

# **Managing Risk in Your Organization with the SCOR Methodology**

by

The Supply Chain Council Risk Research Team

Assembled and Edited by:

Dr. Kevin McCormack

Taylor Wilkerson

Dave Marrow

Melinda Davey

Mitul Shah

Deanna Yee

June, 2008

## **Abstract**

SCC members have reported that less than half of enterprises have established metrics and procedures for assessing and managing supply risks and organizations lack sufficient market intelligence, process, and information systems to effectively predict and mitigate supply chain risks. From this need arose the Risk Management Project Team approved by the SCC to enhance the SCOR model. The objective is to help organizations avoid/minimize costs, mitigate supply chain disruptions by managing risk proactively and thus, offering a competitive edge. This paper presents the outcome of a global multi-industry team that has worked passionately to achieve the same. The SCOR model is now integrated with processes that identify potential risk elements throughout the supply chain, define metrics to assess the potential impact of these risk elements and enable companies to control impact and mitigate service disruptions.

## **Objectives of this paper**

This paper will describe the results of a project chartered by the Supply Chain Council that investigated and developed an approach for including supply risk management activities within the SCOR model. This paper will cover the background, approach, results and recommendations for including supply chain risk management within the SCOR model.

# Table of Contents

<b><i>The Supply Chain Council Risk Research Team</i></b>	<b>3</b>
<b><i>Background</i></b>	<b>6</b>
<b><i>Project Results</i></b>	<b>9</b>
<b><i>Detailed Recommendations</i></b>	<b>13</b>
<b>Enabler Process Model</b>	<b>13</b>
<b>Metrics – Value at Risk (VAR)</b>	<b>15</b>
VAR Definition	16
VAR Example	18
<b>Best Practices</b>	<b>21</b>
Supply Chain Risk Management	21
Supply Chain Risk Identification	22
Supply Chain Risk Monitoring	23
Supply Chain Risk Assessment	23
Sourcing Risk Mitigation Strategies	25
Crisis Communications Planning	25
Risk Management Programs Coordination with Partners	26
Configure to Reduce Risk: Supply Chain Business Rules	26
Configure to Reduce Risk: Supply Chain Information	27
Configure to Reduce Risk: Supply Chain Network	27
<b><i>Implementation Approach and Challenges</i></b>	<b>28</b>
<b><i>Conclusions</i></b>	<b>30</b>

# The Supply Chain Council Risk Research Team

<b>Team Composition : Risk Management through SCOR Model</b>		
<b>Name</b>	<b>Organization Represented</b>	<b>Team Role</b>
<ul style="list-style-type: none"> <li>• Robert E Mansfield Jr.</li> <li>• Dave Morrow</li> <li>• Dr. Kevin McCormack</li> <li>• Taylor Wilkerson</li> <li>• Deanna Yee</li> <li>• Melinda Spring</li> </ul>	<ul style="list-style-type: none"> <li>• Connecticut Center for Advanced Technology, Inc.</li> <li>• IBM</li> <li>• DRK Research</li> <li>• LMI</li> <li>• Satellite Logistics Group</li> <li>• Supply-Chain Council</li> </ul>	<ul style="list-style-type: none"> <li>Chair</li> <li>Vice Chair</li> <li>Team Lead</li> <li>Team Lead</li> <li>Coordinator</li> <li>Project Manager</li> </ul>
<ul style="list-style-type: none"> <li>• Mitul Shah</li> <li>• Melinda Davey</li> <li>• John A. Deasy</li> <li>• Roberto Pinto</li> <li>• Avi Rosezberg</li> <li>• John M. Barineau</li> <li>• Maurice Luterweerd</li> <li>• George Borowsky</li> <li>• Gregory Crehawick</li> <li>• Hitesh Atri</li> <li>• Mark Hillman</li> <li>• Nishanth Vallabh</li> <li>• Ray VanderBok</li> <li>• Andre Rego Macieira</li> <li>• Arne Ziegenbein</li> <li>• Daniel Vital Chiarini</li> <li>• Koh Juay Meng</li> <li>• Marc Finkelstein</li> <li>• Jade Rodysill</li> </ul>	<ul style="list-style-type: none"> <li>• Infosys Technologies, Ltd.</li> <li>• TechTeam Government Solutions, Inc.</li> <li>• Transitions Group LLC</li> <li>• University of Bergamo</li> <li>• AROI</li> <li>• E.I. DuPont de Nemours &amp; Co., Inc</li> <li>• Groenewout</li> <li>• Lockheed Martin Aeronautics</li> <li>• Boz Allen</li> <li>• eKNOWtion</li> <li>• AMR Research, Inc.</li> <li>• Cognizant</li> <li>• TechTeam Government Solutions, Inc.</li> <li>• Grupo de Producao Integrada Coppe/UFRJ</li> <li>• Bosch</li> <li>• Grupo de Produção Integrada</li> <li>• Supply-Chain Council (South East Asia)</li> <li>• Caggemini</li> <li>• Accenture</li> </ul>	<ul style="list-style-type: none"> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> <li>Member</li> </ul>

## Introduction and Purpose

In today's volatile era with businesses and, more specifically, supply chains becoming increasingly global, the industrial environment is heavily affected by uncertainty, which can potentially turn into unexpected disruptions. Financial and political turmoil, socio-cultural changes, highly fragmented and demanding behavior of consumers, rapid development and changeover of products, have seriously modified the economic and industrial environment in which companies act, bringing out new issues related to assuring the continuity of the business against potential disruptive events.

Moreover, one of the key factors contributing to disrupting supply chains is the focus on lean supply chains in academia and industry during the 90s. Zero-inventory and just-in-time movement of goods became the dominant model that increased the sensitivity of supply chains. Little issues quickly become big issues. In addition, supply chains have become more global, increasing the order to delivery cycle times by a factor of four or five. This acts to amplify the potential of a disruption and the impact. Outsourcing has also become the dominant model, increasing the forces driving disruptions such as other customers competing for volume and attention, information flow issues, mistrust, win-lose negotiations, financial stress, misalignment of interests and goals. These have increased the likelihood of a disruption exponentially. According to a 2006 study by Accenture Consulting, three out of four top supply chain executives at major U.S. enterprises say they have had a disruption in the past five years from which it took at least a week – and sometimes several months – to recover.

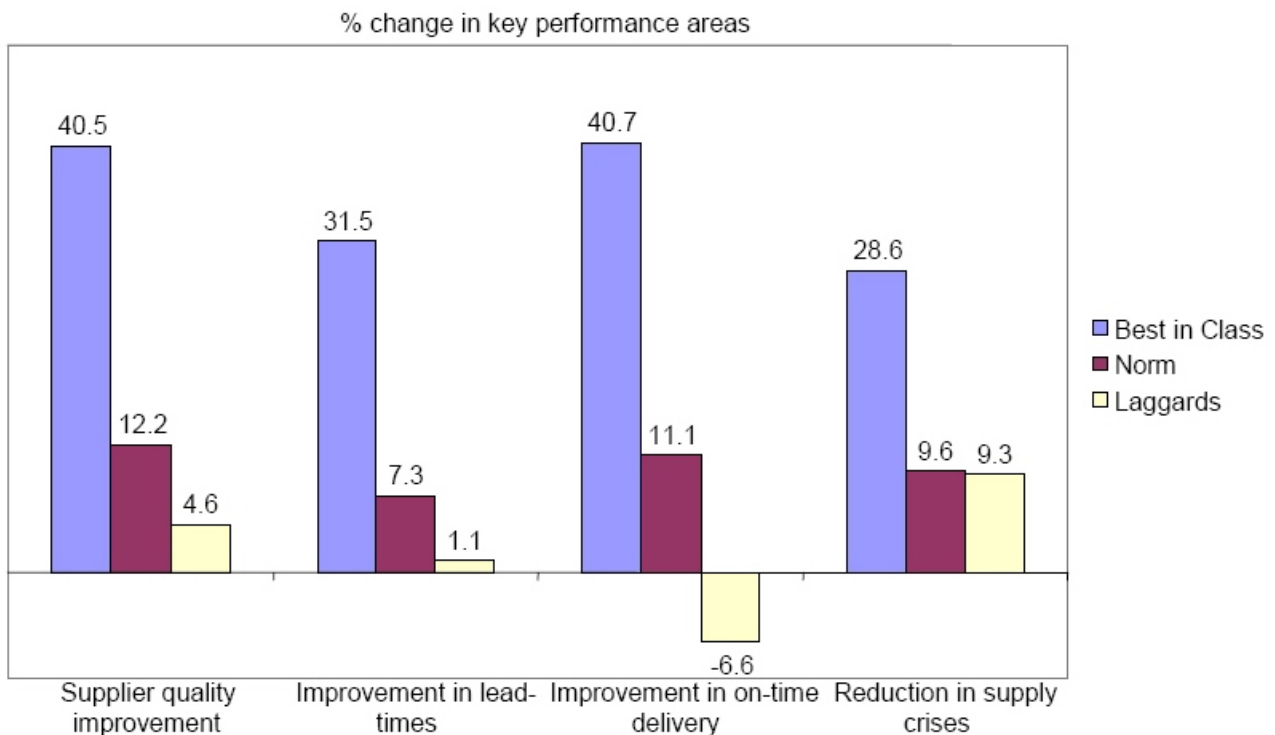
As a common term to designate the likelihood of occurrence of such events we use the word risk: although the concept of risk is multi-dimensional and not univocally defined, it is generally established the fact that it is linked to uncertainties associated with events.

Managing risk in the supply chain has never been as challenging as it is today. As more companies have outsourced production to overseas locations, supply chains have been extended, the number of nodes increased, and the complexity of the networks have moved exponentially. In the past, supply chain managers were mainly concerned with reducing cost, reducing purchase price variance, and managing inventory. Today, supply continuity is the single biggest business driver. Indeed, organizations now recognize that "preservation of shareholder value" is of paramount importance in supply chain management, and it has been assessed that disruptions can exert a tremendous impact on the company's overall performance of supply chain operations, if there are not suitable mechanisms or tools able to prevent or smooth their negative effects, as many real cases have showed in the past few years (Sheffi, 2005).

During the last decade, several events (i.e. earthquake in Kobe in 1995, terrorist attack to WTC in 2001, SARS in 2002-2003) have significantly disrupted supply chains and produced major losses for the companies involved (Tang, 2006). Companies such as Ericsson, Hershey, Apple, Walmart, and a host of other major companies who rely on timely delivery of products and services to meet customer needs have incurred major losses due to supply chain disruptions. Publicly traded firms experiencing supply chain disruptions, for example, have reported negative stock market reactions to announcements of such disruptive events, with the magnitude of the decline in market capitalization being as large as 10% (Knight & Pretty 1996; Hendricks & Singhal 2005). As a matter of fact, Ericsson reported a \$400 million loss because it did not receive chip deliveries from the Philips plant in a timely manner (Latour, 2001). Although the true costs of any supply chain disruption can be difficult to quantify precisely, at least one firm surveyed by Rice and Caniato (2003) estimated that the daily cost impact of a disruption in its supply network to be in the neighborhood of \$50-\$ 100 million.

Due to the new relevance that the concept of risk has assumed, risk management concepts and approaches have been studied and formalized in the past and have been around for several years, but have generally been focused in the financial, project management or safety areas. Such concepts and approaches are generally not immediately suitable for use in the supply chain management arena, since they should be fitted to a completely different context than those they have been thought to. But, before the definition of risk managing model and methods, one of the key question it is worth to consider is: what is the benefit of Supply Chain Risk Management (SCRM)?

According to a recent research report from Aberdeen (Figure 1), it leads to not only cost avoidance by reducing the probability and impact of disruptions it leads to performance improvements.



Source: AberdeenGroup, September 2005

Figure 1. SCRM Benefits

Once the importance of managing risk has been assessed, the further step is to define suitable models to analyze, assess, manage and communicate risk within a company as well as in a complex, geographically dispersed supply chain composed by several, legally independent entities.

With these issues in mind, a team of Supply Chain Council (SCC) members have conducted a multi-year long project to incorporate the processes, practices and metrics of Supply Chain Risk Management (SCRM) into the Supply Chain Operations Reference Model (SCOR).

The purpose of this paper is to provide an overview on the fundamental concepts of supply chain risk management, detailed the process used by the research team and present their findings. In addition, the risk management additions to the SCOR model are discussed and a practical application of SCRM using SCOR is presented.

# Background

What is Supply Chain Risk Management (SCRM)?

Risk is a concept that has applications in everything we do. It has several components, not the least of which is the lack of knowledge about the events that may impact us and our ability to manage them. In order to understand risk we first need to define and decompose it, specifically as it pertains to the supply chain. Under these statements, a common sense definition of risk – acknowledged by the International Organization for Standardization (ISO, 2002) – mainly deals with two of its essential components: *losses* (along with related amounts) and *uncertainty* of their occurrence. Another similar definition given by Culp (2001) states that risk can be defined as any source of randomness that may have an adverse impact on a person or a corporation. In the financial industry, *operational risk* is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (New Basel Capital Accord, 2006).

Formally, risk in general can be defined as a collection of pairs of *likelihood* ( $L$ ) and *outcomes* (or *impact*) ( $O$ ):

$$Risk = \{(L_1, O_1), (L_2, O_2), \dots, (L_n, O_n)\}$$

where  $O_i$  and  $L_i$  denote outcome  $i$  and its related likelihood. The distribution pattern of the (likelihood; outcome) pairs is called a *risk profile* (Ayyub, 2003). Definitions of risk must also have a *time dimension* or a specific time horizon (day, month, year, etc.) and a specific *perspective* or view that defines the unit of analysis (boundaries, what's not included, etc.).

How does this apply to the supply chain? Recently, several publications have advanced the conceptual clarity of the terms used in the domain of supply chain risk management—yet, there is still no commonly agreed nomenclature. According to Wagner and Bode (2006) it is possible to distinguish four interrelated terms:

- *Supply chain risk*: it is defined as the negative deviation from the expected value of a certain performance measure, resulting in negative consequences for the focal firm. Hence, risk is equated with the detriment of a supply chain disruption. The authors explicitly adopt the notion of risk as purely negative as the one that corresponds best to supply chain business reality. As a consequence, they do not consider either “happy disasters” nor the situation where managers intentionally “gamble” on risk.
- *Supply chain disruption*: a supply chain disruption is an unintended, untoward situation, which leads to supply chain risk. For the affected firms, it is an exceptional and anomalous situation in comparison to every-day business. Supply chain disruptions can materialize from various areas internal and external to a supply chain. Consequently, their nature can be highly divergent.
- *Supply chain risk source*: attempting to circumscribe supply chain disruptions (i.e. the demarcation of supply chain risks from other business risk), many scholars have proposed classifications in the form of typologies and/or taxonomies of risks. The derived classes of supply chain disruptions are often labeled *supply chain risk sources*.
- *Supply chain vulnerability*: while a supply chain disruption is the situation that leads to the occurrence of risk, it is not the sole determinant of the final result. It seems consequential that also the susceptibility of the supply chain to the harm of this situation is of significant

relevance. This leads to the concept of *supply chain vulnerability*. In other way, Christopher and Peck (2004) define supply chain vulnerability as “an exposure to serious disturbance”, while Barnes and Oloruntopa (2005) describe vulnerability as “a susceptibility or predisposition to loss because of existing organizational or functional practices or conditions”.

In order to better understand and define risk in the supply chain the different perspectives need to be understood. Figure 2 shows the three perspectives in a supply chain and list some of the risk definitions related to them.

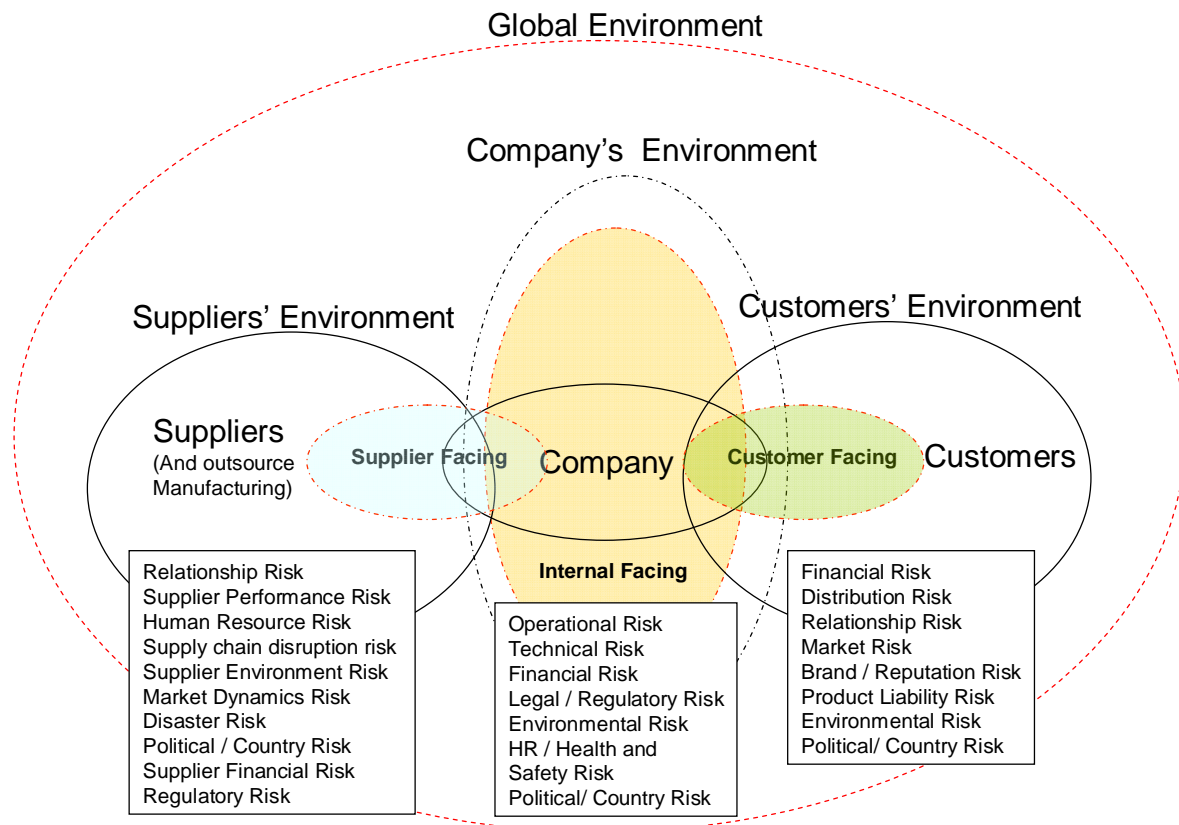


Figure 2. Supply Chain Risk Perspectives

*Supplier Facing* looks at the network of suppliers, their markets and their relationship with the “company”. *Customer Facing* looks at the network of customers and intermediaries, their markets and their relationships with the “company”. *Internal facing* looks at the company, their network of assets, processes, products, systems and people as well as the company’s markets. In all cases, a global perspective is essential.

As a first attempt of definition, supply chain risk can be divided, according to its source, into demand-side (resulting from disruptions emerging from downstream supply chain operations (Jüttner, 2005)), supply-side (residing in purchasing, supplier activities, and supplier relationships), and catastrophic risks (subsumes supply chain disruptions that, when they materialize, have a severe impact in terms of magnitude in the area of their occurrence)(Wagner and Bode, 2006). Treleven and Schweikhart (1988) have classified risks into five categories, connected with disruption, price, inventories and schedule, technology, and quality.

Zsidisin (2003) focused on the definition of 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, while Wu *et al.* (2006) states that inbound supply risk is defined as the potential occurrence of an incident associated with inbound supply from individual supplier failures or the supply market, resulting in the inability of the purchasing firm to meet customer demand and as involving the potential occurrence of events associated with inbound supply that can have significant detrimental effects on the purchasing firm. Finally, Nagurney *et al.* (2005) defines demand side risk as represented by the uncertainty surrounding the random demands at the retailers.

In developing a definition, the team looked at general concepts being used in risk management.

*Business Continuity Management (BCM)*, defined by the Business Continuity Institute as “an holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities” (BCI, 2005).

*Business Vulnerability*, defined as an exposure to serious disturbances, arising from risks within the supply chain as well as risks external to the supply chain (Christopher, 2003). Vulnerability is a result of any weakness within a complex system that can seriously jeopardize its activities (Ayyub, 2003).

*Enterprise Risk Management (ERM)* as a set of coordinated actions about protecting and enhancing share value to satisfy the primary business objective of shareholder wealth maximization (Chapman, 2006).

*Resilient enterprise* meaning the ability of the company to recover quickly from a disruption (Sheffi, 2005).

Several supply specific definitions were examined by the team. For example, Deloitte and Touche (2004) and Tang (2006) define *supply chain risk (SCR)* as the uncertainty of the occurrence of an event that could affect one (or more) partner or link within the supply chain and that could influence (generally in a negative sense) the achievement of company’s business objectives. They define *supply chain risk management (SCRM)* as having the objective to control, monitor and evaluate supply chain risk, optimizing actions in order to prevent disruptions (that is, the occurrence of an event that causes a business interruption) or to quickly recover from them.

## Project Results

With all of the background research in mind, the research team developed the following definition of SCRM:

*Supply chain risk management is the systematic identification, assessment, and quantification of potential supply chain disruptions with the objective to control exposure to risk or reduce its negative impact on supply chain performance. Potential disruptions can either occur within the supply chain (e.g. insufficient quality, unreliable suppliers, machine break-down, uncertain demand, etc.) or outside the supply chain (e.g. flooding, terrorism, labor strikes, natural disasters, large variability in demand, etc.). Management of risk includes the development of continuous strategies designed to control, mitigate, reduce, or eliminate risk.*

The next challenge for the team; where should supply risk management be within the SCOR model? In answering this question the team examined the three different approaches to risk management.

*Proactive:* these approaches take place before the occurrence of an event, aiming at reducing (for negative outcomes) its likelihood. The emphasis here is on those methods related to failure prevention, “near-misses” detection and adoption of layered defense approaches. Proactive approaches are aimed at anticipating the causes of disruptions.

*Reactive:* these approaches deal with the consequence of the occurrence of an event, aiming at reducing the resulting (negative) outcomes. In general, reactive, flexibility based and redundancy methods are known as *disruption management* in that they react after the disruptive event takes place, focusing on the *resilience* of the company or the ability to promptly recover from a disruption.

*Avoid, eliminate or transfer risk:* avoid any action which has inherent risks or eliminate and mitigate the risk and its potential outcomes. In product design this could be the design of a system that reduces or eliminates either the probability of occurrence of a particular risk event or its negative consequences if it occurs. In a supply chain, the risks can be mitigated by using more inventory or alternate suppliers. Risk can be *transferred* to an insurance company or another 3<sup>rd</sup> party that is more capable of handling it.

In order to find the right approach for SCRM in the SCOR model the team looked at the different areas of the model, planning, execution and enablers. Figure 3 shows the definitions for Plan and the execution processes of Source, Make, Deliver, Return.

# Level 1 Process Definitions

SCOR Is Based on Five Core Management Processes



SCOR Process	Definitions
<b>Plan</b>	Processes that balance aggregate demand and supply to develop a course of action which best meets sourcing, production and delivery requirements
<b>Source</b>	Processes that procure goods and services to meet planned or actual demand
<b>Make</b>	Processes that transform product to a finished state to meet planned or actual demand
<b>Deliver</b>	Processes that provide finished goods and services to meet planned or actual demand, typically including order management, transportation management, and distribution management
<b>Return</b>	Processes associated with returning or receiving returned products for any reason. These processes extend into post-delivery customer support

Figure 3. SCOR Process Definitions

Drilling down further, the team ruled out execution as an area not directly involved in SCRM but can be influenced or directed by and SCRM process. This left the Enable area and Plan process as the two alternatives.

As shown in Figure 4, the Plan process aligns expected resources to meet expected demand requirements. It balances aggregated demand and supply, considers consistent planning horizon, occurs at regular, periodic intervals and contributes to supply-chain response time. The Enable area contains processes that prepares, maintains, or manages information or relationships on which planning and execution processes rely.

After several weeks of discussions on the pros and cons of each alternative, it was decided to incorporate SCRM in the Enable areas of the model. This was driven by the fact that the core activity of SCRM, the *systematic identification, assessment, and quantification of potential supply chain disruptions*, seemed to closely match the activities described as *prepares, maintains, or manages information or relationships on which planning and execution processes rely*.

SCOR Process Type	Characteristics
<b>Planning</b>	A process that aligns expected resources to meet expected demand requirements. Planning processes: <ul style="list-style-type: none"> <li>• Balance aggregated demand and supply</li> <li>• Consider consistent planning horizon</li> <li>• (Generally) occur at regular, periodic intervals</li> <li>• Can contribute to supply-chain response time</li> </ul>
<b>Execution</b>	A process triggered by planned or actual demand that changes the state of material goods. Execution processes: <ul style="list-style-type: none"> <li>• Generally involve - <ol style="list-style-type: none"> <li>1. Scheduling/sequencing</li> <li>2. Transforming product, and/or</li> <li>3. Moving product to the next process</li> </ol> </li> <li>• Can contribute to the order fulfillment cycle time</li> </ul>
<b>Enable</b>	A process that prepares, maintains, or manages information or relationships on which planning and execution processes rely

Figure 4. SCOR Process Type

How it would be incorporated was the next challenge of the team. Two alternatives were tested.

1. **Centralized:** A new enabler section was proposed that is the primary process for the process of developing and managing the Supply Chain Risk program and aligning it with the overall business risk management program. This proposal centralizes supply chain risk assessment and program management and guides risk mitigation enablers in each or the other (5) enabler groups (P,S,M,D,R). Benefits of this alternative are:
  - a. better definition of the Plan process scope (i.e., differently from decentralized alternative that follows, the Plan enabler do not act as a coordinator or program manager for the other enablers; this is in charge of the new enabler section)
  - b. possibility to consider an extended set of processes that not necessarily are included (or that could not be included) in the PSMDR enablers (i.e. the managing process of assets, considered in ERM5, can impact on more than one process, but at the same time is not a part of current PSMDR enablers)
  - c. gives a better overview of the supply chain risk management process, considering the whole company (i.e. a set of PSMDR) from a higher level
  - d. allows to better identify the role of coordination of the upper level of company (or supply chain) management
  - e. centralizes supply chain risk assessment and program management and guides risk mitigation enablers in each or the other enabler groups (P,S,M,D,R)
  
2. **Decentralized but Coordinated by Enable Plan:** a new enabler is proposed to be added to each enabler group for the process of developing and managing the Supply Chain Risk program. The Plan enabler will act in a coordinating function by aligning the SCOR risk activities with the overall business risk management program. Each enabler group will have the responsibility for supply chain risk assessment and mitigation planning and actions for their process. The Plan risk enabler will act as program manager and guide risk mitigation strategies, plans and actions undertaken by each or the other (5) enabler groups (P,S,M,D,R). Benefits of this alternative:
  - a. consistent with current SCOR architecture

- b. more likely to be accepted by experienced SCOR users
- c. better definition of the enablers' scope (since each enabler group will have the responsibility for supply chain risk assessment and mitigation planning and actions for their process)

Alternative 2 (decentralized) was finally selected because it was more aligned to the current SCOR model philosophy and function of the Enablers section.

# Detailed Recommendations

## Enabler Process Model

The following section describes the detailed recommendation from the risk enabler team. Figure 5 shows the detailed Enabler Information Flow and Figure 6 shows the interactions and overall information flows for the risk enabler section.

Risk is a combination of interactions with the external and internal environment. Therefore, the information flows are divided in two groups: External and Internal. The purpose of the risk enablers are to:

1. assess the external and internal environment,
2. understand the likelihood and impact of potential events,
3. understand the sensitivity of the supply chain to these events,
4. develop mitigation plans for the supply chain,
5. align these plans with the overall business risk management program,
6. communicate these plans and responsibilities and
7. monitor the internal and external environment in order to detect indicators of risk events.

Figure 5 shows the details of the information types and flows of the typical risk enabler for a process area. The Plan risk enabler has an additional function of coordinating the other risk enablers as show in Figure 6. The Plan risk enabler takes in the overall business risk management program and translates this into the supply chain risk management program requirements. These requirements are then communicated to the other risk enablers. The Plan risk enabler also takes the program and plans for each process area, aggregates them into an overall supply chain risk management program and communicates this to the overall business risk management area.

# Risk Enablers Information Flow

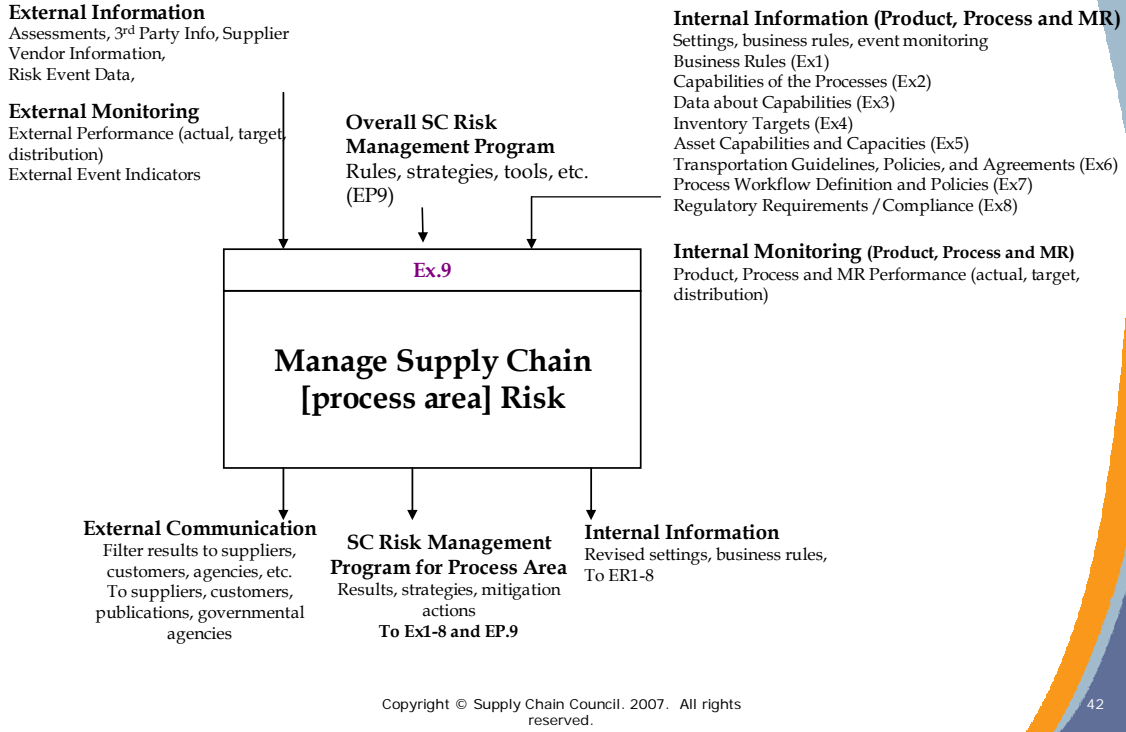


Figure 5. Risk Enabler Information Flow

# Risk Enablers Information Flow (PLAN)

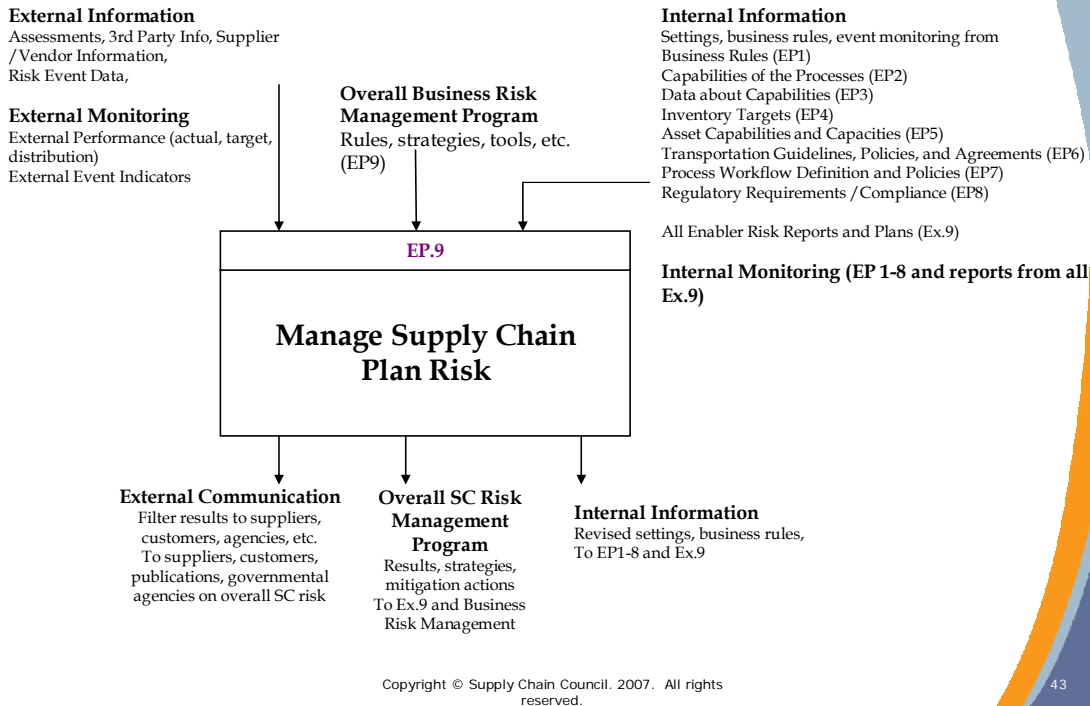


Figure 6. Plan Risk Enabler Information Flow

Figure 7 shows the overall information flows and interactions of the entire risk enabler sections.

## Typical Enabler High Level Flow

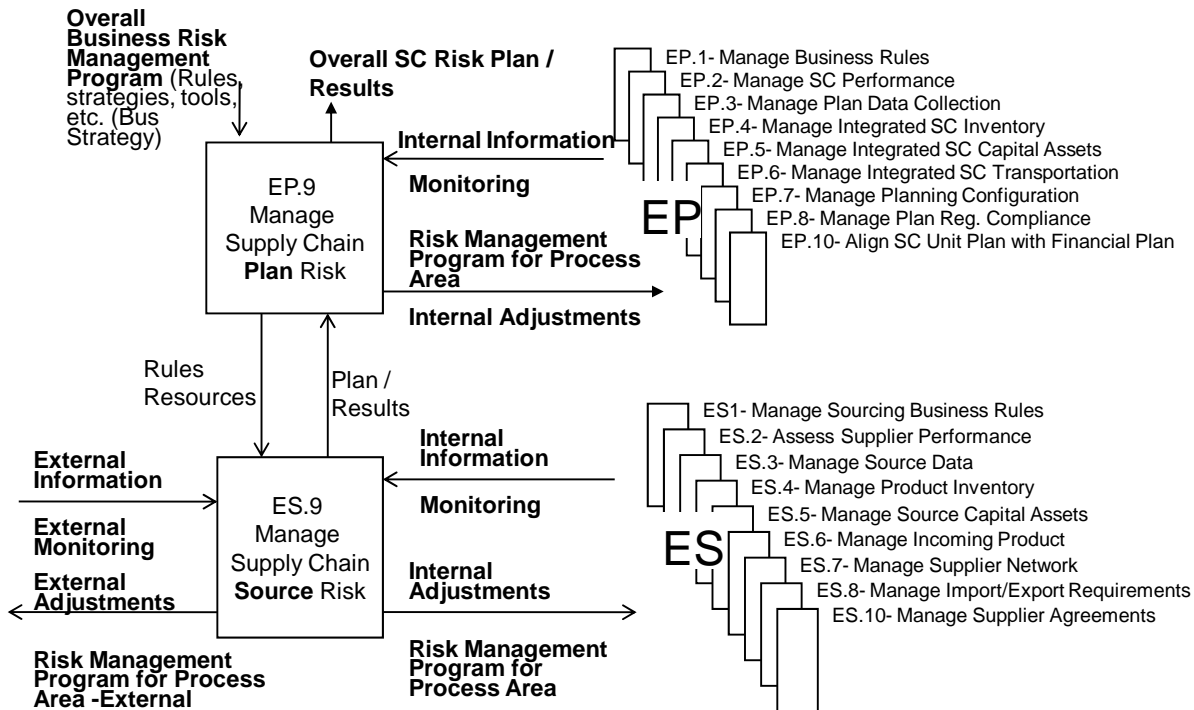


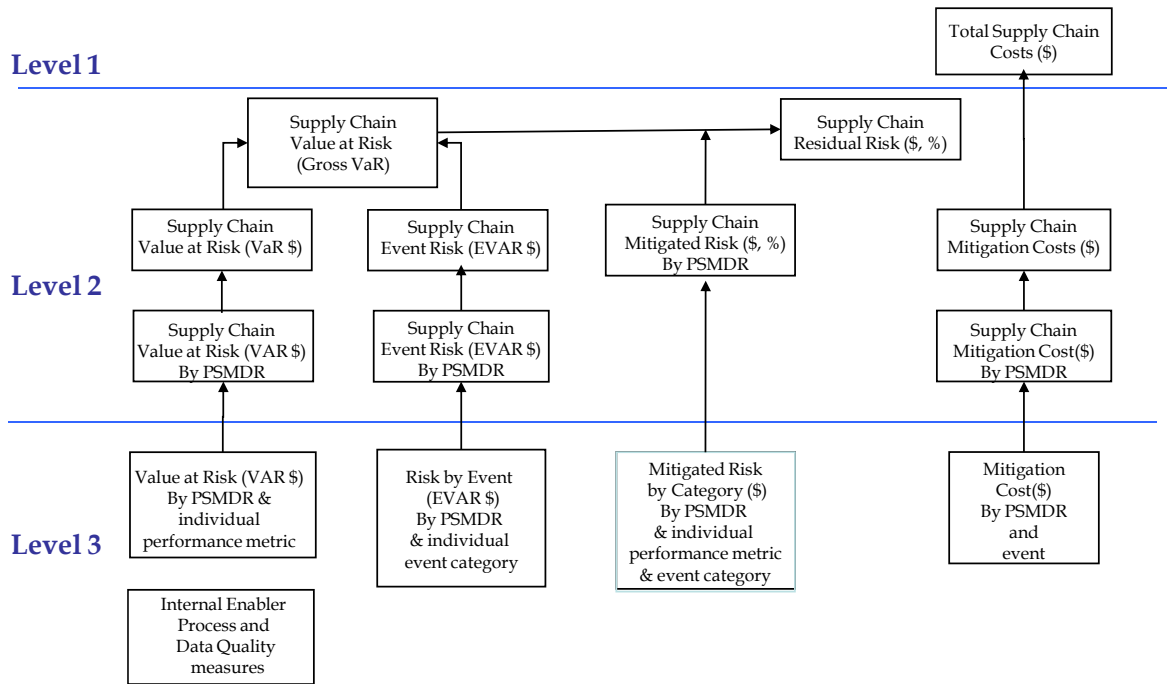
Figure 7. Overall Risk Enablers Information Flows and Interaction

In this process, each risk enabler interacts (two way information flow) with the environment (internal and external), the Plan risk enabler and the other enablers within their specific process area. This continuous process is coordinated by EP, the Plan risk enabler.

### Metrics – Value at Risk (VAR)

This section details the risk metrics team’s recommendations for specific supply chain risk metrics to be incorporated into the SCOR model. After detailed discussions, the team developed the metric hierarchy shown in figure 8.

# Risk Measures Hierarchy



31

Figure 8. Risk Metric Hierarchy

The hierarchy has three levels, as with all other metrics within the SCOR model. Level 2 and 3 are mostly internal to the risk enabler process and are used for analysis and diagnostics. Three specific metrics are rolled up to Level 2 and appear in the level 2 SCOR card. These are Value at Risk (VaR), Residual Risk and Mitigation costs. Mitigation costs are then rolled up and included in Total Supply Chain costs, which is a current level 1 metric within the SCOR model.

## VAR Definition

**Value-at-risk (VaR)** is a category of risk metrics that describe probabilistically the market risk of a trading portfolio over a given period of time. Value-at-risk is widely used by banks, securities firms, commodity merchants, energy merchants, and other trading organizations. Such firms could track their portfolios' market risk by using historical volatility as a risk metric. Figure 9 highlights some key points about the VaR metric.

# Value-At-Risk

- 1 Value-at-risk (VaR) is a category of risk metrics that describe probabilistically the market risk of a trading portfolio.
- 2 Value-at-risk is widely used by banks, securities firms, commodity merchants, energy merchants, and other trading organizations.
- 3 Such firms could track their portfolios' market risk by using historical volatility as a risk metric. They might do so by calculating the historical volatility of their portfolio's market value over a rolling 100 trading days.
- 4 The historical volatility would illustrate how risky the portfolio had been over the previous 100 days.

**Source:** www.riskglossary.com

Copyright © Supply Chain Council. 2007. All rights reserved.

22

Figure 9. Key Points on VaR

VaR is about performance v. expectations (or target). With securities it measures the probability that the actual return will be below the desired (or expected) return. The VaR calculation uses historical data on the securities to calculate the number of times the securities performed below the target (probability) times the amount below the target.

For example, if the target price was \$100 and the security historical pricing was the following:

- 10% at \$70
- 10% at \$80
- 10% at \$90
- 50% at \$100
- 20% at \$110

The VaR would be  $.10(100-70)+.10(100-80)+.10(100-90) = \$6$

This is a very simple, non-statistical application of VaR. There are other, more sophisticated ways to apply this concept but this example is only meant to illustrate the concept. For a more detailed explanation, go to <http://www.riskglossary.com>.

VAR can be also be used to evaluate and manage risk in the supply chain. The SCC defines Value at Risk as *the sum of the probability of events times the monetary impact of the events for the specific process, supplier, product or customer.*

## VAR Example

The following example will explain how VaR can be applied to the supply chain using airlines and on time arrival metrics as an example of a supplier.

Situation:

You are flying to Detroit from Raleigh Durham. There are two airlines with direct flights and you want to know which one is more likely to arrive on time (on time delivery is a key metric). Figure 10 shows the average percent late for each airline.

Which supplier (AA or NW) has the highest likelihood of being late?

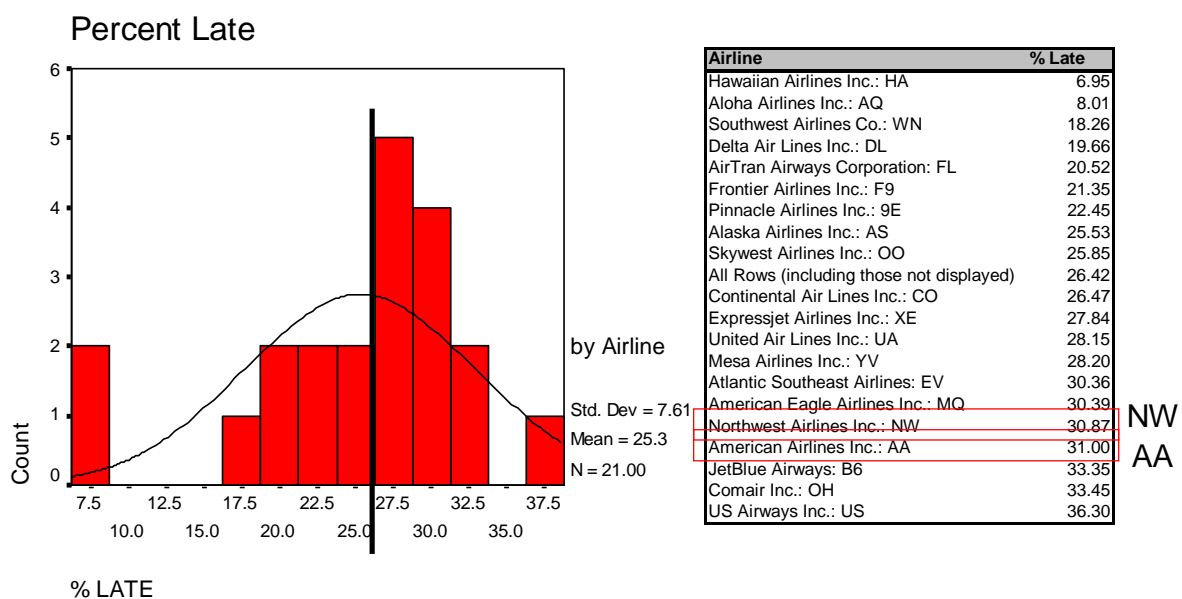


Figure 10: Average Percent Late by Airline.

From figure 10, it looks as if Northwest and American are about equal (31.00 v. 30.87 percent late). If you examine the distributions and the VaR for each airline, it tells a different story. Figure 11 and 12 shows the actual distributions of arrivals for each airline. The number above each bar represents the percent for the group of late events as a percent of the total events (by count only).

Northwest		
Min	Percent	VaR
5	13.20%	0.66
10	10.70%	1.07
15	8.00%	1.20
20	6.00%	1.20
25	4.80%	1.20
30	3.40%	1.02
35	2.80%	0.98
40	2.10%	0.84
45	1.70%	0.77
50	1.40%	0.70
55	1.10%	0.61
60	0.80%	0.48
65	0.70%	0.46
70	0.60%	0.42
75	0.50%	0.38
80	0.40%	0.32
85	0.30%	0.26
90	0.30%	0.27
95	0.20%	0.19
100	0.20%	0.20
105	0.20%	0.21
110	0.20%	0.22
115	0.20%	0.23
120	0.10%	0.12
125	0.10%	0.13
130	0.10%	0.13
VaR		14.24

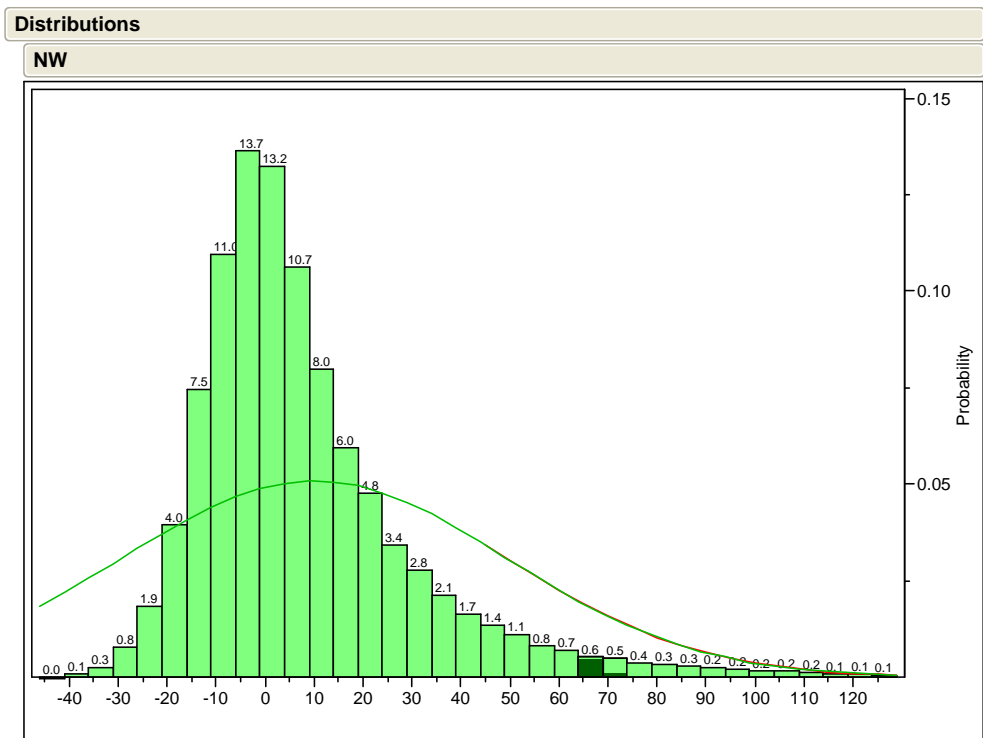


Figure 11: Distribution of Northwest performance (minutes late by flight event) and VaR

American		
Min	Percent	VaR
25	30.20%	7.55
50	9.30%	4.65
75	5.30%	3.98
100	3.10%	3.10
125	1.70%	2.13
150	1.00%	1.50
175	0.60%	1.05
200	0.50%	1.00
225	0.20%	0.45
250	0.10%	0.25
275	0.10%	0.28
VaR		25.93

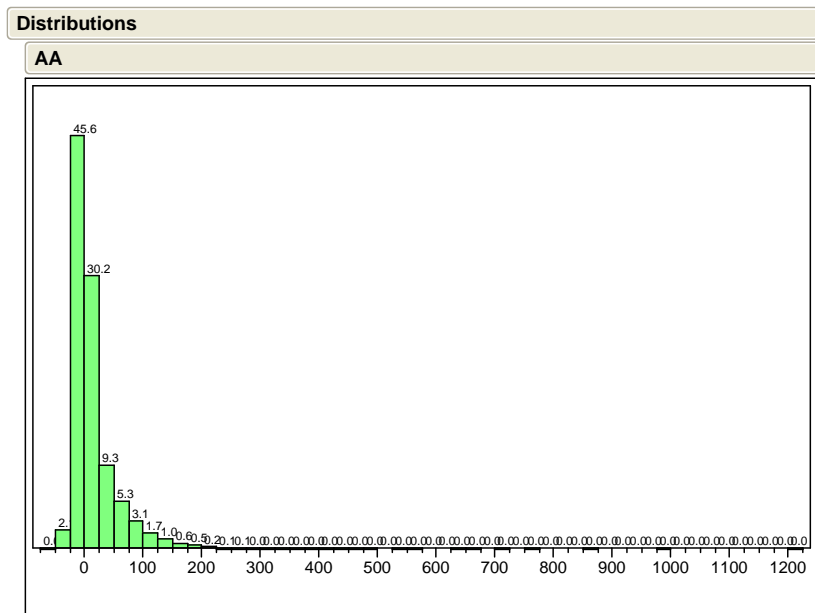


Figure 12: Distribution of American performance (minutes late by flight event) and VaR

As you can see, the average of percent late misleads. As shown in table 1, the VAR for Northwest is \$14.24 (using each minute late as costing \$1) and American is \$25.93. The American distribution shows a high frequency of flights that are very late (over 100 minutes) while Northwest stays within 150 minutes and most late flights are under 100 minutes.

Table 1: Comparison of Airlines: VaR (in dollars) v. Simple % Late

<b>Supplier</b>	<b>Ave % Late</b>	<b>VaR</b>
<b>NW</b>	<b>31.87%</b>	<b>14.24</b>
<b>AA</b>	<b>31.00%</b>	<b>25.93</b>

This example illustrates how VaR can be used in the supply chain to evaluate the different aspects of risk. Suppliers can be evaluated base upon the VaR of performance measures. Customers can also be measured based upon performance measures (profitability, volume growth, returns, and complaints) as well as products (warranty claims, etc.). VaR can also be applied to internal supply chain entities such as manufacturing, distribution or sales locations.

Since VaR can be monetarized by accessing the cost of performance below target, VaR can be rolled up and examined by any demographic or data cut (by region, by customer, by supplier, etc.). Suppliers, Products, Customers, Locations, etc. can be evaluated based upon VaR and ranked according to the risk of poor performance.

Caveats in using VaR :

- VaR calculates the probability of non-adherence to metrics value (expected value) based on historical data. Hence, it is a retrospective view of the event risk. The same may or may not be applicable in the future.
- VaR is a downside Risk Metrics. It calculates the loss for each level of confidence (probability). In a real life scenario, just like a sales forecast, predictive accuracy depends upon how well history predicts the future.
- Calculating VaR from historical data requires a potentially large database of events and metrics, and it could be computationally intensive.

## Best Practices

Many companies have been starting to look at managing risk and several best practices have emerged. Practices in the financial services, project risk management, and insurance industries were studied. The details of these are described in the SCOR Best Practices section. Summaries are provided below. Ten practices have been identified under 4 categories shown in Figure 13. Each practices is described in more detail below.



Figure 13. Risk Best Practice Categories

## Supply Chain Risk Management

Supply chain risk management is the systematic identification, assessment and mitigation of potential disruptions in logistics networks with the objective to reduce their negative impact on the logistics network's performance.

A high number of potential disruptions can negatively impact supply chain performance. Potential disruptions can either occur within the supply chain (e.g. insufficient quality, unreliable suppliers, machine break-down, uncertain demand, etc.) and outside (e.g. flooding, terrorism, labor strikes, natural disasters, etc.). Both are considered in an integral three-phase approach for supply chain risk management:

- **Phase 1 - Risk Identification:** What can go wrong? What is uncertain? Based on a description of a supply chain with SCOR, each single process should be looked at with regards to potential disruptions that may negatively harm the performance and which countermeasures are already in place. Result of this phase is a list of the relevant supply chain risks.
- **Phase 2 - Risk Assessment:** How likely is it that a certain potential incident will occur? What is the impact? The likelihood of occurrence and the negative impact on SCOR performance measures of each supply chain risk should be qualitatively or quantitatively evaluated. Result of this phase is a list of serious risks that can be visualized in a risk portfolio with the dimension probability of occurrence and negative impact.

- Phase 3 – Risk Mitigation: How can the risks be controlled and monitored? Mitigation measures (e.g. improved planning methods, alternative suppliers, response plans, redundant infrastructure, etc.) should be evaluated for the serious risks. After having checked the cost-efficiency of the alternative measures, the appropriate measures should be chosen and implemented. A risk can be mitigated by decreasing the likelihood that it will occur or by decreasing its impact if it does occur. Alternatives to mitigation include acceptance, transfer, and risk sharing.

## Supply Chain Risk Identification

A key aspect of supply chain risk management is identification. Identification involves creating a list of potential events that could harm any aspect of the supply chain's performance. Risk identification allows an organization to take steps to create plans to manage risks before they occur. This is typically more cost effective than waiting to react to adverse events when they occur.

Some methods for identifying risk are:

- Geomapping/Supply chain mapping – Visual maps of supply chains reveal supply chain structures, dependencies, and handoffs that may contain risk. SCOR mapping and Value Stream Mapping are two types of supply chain mapping that can be used.
- Looking at historical problems – Historical problems may have a high chance of recurring. Those problems may have happened to the organization itself or to others.
- Researching industry trends – Other organizations and industry groups may have already researched risks that are applicable.
- Group of experts brainstorming – People with experience in different areas of your organization and supply chain have lots of knowledge of risks. Getting them together increases the knowledge sharing. (The Delphi method is one technique to conduct expert interviews.)
- Assessment surveys – Well designed surveys can be an effective way to quickly gather information on risks in your supply chain.
- Site visits – Site visits to supply chain partners allow you to collect detailed and less “filtered” information on risks.
- Information audits – Data system audits can reveal issues and trends from the past. It can show areas of the supply chain that have had poor performance in the past and are thus more likely to perform poorly in the future.

Some tools used in risk identification are:

- Risk checklists – a list of risks that are common for your environment. It may come from past experience or industry research.
- Cause-and-effect diagrams (i.e. fishbone, Ishikawa) – a diagram that traces back the causes for events
- Gantt charts – a bar chart showing the precedence and timing of activities. It can help identify the critical path, i.e. the most critical organizations and processes that would be bottlenecks if they experienced a disruption. (It can also be used later during Risk Assessment to determine the effect of disruptions at different points in a supply chain.)

In the Plan step of SCOR, an organization can create plans for identifying risk on an ongoing basis. Risks can be classified into Source Risks, Make Risks, Deliver Risks, and Return risks.

- Source risk identification – Standardized source assessments and surveys are effective. Some companies have already developed such assessments.
- Make risk identification – Internal risks to an organization that have been extensively studied and include: Sarbanes-Oxley Compliance; fiscal, environmental, and social responsibility; health and labor laws; loss of manufacturing capability (due to labor loss,

property loss, ...); quality management; increases in production costs; link to source risks (interruptions and increases in costs); capacity (over and under); intellectual property; and personnel management.

- Deliver risk identification – Visibility of customers improves the ability to identify Deliver risks.
- Return risk identification – Data on returns needs to be tracked to identify risks. Excessive returns may reveal risks earlier in the process.

## **Supply Chain Risk Monitoring**

Once areas of risk have been identified, an organization needs to monitor their internal and external environment. This helps them to predict when risky events are becoming more likely. It also helps to identify new risks and is tightly linked to the best practice of Supply Chain Risk Identification.

SCOR's focus on supply chain metrics enables Supply Chain Risk monitoring. Real time metrics and periodic reports give decisions makers knowledge upcoming risks. Statistical analysis of key metrics can reveal trends. Visibility into supplier and customer metrics increases the ability to monitor. Reports on risk monitoring can be combined with existing management reviews and meetings.

Monitoring can also include monitoring qualitative sources of information such as news or weather reports to identify events that are precursors to risks.

In the Plan step, an organization can plan methods for monitoring Source, Make, Deliver, and Return risks. These methods may include specific metrics to monitor and “watch-out” lists of precursor events. It may also include monitoring the environment external to the organization's supply chain.

- Deliver risk monitoring can be done with customer service metrics.
- Make risk monitoring can be done automatically through an organization's data systems such as an ERP system.
- Source risk monitoring is enhanced with visibility into suppliers' metrics.

It is important to monitor indicators that would appear early in a risk event or, better, even before it occurs by indicating an increasing likelihood. If monitoring only reveals a risk well after its first occurrence, it will likely be too late to adequately respond to it.

Monitoring can also be used to test the effectiveness of risk controls. If a plan to mitigate or prevent a risk has been implemented, monitoring can check to see if the corresponding metrics show no signs of the risk occurring.

## **Supply Chain Risk Assessment**

Supply Chain Risk assessment provides management with an understanding of where the greatest risks may exist in order to prioritize resources for risk mitigation and management. Performing such assessments will involve clarifying the nature of the risk, understanding conditions that may lead to the event, knowing how frequently such events have happened or can be expected to happen, and the potential impact of such events. The team can then prioritize addressing the risks.

Risk assessment is typically made up of two measures: Likelihood and Impact.

- Likelihood – measures the probability that the event will occur. The exact probability may be difficult to determine unless there is historical data that can be used to find the frequency of the event occurring. Alternatively an organization can use a subjective

likelihood, or degree of belief, based on the opinions of experts. A time horizon is necessary to define the probability in a useful way (e.g., the likelihood that an event will occur in the next year or 50 years).

- Impact – measures the consequences on the organization if the event occurs. It can be measured directly, for example in terms of dollars. It can also be measured on a scale, for example from zero to one with zero being very little negative consequence and one being a very bad consequence. Methods for measuring impact include “what-if” simulations, financial models, and opinions of teams of experts. Impact may also be measured in terms of other SCOR metrics besides financials.
- Summary risk score – A summary risk score can be calculated for each risk by multiplying the Impact times the Probability to get an expected value of the risk. Then risks can be ranked by risk score. Also the risks can be shown on a map or graph. An example is shown below.

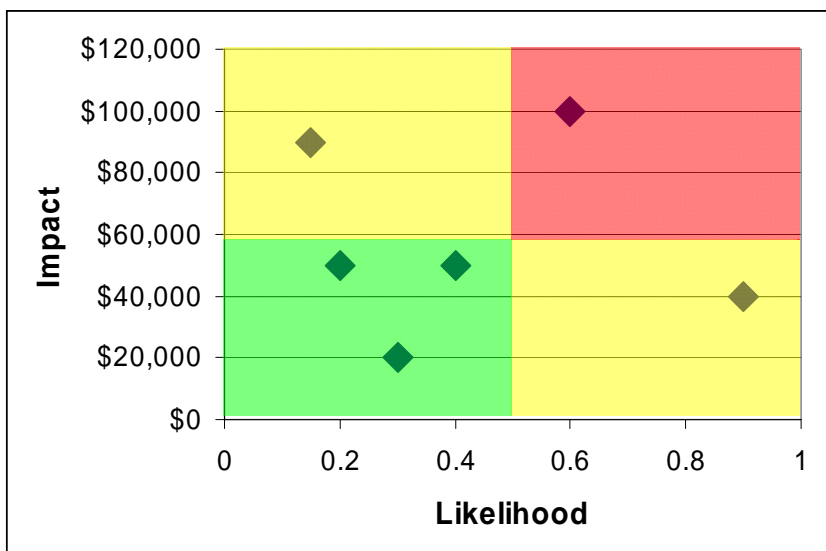


Figure 14. Risk Matrix

Other methods for assessment include:

- Failure Mode Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Event Tree analysis (ETA)

A risk assessment tool in the form of qualitative and quantitative spreadsheet or other software can be used by management teams to organize the assessment of risks to an organization. The tool can contain also contain information on relevant causes of those risks and their assessment, mitigation options and the impact of various mitigation plans. This helps establish standards for the measurement, reporting, and limiting of risk.

Risk management is widely discussed, but practitioners have differing views of the categories, significance, and how to integrate mitigation plans into the overall project or operational plan. A frequent issue is that management focuses on the highest impact risks, overlooking more frequent occurrences. This practice should help standardize risk management vocabulary and practices within an organization.

Some more sophisticated methods of risk assessment involve the use of simulations to derive approximations for the impact of risks. Varieties of different types of supply chain simulation software are available and may be used for this purpose.

## **Sourcing Risk Mitigation Strategies**

For most manufacturing operations, over 70% of cost is associated with purchased goods and services. These organizations may identify some goods or services as posing unacceptable supply risk, in case of suppliers business rationalization, excessive demand, fire, work outage, etc. This best practice identifies some Risk Mitigation strategies. This practice fits well with companies that have a few, significant supplier or a supplier base that is constrained or powerful. It also is useful if the supplier base or the raw materials purchased are inherently high risk.

Source risk mitigation strategies can include:

- Multiple sources of supply—having multiple sources of supply for a raw material reduces the impact of one source failing to deliver materials
- Strategic agreements or partnerships with suppliers—strategic agreements with suppliers can lead to continued service in the event of capacity constraints.
- Collaborative Planning Forecasting and Replenishment CPFR—by sharing demand and fulfillment data with supply chain partners, there is a reduced risk of unforeseen demand swings or supply shortages.
- Joint product design and delivery—designing products with suppliers reduces the risk of material non-performance or material shortages

## **Crisis Communications Planning**

Open communication is necessary for effective risk management, where the term “open” refers to the possibility to directly reach the right person – who can better handle the information about a crisis situations – wherever in the organization (i.e. refer to the Nokia-Ericssons case in Sheffi, 2005).

Managers require direct communication channels up, down and across their business units to help identify risks and take appropriate actions.

The communication should also be fast and reliable: suitable methods of communication (from phone call to e-mail messages or even more advanced means) and redundant communication capabilities should be identified.

Periodic reports shared within the partners of the supply chain can definitively help in coordinating efforts related to risk management activities and initiatives.

Some common components of a crisis communication plan include:

- Crisis definitions
- Crisis roles and responsibilities
- Pre-defined communication points of contact, methods of contact, etc.
- Media relations procedures
- Crisis response operating procedures
- Test and exercise requirements for the plan

This practice aims at smoothing the problems due to lack of communication within company’s functions or within different companies among the supply chain. Establishing an open, reliable and fast communication channel means allow people to work with the right information in the right place at the right time, in order to ensure coordinated Risk Management activities.

## **Risk Management Programs Coordination with Partners**

The process of coordinated risk management places a strong emphasis on cooperation among departments within a single company and among different companies of a supply chain to effectively manage the full range of risks as a whole. A closer coordination of risk management activities performed throughout the supply chain is intended to conserve resources and increase effectiveness. This practice is at the basis of the shared risk approach.

The adoption of a common process framework within the supply chain can foster the share of information in order to improve existing initiatives and removal duplicated or ineffective activities. Moreover, sharing business continuity programs with supply-side and customer-side partners, can help in identifying overlapping areas or uncovered issues.

Risk Management coordination could be achieved by the establishment of a Risk Management Coordination Committee, whose purpose is advises and coordinates the identification and inclusion of risk management treatments within the overall risk management process (see, for example, see Comcover reference)

Coordinated risk management is essential in situations where a significant amount of potential risk lies outside of the subject organization's control, e.g., in other business units, upstream in supplier supply chains, or downstream in customer supply chains. In these cases, risk is best mitigated through close coordination with partners that can directly act on the potential risks.

One important pre-requisite of coordinated risk management is that supply-side partners should be seen from a collaborative rather than a competitive viewpoint. This in order to share best practices, recovery objectives, strategy information, expectations and mutual aid options.

In order to identify critical suppliers, it is possible to send them surveys regarding their business continuity programs. Recurring meetings (some face-to-face) can lead to decreased availability risk and far-greater levels of business continuity program maturity – for both organizations.

Another important pre-requisite is an appropriate visibility into customer events (i.e. inventory level, sales volume, demand forecasts...). This is intended to allow for early detection of risky situations or conditions.

## **Configure to Reduce Risk: Supply Chain Business Rules**

This practice involves establishing business rules (e.g., customer priority, supplier priority, production routing, transportation routing, etc.) based on minimizing the risk to the supply chain. Under this practice, business rules are established or configured in response to the corporate risk management plan with a goal of reducing either the likelihood of a disruption occurring or the impact to the supply chain should a disruption occur.

Business rule reconfiguration typically includes an assessment of the impact of each rule change on the overall supply chain before actual implementation.

Examples of risk management business rules include

- Sharing orders across multiple suppliers to keep supplier base “warm”
- Predefined order re-routing procedures in the event of a node failure
- Customer prioritization to allocate scarce resources during an emergency

This practice is useful in organizations where the cost of supply chain disruptions is high, either from a profit or brand image perspective. Using a risk mitigation configuration will reduce the potential for a disruption and reduce the recovery time after a disruption occurs.

### **Configure to Reduce Risk: Supply Chain Information**

This practice involves managing supply chain information networks to minimize the risk to the supply chain. This includes information sharing with partners as well as internal locations. This helps all parties to be quickly informed of a real or potential disruption and respond quickly and appropriately to minimize the disruption impact.

To be effective, this practice needs to include clear identification of what information each supply chain partner needs in order to reduce the overall risk in the supply chain and agreement on information sharing details:

- Formats—the format that information will be shared in (e.g., e-mail, web portal, phone communications, etc.)
- Frequencies—how frequently communications are expected to occur (e.g., daily, hourly, weekly, etc.)
- Technologies—what technologies will be used to communicate (e.g., electronic communications, SMS, telephone, etc.)
- Processes—the processes for communication across partners (e.g., points of contact, mobilization, etc.)

### **Configure to Reduce Risk: Supply Chain Network**

This practice relies on a risk evaluation of the supply chain to guide the design of the supply chain network. Node locations, transportation routes, capacity size and location, number of suppliers, number of production locations, etc. are all determined in a fashion that mitigates potential disruptions to the ability to deliver product and service to the end customer.

This practice relies on the information collected through risk identification and risk assessment processes to identify nodes that are at a high risk of disruption due to the location of the node. Location specific risks can include tactical strike risks, natural disaster risks, single point of failure risks, etc.

# Implementation Approach and Challenges

The approach to implementing risk management using the SCOR model enablers as proposed by the team is shown in Figure 14

Phase	Name	Deliverable	Resolves
Initial	BUILD	<ul style="list-style-type: none"> <li>Organizational Support</li> <li>Risk Management Program</li> </ul>	Who is the sponsor?
I	DISCOVER	<ul style="list-style-type: none"> <li>Supply-Chain Definition</li> <li>Supply-Chain Risk Priorities</li> <li>Project Charter/Risk Program definition</li> </ul>	What will the program cover?
II	ANALYZE	<ul style="list-style-type: none"> <li>Scorecard</li> <li>Benchmark</li> <li>Competitive Requirements</li> <li>Customer service requirements</li> </ul>	What is the risk tolerance of your supply chain?
III	ASSESS	<ul style="list-style-type: none"> <li>Geo Map</li> <li>Thread Diagram</li> <li>Risk assessment</li> </ul>	Initial Analysis – where and how big are the risks?
IV	MITIGATE	<ul style="list-style-type: none"> <li>Mitigation plans</li> <li>Level 3, Level 4 Processes</li> <li>Best Practices Analysis</li> </ul>	Final Analysis – how will risk be eliminated or mitigated?
V	IMPLEMENT	<ul style="list-style-type: none"> <li>Opportunity Analysis</li> <li>Mitigation Definition</li> <li>Deployment Organization</li> <li>Monitoring and response programs</li> </ul>	How to deploy mitigations?

Figure 14 SCOR Risk Management Implementation Approach

Some of the challenges of implementing a supply chain risk management program are:

*Organizational Support:* supply chain risk management needs cross-functional participation, agreement and cooperation in order to succeed. It cannot be done within a department without significantly limiting the impact on the business. This requires executive level commitment and active participation. Building this is a critical first step in the implementation process.

*Rules and strategies:* Before risk management activities can start, a decision must be made as to the approach and the strategy. The main guidelines for managing risks and the rationale behind them must be developed, documented and communicated.

*Roles, Responsibility:* Clear roles and responsibility are critical for any process or program. In the case of supply risk management, even more so. Cross-functional, company wide responsibility and authority are critical for success. In addition, supply risk management adds new responsibilities to existing jobs. These must be clearly communicated, current skill levels of incumbents assessed and corrections made (training or replacement) as required.

*Funding:* Effective levels of funding are always a challenge in any company. The amount depends upon the scope of your program and how much detail is requirement. Top line annual risk assessment can be very inexpensive and might be a good place to start while the organization is training in new concepts of risk management.

*Mitigation:* The mitigation of risk considers options for treating risks that were not considered acceptable. This phase aims at identifying options to either reduce negative consequences, or to reduce the likelihood of adverse outcomes. In general terms, risk identification, analysis, assessment and mitigation means answering the following questions: (i) what can happen? (ii) how can it happen? (iii) why could it happen? (iv) what are the potential outcomes? (v) how we can overcome potential disruptions? Once these questions have been answered, this 3<sup>rd</sup> phase aims at identifying available actions in order to reduce risk's negative outcomes. These actions will take place at the operational level. This phase clearly requires an intimate knowledge of the organization, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives.

*Coordinate and align the program:* This phase places a strong emphasis on cooperation among departments within a single company and among different companies of a supply chain to effectively manage the full range of risks as a whole. A closer coordination of risk management activities performed throughout the supply chain is intended to conserve resources and increase effectiveness. The adoption of a common process framework within the supply chain can foster the share of information in order to improve existing initiatives and removal duplicated or ineffective activities. Moreover, sharing business continuity programs with supply-side and customer-side partners can help in identifying overlapping areas or uncovered issues. Risk Management coordination could be achieved by the establishment of a *Risk Management Coordination Committee*, whose purpose is to advise and coordinate the identification and inclusion of risk management treatments within the overall risk management process.

*Monitor and act:* Finally, after all decisions have been made and roles and responsibility have been assigned, the results have to be continuously monitored in order to act (or react) when necessary. The monitoring process goes along the entire supply chain risk management process and interacts with each step bi-directionally, allowing for feedback and reconsideration of choices.

## Conclusions

According to Hallikas *et al.* (2004), an effective collaborative process for risk management is possible only if there is a “risk management” mindset and culture. The SCOR model can play a substantial role in pursuing the overall objective of a real collaborative process within and between companies, aiming at maximizing the overall performances of the supply chain. Having a supply chain reference model that allows the definition of individual as well as collaborative risk management processes seems to be just a preliminary condition to pave the way for the design of a shared risk management process for the whole supply chain network.

Obviously, this offers further theoretical and practical issues: how can a collaborative risk management process be implemented? Which companies are responsible for the definition, the implementation and the management of the process? Which are the partners?

In our opinion, future studies have to provide some valuable answers to these issues, contributing in particular to the definition of a systematic model in order to understand the relationships between individual risk management processes and a collaborative risk management process, and the definition of a risk management reference model encompassing the entire supply chain network.

## References

- [1] APICS, Protiviti Inc., 2004, “Understanding supply chain risk areas, solutions, and plans. A five-parts series”. (<http://www.protiviti.com> - September 2006)
- [2] Attis D., Monahad S., and P. Laudicina, 2003, “Supply Chains in a vulnerable, volatile world”, *A.T. Kearney Executive agenda – Third Quarter 2003*
- [3] Ayyub, B.M. , 2003, “Risk Analysis in Engineering and Economics”, *Chapman & Hall/CRC*, Florida – ISBN 1-58488-395-2
- [4] Barton, T.H., Shekir, W.G. and P.L. Walker, 2002, “Making enterprise Risk Management Pay Off”, *Fei Research Foundation. Financial Times Prentice Hall. Pearson Education*
- [5] Basel Committee on Banking Supervision, 2006, “International Convergence of Capital and Capital Standards”. ISBN print: 92-9131-720-9; ISBN web: 92-9197-720-9 (<http://www.bis.org/> - September 2006)
- [6] (The) Business Continuity Institute (BCI), 2005, “Good Practice Guidelines 2005 – A Framework for Business Continuity Management” (<http://www.thebci.org/> - September 2006)
- [7] Chapman, R.J., 2006, “Simple Tools and Techniques for Enterprise Risk Management”, *John Wiley & Sons*. England, ISBN 978-0-470-01466-0
- [8] Christopher, M., 2003, “Creating Resilient Supply Chains: a Practical Guide”, *Cranfield University School of Management*. ISBN 1-861941-02-1 (<http://www.som.cranfield.ac.uk/> - September 2006)
- [9] Clarke C.J. and S. Varma, 1999, “Strategic Risk Management: the New Competitive Edge”, *Long Range Planning*, Vol. 32, No. 4, 414-424
- [10] Cornalba, C. and P. Giudici, 2004, “Statistical models for operational risk management”, *Physica A*, N° 388. 166-172
- [11] Culp, C.L., 2001, “The risk management process. Business strategy and tactics”, *John Wiley & Sons, Inc*. New York – NY - ISBN 0-471-40554-X
- [12] Deloitte and Touche, 2004, “Supply Chain Risk Management”, ([http://www.deloitte.com/dtt/cda/doc/content/nl\\_eng\\_brochure\\_supply\\_chain\\_risk\\_management\\_070704x\(1\).pdf](http://www.deloitte.com/dtt/cda/doc/content/nl_eng_brochure_supply_chain_risk_management_070704x(1).pdf))
- [13] Daniell, M.H., 2000, “World of risk”, *John Wiley&Sons (Asia) Pte Ltd* - ISBN 0-471-84085-8
- [14] Goodman, R.W., 2004, “Is Your Supply Chain ready for Sarbanes-Oxley?”, *Global Logistics and Supply Chain Strategies*, February 2004, 32-39
- [15] Hallikas, J., I. Karvonen, U. Pulkkinen, V.-M. Virolainen and M. Tuomine, 2004, “Risk management processes in supplier networks”, *International Journal of Production Economics*, 90, 47-58
- [16] Hendricks, K.and V.R. Singhal, 2005, “The Effect of Supply Chain Disruptions on Long-term Shareholder Value, Profitability, and Share Price Volatility”
- [17] ISO: International Organization for Standardization, 1999, “ISO/IEC Guide 51 – Safety aspects – Guidelines for their inclusion in standards”
- [18] ISO: International Organization for Standardization, 2002, “ISO/IEC Guide 73 – Risk management – Vocabulary – Guidelines for use in standards”
- [19] Knight, R., & Pretty, D. (1996). The impact of catastrophes on shareholder value. In *The Oxford Executive Research Briefings*. Oxford, UK: Templeton College, University of Oxford.
- [20] Kunamoto H. and E. J. Henley, 1996, “Probabilistic risk assessment and management for engineers and scientists”, *IEEE Press*, New York, NY.
- [21] Latour, A. (2001). Trial by fire: A blaze in Albuquerque sets off major crisis for cell-phone giants-Nokia handles supply shock with aplomb as Ericsson of Sweden gets burned-Was SISU the difference? *Wall Street Journal*, January 29, A1.

- [22] NSW Small Business, 2005, "Risk management guide for small business", *Department of State and Regional Development* ([www.smallbiz.nsw.gov.au](http://www.smallbiz.nsw.gov.au)) - ISBN 0-7313-32490
- [23] Sheffi, Y., 2005, "The Resilient Enterprise. Overcoming Vulnerability for Competitive Advantage", *The MIT-Press*, Boston - MA
- [24] Sitkin, S.B. and A.L. Pablo, 1992, "Reconceptualizing the Determinants of Risk Behavior", *The Academy of Management Review*, 17, 9-38.
- [25] Tang, C., S., 2006, "Perspective in supply chain risk management", *International Journal of Production Economics*, 103, 451-488
- [26] Vose, D., 1996, "Quantitative Risk Analysis – A guide to Monte Carlo Simulation Modeling", *John Wiley & Sons* – England - ISBN 0-471-95803-4, 96-99
- [27] Woodman, P., 2006, "Business Continuity Management (May 2006)", ISBN: 0-85946-445-8. (<http://www.managers.org.uk> - September (2006))
- [28] Zimmermann, H.-J., 2000, "An application-oriented view of modelling uncertainty", *European Journal of Operational Research*, 122, 190-198
- [29] Zsidisin, G.A. 2003, "A grounded definition of supply risk", *Journal of Purchasing & Supply Management* 9, 217–224
- [30] M. Treleven, S.B. Schweikhart, 1988, A risk/benefit analysis of sourcing strategies: Single vs. multiple sourcing, *Journal of Operations Management* 7(4), 93-114.
- [31] Anna Nagurney, Jose Cruz, June Dong, Ding Zhang, 2005, Supply chain networks, electronic commerce, and supply side and demand side risk, *European Journal of Operational Research* 164, 120–142
- [32] Brindley, C. (ed.) (2004): *Supply Chain Risk – A Reader*. Ashgate Publishing Limited.
- [33] Handfield, R., Blackhurst, J., Craighead, C.W. (2007): *Supply Chain Risk Management: Minimizing Disruptions in Global Sourcing*. CRC press.
- [34] Modarres, M. (2006): *Risk Analysis in Engineering – Techniques, Tools, and Trends*. Taylor & Francis.
- [35] Ziegenbein, A. (2007): *Supply Chain Risk – Identification, Assessment and Mitigation*. vdf Hochschulverlag Zürich (in German).
- [36] (2004) *A Guide to Project Management Body of Knowledge*. PMBOK guide – Project Management Institute, Inc
- [37] (2002). *Risk Management Guide for DoD Acquisition* – Defense Acquisition University US Department of Defense.
- [38] Hoelt, S., Davey M., Newsome, D., (May-June 2007) *Proactively Managing Risk: The New Waste*. Defense AT&L.
- [39] "Best Practices in Risk Management: Private and Public Sectors Internationally" Treasury Board of Canada Secretariat. Accessed on 10/25/2007 at [http://www.tbs-sct.gc.ca/pubs\\_pol/dcgpubs/RiskManagement/rm-pps1\\_e.asp](http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rm-pps1_e.asp)
- [40] "Comcover's Awards for Excellence in Risk Management 2004: National Capital Authority". Australian Government Comcover. Accessed on 10/25/2007 at: [http://www.finance.gov.au/COMCOVER/docs/2004\\_NCA.pdf](http://www.finance.gov.au/COMCOVER/docs/2004_NCA.pdf)