Variorum Multi-Disciplinary e-Research Journal
Vol.,-05, Issue-I August 2014

Risk Management in Supply Chains

S Rajagopalan: Research Scholar, JJT University, Rajasthan
Dr. Subhash P. Desai CA: Research Guide, JJT University, Rajasthan

Abstract

Supply Chains are subjected to various types of risks and it is one of the major issues today. Every organisation strives for success and uninterrupted operations. Hence efficient management of supply chain risk is very crucial. Presently, we lack suitable instruments which can make risk management in an organisation easier and more efficient. This article focuses on the risks by defining them by different key dimensions, so that risk management is simplified and can be undertaken in every supply chain and organisations within them. A risk catalog is available online, from the risks that have been identified so far. This catalog can serve as a checklist and a starting point in supply chain risk management in organisations.

Key Words: Supply Chain, Risk Management, Risk Catalog, Checklist

1. Introduction

Today, no company can operate in a completely secure environment without any risk deriving from supply chains, particularly in the present era of globalisation and global sourcing. Supply chain risks are a major concern in logistics and other business processes in any organisation. Therefore, the process of risk management is crucial for uninterrupted operations in all fields of business. We may define supply chain risk management as **"a process that supports the achievement of supply chain management objectives through the whole supply chain, not just in a single company".**

Risks have always been an integral part of our everyday life, but it is only now that we are devoting much attention to the challenges of risks. There are many conceptions and definitions of the term "risk". Even if we agree on a single definition of risk, it is still not sure whether we will be able to arrive at uniform opinions or answers to questions such as

- How to perceive risks?
- How to measure them?
- Which risks we are most exposed to in a given moment?
- What are the consequences of exposure to risks?
- What is the impact of risks?
- Which risks are acceptable and to what magnitude or extent?
- To whom are the risks acceptable and to whom they are not acceptable?
- How do risks change through time?
- What is their impact when observed individually and when taken together?
- What are their mutual effects and what are the consequences of these interactions?
- How to manage risks?
- How to assess the amount of resources required for mitigating or hedging the risks?

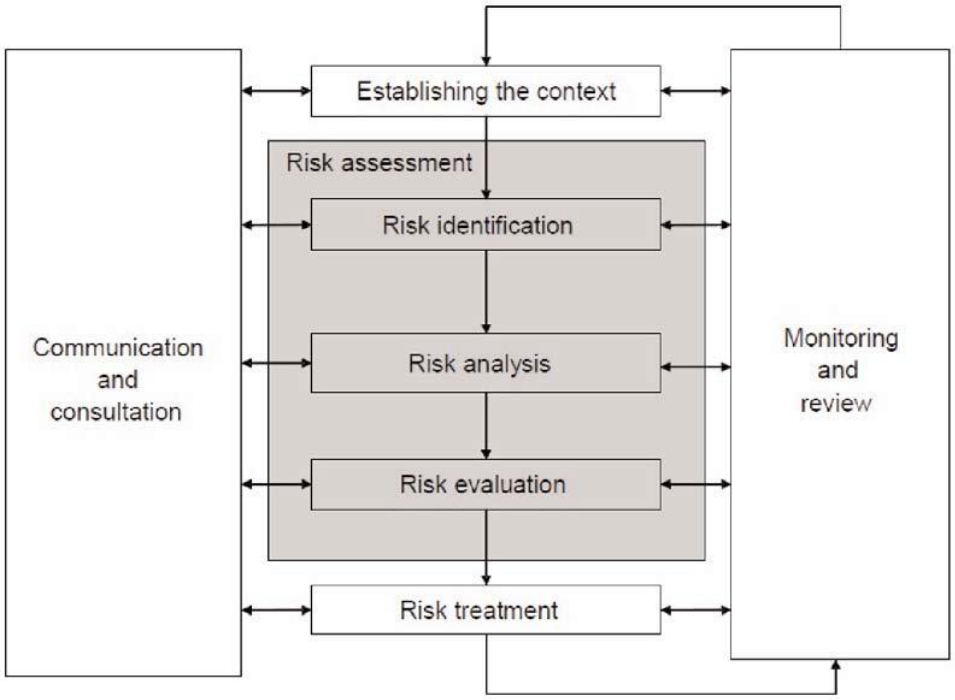
The fact that these questions remain unanswered, points to the complexity of the problem when one tries to address and manage the risks in a comprehensive manner. Perhaps the best way to understand is through the example of investments. Investments are the foundation of any

business activity – investments enable maintenance, increase of scope of business operations, or changing the business activity – and involve risks and their management is a vital part of operating activities. There are virtually no investments without risks.

The general risk management international standard – ISO 31000: 2009 (Risk Management – Principles and Guidelines), provides a definition of risk as under:

"Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organisation's objectives is "risk" (ISO 2009)". Further, it is stated in the standard that risk can be categorised by reference to potential events and consequences, and is often expressed in terms of a combination of the consequences of an event and the associated likelihood.

The use of ISO 31000 families of international standards provides a framework for risk management in all types of organisations and the supply chains they form. The standard takes into account different aspects of an organisation and its risk management, including internal and external context, structures, processes, functions etc. The basic risk management process as defined in ISO 31010:2009 is as shown in the figure below:



The risk management process as defined in ISO 31010 (IEC, 2009)

The processes included in risk assessment, particularly risk identification and analysis are the most crucial in the whole risk management process. Risks that are not identified and defined in the first stages of risk assessment are not later treated and therefore go unseen and unmanaged.

2. The Model for Risk Assessment

The first step in risk assessment is always risk identification. This process should be as extensive as possible in order to identify as many potential risks as possible and to avoid overlooking crucial risks.

Every organization should approach risk identification using methods they find most suitable in their context. Every identified risk has its specific attributes. The attributes of a certain risk can be general, i.e. the same attributes are true in every organisation, or they can be organisation-specific, i.e. some attributes of a risk have to be defined in a specific organisation that is undertaking risk assessment. There are five dimensions of risk definition that are not dependant on a specific organisation and can therefore be generalized:

1. Type of risk which is in accordance with risk groups as defined in ISO 28000
2. Logistics resources on the use of which a certain risk can have an influence
3. Publics that are highly exposed to a certain risk
4. Risk origin according to the organisation and its supply chain
5. Domain of risk management with regard to business or technological area

2.1 Risk Segmentation

The international standard for security in supply chains, ISO 28000, defines several fields from where risks or security threats to a company or a supply chain can originate. The standard defines these groups broadly enough and yet in a manner that includes all relevant aspects of potential risks. The various groups are:

1. Physical failure threats and risks such as functional failure, incidental damage, malicious damage or terrorist or criminal action
2. Operational threats and risks, including control of the security, human factors and other activities which affect the organisation's performance, condition, or safety
3. Natural environmental events (storm, floods, etc.) which may render security measures and equipment ineffective
4. Factors outside the organisation's control, such as failures in externally supplied equipment and services
5. Stakeholder threats and risks such as failure to meet regulatory requirements, or damage to reputation or brand
6. Design and installation of security equipment including replacement, maintenance, etc.
7. Information and data management and communications
8. A threat to continuity of operations

The description of a risk based on the group from ISO 28000 is also the first dimension of risk definition in the risk catalog.

2.2 Risk Segmentation according to the affected logistics resources

There are different fundamental resources of logistics operations which are used in logistics processes and consequently in supply chain management processes. Supply chain risks can have a significant effect on the use of these resources and therefore this interaction needs to be considered. For example in the field of IT, risk management is based on interactions between resources and IT risks. Any consequence of risk, occurring in a supply chain, can influence one or more of these resources. In order to effectively manage the risks, we need to be aware of logistics resources that a specific risk and its consequences possibly affect. Some risks are complex and have wider influences; therefore, they have to be defined as influential on more than one resource of logistics.

2.3 Risk Segmentation according to risk taker – People

People have a different view on and a relation to the same risk, which may be the result of different exposure as well as of different levels of uncertainty. The problem is most commonly

addressed in relation to groups of people, rather than individuals, i.e. segments of the public that share a common stance with regard to a particular risk. The risk is composed of

1. Uncertainty which should be divided into
   a. Objective uncertainty and
   b. Subjective uncertainty
2. Exposure

2.3.1 Uncertainty

Uncertainty is a condition when one does not know whether a proposition or assertion is true or false. Probability is the metrics that is most commonly used to express uncertainty; however, its applicability is limited. At best, it can assess the uncertainty we are able to perceive.

While objective uncertainty includes logic, probability and statistical methods, on the other quantifying probability is hardly helpful considering subjective uncertainty, quantification of these subjective viewpoints is nearly impossible.

2.3.2 Exposure

A person is said to be exposed to risk when an event has some material or non-material consequences for that person. We can be exposed to risk and be fully aware of it or not be aware of it at all. Risk can be taken very seriously or we can act quite indifferently to it. Thus, exposure introduces additional indistinctness, or undefinability, which depends primarily on the individual or a certain segment of the public and its perception of exposure and, consequently, of risk. Hence, we are not only dealing with the problem of metrics of uncertainty, but rather with a problem of the metrics of exposure.

2.3.3 Risk

Risk can be described as exposure to objective and subjective uncertainty. Since both uncertainty and exposure are difficult to define, risk is not easily definable either. Segments of public are seen as a mandatory defined parameter of each risk, because risk depends on uncertainty and exposure, which is ultimately an attribute of human beings and not of things or concepts.

2.3.4 Segments of the public in risk management

We segment all people, involved in a supply chain and its surroundings, to different publics, i.e. different groups of people with same interests or functions according to the individual risk. This is also in accordance with ISO 31000, where one of the main principles for effective risk management is that "risk management takes human and cultural factors into account. It recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organisation's objectives (ISO 2009)". Communication and consultation with stakeholders is important as they make judgments about risks based on their perceptions of risk. The perceptions can vary due to differences in values, needs, assumptions, concepts, and concerns of stakeholders. As their views have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and taken into account in the decision making process (ISO 2009).

2.4 Risk segmentation according to the origin from the point of view of supply chain

A supply chain is a complex system of several organisations that work together in a specific environment, where they face internal and external factors and influences that make it uncertain

whether and when they will achieve their objectives (ISO 2009). A risk can come from three different origins:

1. From a company that is included in the supply chain
2. From the whole supply chain (but not from the observed company)
3. From outside of the supply chain, in its environment

Every company has dependencies on multiple third parties. As part of a supply chain, a company is usually tightly connected with parties in the same supply chain, more than with other companies from outside. Therefore, companies involved in specific supply chain, have some kind of influence between themselves. Dependencies are risks, because, by definition, if you depend on someone, then they could act in a way that negatively impacts you. Thus, dependency is a crucial dimension of risk that is often not considered as part of risk assessment or is ignored for political reasons. These risks tend to be more subtle and only emerge when analysing business processes and not the technology components or infrastructure.

2.5 Risk segmentation according to business or technological significance

All organizations' activities can be characterised as technological or commercial. Thus, we can define risk as technological, commercial or universal. This is another dimension of risk definition model.

3. Further Definitions during Risk Assessment

Supply chains are as diverse as today's consumer markets. Based on the type of supply chain or goods that are supplied in a specific chain, we can define risks according to another dimension. Some risks can occur in all types of supply chains, but some are specific to a certain type of a chain, for example, cold chains, production of flammable materials etc.

For evaluating risks we also need to define their impact (or influence) to a specific public during assessment process. Every specific public is influenced by a certain risk in its own way and responds to risks differently.

In many real situations, some or all risks and impacts depend on time. These time frames, if present, have to be defined in the process of risk assessment to gain a perspective over changes with time. For every risk, an acceptability level has to be defined. We also have to consider the time component of the risk, when applicable, in order to fully acknowledge all levels of potential impact and to correctly define the acceptability level.

No process in a company can exist without links to other processes. Similarly, not a single risk can be isolated, not having any effect on other processes and also risks in a company or a supply chain as a whole. Because of this, we need to define connections between all identified risks.

A general idea of risk management is that every risk should have a person or group, designated for its management, usually named risk owner. According to ISO 31000, a risk owner is a "person or entity with the accountability and authority to manage a risk" and "the organisation should ensure that there is accountability, authority, and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy".

4. Results – Risk Catalog

The final product of conventional risk identification and risk analysis is a risk catalog which contains all identified and defined risks in a single organisation. This risk catalog is

publicly available. This risk catalog contains supply chain risks as were defined in different companies from different branches of operations, and can therefore be an excellent source for any manager considering risks, to use as a guideline and a check list.
The catalog is available online at http://labinf.fl.uni-mb.si/risk-catalog/.

5. Conclusion

Based on today's uncertain market conditions, demands of globalisation, and increasing external threats, we can conclude that in order to assure continuity of operations, in an organisation and in a supply chain, certain measures have to be taken. Risk management should be a primary concern for every organisation and should be included in every aspect of an organisation's operations to ensure its efficiency and thoroughness.
Managers should be aware of threats to their organisation and of tools to manage them. The risk catalog presents an excellent resource for risk management in all supply chains. The supply chain risk catalog provides a simple check list of risks as were identified by experts

References:

1. Christopher, Martin & Denis Towill, "Developing Market Specific Supply Chain Strategies", *International Journal of Logistics Management*, Vol. 13, No. 1, (2002), pp 1-13
2. Diana BOŽIĆ, et.al., (2010), "Evaluation of Risk Management Status for Croatian Logistic Operators, 5 (3), pp 67-73
3. Szuster, M., (2010), "Theoretical and practical aspects of risk management in contemporary global supply chains", LogForum, 6 (3), pp 91-97
4. Scannel, T. et.al., (2013), "Integration of ISO 31000:2009 and Supply Chain Risk Management", American Journal of Industrial and Business Management, 3 (4), pp 367-377
5. Jereb, B. et.al., (2012), "Mastering Supply Chain Risks", Serbian Journal of Management, 7 (2), pp 271-285