

RISK ASSESSMENT MODEL AND SUPPLY CHAIN RISK CATALOG

Dr. Borut Jereb

Tina Cvahte

Dr. Bojan Rosi

University of Maribor, Faculty of logistics

Mariborska 7, SI-3000 Celje, Slovenia

Phone number: +386 3 428 53 62, Phone number: +386 3 428 53 23

E – Mail: borut.jereb@fl.uni-mb.si ; tina.cvahte@fl.uni-mb.si ; bojan.rosi@fl.uni-mb.si

Abstract

By managing risk on the level of the supply chain we gain insight of all potential threats to all organizations involved in the chain as well as to the supply chain itself, especially to the logistics resources: flow of goods, services and information; logistics infrastructure and suprastructure; and people.

Supply chain risk management should represent a crucial activity in every organization. As there is currently no standard specifically aimed at holistic supply chain risk management, we propose the use of a combination of the ISO 31000 family, concerning risk management in general, and ISO 28000 family, concerning safety in supply chains. Both families of standards are described with propositions for effective use in supply chains.

Based on supply chain risk management research at Faculty of logistics we developed a model for the activity of risk assessment in the process of risk management in supply chains and organizations. Especially risk identification as a part of risk assessment can be considered the single most important activity in the risk management process, because a risk that is not identified cannot be managed. Our model is the base for the development of the Risk Catalog in Supply Chains, which is already in place and accessible online. Because of the open source philosophy applied to the Catalog, every interested individual can provide their input. We hope that over time with the help of the relevant "community" the Catalog becomes more complete.

With the Catalog we propose a solution for risk assessment in organizations. Some aspects of risk assessment can be generalized and are a part of our risk Catalog. Other, organization specific, aspects are described in this article and in the Catalog, but their use and consideration have to be based on a specific organization's context.

Keywords: supply chain, risk management, risk assessment, risk catalog

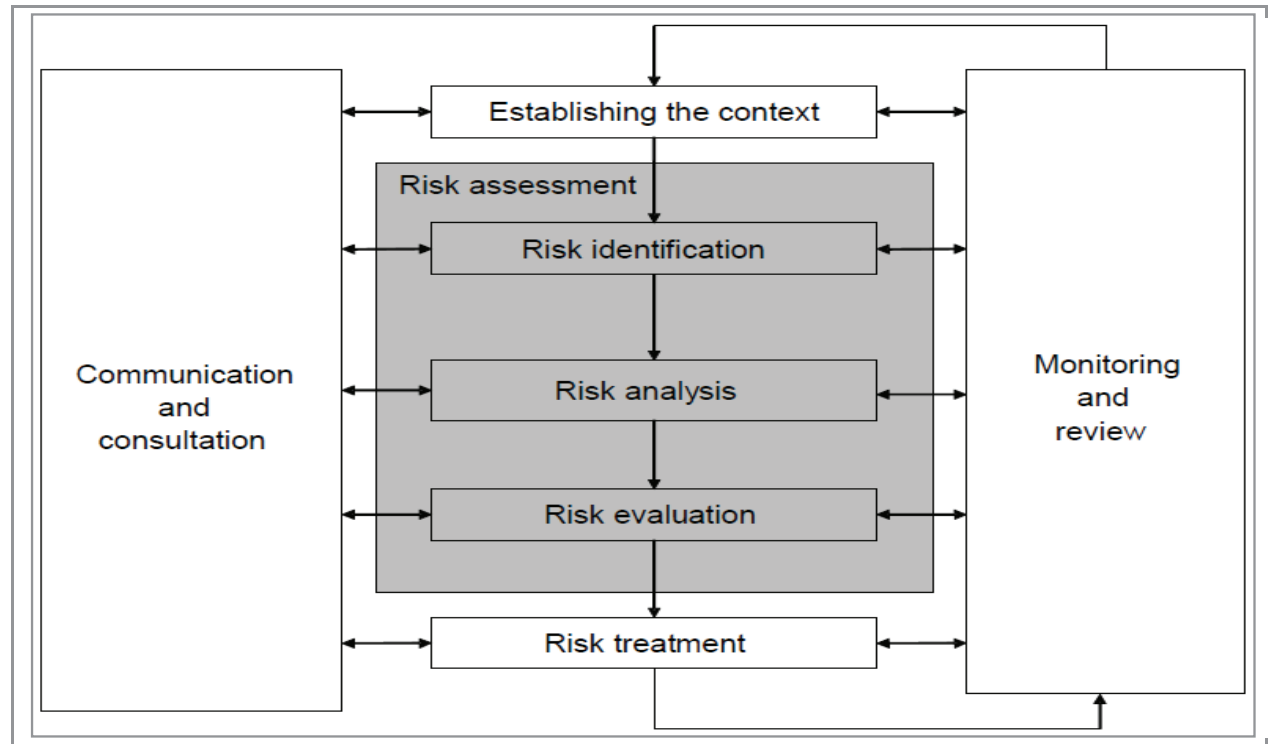
1. INTRODUCTION

Supply chain risks should be a main concern in today's operations in any company. Considering trends of globalization and global sourcing, no company today can operate in a completely secure environment without risk, deriving from supply chains. Therefore we can say that the process of risk management is crucial for continuous operations of companies in all fields of business.

Risk is a word we encounter on a daily basis; however a simple and clear definition of the word is hard to find, especially in the business sphere. A general definition seems to be the one also used in ISO 31000 (Risk management – Principles and guidelines): '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.

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. The basic risk management process, as is defined in ISO 31010, can be seen on Picture 1.

Picture 1. The risk management process as defined in ISO 31010



Source: ISO [International Organization for Standardization] (2009): *ISO 31000:2009 Risk management – Principles and guidelines*. International Organization for Standardization: Geneva, Switzerland, p. 14.

We believe that the process of risk assessment, especially risk identification, is 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 management are not later treated and therefore go unseen and unmanaged. Because of that, a model for efficient risk assessment in organizations was developed. This model was tested in real life, on an actual logistics company that focuses mainly on warehousing. The output we got from this test 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 company we have reason to believe that we are on the right path to achieving our goal, which is to develop a widely usable model for risk assessment. Moreover, our goal is to implement a web-based catalog of supply chain risks, which is to be published under an open source 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 management 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.

In our model, risk identification is based on three methods that are also proposed by ISO 31010 – free interviews, structured interviews and brainstorming. During sessions between trained external personnel and organization's employees risks are identified and then later put into the description model.

Since we believe that risk identification and analysis are the key activities in managing risks, we defined several dimensions by which each identified risk in a company or supply chain should be described. A thorough description gives us a base for informed decisions about further actions. We also have to be aware of the time and process component of this phase of risk management. As a risk is identified, we strive to define it by some basic dimensions of risk description, which are included in the risk catalog. Later in the process, during further risk identification, analysis and evaluation, several other dimensions should be implemented. These next stages of risk assessment are more complex and involve company specific relations between risks, specific consequences some risks can have and alike.

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 to a company or a supply chain can originate are defined. In the first step each identified risk is placed in these groups (extracted from ISO 28000):

- a) physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action;
- b) operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety;
- c) natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective;
- d) factors outside of the organization's control, such as failures in externally supplied equipment and services;
- e) stakeholder threats and risks such as failure to meet regulatory requirements or damage to reputation or brand;
- f) design and installation of security equipment including replacement, maintenance, etc.;
- g) information and data management and communications.;
- h) 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.

As we analyze risks we need to be aware that there are different sources of logistics operations in supply chains. In our model, we use a simplified view on logistics sources, which we developed specifically for the use in the risk catalog. We believe that the implementation of logistics is based on the following sources of logistics:

- the flow of goods or services,
- information,
- logistics infrastructure and suprastructure and
- people.

Any consequence of risk, occurring in a supply chain, can influence one or more of these sources. If we wish to effectively manage risks, we need to be aware of logistics sources 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 sources 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 source of logistics.

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 the third dimension of risk identification is exactly that – defining, which publics are affected by a certain risk.

A supply chain is a complex system of several organizations that work together in a specific environment. Based on the extent of risk consequences regarding the supply chain, we can define risks according to the fourth dimension in our model. A risk can occur in three different scopes:

- in a company that is included in the supply chain,
- in the whole supply chain,
- outside of the supply chain, in its environment.

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 the fifth 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 have to define their influence on the organization and the consequences of its occurrence. This represents a base for later defining risk impact and according to that deciding the needed measures for risk management.

When talking about publics that were defined during risk description we also have to look at the influence of risks on them.

The time component is not only important when looking at the processes of risk management, but also when looking at risks themselves. Some risks can change over time or their potential impact can change. 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.

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. 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. 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 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 risk manager 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'. 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'. 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, is 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.

The catalog is available online at <http://labinf.fl.uni-mb.si/risk-catalog/>. An extensive list of 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, the actual list of risks is given for easy access, as well as the categorization of these risks by the dimension we see as most important, which is grouping according to ISO 28000. Every categorization is performed with a code for the relevant category in ISO 28000, which is also a hyperlink leading to a subpage with the description of the category and a list of all risks that fall into that group. The picture below shows a part of the first page of the risk catalog.

Picture 2. First page of the online 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 additionally defined by several relevant categories.

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), the primary dimension by which we believe risks in a company should be categorized is grouping of risks according to ISO 28000. The list below shows risks, identified in the risk identification process in cooperating organizations, their description where needed, and their [grouping by ISO 28000](#). A more extensive list of definitions can be found in [Risk analysis](#).

Risk	Group according to ISO 28000	Secondary group according to ISO 28000	Description
Limited or no access to the key locker	a.PHY		
Fall of wall/ceiling	a.PHY		
Collapse of tent	a.PHY		
Planted bomb or explosive	a.PHY		
Damage to the forklift ramp	a.PHY		
Damage of cranes, lifts	a.PHY		
Collapse of the roof (snow...)	a.PHY		The collapse of a roof due to events that could not be influenced.
Destruction or reduction of value of goods	a.PHY		Destruction - the goods cannot serve its purpose anymore; Reduction of value - the goods cannot serve its intended purpose in the specified scope anymore (wet packaging, expired expiration date...) .
Destruction of equipment	a.PHY		Damage or an unforeseen breakdown of such scope, that the equipment is temporarily or permanently unfit for use.
Employees are not acquainted with measures in case of work accidents	b.OPT		
Work accidents involving employees	b.OPT		Accidents while executing operations - including physical damage to employees, goods or equipment.
Long revolution of storage goods	b.OPT		Stocks are increasing, the average time of storage is longer than usual.
Ad-Hoc investments	b.OPT		Unexpected investments that are required to maintain the scope of operations as before in an organization.

Source: Authors .

At the bottom of the start page, 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. The bottom section of the page is shown below.

Picture 3. Creative commons license and contact information

License

This website and its contents are published under the Creative Commons License: "Attribution-NonCommercial-NoDerivs (version 2.5 and higher)". You can find the license online at this address: <http://www.creativecommons.org>, or in person at the Institute for intellectual property:


Inštitut za intelektualno lastnino
 Streliška 1
 SI - 1000 Ljubljana

Propositions for changes and additions to the Risk Catalog

When sending propositions for changing or adding to the Risk Catalog I FULLY AGREE WITH THE STATEMENT BELOW:

If the Editor board of the Risk Catalog accepts my contribution and publishes them in the Catalog, I waive all material authoring rights, that are derived from my authoring, and I agree with the publishing of my name among the authors of the Risk Catalog.

You can send your contribution to SC.RiskCatalog@gmail.com.



Source: Authors.

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, click on 'Risk assessment'. You are transferred to another subpage, where 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. The picture below shows a part of this page.

Picture 4. Risk assessment page



Source: Authors.

When you click on a certain dimension of definitions, for example 'List of affected logistics sources', a supage 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. An example is shown in the picture below.

Picture 5. Subpage for List of affected logistics sources

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

[Risk Catalog](#) [Risk assessment](#) [Contact](#)

List of affected logistics sources

As we identify risks we need to be aware that there are four main sources of logistics operations in supply chains: the flow of goods or services, information, logistics infrastructure and suprastructure and people. Any risk, occurring in a supply chain, can have an effect only on one or more of these sources. If we wish to effectively manage risks, we need to be aware of logistics sources that a specific risk possibly affects. That is why this dimension of defining risk in our model is to ascertain which sources of logistics can be affected by an identified risk. You can find the description of a certain code and all connected risks if you click on a code.

Code	Description
FLW	Flow of goods or services
INT	Information
ISL	Logistics infrastructure and suprastructure
PPL	People
ALS	All logistics sources

Source: Authors.

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. Below, you can see the current Risk identification page of our catalog.

Picture 6. Risk identification page

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

[Risk catalog](#) [Risk assessment](#) [Contact](#)

Risk identification

The first step in risk management 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.

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 risk manager 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'. 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 can not 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 table below defines these risk parameters. 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 phase of risk assessment according to ISO 31000 is risk analysis, which is based on outputs of risk identification. Our catalog includes extensive general definitions of risks also, which you can find in [Risk analysis](#).

Risk	Group according to ISO 28000	Secondary group according to ISO 28000	Source of risk	Area of impact	Risk cause	Potential consequences
Limited or no access to the key locker	a.PHY					
Fall of wall/ceiling	a.PHY					
Collapse of tent	a.PHY					
Planted bomb or explosive	a.PHY					
Damage to the forklift ramp	a.PHY					
Damage of cranes, lifts	a.PHY					
Collapse of the roof (snow...)	a.PHY					
Destruction or reduction of value of goods	a.PHY					
Destruction of equipment	a.PHY					
Employees are not acquainted with measures in case of work accidents	b.OPT					
Work accidents involving employees	b.OPT					
Long revolution of storage goods	b.OPT					
Ad-Hoc investments	b.OPT					
Loss or theft of keys	b.OPT					
Theft of goods	b.OPT					
Theft of computer components	b.OPT	a.IDC				
Theft of forklifts	b.OPT					
Technical malfunctions of security systems	b.OPT					

Source: Authors.

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 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 subpage with the description of the category and a list of all risks that fall into that category of a certain dimension.

Picture 7. Risk analysis page

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 be treated, and on the most appropriate risk treatment strategies and 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 definition dimensions are included. Additional dimensions by which we 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 source of logistics	Secondary source of logistics	Primary public	Secondary public	Scope of risk	Description by processes	Description
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 collapse of a roof due to events that could not be influenced.
Destruction or reduction of value of goods	a.PHY		ISL		MNG	CCU	COM	UNR	Destruction - the goods cannot serve its purpose anymore; Reduction of value - the goods cannot serve its intended purpose in the specified scope anymore (wet packaging, expired expiration date...).
Destruction of equipment	a.PHY		ISL		EMP		COM	TCH	Damage or an unforeseen breakdown of such scope, that the equipment is temporarily or permanently unfit for use.
Employees are not acquainted with measures in case of work accidents	b.OPT		PPL		OPE		COM	CMM	
Work accidents involving employees	b.OPT		PPL		OPE		COM	UNR	Accidents while executing operations - including physical damage to employees, goods or equipment.
Long revolution of storage goods	b.OPT		FLW		MNG	CCU	COM	CMM	Stocks are increasing, the average time of storage is longer than usual.
Ad-Hoc investments	b.OPT		ISL		MNG	FIS	ANY	CMM	Unexpected investments that are required to maintain the scope of operations as before in an organization.
Loss or theft of keys	b.OPT		ISL		OPE		ANY	TCH	
Theft of goods	b.OPT		FLW		MNG		ANY	UNR	Three levels of theft - occasional minor thefts (food, beverages...), minor thefts, organized thefts.

Source: Authors.

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. An example for 'b.OPT' is shown below.

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.

Picture 8. Subpage for a single category - b.OPT

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

[Risk catalog](#) [Risk assessment](#) [List of groups by ISO 28000](#) [Contact](#)

Group by ISO 28000 - 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.

All risks in this category

Risk	Group	Secondary Group	Primary source of logistics	Secondary source of logistics	Primary public	Secondary public	Scope of risk	Description by processes	Description
Employees are not acquainted with measures in case of work accidents	b.OPT		PPL		OPE		COM	CMM	
Work accidents involving employees	b.OPT		PPL		OPE		COM	UNR	Accidents while executing operations - including physical damage to employees, goods or equipment.
Long revolution of storage goods	b.OPT		FLW		MNG	CCU	COM	CMM	Stocks are increasing, the average time of storage is longer than usual.
Ad-Hoc investments	b.OPT		ISL		MNG	FIS	ANY	CMM	Unexpected investments that are required to maintain the scope of operations as before in an organization.
Loss or theft of keys	b.OPT		ISL		OPE		ANY	TCH	
Theft of goods	b.OPT		FLW		MNG		ANY	UNR	Three levels of theft - occasional minor thefts (food, beverages...), minor thefts, organized thefts.
Theft of computer components	b.OPT	g.IDC	INT	FLW	ITP	ALL	ANY	UNR	
Theft of forklifts	b.OPT		ISL	FLW	OPE		ANY	UNR	
Interrupted supply of goods to customers	b.OPT		FLW		CCU		COM	CMM	Delivery of goods to customers was not complete - documentation issues, commissioning, incomplete shipments...
Loading ramps not operating	b.OPT		ISL	FLW	OPE		COM	TCH	
Scanners not operating	b.OPT		PPL	FLW	OPE		COM	TCH	
Workforce not effectively burdened	b.OPT		PPL		OPE		COM	CMM	Reduced productivity of workforce due to ineffective task distribution.
Negative personnel changes	b.OPT		PPL		ALL		COM	CMM	
Noncompatibility of customers or suppliers with ISO 9001 standard, business usances etc.	b.OPT		FLW		MNG		SCR	CMM	
Task not completed	b.OPT		FLW	FLW	ALL	CCU	COM	UNR	Work tasks are not completed fully or in the specified time frame.
Nonoptimal limitations of transport	b.OPT		ISL	FLW	DRV		ANY	UNR	Requests for less than optimal transport organizing - longer routes, vehicles with greater capacity than needed, time limitations...
Norms are not correctly formed	b.OPT		PPL	FLW	OPE		COM	CMM	

Source: Authors.

From any page in the risk catalog you can return to the first page by clicking the link at the top of the page. Depending on where in the catalog you are, links are also given to return to the 'Model of risk identification' page and the descriptive page for the dimension of risk definition you are currently browsing through. The top navigation menu also includes a hyperlink that allows you to send an email to the editorial board of the catalog. An example of the top navigation menu, when you are browsing through the subpage for 'INT' (in the 'Definition of affected logistics sources' dimension), is shown below.

Picture 9. Top navigation menu

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

[Risk catalog](#) [Risk assessment](#) [List of affected logistics sources](#) [Contact](#)

Affected logistics source - INT

Source: Authors.

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.

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.

REFERENCES

- Creative Commons (2011): *Attribution- NonCommercial- NoDerivs 3.0 Unported*. URL: <http://creativecommons.org/licenses/by-nc-nd/3.0/> (accessed 01.08.2011).
- IEC (2009): *IEC/ISO 31010:2009 – Risk management – Risk assessment techniques*. International Electrotechnical Commission: Geneva, Switzerland.
- ISO (2007): *ISO 28000:2007 – Specifications for security management systems for the supply chain*. International Organization for Standardization: Geneva, Switzerland.
- ISO (2009): *ISO 31000:2009 Risk management – Principles and guidelines*. International Organization for Standardization: Geneva, Switzerland.