Jereb, Borut; Ivanuša, Teodora; Rosi, Bojan

Article

Systemic Thinking and Requisite Holism in Mastering Logistics Risks: the Model for Identifying Risks in Organisations and Supply Chain

Amfiteatru Economic Journal

Provided in Cooperation with:
The Bucharest University of Economic Studies

Suggested Citation: Jereb, Borut; Ivanuša, Teodora; Rosi, Bojan (2013) : Systemic Thinking and Requisite Holism in Mastering Logistics Risks: the Model for Identifying Risks in Organisations and Supply Chain, Amfiteatru Economic Journal, ISSN 2247-9104, The Bucharest University of Economic Studies, Bucharest, Vol. 15, Iss. 33, pp. 56-73

This Version is available at:
https://hdl.handle.net/10419/168776

SYSTEMIC THINKING AND REQUISITE HOLISM IN MASTERING LOGISTICS RISKS: THE MODEL FOR IDENTIFYING RISKS IN ORGANISATIONS AND SUPPLY CHAIN

Borut Jereb[1*], Teodora Ivanuša[2] and Bojan Rosi[3]
[1) 3)] *University of Maribor, Faculty of Logistics, Slovenia*
[2)] *University of Maribor, Faculty of Criminal Justice and Security, Slovenia*

Abstract
Risks in logistic processes represent one of the major issues in supply chain management nowadays. Every organization strives for success, and uninterrupted operations are the key factors in achieving this goal, which cannot be achieved without efficient risk management. In the scope of supply chain risk research, we identified some key issues in the field, the major issue being the lack of standardization and models, which can make risk management in an organization easier and more efficient. Consequently, we developed a model, which captures and identifies risks in an organization and its supply chain. It is in accordance with the general risk management standard – ISO 31000, and incorporates some relevant recent findings from general and supply chain risk management, especially from the viewpoint of public segmentation. This experimental catalogue (which is also published online) can serve as a checklist and a starting point of supply chain risk management in organizations. Its main idea is cooperation between experts from the area in order to compile an ever-growing list of possible risks and to provide an insight in the model and its value in practice, for which reason input and opinions of anyone who uses our model are greatly appreciated and included in the catalogue.

Keywords: Supply Chain, Risk Management, Systemic Thinking, Risk Catalogue, Requisite Holism

JEL Classification: D81

Introduction

Nowadays no company can operate in a completely secure environment without risk, deriving from supply chains, and particularly considering trends of globalization and global sourcing. Supply chain risks have become the major concern of today's logistics and other business processes in any company. As ISO/PAS 28002 states the survivability of

[*] Corresponding author, **Borut Jereb** - borut.jereb@fl.uni-mb.si

organizations within a supply chain mostly depends on the resilience of their suppliers and customers. Incorporating resilience (and improving the resilience of an organization within the supply chain) must be focused 1) within the organization and 2) externally on its suppliers and customers (ISO, 2011). Therefore, we can say that the process of risk management is crucial for uninterrupted operations of companies in all fields of business. Risks are perhaps 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.

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 in 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 form 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? Whom are risks acceptable for and not? 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.

A general definition seems to be the one also used in ISO 31000:2009 (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, p.V) 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 creating the risk model based on ISO 31000 and on the proposal of segmenting the risks into any given number of dimensions.

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, and the systemic thinking. Systemic thinking is the key to solve most of the organizational-related problems and it can be used in any field of science. Its main goal is to achieve holism in a particular (dialectical) system. It can be explained with a figure (Figure 1) (Mulej, et al., 2000):

Systemic thinking is a way of thinking that
• Considers and places particular emphasis of attention to the **interdependence(s)**.
• It is integrative thinking, which forms bridges between specialists.

• Neither challenges nor nullifies the importance of specialization, but it complements it by cooperation between specialists that would lead to synergies.
• Do not conceal the real complexity or complications, so that **over-simplification** would **not** lead to the oversights and therefore, to complicated consequences.

Figure no. 1: Systemic Thinking - short definition

Source: Mulej, et al., 2000

The Mulej's (Mulej, 2000) Dialectical System Theory (DST) has been applied as a general methodology in this particular research. Such approach is rather new in building an experimental model and risk catalogue, but, doubtlessly, provides the Systemic Thinking and Requisite Holism, regarding the outcomes of the presented research. According to published international literature in this particular research area, we didn't detect a similar projects or researches, which can be combined with the presented one.

The basic risk management process, as is defined in ISO 31010:2009, can be seen below (Figure 2).

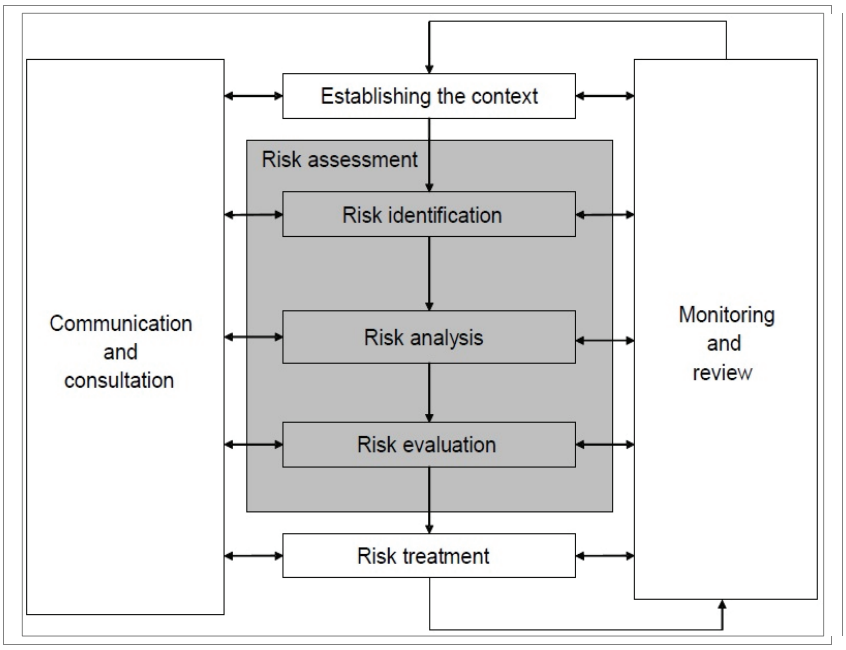


Figure no. 2: The risk management process as defined in ISO 31010

Source: ISO, 2009

The processes included in the risk assessment, especially the risk identification and analysis, are most crucial in the whole risk management process. We have to be aware that risks, which are not identified and defined in the first stages of the risk assessment, are not treated later 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; the pilot testing was done in an actual logistics company that focuses mainly on warehousing. The output we got from this preliminary test and subsequent testing is a catalogue of identified

risks, in which 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 every reason to believe that we are proceeding the right way to achieve our goal, which is to develop a widely usable risk assessment model. Moreover, our goal is to create a web-based catalogue of supply chain risks, which is to be published under the Creative Common License, allowing everyone to use it as a reference and to propose changes and additions to it.

It is also crucial to point out that our model is in accordance with ISO 28000 (Specifications for security management systems for the supply chain). This standard is used for providing systems for supply chain's security management in organizations. The main idea behind the use of this standard is that "a formal approach to security management can contribute directly to the business capability and credibility of the organization". (ISO, 2007, p.vi) In order to efficiently use both this standard and ISO 31000, their relationship has to be clarified. ISO 31000 is a general standard for risk management, and ISO 28000 is a supply chain specific standard. Where ISO 31000 focuses on risks from all organization's activities, ISO 28000 takes risk management as a part of security management in organizations. It describes security management as "systematic and coordinated activities and practices through which an organization optimally manages its risks and the associated potential threats and impacts therefrom". (ISO, 2007, p.1)

The use of standards depends of many different factors, which can be independent or mutually dependent or interdependent. To successfully deal with all of them, we should use the systemic thinking to achieve the holism. Holism is defined in this way (Figure 3):

Holism covers
(1) The Whole (Systemic)
(2) Parts (Systematic)
(3) Relations (Correlation, Dialectics, Interdependence) and
(4) Realism (Closeness to reality, Materialism) as a **system (i.e. interlacement)**, i.e. everything simultaneously and interlaced, interdependently and with interaction.

Figure no. 3: Definition of Holism after the Dialectical systems theory

Source: Mulej, et al., 2000

Holism applies markedly also to the supply chains and logistics: one-sided creation and applicatio of insights and measures cannot be useful, at least not in the longer term. It causes oversights and uncontrolled consequences (Mulej, et al., 2000; 2008; Ivanuša, Mulej, Pečan, Tičar and Podbregar 2009).

1. The risk assessment model

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 many potential risks as possible in order 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. At sessions with

representatives of organizations where risk assessment takes place under supervision of experts, trained in using our developed model, risks are identified by these external personnel and organization's employees and later put into the description model as is defined further in this paper.

Since we believe that risk identification and analysis are the key activities in managing risks, we have defined several dimensions according to which each identified risk in a company or supply chain should be described. Once a risk is identified, we describe it with some basic dimensions of the risk description, which are included in the risk catalogue. Later in the process, during further risk identification and analysis, several other dimensions have to be considered. These further stages of risk assessment are more complex and involve company specific relations between risks, specific consequences some risks can have and the like, and as such are not part of the general risk catalogue which is available online.

2. Risk segmentation according to ISO 28000:2007

This model and the catalogue that derives from it are structured, thus complementing an international standard on security in supply chains, ISO 28000. In this standard, several fields from which risks to a company or a supply chain can originate are defined. In the first step, each identified risk is classified in these groups (ISO, 2007):

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

The description of a risk based on the group from ISO 28000 is also the first dimension of the risk definition in the risk catalogue. Since some risks are more complex than others are, some cannot be defined simply by one group; therefore, some risks also have a secondary group placement.

By categorizing risk in this way, we achieve a means of looking at categories of risks instead of each individual risk separately. We can assess which areas of risk are most important for our organization or a supply chain, and plan for mitigating these groups of

risks. We can assess which risks are under our influence or under the influence of our partners, and which no one can influence, and prepare accordingly.

3. Risk segmentation according to the affected logistics resources

As we analyse risks we need to be aware that there are different resources of logistics operations in supply chains. Based on our research of different definitions of logistics and consultations with a logistics expert, we defined four primary logistics resources, without which logistics processes cannot take place. This definition has so far been exclusively used in our model in order to easily define categories of risk influences. We believe that the implementation of logistics is based on the following logistics resources:

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

By grouping risks this way, and at the same time defining which logistics resources are most important for continuous operations, we gain insight into priorities of risk management in organizations and supply chains.

4. 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 behaviour 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. A study, published by Pelău and

Bena (2010), proved and showed exactly these differences in perceptions of same risks by different individuals or groups of individuals on the case of risks in e-commerce. 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. Each person shapes one's own perceptions of reality based on received information, their perception and interpretation. In addition to individual level of perception, it is yet necessary to take into account the organizational or group level, since modern man does not function in an enclosed environment, but mostly in the context of small groups, organizations, as a member of a community and citizen, and in international relations, etc. The latter with their stable organizational processes in a sense also affect the user's ordinarily perception. Generally looking, each individual is constantly in a state or in a certain gap between his own perception and the reality of the threat. The larger this gap, the more time we need for decision-making and thus for the beginning of a successful problem resolution. Time, which is our permanent enemy and ally, is working relentlessly and is running in its completely independent rhythm and also causes a difference between our perception and reality of the threat (Podbregar and Ivanuša, 2011).

Individuals in company or supply chain, when searching and detecting risks, should be interdependent. As individuals - due to immense amounts of mankind expertise and knowledge – we just are necessarily narrowly specialized to some fragment of expertise, knowledge and reality, therefore indispensible to others and in need of others, thus interdependent (Mulej, et al., 2000; 2008; Ivanuša, et al., 2009). Since reality is complex and the humanity as whole knows a lot about it, individuals we necessarily specialize and inevitably simplify. The question is how much. The answer of great scientist Albert Einstein is said to be as follow: "Everything should be made as simple as possible, but not simpler."

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

- Uncertainty, which should be divided into:
- Objective uncertainty and
- Subjective uncertainty;
- Exposure.

5. Uncertainty

Uncertainty is a condition when one does not know whether a proposal 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. It is utterly clear that it is impossible to cover all possible uncertainties raised by the individual. Therefore: what should our steps to reduce the gap between perception and reality be? Based on past experience each person searches answers within himself first, after that one searches for answers in the environment that has the ability for the individual to communicate with it different dimensions and hence very different quantitative and qualitative data and information. The more questions and answers, of course, that we obtain based of the presented questions and answers and based on repeated or new questions, as the process must be ceaseless, the greater the likelihood that actions, reactions and solutions

will be properly measured out, as the perception will be increasingly more identical to reality. Each individual must find for himself the best, the most rational way out of uncertainty.

While the objective uncertainty includes logic, probability and statistical methods, on the other hand quantifying probability is hardly helpful considering the 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.

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 proposal is true or false.

6. Exposure

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 non-definability, 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.

7. Segments of the public in risk management

By defining risks and their influences, we can take a different approach to the subject from that described in most literature of today. 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 public, 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 public 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, p.8) Also, the standard defines the importance of communication and consultation with stakeholders, which our model achieves by segmenting them into public. 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, p.15)

Attention should also be paid to the social responsibility, since stakeholders represent an important part of risk management and organization's policy "identification of and engagement with stakeholders are fundamental to social responsibility. An organization should determine who has an interest in its decisions and activities, so that it can understand its impacts and how to address them. Although stakeholders can help an organization identify the relevance of particular matters to its decisions and activities, stakeholders do not replace broader society in determining norms and expectations of behaviour. A matter may be relevant to the social responsibility of an organization even if not specifically identified by the stakeholders it consults". (ISO, 2010, p.7)

8. Risk segmentation according to the origin 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, p.V) 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:

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

Every company is dependent on multiple third parties. As a part of a supply chain, a company is usually tightly connected to parties in the supply chain, more than to 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). The same author also recognized that dependency is a crucial dimension of risk that is often not considered as part of the 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.

To avoid the risks that derive from dependencies, the company should change the view on its relations with other people, involved in a supply chain – not as dependencies but as interdependencies. It is necessary to understand that all involved parties should cooperate with each other in both ways to avoid risks: to accept knowledge, resources, transport or power (or other) and to give it. As individuals who do not cooperate with each other, of course, we cannot be sufficiently holistic, therefore we need to take the fact that we are interdependent, although we are trying to be legally independent.

As we already stated, knowing where risks come from can help us make plans for their mitigation and management. By defining their origin as we do in our model we determine which risk groups we can manage and which our supply chain partners can manage or with which we need to cooperate in risk management. With risks that derive from the environment and generally from outside of the supply chain, special attention has to be paid to all measures of mitigation in case of their occurrence, since the organizations in the supply chain have no possible influence on whether these risks are realized or not.

9. Risk segmentation according to levels of logistics planning

In every organization, different levels of planning and control are established. These levels represent the importance of decisions of a certain level and also the time span in which they are relevant. The same can be said for risks in an organization – they appear at different levels of significance and impact, and can correlate to the levels of logistics planning.

According to Rushton, Croucher and Baker, the general levels of logistics planning in organizations are strategic, tactical and operational. The strategic level includes medium to long-term decisions, overall structural decisions, corporate financial plans and policies, trade-offs between company functions and with other organizations and alike. The tactical level includes short-term to medium-term decisions, such as subsystem decisions, annual budgets and alike, providing a base for operational plans. The operational level includes day-to-day decision making, where operations are controlled against standards and rules (Rushton, Croucher and Baker, 2010).

In some business fields, especially in those dealing with project management, the levels of planning are differently defined, but some general guidelines regarding the timeline of decision making, especially, and the scope of their influence correlate to the levels of logistics planning as defined by Rushton et al. In project management, the highest level of planning and decision making is portfolio management, followed by the programme management and project management at the lowest level (Robertson, 2012). In this article and in our model in general, the levels that we use are those of logistics planning, but we would like to point out, that project management levels can also be applied.

Risks in supply chains can be segmented into correlative levels of strategic, tactical and operational risks. This idea is new to the field of supply chain risk management. Strategic risks are at the highest level of significance and influence strategic logistics planning. Tactical risks influence tactical planning and operational risks influence day-to-day plans and operations. It is important to raise awareness of the interrelations of these risks at various levels – for example, a risk at the tactical level can influence other decisions and risks at all three levels.

Figure below (Figure 4) graphically presents the number and complexity of risks that occur in supply chains.

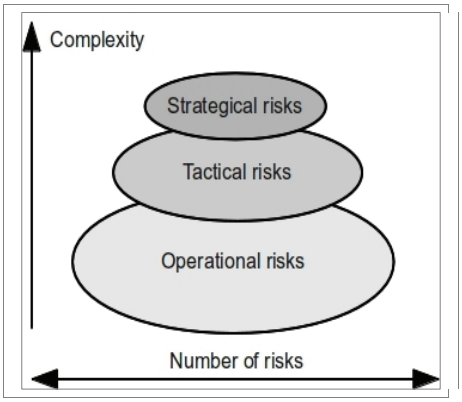


Figure no. 4: Number and complexity of supply chain risks by levels of planning and decision making

As with decisions, risks at the strategic level are more complex and fewer in number. Because of their complexity they have the potential for greater impacts on the organization and the supply chain as a whole, and they can influence a larger scope of consequentially occurring risks at all three levels. Tactical risks are generally larger in number and less complex than strategic risks, but they also have a potential impact on risks and decisions at all three levels. Operational risks are the largest group by quantity, which correlates to the number of decisions during planning and decision making in logistics. These risks occur on a daily basis from the operations in an organization and are generally less complex, but they still have the potential to impact risks and decisions at the tactical and even strategic level. It is important to point out that there is a subjective element involved in placing specific risks into certain levels, as each individual can have their own view of the complexity of a risk. The real complexity (at all levels) should not be concealed, so that over-simplification would not lead to the oversight and therefore, to complicated consequences (Mulej, et al., 2000). We can expect that these general boundaries between levels will become clearer with more input from the professional community.

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

10. Further definitions during risk assessment

As stated earlier, in the process of risk identification, analysis and evaluation in a specific organization, we should consider additional dimensions of risk definitions in order to completely understand risks, their connections and impact. All of these can be seen as complementary to one another and to the previously mentioned dimensions of definitions, and represent a unique way of managing risks in supply chains.

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. This is important that we retain the competitive advantage in our field of business by ensuring the maximum quality and continuity for our business partners.

In order to evaluate risks we also have to define their impact (or influence) on 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 public, we can gain a better insight into the consequences of a risk. This is not the same as only defining which public is affected, moreover, it is an expansion of that previous dimension, as possible effects of the risk are analyzed in more detail.

In many real situations, some or all the 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 have a minor and in some a major impact on the organization. These time frames, if present, have to be defined in the process of risk assessment to gain a perspective over changes in time. Thus we ensure, that each risk is managed when needed and that we are constantly aware of their changing nature.

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 every level of potential impact and to correctly define the acceptability level. By defining these levels we can later decide how and if we will manage certain risks, and also prioritize them according to their defined levels of acceptability.

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 that goes also for the risks in a company or in the supply chain as a whole. Because of that, we need to define connections between all the identified risks, and that is the next dimension in our model. By doing this we gain a better insight into the impacts of a certain risk across the whole range of possible risks. It will be necessary to use the systemic thinking, which will embrace all the components of a particular system (network of employees or stakeholders, connected risks) and determine the relations between them, level of interdependence and show the possible solutions to solve the problem.

A general idea of risk management is that every risk should have a person or group, designated for its management, usually named a 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 the risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls". (ISO, 2009, p.11) By defining a specific person for every risk we achieve a higher level of awareness with those who need to partake in risk management and contribute to the effective risk management. Accountability is one of the principles of the social responsibility. This is an important aspect of risk management, "because social responsibility concerns the potential and actual impacts of an organization's decisions and activities, the ongoing, regular daily activities of the organization constitute the most important behaviour to be addressed. Social responsibility should be an integral part of core organizational strategy, with assigned responsibilities and accountability at all appropriate levels of the organization. It should be reflected in decision making and considered in implementing activities" (ISO, 2010, p.7) as well as in risk management.

11. Risk catalogue

The final product of the conventional risk identification and risk analysis is a risk catalogue, which contains all the identified and defined risks in a single organization. We have collected these results in a risk catalogue, extending it with the whole range of the supply chain risks and making it 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 available catalogue provides organizations with the option to use previously gained knowledge of the risk management process. This risk catalogue contains supply chain risks as defined in different companies from different branches of operations, which can therefore be an excellent resource for any manager dealing with risks to use as a guideline and a check list. The use of a check list 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

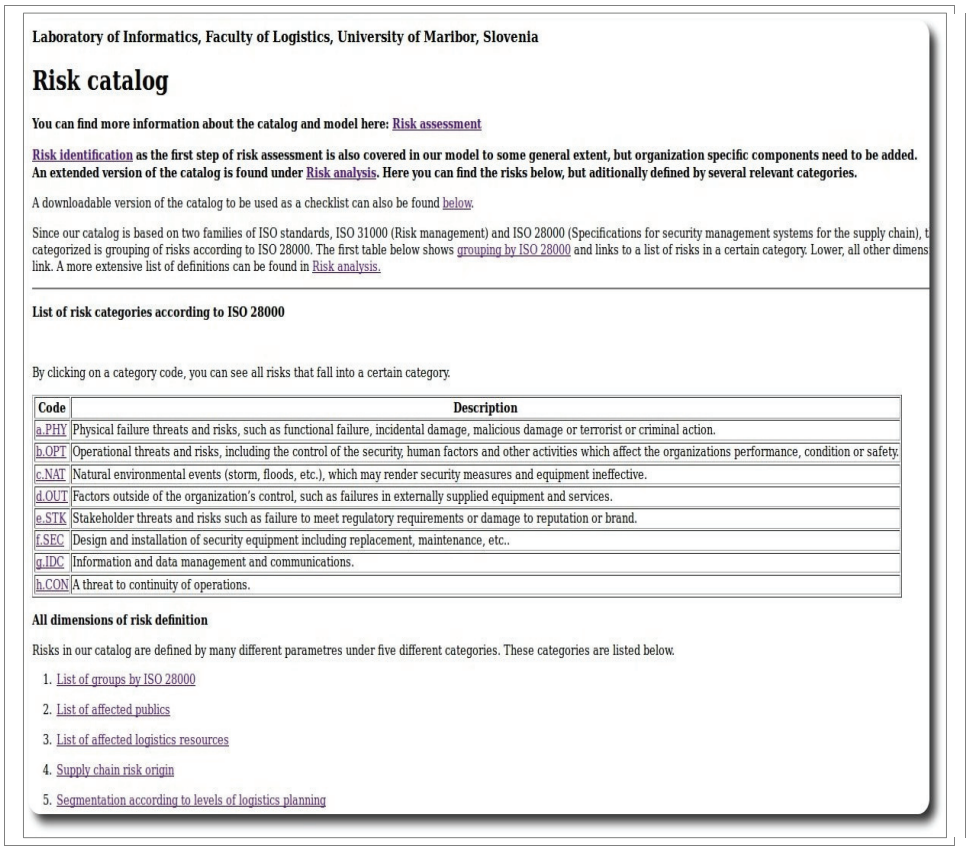
risk assessment or as a result of the past failures". (IEC, 2009, p.30) Based on that we believe our risk catalogue is in accordance with the ISO risk management set of standards, which also takes the frameworks proposed in the standards to a higher level with the inclusion of more supply chain risk management experts and through disseminating the knowledge throughout the community.

The need for a risk catalogue can be recognized from many perspectives. Even ISO 31000 (2009, p.17) 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 catalogue as a resource and a check list, the major step of risk management has already been undertaken, allowing the organization to approach risk management more prepared and with fewer complications. We can see that a risk catalogue of this scope, which to this day has not yet existed as a publicly accessible source of information, is much needed in today's business environment. Even if the catalogue is 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 catalogue 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 catalogue is an ever growing publication, we believe that all users should be able to contribute, comment or add to the catalogue. This is to be done by submissions of ideas to the editorial board, which shall assess the contributions and include them in the catalogue 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 catalogue 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 across supply chains all over the world and establish a community with a common goal – to provide an insight into risk assessment and the risk catalogue.

The catalogue is available online at http://labinf.fl.uni-mb.si/risk-catalog/. An extensive list of supply chain risks is provided, and the risks are described by the categories listed above. Additionally, and explanation of the dimensions is provided, accompanied with the list of catalogue codes. For every dimension code, a list of risks under that code is also given.

On the first page of the catalogue website there is a short description of the model and the catalogue, followed by the most important dimension of the risk definition, grouped by ISO 28000 categories of risks. Additionally, all dimensions of the risk definition are listed. At the bottom of this page you can also find a downloadable version of the catalogue. Below a part of the first page of the risk catalogue is shown (Figure 5).



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 no. 5: First page of the online Risk catalogue

An explanation of the 'Creative Commons' license, under which the risk catalogue is published, is produced, as well as the contact e-mail address you can use if you wish to comment the catalogue or make a contribution.

When you wish to find out more about the catalogue itself and also about the risk assessment process, we recommend that you should visit the sub-page named 'Risk assessment'. There you can find a short description of the risk assessment process and our proposals for it. Most importantly, here you can find links to the descriptions of different dimensions by which risks are defined in the risk catalogue. Below a part of this page is shown (Figure 6).

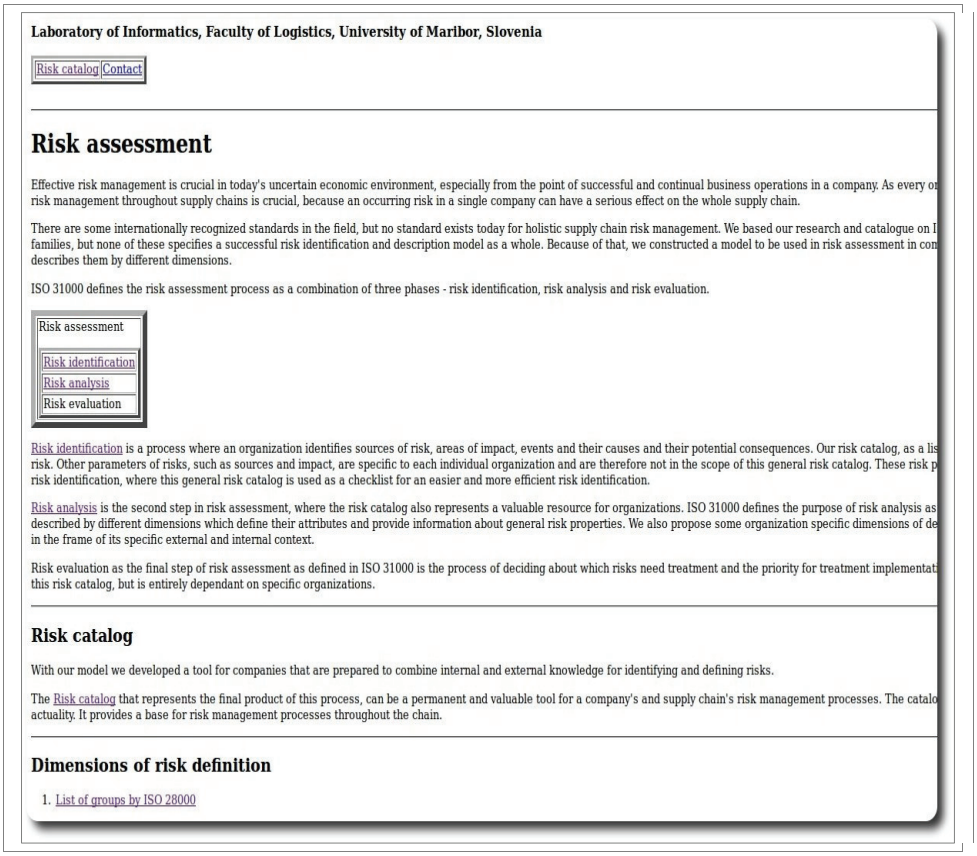


Figure no. 6: Risk assessment page

A certain dimension of definitions, for example 'List of affected logistics resources', can be accessed easily by clicking on the title, then a sub-page would open with a short description of the dimension and with all the 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 have made use of the same principle in our risk catalogue and divided our processes into these three categories. Risk identification is the first process of the risk assessment. The risk catalogue 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 catalogue. 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 be more complete.

The next stage is the risk analysis, which provides an input to the 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 catalogue 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 in this article in the chapter 'Further definitions during risk assessment'. In the 'Risk analysis' sub-page, a list of all risks is provided, 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 hyper-link, leading to a sub-page with the description of the category and a list of all risks that fall into that category of a certain dimension.

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 sub-page will open with its description and a list of relevant risks.

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

Conclusions

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. This point is in more detail described by Swoboda, Pop and Dabija (2010) who specifically outline the benefits of cooperation and the formation of alliances between participants in a supply chain. Risk management should be a primary concern of every organization and should be included in every aspect of an organization's operations in order to ensure its efficiency and thoroughness. Managers should be aware of the threats to their organization and of tools to manage them.

Our risk assessment model 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 catalogue, which is freely accessible online, provides a simple check list 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 catalogue, especially with its focus on people and public, presents an excellent risk management resource in all supply chains. As stated before, we didn’t detect similar projects or researches in published international literature in this particular research area, therefore our research (so far) represents a unique model, making step forward to easier, faster and systematically identifying risks in supply chain’s management.

The originality of the suggested experimental model and risk catalogue lies in the possibility of initiation of ISO 26000 into supply chain risk management; which is the next dimension of a model, which should include elements of social responsibility from the mentioned standard. The ISO 26000 suggests the organizations to “take into consideration

societal, environmental, legal, cultural, political and organizational diversity, as well as differences in economic conditions, while being consistent with international norms of behaviour". (ISO, 2010, p.10) These factors should be considered if we want to detect and understand different risks in a supply chain. But why? One of the main reasons is that "the expectations of society regarding the performance of organizations continue to grow" (ISO, 2010, p.6), which is, at the same time, forcing organizations to ensure the safety and operability of supply chain. To ensure the safety and operability, the interdependence between organizations, individuals and stakeholders should be established. Some organizations have already established the interdependence and "are communicating with their stakeholders, including by producing social responsibility reports, to meet their needs for information about the organization's performance". (ISO, 2010, p.6) We must not forget about the needed knowledge (specialization), cooperation between specialists and simplification, which are also the essence of systemic thinking. It is therefore important for the next dimension of the model to include social responsibility factors as it not only leads to holism, it also facilitates the systemic thinking and making it easier to use it in practice, while considering the societal, environmental, legal, cultural, political and organizational diversity.

As we believe that only a group of experts can provide the needed knowledge to perfect the model, compile a list of risks, and make it as extensive as possible, our experimental model and catalogue are freely accessible. Perfection of the model is easier to attain with creative inter-expert cooperation than without it. It is therefore, essential to move from one-expert to inter-expert creative cooperation whenever it appears that an individual profession probably does not provide necessary and sufficient holism and a broader definition of holism is needed. 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 catalogue. The authors will carefully follow the possible transformation of suggested model and catalogue in to the daily management and decision-making.

References

Creative Commons, 2011. *Attribution- NonCommercial- NoDerivs 3.0 Unported*. [online] Available at: <http://creativecommons.org/licenses/by-nc-nd/3.0/> [Accessed 1 September 2011]

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

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

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

ISO, 2010. *ISO/FDIS 26000:2010 – Guidance on social responsibility*. Geneva: International Organization for Standardization.

ISO, 2011. *ISO/PAS 28002 Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use.* Geneva: International Organization for Standardization.

IT Governance Institute, 2008. *Enterprise Value: Governance of IT Investments: The Val IT Framework 2.0.* Rolling Meadows, Illinois: IT Governance Institute.

Ivanuša, T., Mulej, M., Pečan, S., Tičar, B. and Podbregar, I., 2009. *Pandemija: upravljanje in obvladovanje omejitve gibanja*. Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.

Jereb, B., 2009. Segmenting risks in risk management. *Logistics and sustainable transport*, 1(4), p.11.

Jereb, B., 2010. Princip modeliranja tveganj s segmentacijo javnosti pri upravljanju procesov. *Uporabna informatika*, 18(2), pp.90-100.

Mulej, M. ed., 2000. *Dialektična in druge mehkosistemske teorije – podlage za celovitost in uspeh managementa*. Maribor: Univerza v Mariboru, Ekonomsko-poslovna fakulteta.

Mulej, M. ed., 2008. *Invencijsko-inovacijski management z uporabo Dialektične teorije sistemov (podlaga za uresničitev ciljev Evropske unije glede inoviranja)*. Maribor: Univerza v Mariboru, Ekonomsko-poslovna fakulteta.

Pelău, C. and Bena, I., 2010. The Risk Perception For Consumer Segments In E-commerce And Its Implication For The Marketing Strategy. *Amfiteatru Economic*, XII(28), pp.373-387.

Podbregar, I. and Ivanuša, T., 2011. Contemporary consideration and national security system reengineering. *Economics and Management*, Iss. 3, pp.53-61.

Robertson, K., 2012. *Project / Program / Portfolio Management – What Does it Really Mean?* [online] Available at: <http://www.klr.com/articles/Articles_PM_project_program_portfolio_mgmt.pdf> [Accessed 4 February 2012]

Rushton, A., Croucher, P. and Baker, P., 2010. *The Handbook of Logistics & Distribution Management*. 4th ed. London: Kogan Page Ltd.

Steward, A., 2004. On risk: Perception and direction. *Computers & Security*, Iss. 23, pp.362-370.

Swoboda, B., Pop, N.Al. and Dabija, D.C., 2010. Vertical Alliances Between Retail And Manufacturer Companies In The Fashion Industry. *Amfiteatru Economic*, XII(28), pp.634-649.