular supply chain, and can help determine on which risk-preventive actions should be performed. The triangular shape of Figure 2 implies that most risks will be acceptable and tolerable, while only few risks will be completely unacceptable, for which therefore mitigation strategies should definitely be developed. The next section elaborates on this aspect.

2.2.2 Risk mitigation and contingency plans

The risk mitigation and contingency plans component, which is the second step of Phase II (Figure 1), involves the development of risk response action plans to contain and control the risks (risk planning). An evaluation technique, the hazard totem pole (HTP) analysis, already applied by Tummala and colleagues (Tummala *et al.*, 1994; Tummala and Mak, 2001), can be very helpful in this regard. This technique, described next, is repeated here to stress its applicability also within the supply chain context. It is a useful technique since it integrates in a coherent fashion risk aspects discussed in prior sections, specifically risk consequence severity and probability.

2.2.2.1 Risk planning. Once risks have been identified, their consequence severity has been assessed, and their probability determined, risk mitigation action plans can be developed. Since it is not feasible and practical to develop mitigation and prevention strategies for every risk identified, risk-planning begins with the examination of the costs required to implement each preventive action to contain and manage the identified SC risks. Supply chain risks can for example be reduced by buffer inventories, information technologies, effective relationships with suppliers and downstream customers, involvement of alternative or multiple suppliers, risk pooling, and the conduct of "what if' analyses (Choi, 2007; Choi and Krause, 2006; Chopra and Sodhi, 2004; Cook, 2007; Mentzer *et al.*, 2006; Stalk, 2006; Swaminathan and Tomlin, 2007). Findings from AMR Research's recent supply chain risk survey indicate that closer collaboration with trading partners, the passing of cost increases to customers,

Supply Chain Management: An International Journal
Volume 16 · Number 6 · 2011 · 474–483

the use of dual/multi-sourcing strategies and redundant suppliers, and performance-based contracts with suppliers and service partners are the most successful methods most often used to mitigate risks (Tohamy, 2009). These plans are evaluated and the best course of action is selected. A four-level cost-category system as shown in Table V (Tummala and Mak, 2001; Ng *et al.*, 2003) is adopted to facilitate the selection of the best course of action. Each category is associated with a cost index and an HTP code. Similar as above in Tables II-III, specific cost values provided in Table V can be adapted to the specific supply chain context (they here refer again to the delivery risk example introduced above), and are provided here merely for illustrative purposes. Risk mitigation plans can also be evaluated based on their relative cost to each other.

2.2.2.2 Hazard Totem Pole (HTP) analysis. The hazard totem pole analysis provides a method for the systematic evaluation of SC risks, integrating the risk evaluation aspects of their severity, probability and cost, as described above in Table II, Table III and Table V, respectively. The HTP diagram is designed to combine these three risk dimensions, which enables the determination of a singular ranking and the integrated depiction in a single figure. Codes and numerical values, as introduced above in Table II, Table III and Table V, are now integrated and used to represent different category levels.

Based on these three coding levels of severity, probability and cost, each risk factor is assigned a three-letter code. For example a risk factor with a code of AJP (or 4, 4, 4) possesses a consequence severity of "catastrophic", a probability of occurrence of "often", and has an implementation cost to contain the identified risk factor of less than $1,000. The corresponding total HTP risk index is then determined as $12 (= 4 + 4 + 4)$. Similarly, a risk factor with a code of BJQ (or 3, 4, 3), having a total risk index of 10, is associated with a "critical" consequence severity and a likelihood of occurrence of "often", involving costs between $1,000 and $10,000 to implement risk reduction action plans. In this fashion respective risk codes and risk indices can be assigned to the identified SC risks. Risks with a higher index number, determined based on the risk's severity, probability and mitigation cost, should be first in line for management consideration.

With this input the HTP diagram can be constructed (Figure 3). First, all risks are ordered according to their total HTP index value from highest to lowest. Second, the corresponding three-letter risk factor code is added to each line, to provide more information about the particular risk. And third, additional columns can be created that denote the cumulative risk factor count and the cumulative risk control cost. The pyramidal HTP diagram lists the most significant risks at the top (sharply pointed for immediate management attention), and the less significant risks at the bottom (Grose, 1987).

The risk factors at the top of the HTP represent catastrophic consequences that can be eliminated or contained for a small amount of money. As we go down the HTP, the impact of the ranked risk factors diminishes. Since no firm can afford to eliminate every identified risk, one can find a level in the HTP below which management accepts the risks, instead of implementing risk response action plans for their removal (similar to Figure 2 above, which is a pre-version to the fully developed HTP here). Alternatively, a firm may have a certain budget amount available to implement mitigation strategies. Starting from the top, the firm could then decide to implement all risk mitigation plans until the cumulative risk control cost equals or exceeds the budget. This cumulative cost is the cumulative sum of the risk prevention costs, which are based on the values in Table V. With this approach, the most critical risks can be addressed, while at the same time being constrained by a limited amount of resources. As a result, risk response actions can be selected for implementation according to the priority and the available resources. The cumulative risk factor count at that point indicates how many risks (irrespective of their severity, probability and prevention cost) could be eliminated. The HTP analysis thus represents an effective decision tool for integrating the severity of the consequence, the probability of occurrence, and the implementation cost of a risk response action plan for an identified SC risk.

While the HTP analysis just described can serve as a useful decision aid, certain limitations must be noted which relate mostly to assumptions and the subjective nature of the rankings and evaluations. For example, the implementation costs for risk mitigation action plans are assumed to be fixed. However, after the resources have been expended, the risk may not be completely eliminated; its severity may be merely lowered, for instance from "catastrophic" to "severe." Here, the budget estimated was not sufficient to completely eliminate the risk. The risk might also emerge in a modified form, for which the implementation action plan may be not as effective. The HTP analysis in Figure 3 can therefore only be a decision aid, and not a tool that makes decisions for the supply chain manager. It must be realized that almost all evaluations are subjective, and that assumptions made today may not be valid tomorrow any more. Modifications to Figure 3 may therefore be necessary. Nevertheless, considering these caveats, the suggested approach can help conceptualize and understand the problem in a more structured way.

2.3 Phase III of SCRMP

In the last phase of the SCRMP, risk control and monitoring, one can examine the progress made regarding the implemented risk response action plans; corrective actions can be taken if deviations occur in achieving the desired SC performance. This is Phase III in Figure 1. The process is a means to determine possible preventive measures and to provide guidelines for further improvement. Deviation from desired outcomes, abnormal cases, and SC disruptions are reported.

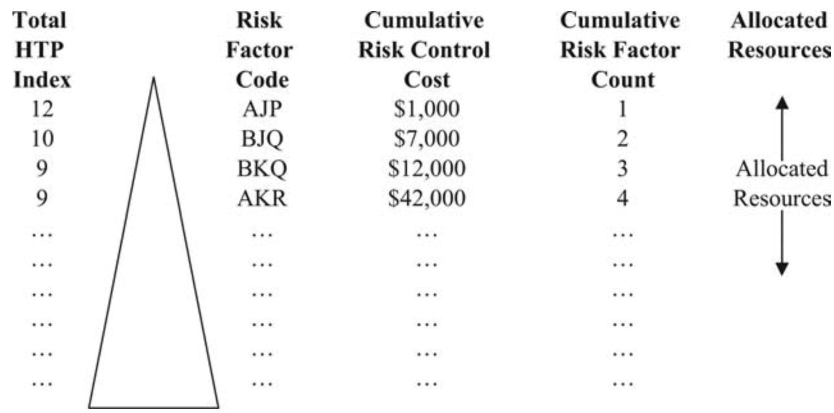
Data management systems can aid in this task, for example by the following modular structure: a catalog of the identified SC risk factors, consequence severity levels, risk probabilities, hazard totem pole analysis, government regulations/policies,

Table V Implementation cost categories for risk-response action-plans

Cost categories	Implementation costs	Cost Index	HTP Code
Substantial	More than $100,000	1	S
High	Between $10,000 and $100,000	2	R
Low	Between $1,000 and $10,000	3	Q
Trivial	Less than $1,000	4	P

Supply Chain Management: An International Journal
Volume 16 · Number 6 · 2011 · 474–483

Figure 3 Hazard Totem Pole (HTP)



tariffs and customs policies, transport schedules, and SC risk triggers. Related risk information can be stored and updated as needed. It can be used not only for effective monitoring and the taking of corrective actions, but also for continuous improvement of risk assessment and management. While such a system may be sufficient, there are also a number of sophisticated supply chain risk management software provides who offer commercial solutions, also on a Software as a Service (SaaS) basis, for risk management.

Based on the conduct of these three phases, a supply chain decision can be reached. However, as is the case with so many business processes, the exercise does not stop here. Management must continuously reiterate the SCRMP to account for any changes having occurred in the environment. Risk tolerances may also change, as may prevention costs and severity levels. Therefore, a continuous monitoring and assessment should be practiced.

3. Conclusion

The proposed supply chain risk management process is a tool to provide management with useful and strategic information concerning the SC risk profiles associated with a given situation. This is in contrast to the traditional approach based on single point estimates. The SCRMP ensures SC managers adopt strategic thinking and strategic decision making in evaluating options to improve supply chain performance. The analysis can be used not only for evaluating progress but also for selecting alternative courses of action, based on their respective SC risk profiles. Ultimately the SCRMP provides insight into how to make the most appropriate decision.

The SCRMP methodology proposed here is a comprehensive and coherent approach for managing risks and uncertainties associated with a given problem. The SCRMP methodology is practitioner-oriented in evaluating projects. Supply chain managers can apply it as an audit framework, in much the same way as the ISO 9000 quality system, in coping with risks and uncertainties, as well as in accomplishing the desired supply chain performance. It is important to recognize though that the approach cannot be applied blindly. As noted above, the SCRMP is a suggested aid that can help in making decisions, however, it does not make the decisions for the supply chain manager. It can merely serve as a tool to help in decision making. It is then always the intuitive judgment, tacit knowledge, and the unique situation that come into play and that must be considered.

From an academic research perspective, the paper contributes a conceptual risk assessment framework. As was noted in Manuj and Mentzer (2008, p. 133), "there is a lack of conceptual frameworks and empirical findings to provide clear meaning and normative guidance on the phenomenon of global supply chain risk management." While we have responded to the first observation by the development of the SCRMP, empirical testing of this model is warranted. Future research is encouraged to test the SCRMP at a range of company and to report the findings. Based on the results, the SCRMP can be refined and modified. Furthermore, different versions of the SCRMP can be developed depending on the company's context and environment, for example of whether sourcing is done domestically or internationally. Insightful will then also be the classification of companies into risk profile groups, based on their application of the SCRMP. What makes some companies more or less risk averse than others, and what is the subsequent impact on performance? These are just some of the questions pressing for answers.

In addition, while the focus of this paper was on a detailed description of the three phases, the other components of Figure 1, such as drivers, risk categories, supplier/logistics evaluation criteria and performance measures should not be neglected. These issues can impact the level or risk significantly. Future research is encouraged to investigate these components in greater detail, and integrate them with the SCRMP. The cohesive framework presented herein provides structure and guidance for such further investigations of supply chain risk management. As such, Figure 1 stakes out the research landscape of supply chain risk management. More fine-grained research looking at the individual phases of the SCRMP is also needed. Right now, evaluations are based on subjective judgments, and inherently include some error. Therefore, more quantitative approaches of risk management are called for. Sensitivity analyses could for example be conducted by simulating a range of feasible values and investigating their impact on both cost and risk. Going even a step deeper, future research should investigate how data available on company internal systems can be leveraged to determine these values. Based on the results, an optimal solution could then ideally be determined.

References

Blos, M.F., Quaddus, M., Wee, H.M. and Watanabe, K. (2009), "Supply chain risk management (SCRM): a case study on the automotive and electronic industries in Brazil", *Supply Chain Management: An International Journal*, Vol. 14 No. 4, pp. 247-52.

BS 4778 (1991), *Quality Vocabulary*, British Standards Institute.

Burchett, J.F. and Tummala, V.M.R. (1998), "An application of the risk management process (RMP) in capital investment decisions for an EHV transmission line construction project", *Construction Management and Economics*, Vol. 16 No. 2, pp. 235-44.

Charette, R.N. (1989), *Software Engineering Risk Analysis and Management*, McGraw-Hill, New York, NY.

Chase, R.B., Jacobs, F.R. and Aquilano, N.J. (2006), *Operations Management for Competitive Advantage*, McGraw-Hill Irwin, New York, NY.

Choi, T.Y. (2007), "Supplier-supplier relationships: why they matter", *Supply Chain Management Review*, Vol. 11 No. 5, pp. 51-6.

Choi, T.Y. and Krause, D.R. (2006), "The supply base and its complexity: implications for transaction costs, risks, responsiveness, and innovation", *Journal of Operations Management*, Vol. 24 No. 5, pp. 637-52.

Chopra, S. and Sodhi, M.S. (2004), "Managing risk to avoid supply-chain breakdown", *Sloan Management Review*, Vol. 46 No. 1, pp. 53-61.

Cook, T.A. (2007), *Global Sourcing Logistics: How to Manage Risk and Gain Competitive Advantage in a Worldwide Market Place*, AMACOM, American Management Association, New York, NY.

Crockford, N. (1986), *An Introduction to Risk Management*, 2nd ed., Woodhead-Faulkner.

De Waart, D. (2006), "Getting smart about risk management", *Supply Chain Management Review*, Vol. 10 No. 8, pp. 27-34.

Devlin, M. (2005), "Functional matters: Hurricane Katrina and the supply chain", ThomasNet, Industrial Market Trends, available at: http://news.thomasnet.com/IMT/archives/2005/09/functional_matt.html (accessed July 6, 2009).

Ellegaard, C. (2008), "Supply risk management in a small company perspective", *Supply Chain Management: An International Journal*, Vol. 13 No. 6, pp. 425-34.

Engineering Council (1994), *Guidelines and Risk Issues*, Lloyd's Register, London.

FDA (2008), "Pet foods recall (melamine)/tainted animal feed", US Food and Drug Administration, updated February 6, 2008, available at: www.fda.gov/oc/opacom/hottopics/petfood.html (accessed December 8, 2008).

Finch, P. (2004), "Supply chain risk management", *Supply Chain Management: An International Journal*, Vol. 9 No. 2, pp. 183-96.

Gardner, J.T. and Cooper, M.C. (2003), "Strategic supply chain mapping approaches", *Journal of Business Logistics*, Vol. 24 No. 2, pp. 37-64.

Grose, V.L. (1987), *Managing Risk: Systematic Loss Prevention for Executives*, Prentice-Hall, Englewood Cliffs, NJ.

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

Hauser, L.M. (2003), "Risk-adjusted supply chain management", *Supply Chain Management Review*, Vol. 7 No. 6, pp. 64-71.

Hayes, R.W., Perry, J.G., Nompson, P.A. and Willmer, G. (1986), *Risk Management in Engineering Construction, Implications for Project Managers*, Thomas Telford, Westminster, London.

Hertz, D.B. and Thomas, H. (1983), *Risk Analysis and Its Applications*, John Wiley & Sons, Chichester.

Hollnagel, E. (2004), *Barriers and Accident Prevention*, Ashgate Publishing, Farnham.

Karim, M.A., Smith, A.J.R. and Halgamuge, S. (2008), "Empirical relationships between some manufacturing practices and performance", *International Journal of Production Research*, Vol. 46 No. 13, pp. 3583-613.

Kilgore, J.M. (2004), "Mitigating supply chain risks", 89th Annual International Supply Management Conference, April 2004.

Kleindorfer, P.R. and Saad, G.H. (2005), "Managing disruption risks supply chains", *Production and Operations Management*, Vol. 14 No. 1, pp. 53-68.

Kleindorfer, P.R. and Van Wassenhove, L.K. (2004), "Risk management for global supply chains: an overview", in Gatignan, H. and Kimberly, J. (Eds), *The Alliances on Globalizing*, Cambridge University Press, Cambridge, MA, Ch. 12.

Lowrance, W.W. (1976), *Of Acceptable Risk, Science and the Determination of Safety*, William Kaufmann, Los Altos, CA.

McDermott, R.E., Mikulak, R.J. and Beauregard, M.R. (1996), *The Basics of FMEA*, Productivity Inc, Portland, OR.

Manuj, I. and Mentzer, J.T. (2008), "Global supply chain risk management", *Journal of Business Logistics*, Vol. 29 No. 1, pp. 133-55.

Mentzer, J.T., Myers, M.B. and Stank, T.P. (2006), *Handbook of Global Supply Chain Management*, Sage Publications, Thousand Oaks, CA.

Military Standard, MIL-STD-882C (1993), *System Hazard Analysis, System Safety Program Requirements*, United States Department of Defense, January 1993, pp. A4-A6.

Ng, M.F., Tummala, V.M.R. and Yam, C.Y. (2003), "A risk based maintenance management model for toll road/tunnel operations", *Construction Management and Economics*, Vol. 21 No. 5, pp. 495-510.

Pate-Cornell, M.E. (1984), "Fault tree vs event trees in reliability analysis", *Risk Analysis*, Vol. 4 No. 3, pp. 177-86.

Paulsson, U. (2004), "Supply chain risk management", in Brindley, C. (Ed.), *Supply Chain Risk*, Ashgate Publishing, Aldershot.

Peats, B. (2008), "How to stop the pirates?", New Statesman, December 5, 2008, available at: www.newstatesman.com/africa/2008/12/merchant-ships-pirates-piracy (accessed July 6, 2009).

Raiffa, H. (1982), "Science and policy: their separation and integration in risk analysis", *The American Statistician*, Vol. 36 Nos 3, Part 2, pp. 225-37.

Rowe, W.D. (1977), *An Anatomy of Risk*, John Wiley & Sons, New York, NY.

Schoenherr, T., Tummala, V.M.R. and Harrison, T. (2008), "Assessing supply chain risks with the analytic hierarchy process: providing decision support for the offshoring decision by a US manufacturing company", *Journal of Purchasing and Supply Management*, Vol. 14 No. 2, pp. 100-11.

Supply Chain Management: An International Journal
Volume 16 · Number 6 · 2011 · 474–483

Shaer, S. and Goedhart, J. (2009), "Risk and the consolidated supply chain: rethinking established best practices", *APICS Magazine*, July/August, pp. 41-3.

Sinha, P.R., Whitman, L.E. and Malzahn, D. (2004), "Methodology to mitigate supplier risk in an aerospace supply chain", *Supply Chain Management: An International Journal*, Vol. 9 No. 2, pp. 154-68.

Stalk, G. Jr (2006), "Surviving the China riptide", *Supply Chain Management Review*, Vol. 10 No. 4, pp. 19-26.

Starr, C. and Whipple, C. (1980), "Risks of risk decisions", *Science*, Vol. 208 No. 6, pp. 1114-9.

Story, L. (2007), "Lead paint prompts Mattel to recall 967,000 toys", *The New York Times*, August 2, 2007, available at: www.nytimes.com/2007/08/02/business/02toy.html (accessed December 8, 2008).

Swaminathan, J.M. and Tomlin, B. (2007), "How to avoid the risk management pitfalls", *Supply Chain Management Review*, Vol. 11 No. 5, pp. 34-42.

Tohamy, N. (2009), "Can Indian parlay its IT services success into manufacturing outsourcing?", Supply Chain Technologies and Services, AMR Research, Boston, MA.

Tummala, V.M.R. and Burchett, J.F. (1999), "Applying a risk management process to manage cost risk for an EHV transmission line project", *International Journal of Project Management*, Vol. 17 No. 4, pp. 223-35.

Tummala, V.M.R. and Mak, C.L. (2001), "A risk management model for improving operation and maintenance activities in electricity transmission networks", *Journal of the Operational Research Society*, Vol. 52 No. 2, pp. 125-34.

Tummala, V.M.R., Nkasu, M.M. and Chuah, K.B. (1994), "A framework for project risk management", *ME Research Bulletin*, Vol. 2, pp. 145-71.

Zsidisin, G.A. and Ellram, L.M. (2003), "An agency theory investigation of supply risk management", *The Journal of Supply Chain Management*, Vol. 39 No. 3, pp. 15-27.

Zsidisin, G.A., Panelli, A. and Upton, R. (2000), "Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study", *Supply Chain Management: An International Journal*, Vol. 5 No. 4, pp. 187-97.

Zsidisin, G.A., Ellram, L.M., Carter, J.R. and Cavinato, J.L. (2004), "An analysis of supply risk assessment techniques", *International Journal of Physical Distribution & Logistics Management*, Vol. 34 No. 5, pp. 397-409.

Further reading

Tummala, V.M.R. and Lo, C.K. (2004), "Risk management model for improving electricity supply reliability", *International Journal of Business & Economics*, Vol. 3 No. 1, pp. 43-55.

About the authors

Rao Tummala is Professor of Operations and Supply Chain Management in the College of Business, Eastern Michigan University, Ypsilanti, MI, USA. Professor Tummala is widely recognized for his scholarly contributions in Project Risk Management, Quality Management, Supply Chain Management, Bayesian Decision Theory, and Analytic Hierarchy Process. Some of the journals in which he has published papers include *Supply Chain Management – An International Journal*, *Quality Management Journal*, *OMEGA – The International Journal of Management Science*, *Journal of Operational Research Society*, *The Journal of Supply Chain Management*, *International Journal of Project Management*, *Construction Management and Economics* and *PRACTIX*.

Tobias Schoenherr is Assistant Professor of Supply Chain Management at the Eli Broad Graduate School of Management at Michigan State Michigan University, East Lansing, MI, USA. He holds a PhD in Operations Management and Decision Sciences from Indiana University, Bloomington. Dr Schoenherr's research focuses on strategic supply chain management, including strategic sourcing, (global) operations strategy, use of technology in SCM, and outsourcing. His work has appeared or is forthcoming in the *Journal of Operations Management*, *Production and Operations Management*, *Management Science*, the *Journal of Supply Chain Management*, the *International Journal of Production Research*, the *International Journal of Operations and Production Management*, *OMEGA – The International Journal of Management Science*, *Business Horizons*, the *Journal of Purchasing and Supply Management*, and others. For recent publications, please visit: http://broad.msu.edu/supplychain/faculty/member?id = 748. Tobias Schoenherr is the corresponding author and can be contacted at: Schoenherr@bus.msu.edu