www.sjm06.com

Serbian Journal of Management 7 (2) (2012) 271 - 285

Serbian Journal of Management

MASTERING SUPPLY CHAIN RISKS

Borut Jereb*, Tina Cvahte and Bojan Rosi

[a]*University of Maribor, Faculty of Logistics, Maribor, Slovenia*

(Received 23 December 2011; accepted 19 January 2012)

Abstract

Risks in supply chains represent one of the major business issues today. Since every organization strives for success and uninterrupted operations, efficient supply chain risk management is crucial.

During supply chain risk research at the Faculty of Logistics in Maribor (Slovenia) some key issues in the field were identified, the major being the lack of instruments which can make risk management in an organization easier and more efficient. Consequently, a model which captures and describes risks in an organization and its supply chain was developed. It is in accordance with the general risk management and supply chain security standards, the ISO 31000 and ISO 28000 families. It also incorporates recent finding from the risk management field, especially from the viewpoint of segmenting of the public.

The model described in this paper focuses on the risks itself by defining them by different key dimensions, so that risk management is simplified and can be undertaken in every supply chain and organizations within them. Based on our mode and consequent practical research in actual organizations, a freely accessible risk catalog has been assembled and published 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 organizations. It also incorporates experts from the field into a community, in order to assemble an ever growing list of possible risks and to provide insight into the model and its value in practice.

Keywords: Supply Chain, Risk Management, Risk Assessment, Risk Catalog, ISO 31000:2009, ISO 28000:2007

1. INTRODUCTION

No company today can operate in a completely secure environment without risk, deriving from supply chains, particularly considering trends of globalization and global sourcing. Supply chain risks have become a main concern in today's logistic

* *Corresponding author:bojan.rosi@fl.uni-mb.si*

DOI: 10.5937/sjm7-1360

and other business processes in any company. Therefore we can say that the process of risk management is crucial for uninterrupted operations of companies in all fields of business and supply chain risk management is "a process that supports the achievement of supply chain management objectives" (Gaudenzi & Borghesi, 2006) through the whole supply chain, not only in a single company.

Risks are an integral part of our lives and it appears that people have never devoted as much attention to the challenges of risks as we do today. Risks are addressed by numerous articles, comments, and conversations. Perhaps expectedly, there are virtually countless conceptions and definitions of the term "risk". Even if a particular community agrees upon a single definition of risk, it is still anything but certain that such a community will reach uniform opinions or answers to questions such as: How to perceive risks? How to measure them? Which risks are we 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 which magnitude or extent? Who are the risks acceptable to and who are they not acceptable to? How do risks change through time? What is their impact when observed individually and when taken together? What is their mutual effect and what are the consequences of these interactions? How should risks be managed? How to assess the amount of assets required for mitigating or hedging the risks? The myriad of questions that have remained unanswered to this day points to the complexity of the problem imposed when one embarks on a quest to address and manage the risks in a comprehensive manner.

Risks need to be understood in order to begin their efficient management. Perhaps they can be most easily grasped through the example of investments. Investments are the foundation of any business activity – investments enable maintenance, increase of the scope of business operations, or changing the business activity (IT Governance Institute, 2008) – and involve risks and their management as a vital part of operating activities; there are virtually no investments without risks.

It seems today that almost every field where risk management takes place has a certain specific definition of risk or at least a specific understanding of the term. Considering that risk management is applied in many different fields of science and engineering practice (Olsson, 2007; Alhawari, et al., 2012), there is large number of different definitions. As we try to generalize and standardize basic risk management concepts, some definitions also have to be given. This is best accomplished in the general risk management international standard, ISO 31000:2009 (Risk management – Principles and guidelines), which also provides a definition of risk: '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 organization's objectives is "risk". (ISO, 2009)' Furthermore, it is stated in this standard that risk can often be characterized 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.

This paper proposes a general principle for risk model based on ISO 31000 and on the proposition of segmenting the risks into

any given number of dimensions. With this we follow the guidelines for further research on the topic of supply chain risk management, as were layed down by Khan and Burnes (2007), specifically the "need to devise robust and weel-grounded models of supply chain risk management, which incorporate risk management tools and techniques from other disciplines of research".

When considering risk management in organizations and in the supply chains they form, following certain guidelines is advised to ensure the process is thorough and efficient. We propose the use of ISO 31000 family of international standards, which provides a framework for risk management in all types of organizations. It takes into account different aspects of an organization and its risk management, including internal and external context, structures, processes, functions etc. The basic risk management process, as is defined in ISO 31010:2009, can be seen on Figure 1.

The processes included in risk assessment, especially risk identification and analysis, are the most crucial in the whole risk management process. We have to be aware that risks that are not identified and defined in the first stages of risk assessment are not later treated and therefore go unseen and unmanaged. Because of that, a model for efficient supply chain risk assessment in organizations was developed. This model was tested in real life; the pilot testing was done on an actual logistics company that focuses mainly on warehousing. The output we got from this preliminary test and subsequent testing is a catalog of identified risks, where each risk is also defined or categorized according to different dimensions that will be explained later in the paper. As this test was well accepted by the test companies we have reason to believe that we are on the right path to achieving our goal, which is to develop a widely usable

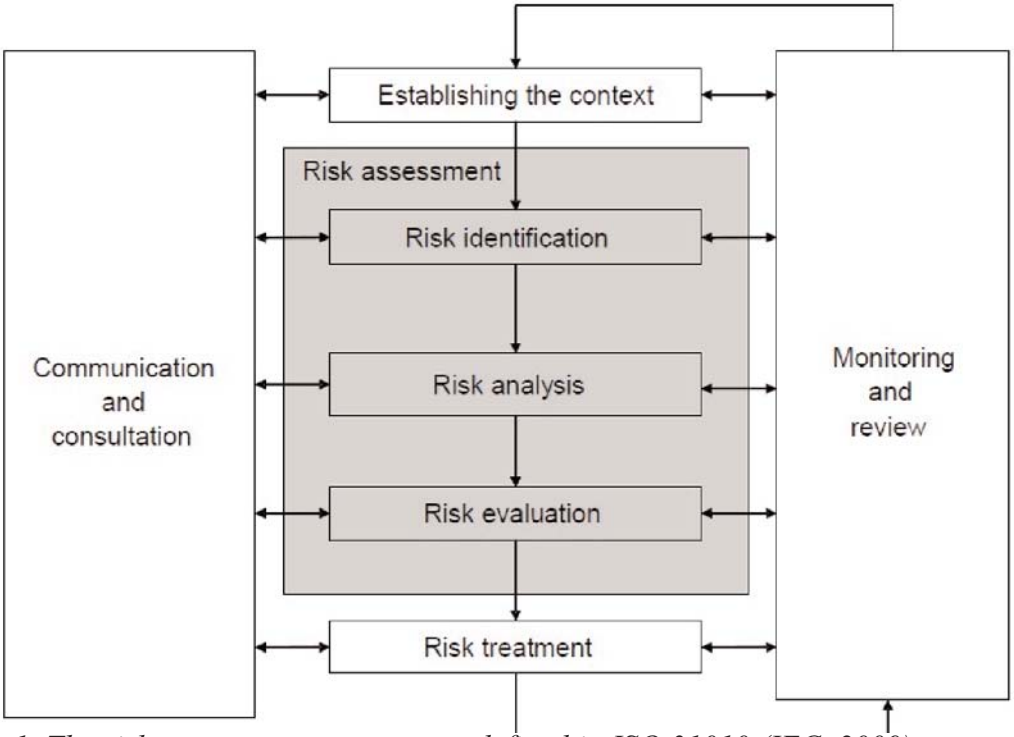


Figure 1. The risk management process as defined in ISO 31010 (IEC, 2009)

model for supply chain risk assessment. Moreover, our goal is to implement a web-based catalog of supply chain risks, which is published under the Creative Common License, allowing everyone to use the catalog as a reference and to propose changes and additions to it.

2 THE MODEL FOR RISK ASSESSMENT

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

ISO 31010 proposes numerous techniques and methods for risk assessment. Out of those, we selected three – free interviews, structured interviews and brainstorming, which we used in the phase of risk identification in the first steps of assessing risks in our pilot testing. During sessions between trained external personnel and organization's employees risks are identified and then later put into the description model. It has to be noted though that the use of our model and the catalog that is derived from it is in no way connected to the use of these three methods. Every organization should approach risk identification using methods they find most suitable in their context.

Every identified risk has its specific attributes, which we strive to describe with the use of our model. Since we believe that risk identification and analysis are the key activities in managing risks, several dimensions by which each identified risk in a company or supply chain should be described are included in the model and consequently in the risk catalog which serves as a base for risk analysis. These attributes of a certain risk can be general, where we can be quite certain that the same attributes are true in every organization, or they can be organization specific, where some attributes of a risk have to be defined in a specific organization that is undertaking risk assessment.

Each of the above mentioned attributes that can be generalized are infiltrated in our model in the form of dimensions, where each risk is described by being placed in a certain group within a dimension. With this we also provide risk segmentation and consequently some additional ease of manipulation with lists of identified risks. At the moment, our model proposes five dimensions of risk definition that are not dependant on a certain organization 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 organization and its supply chain,
5. domain of risk management in regard of business or technological area.

As stated earlier, some dimensions of risk definition have to be additionally implemented to achieve a thorough understanding of risks, such as influences between risks, its consequences etc., but these risk attributes are mainly dependant on the organization’s environment and therefore have to be defines specifically.

Dimensions that are included in our model are described in this article, and short descriptions of organization specific dimensions that need to be implemented are given.

2.1. Risk segmentation according to ISO 28000:2007

This model and the catalog that derives from it are structured so that they complement an international standard on security in supply chains, ISO 28000. In this standard, several fields from where risks or security threats to a company or a supply chain can originate are defined. Because the standard defines these groups broadly enough and yet in a manner that includes all relevant aspects of potential risks, we use this groping as the base for our risk assessment process. In the first step each identified risk is placed in these groups (ISO, 2007):

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 the control of the security, human factors and other activities which affect the organizations performance, condition or safety;
3. natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective;
4. factors outside of the organization'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. Since some risks are more complex than others, some cannot be defined simply by one group; therefore some risks also have a secondary group placement.

2.2. Risk segmentation according to the affected logistics resources

As we analyze risks we need to be aware that there are different resources of logistics operations in supply chains. These resources represent fundamental resources which are used in logistic processes and consequently in supply chain management processes. Supply chain risks can have a significant effect on the use of this resources and therefore this interaction has to be recorded, which we achieve by defining, on which logistics resource or its use a certain risk can have an effect. The idea behind resources definition and their use in risk management comes from the field of IT, where risk management is based on interactions between resources and IT risks, as are defined in COBIT 4.1 (ISACA, 2007). Based on our research of different definitions of logistics and also consultations with logistics expert, we defined four primary logistics resources, without which logistics processes cannot take place. We believe that the implementation of logistics is based on the following logistics resources:

1. Flow of goods and services should be managed from the point of origin to the point of use in order to meet the requirements of customers.
2. Information, which cause a change in the state of a dynamic system, if the system was able to decode data and to attribute them with a relevant meaning, and also deliver a

change of knowledge in accordance with certain rules where the system has access to them.

3. Logistics infrastructure and suprastructure as basic physical and organizational structures needed for the operation of logistics.

4. People are the personnel required to plan, organize, acquire, implement, deliver, support, monitor and evaluate the logistics systems and services. They may be internal, outsourced or contracted as required.

Any consequence of risk, occurring in a supply chain, can influence one or more of these resources. If we wish to effectively manage risks, we need to be aware of logistics resources that a specific risk and its consequences possibly affect. That is why the second dimension of defining risk in our model is to ascertain which resources of logistics can be affected by an identified risk. Again, as with ISO 28000 grouping, 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 takers – public

Segments of the public are groups of people that have been identified by their current interest in, attitude to, or current behavior around, a particular issue, representing the most important part of the environment which is considered in risk management. Such an approach in which segments of the public play the central role in risk management is new in scientific technically oriented literature.

As every human being is unique, different from all others, our relations to a certain risk encountered with regards to a particular situation can also differ greatly. Hence, people have a different view on and a relation to the same risk, which may be a result of different exposure as well as of different levels of uncertainty. The problem is most commonly addressed not in relation to individuals, but in relation to groups of people, i.e. segments of the public that share a common stance with regard to a particular risk.

Our approach is based on the assumption that the risk is composed of (Jereb, 2009; Jereb, 2010):

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

All four terms: objective and subjective uncertainty, exposure and risk, will be shortly explained in the text which follows.

2.3.1. Uncertainty

Uncertainty is a condition when one does not know whether a proposition or an 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 (Jereb, 2009).

While objective uncertainty includes logic, probability and statistical methods, on the other hand quantifying probability is hardly helpful considering subjective uncertainty – when probabilities are defined by individuals based on their beliefs, or when a system of values is established based on opinions in order to describe their

uncertainty, quantification of these subjective viewpoints is nearly impossible.

2.3.2. Exposure

The litmus test for exposure is "Would we care?" In other words, a person is exposed when an event has some material or non-material consequences for that person. People are thus exposed when they care about whether a certain proposition is true or false. We can be exposed to risk and be fully aware of it (balancing on the fence of a high bridge) or not be aware of it at all (balancing on the same fence while sleepwalking). Risk can be taken very seriously (speed limits in a village where a police patrol is always on duty), or we can act quite indifferently to it (speeding through the village in the middle of the night, knowing that the police patrol is not there and assuming that everyone is asleep). 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. (Jereb, 2009)

2.3.3. Risk

Risk can be described as exposure to objective and subjective uncertainty (Jereb, 2010). Since both uncertainty and exposure are difficult to define, risk is not easily definable either.

Technical science, engineering, economics, etc., employ a simplified approach, where risk simulation models predominantly, or even exclusively, use objective uncertainty (i.e. probability distributions of risk), while failing to account for their interdependence or dependence on the environment, with human beings being the most important and complex part of it. For example a well known simplified approach is multiplying probability by potential loss. The confidence in such models in practice is relatively low, except in specific areas such as actuarial science. This is the reason why manager decisions regarding risk management are mostly based on "common sense", which in practice presents a better choice than making decisions based on the output of simplified models of risk.

Segments of the 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

When defining risks and their influences, we can take a different approach as that of most today's literature on the subject. If we assume that only people can perceive themselves and inanimate things cannot, we can also assert that finally, a certain risk can only influence people, who are susceptible to perceptions. According to this theory we segment all people, involved in a supply chain and its surroundings, to different publics, that is different groups of people with same interests or functions according to the individual risk. When defining risks in our model, we say that this dimension of risk identification is exactly that – defining, which publics are affected by a certain 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 organization's objectives. (ISO, 2009)'

Also, the standard defines the importance of communication and consultation with stakeholders, which our model achieves by segmenting them into publics. ISO 31000 describes this importance: 'Communication and consultation with stakeholders is important as they make judgments about risks based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perception should be identified, recorded, and taken into account in the decision making process. (ISO, 2009)' Specific shareholders, as the standard names them, are publics as are defined in our model. We chose to use the term publics based on the knowledge from public relations, which is a field that uses segmenting of the public with best results and where this segmentation is most widely used in practice.

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

A supply chain is a complex system of several organizations 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; Oyatoye & Fabson, 2011). Based on the extent of risk consequences regarding the supply chain, we can define risks according to another dimension in our model. 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 a part of a supply chain, a company is usually tightly connected with parties in the supply chain, more than with other companies from “outside". Therefore any company should suppose that companies, involved in a specific supply chain, have some kind of influence between themselves. However, Andrew Steward wrote that dependencies are risks, because, by definition, if you depend on someone than they could act in a way that negatively impacts you (Steward, 2004). Steward also recognized that 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 analyzing business processes and not the technology components or infrastructure.

2.5. Risk segmentation according to business or technological significance

All organizations’ activities can be characterized as technological or commercial. In accordance we can also define risks as mainly technological, commercial or universal. This is another dimension of our risk definition model.

Together, a list of identified risks, their definitions by dimensions and additional descriptions where needed form a base for the risk catalog, published on the Internet.

3 FURTHER DEFINITIONS DURING RISK ASSESSMENT

As stated earlier, in the process of risk identification, analysis and evaluation in a specific organization, we have to implement additional dimensions of risk definitions in order to completely understand risks, their connections and impact.

As we know, supply chains are as diverse as today's consumer markets. Based on the type of a supply chain or goods that are supplied in a specific chain, we can define risks according to another dimension in our model. 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 have to define their impact (or influence) to a specific public during the assessment process. We have to be aware that every specific public is influenced by a certain risk in its own way and responds to risks differently. By analyzing the impact with aspect to publics, we can gain a better insight into the consequences of a risk. This is not the same as only defining which public is affected, it is an expansion of that previous dimension; here possible effects of the risk are analyzed in more detail.

In many real situations, some or all risks and impacts depend on time. It is the reason why the model should include the dimension of time, which introduces non-determinism. In some time frames a single risk can be minor and in some a major influence on the organization. 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. With this, a frame is set where we can assess to which extent and if even a risk needs to be managed.

We have to acknowledge that no process in a company can exist without links to other processes. The same goes for any risk – not a single risk can be isolated, not having any effect on other processes and also risks in a company or in the supply chain as a whole. Because of that, we need to define connections between all identified risks, and that is the next dimension in our model.

A general idea of risk management is that every risk should have a person or group, designated for its management, usually named risk owner. ISO 31000 defines a risk owner as a 'person or entity with the accountability and authority to manage a risk', and that 'the organization 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, effectiveness and efficiency of any controls. (ISO, 2009)' By defining a specific person for every risk we achieve a higher level of awareness with those who need to partake in risk management.

4. RESULTS - RISK CATALOG

The final product of conventional risk identification and risk analysis, described in this paper, is a risk catalog which contains all identified and defined risks in a single organization. We strive to collect these results into a risk catalog which is expanded onto the whole field of supply chain risks and publicly available as a valuable resource in this field. Since the process of risk assessment is slow and can be insufficiently accurate, our idea of a publicly published catalog gives organizations an option to use previously gained knowledge of the field in their risk management process. This risk catalog contains supply chain risks as were defined in different companies from different branches of operations, and can therefore be an excellent resource for any manager considering risks to use as a guideline and a checklist. The use of a checklist as a tool for risk identification is also strongly recommended by ISO 31010, which defines it as 'a list of hazards, risks or control failures that have been developed usually from experience, either as a result of a previous risk assessment or as a result of past failures (IEC, 2009)'. Based on that we believe the risk catalog we are implementing is in accordance with the ISO risk management family of standards, and also takes the frameworks proposed in the standards to a higher level with the inclusion of more supply chain risk management experts and through sharing of knowledge throughout the community.

The need for a risk catalog can be seen from many perspectives. Even ISO 31000 defines the output of risk identification as 'a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives (ISO, 2009)'. An organization can undertake the process of risk management by itself, but because of the daunting scope of this project many decide not to manage their risks all together. By using the catalog as a resource and checklist, a major step of risk management is already completed, allowing the organization to approach risk management more prepared and with less complications. We can see that a risk catalog of this scope, which to this day does not yet exist as a freely accessible source of information, is much needed in today's business environment. Even if the catalog will be used only as a check list of possible risks in supply chain operations it represents a crucial next step in the evolution of supply chain risk management worldwide.

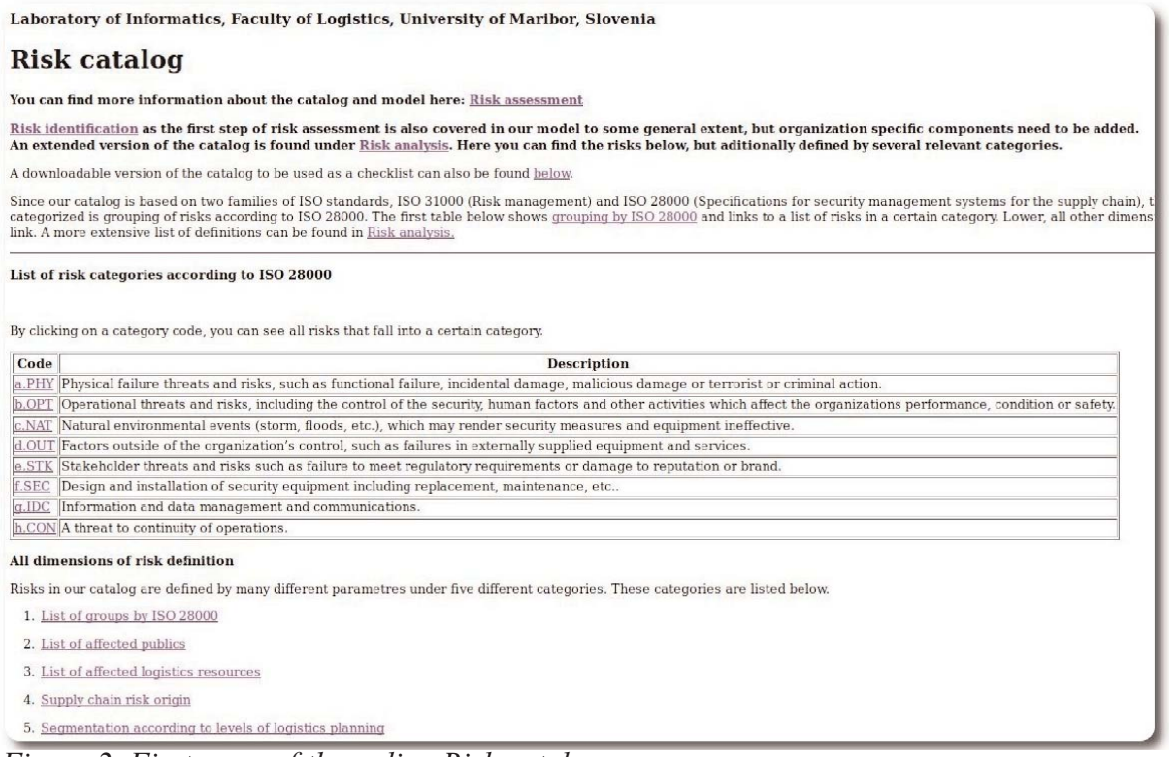
Since we believe a resource like that should be freely accessible, it is published under a Creative Commons license that allows interested users to look at, download and share the risk catalog with others, as long as proper credit is given to the authors, but they cannot change it or use it commercially; this is the 'Attribution- NonCommercial –NoDerivs' licence (Creative Commons, 2011). However, since our philosophy is that the catalog is an ever growing publication, we believe that all users should be able to contribute, comment or add to the catalog. This is achieved by submissions of ideas to the editorial board, which assesses the contributions and incorporates them in the catalog when appropriate. Submissions are expected via email SC.RiskCatalog@gmail.com. With this we hope to achieve a widespread interest in the use of the catalog among professionals from the supply chain field and to additionally increase its scope and quality. As supply chain risk managers we have to be aware of the importance of cooperation between

companies. One single company or its employees can never identify as many risks as a group of companies can. Our aim is to connect experts throughout supply chains all over the world and establish a community with a common goal – to provide insight into risk assessment and the risk catalog. Even Manuj and Mentzer (2008) stress the significance of cooperation in supply chain risk management. Their research, which focused on SCRM research in global companies through interviews with professionals from the field, pointed out the importance of involving many professionals and forming teams to manage risks. We can deduct that forming global "teams" of experts as is the goal of our catalogue is in accordance with their theory and can therefore provide better insight and quality of risk identification and management.

4.1. Risk catalog description

The catalog is available online at http://labinf.fl.uni-mb.si/risk-catalog/. An extensive list of so far identified supply chain risks is given, and the risks are described by the categories listed above. Additionally, and explanation of the dimensions is given, and also a list of coding for the catalog. On every dimension code, a list of risks under that code is also given.

On the first page of the catalog website, a short description of the model and catalog is given, followed by the most important dimension of risk definition, grouping by ISO 28000 categories of risks. Additionally, all dimensions of risk definition are given. At the bottom of this page you can also find a downloadable version of the catalog. Figure 2 shows a part of the first page of the risk catalog.



Laboratory of Informatics, Faculty of Logistics, University of Maribor, Slovenia

Risk catalog

You can find more information about the catalog and model here: Risk assessment

Risk identification as the first step of risk assessment is also covered in our model to some general extent, but organization specific components need to be added. An extended version of the catalog is found under Risk analysis. Here you can find the risks below, but aditionally defined by several relevant categories.

A downloadable version of the catalog to be used as a checklist can also be found below.

Since our catalog is based on two families of ISO standards, ISO 31000 (Risk management) and ISO 28000 (Specifications for security management systems for the supply chain), t categorized is grouping of risks according to ISO 28000. The first table below shows grouping by ISO 28000 and links to a list of risks in a certain category. Lower, all other dimens link. A more extensive list of definitions can be found in Risk analysis.

List of risk categories according to ISO 28000

By clicking on a category code, you can see all risks that fall into a certain category.

Code	Description
a.PHY	Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action.
b.OPT	Operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety.
c.NAT	Natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective.
d.OUT	Factors outside of the organization's control, such as failures in externally supplied equipment and services.
e.STK	Stakeholder threats and risks such as failure to meet regulatory requirements or damage to reputation or brand.
f.SEC	Design and installation of security equipment including replacement, maintenance, etc..
g.IDC	Information and data management and communications.
h.CON	A threat to continuity of operations.

All dimensions of risk definition

Risks in our catalog are defined by many different parametres under five different categories. These categories are listed below.

1. List of groups by ISO 28000
2. List of affected publics
3. List of affected logistics resources
4. Supply chain risk origin
5. Segmentation according to levels of logistics planning

Figure 2. First page of the online Risk catalog

An explanation of the 'Creative Commons' license, which the risk catalog is published under, is given, as well as the contact email address you can use if you wish to comment the catalog or make a contribution.

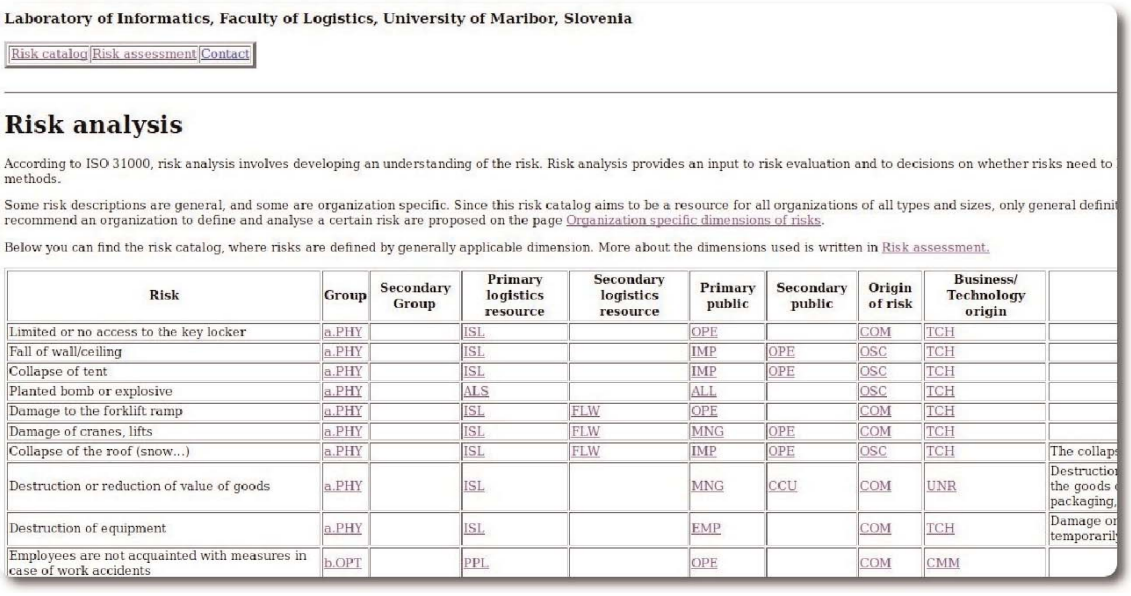
When you wish to find out more about the catalog itself and also about the risk assessment process we recommend and was used when compiling it, you can do so on the subpage named 'Risk assessment'. There you can find a short description of the risk assessment process and our propositions for it. Most importantly, here you can find links to descriptions of different dimensions by which risks are defined in the risk catalog.

A certain dimension of definitions, for example 'List of affected logistics resources', can be accessed easily by clicking on the title, then a subpage opens with a short description of the dimension and with all category codes and categories by which a risk can be described in this dimension.

Since risk assessment according to ISO 31000 is comprised out of three different processes, we maintain the same philosophy in our risk catalog and divide our processes into these three categories. Risk identification is the first process of risk assessment. The risk catalog is a very useful tool for identifying risks, but in every specific organization, additional parameters of risk have to be defined in order to complete the risk identification phase according to ISO 31000 - sources of risk, areas of impact, risk causes and their potential consequences. As these cannot be generalized, they are out of the current scope of this catalog. In most cases though, many organizations share similar sources of risk, risk consequences and impact. The list is currently under development. We hope that with more contributions by supply chain risk experts, this list will also become more complete.

The next stage is risk analysis, which provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

Some risk descriptions are general, and some are organization specific. Since this



Laboratory of Informatics, Faculty of Logistics, University of Maribor, Slovenia

Risk catalog | Risk assessment | Contact

Risk analysis

According to ISO 31000, risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to methods.

Some risk descriptions are general, and some are organization specific. Since this risk catalog aims to be a resource for all organizations of all types and sizes, only general definit recommend an organization to define and analyse a certain risk are proposed on the page Organization specific dimensions of risks.

Below you can find the risk catalog, where risks are defined by generally applicable dimension. More about the dimensions used is written in Risk assessment.

Risk	Group	Secondary Group	Primary logistics resource	Secondary logistics resource	Primary public	Secondary public	Origin of risk	Business/ Technology origin	
Limited or no access to the key locker	a.PHY		ISL		OPE		COM	TCH	
Fall of wall/ceiling	a.PHY		ISL		IMP	OPE	OSC	TCH	
Collapse of tent	a.PHY		ISL		IMP	OPE	OSC	TCH	
Planted bomb or explosive	a.PHY		ALS		ALL		OSC	TCH	
Damage to the forklift ramp	a.PHY		ISL	FLW	OPE		COM	TCH	
Damage of cranes, lifts	a.PHY		ISL	FLW	MNG	OPE	COM	TCH	
Collapse of the roof (snow...)	a.PHY		ISL	FLW	IMP	OPE	OSC	TCH	The collaps
Destruction or reduction of value of goods	a.PHY		ISL		MNG	CCU	COM	UNR	Destructio the goods packaging,
Destruction of equipment	a.PHY		ISL		EMP		COM	TCH	Damage o temporarily
Employees are not acquainted with measures in case of work accidents	b.OPT		PPL		OPE		COM	CMM	

Figure 3. Risk analysis page

risk catalog aims to be a resource for all organizations of all types and sizes, only general definition dimensions are included. Additional dimensions by which we recommend an organization to define and analyze a certain risk are proposed in this article in the chapter 'Further definitions during risk assessment'. In the 'Risk analysis' subpage, a list of all risks is given, and those risks are defined by different dimensions. Every categorization is performed with a code of a relevant category of a dimension, which is also a hyperlink, leading to a supbage with the description of the category and a list of all risks that fall into that category of a certain dimension. Figure 3 show a part of the Risk analysis page.

When you wish to know more about a certain category or you wish to see all risks that fall into the category, click on the code in the first column and a subpage will open with its description and a list of relevant risks.

Risk evaluation as the final step of risk assessment, as defined in ISO 31000, is the process of deciding about which risks need treatment and the priority for treatment implementation. This step cannot be generalized and is therefore not in the scope of this risk catalog, but is entirely dependent on specific organizations.

5. CONCLUSION

Based on today's uncertain market conditions, demands of globalization and increasing external threats, we can conclude that in order to assure continuity of operations in an organization and in a supply chain certain measures have to be taken. Risk management should be a primary concern for every organization and should be included in every aspect of an organization's operations to ensure its efficiency and thoroughness. Managers should be aware of threats to their organization and of tools to manage them.

Our model for risk assessment allows managers to approach risk management in a simplified manner, detailing recommended steps, and at the same time providing them with a tool for risk assessment. The supply chain risk catalog, which is freely accessible online, provides a simple checklist of risks as were identified by experts, and additionally some general descriptions according to different dimensions. Organization specific aspects of risks should be added during the risk assessment process to ensure a thorough understanding of an organization's risks and to provide an extensive input into the process of risk treatment. We believe that this catalog, especially with its focus on people and publics, presents an excellent resource for risk management in all supply chains.

Every user of our model and the catalog that is derived from it can find it as a new approach to supply chain risk management which is based on a detailed description of every identified risk. This approach is new in today’s scientific literature, and the same is true for the supply chain risk catalog, which is the first of its kind to be published as “open” under a Creative Commons license.

As we believe that only a group of experts can provide the needed knowledge to perfect the model and assemble a list of risks, as extensive as possible, our model and catalog are freely accessible. We encourage managers and other experts from the field of risk management to use it in their work, and consequently provide us with ideas about possible improvements to the model and additions to the catalog.

УПРАВЉАЊЕ РИЗИКОМ ЛАНАЦА СНАБДЕВАЊА

Borut Jereb, Tina Cvahte, Bojan Rosi

Извод

Ризици у ланцима снабдевања, представљају један од основних изазова у савременом пословању. Обзиром да свака организација тежи успеху и неометаном одвијању операција, од суштинског је значаја ефикасно управљање ризицима ланаца снабдевања.

Током истраживања ризика ланаца снабдевања на Факултету за логистику у Марибору (Словенија), идентификовани су неки од кључних аспеката. Основни аспект је недостатак инструмената који могу учинити управљање ризицима у организацији лакшим и ефикаснијим. Као исход, развијен је модел који садржи и описује ризике у организацији и њеном ланцу снабдевања. Модел је у сагласности са општим стандардима управљања ризиком и ризиком у ланцима снабдевања ISO 31000 и ISO 28000. Такође укључује новија открића из области управљања ризиком, посебно са гледишта сегментације јавности.

Модел описан у овом раду фокусира се на дефиницији ризика према различитости кључних димензија. На тај начин је управљање ризиком поједностављено и може се применити у сваком ланцу снабдевања у циљу оптимизације.

Засновано на овом моделу и приказаном практичном истраживању у стварним организацијама, развијен је каталог ризика, који је јавно доступан и доступан на интернету, према ризицима који су идентификовани до сада. Овај каталог се може користити као чек листа и полазна тачка у управљању ризицима ланаца снабдевања разних организација. Такође, на каталогу су ангажовани бројни експерти из ове области, како би се омогућио наставак његовог развоја и даљи раст.

Кључне речи: Ланци снабдевања, Управљање ризиком, Процена ризика, Каталог ризика, ISO 31000:2009, ISO 28000:2007

References

Alhawari, S., Karadsheh, L., Talet, A.N., & Mansour, E.(2012). Knowlebge Based Risk Management. International Journal of Information Management, 32(1): 50-65.

Creative Commons (2011). Attribution-NonCommercial- NoDerivs 3.0 Unported. U R L : http://creativecommons.org/licenses/by-nc-nd/3.0/ (accessed 15.10.2011)

Gaudenzi, B. & Borghesi, A. (2006). Managing risks in the supply chain using the AHP method. International Journal of Logistics Management, 17(1):114-136. Emerald Group Publishing Limited.

IEC (2009). IEC/ISO 31010:2009 – Risk management – Risk assessment techniques. Geneva, Switzerland: International Electrotechnical Commission.

ISACA (2007). Cobit 4.1. Rolling Meadows, IL, USA: International Systems audit and Control association.

ISO (2007). ISO 28000:2007 – Specifications for security management systems for the supply chain. Geneva, Switzerland: International Organization for Standardization.

ISO (2009). ISO 31000:2009 Risk management – Principles and guidelines. Geneva, Switzerland: International Organization for Standardization.

IT Governance Institute (2008). Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0. Rolling Meadows, IL, USA: IT Governance Institute.

Jereb, B. (2009). Segmenting risks in risk management. Logistics and sustainable transport, 1(4):11. Celje, Slovenia: European Association for Traffic, Transport and Business Logistics.

Jereb, B. (2010). Risk modelling in process management wit the use of public segmentation (in Slovene). Uporabna informatika, 18(2);90-100. Ljubljana, Slovenia: Slovensko društvo Informatika.

Khan, O. & Burnes, B. (2007). Risk and supply chain management: creating a research agenda. The International Journal of Logistics Management, 18(2): 197-216. Emerald Group Publishing Limited.

Katalog web address: http://labinf.fl.uni-mb.si/risk-catalog/.

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

Olsson, R. (2007). Insearch of opportunity management: is the risk management process enough? International Journal of Project Management, 25(8):745-752.

Oyatoye, E.O., & Fabson, T.V.O. (2011). A comparative study of simulation and time series model in quantifying bullwhip effect in supply chain. Serbian Journal of Managenent, 6(2): 145-154.

Steward, A. (2004). On risk: Perception and direction. Computers & Security, 23:362-370. Maryland Heights, MO, USA:Elsevier.