1. RISK MANAGEMENT IN SUPPY CHAINS*

1.1 Risk Management as Part of A Management System and Quality Assurance

Due to the trends of globalization and global sourcing, no company today can operate in a risk-free environment with regard to supply chains. The risks inherent to supply chains have become a primary concern in the current logistics and other business processes of different companies. The process of risk management is, therefore, crucial for the uninterrupted operations of companies in all sectors. (Jereb, Cvahte & Rosi, 2012, p. 271–272)

Many organizations only have recently begun to realize the importance of effective risk management, as large numbers of employees, especially top management, begins to manage the risks. However, risk management has to be transferred from the top management to the operational level and back, as risks can be transmitted horizontally (between sections), as well as vertically (from level to level); therefore, risks cannot be managed separately. The organization usually becomes aware of the importance of risk management only when undertaking the preparation of a plan for business continuity. (Jereb, 2014, p. 13-14)

Despite the growing awareness of the importance of risk management, the management of specific risks, such as risks in logistics or natural risks, for the most part is not an integral part of the strategic planning of organizations, as top management still does not perceive this area as being of significant importance so as to establish a representative to manage risks. Moreover, this area still suffers a lack of staff and know-how, which in practice is reflected in the ineffective and non-pragmatic realization of risk management. Often after an accurate risk assessment has already been done, no intelligent decision is made regarding how to manage concrete risks. In such circumstances, the universal ISO 31000 standard was created, which can be used in any type of organization. (Jereb, 2014, p. 13-14)

Risk

Risks are part of our daily lives, and we have never had to deal with the challenges of risk as much as we do in modern times. They can be seen in a variety of everyday public discussions, especially those of a professional and scientific manner; it should be noted that there are many different perceptions and definitions of this term, which may often reflect the complexity of the problems we encounter when we try to comprehensively address risks and manage them. (Jereb, 2014, p. 15-16)

---

* Borut JEREB

Risk is often defined in terms of the possible and/or probable events and their consequences, or a combination of both. The uncertainty of the situation is the lack of information and knowledge (Lakshmi & Mathew, 2013, p. 1) related to the understanding and knowledge of the event, its consequences and/or the likelihood of their occurrence. The level of risk can be defined as the extent of the risk or combination of risks, expressed as a combination of consequences and their probability. In risk management terminology, the word 'probability' refers to the possibility of an event, which can be identified, measured or determined objectively and subjectively, qualitatively and quantitatively or mathematically (such as the probability or frequency in a given time period) (ISO 31000, 2009).

According to Holton (Holton, 2004), risk includes only two essential components:

a) *uncertainty*, and
b) *exposure*.

Uncertainty is a condition that occurs when a proposition or an assertion is true or false, and probability is the metric that is most commonly used to express the uncertainty; at best, it can assess the uncertainty we are able to perceive. Objective uncertainty includes logic, probability and statistical methods, while quantifying probability is scarcely helpful in considering subjective uncertainty, as probabilities in this case are defined by individuals and their systems of values. Exposure occurs when an event has some material or non-material consequences for a person. People are thus exposed when they care about whether a certain proposition is true or false. (Jereb, 2009, p.11)

We can be exposed to risk and be fully aware of it or not; we can also take risk very seriously or remain quite indifferent to it; exposure thus introduces an additional indistinctness, which depends primarily on the individual or a certain segment of the public and its perception of exposure and, consequently, of risk. Therefore, we are not dealing with the problem of the metrics of uncertainty, but rather with the problem of the metrics of exposure. (Jereb, 2009, p.11)

Despite the wide variety of perceptions, interpretations, and definitions of risk, we can define risk as the exposure to uncertainty (Jereb, 2014, p. 66). The ISO 31000 standard (2009) further defines risk when it explains that organizations of various types and sizes face internal and external factors that cause uncertainty about the time within which the goals of an organization should be achieved, and about the achievement itself; the impact of this uncertainty is the risk. Indeed, the concept of risk is difficult to identify, because of the problems in defining uncertainty and exposure. Due to this complexity, risk is difficult to model and simulate; mostly simplified models can be used, which are therefore applicable to a very limited extent. Due to the dimensions of insecurity and exposure, the concept of risk

involves individuals or the public as strictly defined parameters. (Jereb, 2014, p. 66)

Risks can best be understood if they are examined in the case of investments. These are the basis of every business activity: they allow the maintenance of the business, increase its volume, or allow changes in business activities (Jereb, 2014, p. 81); at the same time, investments involve risks and their management as a key factor in operating activities.

Different experts usually employ a simplified approach, in which risk-simulation models predominantly use objective uncertainty, 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; managers' decisions regarding risk management are thus 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 mandatorily defined parameter of each risk, because risk depends on uncertainty and exposure, which is ultimately an attribute of human beings. (Jereb et al., 2012, p. 276-277)

As a part of a particular supply chain, each organization is closely linked and dependent on other organizations in this supply chain; therefore, every organization should be aware of this interdependence in the sense that other organizations in the chain have significant influence on it. In such a way, the dependence on other organizations in the supply chain also represents a risk, as an organization on which we depend might behave in a manner whose consequences have a negative effect on our organization. Often, these relationships are not recognized as risks; therefore, they are not considered in the process of risk assessment, so they can be found only in the analysis of business processes, rather than in the analysis of technological components or infrastructure. (Jereb, 2014, p. 85-86)

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, risks can be defined according to three different origins (Jereb et al., 2012, p. 278):

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.

All organizations' activities can be characterized as technological or commercial; thus risks can be defined as mainly technological, commercial or even universal (Jereb et al. 2012, p. 279). Together, a list of identified risks, their definitions by dimensions and additional descriptions are needed to form a risk catalogue, which is presented below.

1.2 The introduction of ISO 31000:2009 and ISO 28000:2007 for the process of risk management

Uncertain market conditions, the requirements of globalization, and increasingly frequent and destructive external threats require effective risk management in supply chains to ensure the continuity of operations of the organization. Risk management should be the priority in any organization, and should also be included in all aspects of business, in order to ensure its effectiveness and efficiency. Top management should be aware of the risks that threaten the organization, but they should also be familiar with the variety of tools available so that risks can be managed and controlled. (Jereb, 2014, p. 89-90) The basic mission of the organization is the effective and efficient achievement of set objectives, but in their realization the organization is always faced with some uncertainty, the impact of which is reflected in the risks. For this reason, all activities within the organization include risks that need to be managed so that they are it first assessed through identification, analysis, and evaluation; they should then be handled appropriately. (Jereb, 2011, p. 200-201)

The ISO 31000 Standard for Risk Management (2009) explains the key concepts and terminology of risk management, as well as offering a variety of techniques and methods for efficient risk management. When defining terminology, the standard resolves the issues of the use of different terms to describe the risks, measuring impacts, likelihoods, uncertaintis, and other dimensions of risk management between technology- and business-oriented personnel within the organization and between organizations (Jereb, 2014, p. 14).

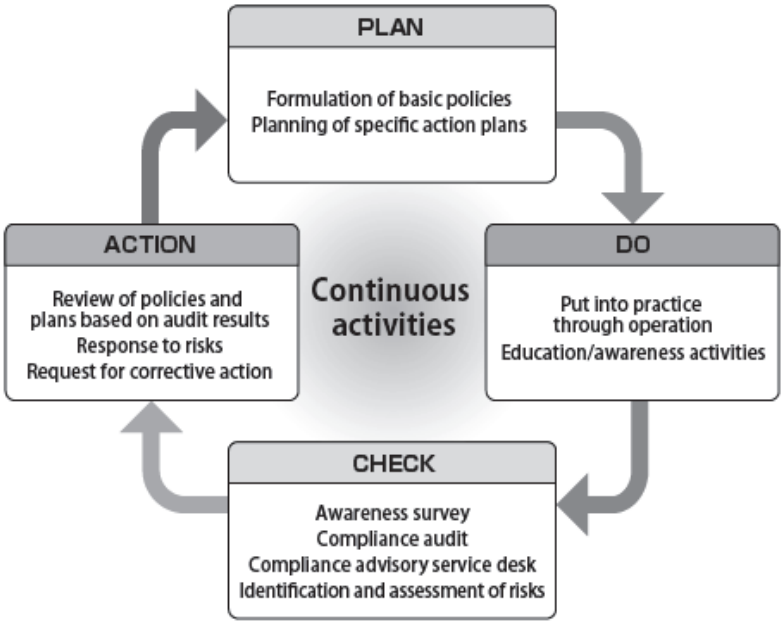
ISO 31000 (2009) sts out the principles and general guidelines for risk management. It can be used for all kinds of risks, irrespective of their nature, and provides both positive and negative consequences. It provides general guidelines, but in setting and implementing plans and frameworks for risk management it also takes into account different needs of organizations that may be reflected in their objectives, context, structure, mode of action, processes, functions, projects, products or services, and resources. (Jereb, 2014, p. 14)

Due to the overall context, it provides comprehensive guidance for managing risks in different areas and is thus open to all types of organizations throughout the life of the organization, with the widest range of activities, including the creation of strategies, decision-making, management, the implementation of projects, the implementation of the other functions of the organization, production and management products, services and resources, etc. (Jereb, 2014, p. 14). It must be noted that the standard is not intended for certification, but rather for consistent application.

In accordance with ISO 3100, the risk management process within the organization or across the supply chain is set within the cycle of Plan-Do-Check-Act

(PDCA), adapted for the purposes of risk management (see Figure 1.1). The basic idea of the cycle is that a process should first be planned (Plan), then carried out (Do), then checked and monitored (Check), and finally complemented and improved (Act). (Jereb, 2014, p. 19-20)

Figure 1.1: PDCAcycle

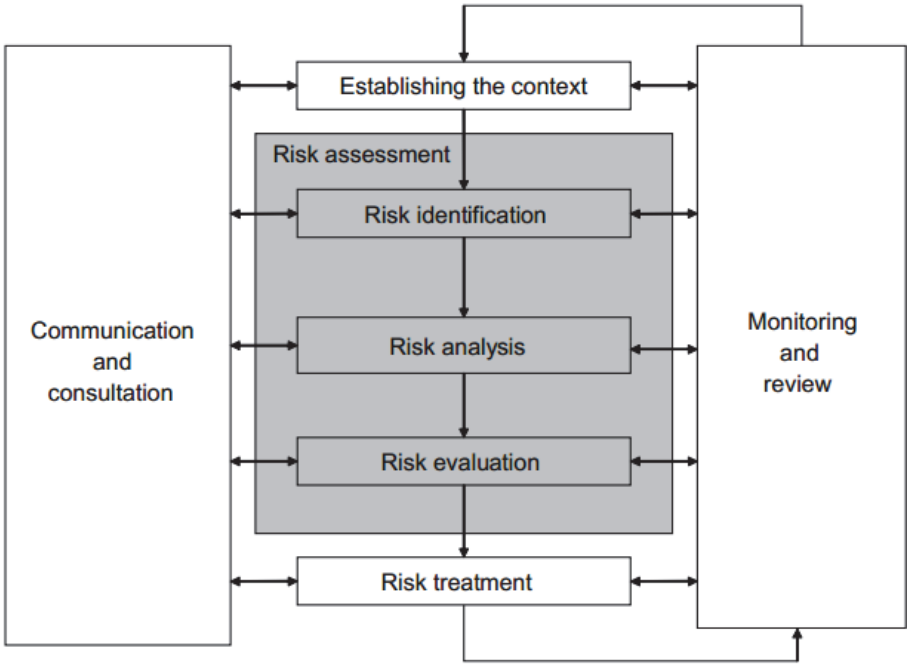


Source: Tokyo Gas CSR Report 2014 [Tokyo Gas], 2014.

According to ISO 31000 (2009), risk assessment is a process in which risks are identified, analysed, and evaluated. On the basis of this assessment, a risk treatment is selected. The process of risk management and the process of risk assessment are shown on Figure 1.2.

One of the most important standards in the field of security in logistics that is directly related to risk management is certainly the ISO 28000 standard, which aims to improve the security of the supply chain. It targets the top management of organizations, who are responsible for establishing a comprehensive system of security management of the supply chain. Using this standard, an organization assesses the environment in which it operates, and determines whether there are adequate safety measures, and whether the organization meets all legal requirements. (Jereb, 2014, p. 15)

Figure 1.2: The process of risk management



Source: ISO 31000, 2009.

The primary purpose of the standard is to accede to the safety management of organizations in such a way that the business success and credibility of organizations are ensured. (ISO 28000, 2007). ISO 31000 is a generic standard for risk management, while ISO 28000 is the standard specific for safety management in supply chains. ISO 28000 (2007) defines security management as the application of systematic and coordinated activities and practices through which an organization optimally manages risk at the level of the supply chain and the associated potential hazards and their impacts (ISO 28000, 2007).

This standard can be used by organizations of different sizes, in particular, those in supply chain management, that are attempting to (ISO 28000, 2007; Jereb, 2014, p. 61-62):

- establish, implement, maintain or improve their security management system;
- ensure compliance with established security management policy;
- demonstrate such compliance to others;

- certify its security management system so that it is accredited by the certification body; and/or
- achieve compliance with the standard ISO 28000.

According to ISO 28000 (2007), areas that may be affected by risk are the following (Jereb, 2014, p. 62):

- risks of physical failure, such as functional equipment failure, accidental failure, malicious damage, terrorism or criminal acts;
- operational risk, including control of security, the human factor, and other activities that affect the performance, status and safety of organizations;
- natural environmental events (storms, floods, etc.), due to which safety measures and equipment can become less effective;
- factors that are not under the control of an organization, such as the failure of equipment or services, carried out by external providers;
- the risks of all stakeholders of the organization, such as the failure to achieve regulatory requirements, or decreased brand reputation;
- the design and installation of security equipment, including substitution, maintenance, etc.
- information management and communication; an/or
- threats to the continuity of operations.

Each consequence of the risks that arise in the supply chain may affect one or more logistics resources. If we want to effectively manage risks, we have to be aware of the impact of an individual risk on different resources. As an individual risk might affect more than one logistics resource; in this category, the secondary effect on the logistics resources is incorporated. (Jereb, 2014, p. 83-84)

1.2.1 Establishing the context

By establishing the contex, the organization articulates its goals, defines the internal and external parameters that need to be considered during risk management, and defines the scope and criteria for the remaining part of the risk management process. In this process, the difference between internal and external contexts can be distinguished, as well as the context for the risk management process itself. (Jereb, 2014, 40)

The external context is the external environment, for which it is necessary to take into account the objectives of external stakeholders in the development of criteria for risk. In particular, the perceptions of stakeholders are taken into account as well as legal and regulatory requirements. The internal context, in contrast, is the internal environment, for which risk management must be appropriate for the or-

ganizational culture, other processes, the structure of the organization, as well as for its strategy. (Jereb, 2014, 40-41)

Risk management must be done in such a way that any means are justified; therefore, means should be defined, as well as responsibilities and authorizations, and records that should be kept. Organizations must also define the criteria that are used in evaluating the significance of individual risks and, therefore, should be in accordance with the risk management policy. These criteria reflect the values, systems, goals, and resources of the organization. (Jereb, 2014, 42)

1.2.2 Risk assessment

Risk identification

The identification of risks involves finding, identifying and describing risks; it also includes sourcing the risks, their causes and potential consequences; historical data, theoretical analysis, and the opinions of specialists can be used for this (IEC / FDIS 31010, 2009, p. 12). Every organization should find the most suitable methods to approach risk identification (Jereb et al., 2012, p. 274).

Risks and their impacts frequently also depend on the time in which they happen; therefore, this dimension should be taken into consideration in risk assessment. In certain time frames, a risk is barely worth considering, while the same risk in a different time frame is crucial to the success of a business organization. If different time frames are present, they must also be included in the risk assessment phase in order to obtain an overview of the risk changing over time. For each risk, it is necessary to determine the limit of acceptability, for which possible time frames should be considered. Since an isolated risk that does not affect the processes within the organization or the supply chain does not exist, interdependencies between risks must be defined (Jereb, 2014, p. 86-87)

Every identified risk has its attributes, which can be general, if it can be ascertained that the same attributes are true in every organization, or they can be organization specific, for which some attributes of a particular risk have to be defined in the specific organization that is undertaking risk assessment. (Jereb, Cvahte & Rosi, 2012, p. 274)

As every human being is unique, the relation to a certain risk in a particular situation can also differ greatly: people have different views of the same risk, which may be a result of different levels of exposure as well as of different levels of uncertainty. This issue is most commonly addressed to segments of the public that share a common stance with regard to a particular risk. The approach in which segments of the public play the central role in risk management has only recently been covered in the relevant academic literature.

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 that is considered in risk management (Jereb et al., 2012, p. 276).

Such an approach is also in accordance with ISO 31000, in which 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' (Jereb et al., 2012, p. 278).

If we assume that only people can perceive themselves and inanimate things cannot, we can also assert that certains risk can only influence people, who are susceptible to perceptions. According to this theory, we should segment all peopl, involved in a supply chain and its surroundings, to different publics, i.e. different groups of people with same interests or functions according to the individual risk. (Jereb et al., 2012, p. 277)

The general idea of risk management is that each identified risk must be assigned to a person or group of people who are responsible for its management – risk owners. They should have the responsibility, authority and appropriate skills to manage risks for the introduction and maintenance of adequate and effective controls for risk management (ISO 31000, 2009). By establishing the 'owner' of risks, a higher level of awareness is also achieved in those who need to be included in the risk management process within the organization or supply chain. (Jereb, 2014, p. 86-87)

Risk analysis

Risk analysis is the development of the understanding of risk, which includes decisions regarding whether it is necessary to deal with individual risk, and what appropriate strategies and methods for its treatment are. Risk analysis includes determining the implications of the risk and its probability, which is reflected in the level of risk. It is also necessary to define or determine the presence and efficacy of any control over risks. Risk analysis must include an examination of the effects of special effects, including cascades and cumulative effects, as a single event can have multiple impacts. (ISO 31000, 2009)

As we analyse risks, we also need to be aware of different logistics resources for the operations in the supply chain. These resources represent fundamental resources that are used in logistic processes and, consequently, in supply chain management processes. Risks can have a significant effect on these resources and, therefore, we should define which logistics resource or its use a certain risk can have an effect. The concept of resource definition and its 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).

Within the processes in a supply chain, there are four key logistics resources, without which logistics processes cannot take place (Jereb, Cvahte & Rosi, 2012, p. 275-276):

- The flow of goods and/or services must be managed from the source point to a durable point in order to fulfil the expectations of users.
- Information flow flows in two directions: the input data comes into the information system for their processing and the generation of output information, which should be useful for the organization.
- The logistics infrastructure and superstructure are the basic physical and organizational structures needed for logistics operations.
- People as personnel are required for the planning, organizing, acquisition, implementation, delivery, support, monitoring and evaluation of logistics systems and services. They may be internal, external or contract, depending on the needs of the organization.
- The list of identified risks and the description of every particular risk based on the predefined definitions by dimensions form a basis on which a risk catalogue of the supply chains is created. (Jereb, 2014, p. 86) The risk catalogue and its use is presented in a subchapter below.

Risk evaluation

The purpose of risk evaluation is to determine the importance of the level and nature of risks and the determination of the necessary measures. The evaluation of the risk is primarily the decision regarding which risks need to be treated and what the priorities are for implementation of this treatment (IEC / FDIS 31010, 2009, p. 16). When evaluating risk, we must also define the impact of risk to the specific publics, as different risks have different impacts on different publics, and various publics perceive them differently. By analysing the effects on the publics, we gain a greater insight into the consequences of risk. This is not the segmentation of the public, which searches for the impacts and effects of risks to different publics (Jereb, 2014, p. 84-85).

The process of risk assessment specifically supports the ISO 31010 standard (IEC / FDIS 31010, 2009), which provides a number of methods and techniques for the assessment of risks, of which some are useful in all three phases of the risk assessment, while others are useful only in an individual phase. Thus, for the identification various interviews, review of historical data, brainstorming, Delphi-method, checklists, and other methods are suitable. Risk analysis is primarily a reflection on the causes and sources of risks, their consequences and the likelihood that they will occur, so it is necessary to define the factors that affect the likelihood and consequences. At this stage, the qualitative, quantitative, or mixed methods can be used, and control mechanisms must be set. Among the techniques that are appropriate at this stage, the method of different scenarios, the 'SWIFT' method, the analysis of the causes, 'bow-tie' diagrams, and others are very useful. In the evaluation phase

of the risks, in which priorities and measures are decided upon, it is very sensible to use cost-benefit analysis, which can also be used with a variety of methods and techniques. (IEC/FDIS 31010, 2009, p. 12)

1.2.3 Risk treatment

Risk treatment includes the selecting of one or more appropriate options to change the likelihood of risks, the effects of risk, or both, and the exercise of those options. This is followed by a cyclic process of re-evaluating risks to re-determine the type of treatment. (Jereb 2011, p. 208). Risk treatment, which deals with the negative consequences, is sometimes termed 'risk mitigation', 'risk elimination', or 'risk prevention'. The treatment or modification of risk can thus mean the removal of a source of threat, reducing the likelihood of an adverse event, changing its consequences, or risk sharing with other contractors in order to avoid the risk that activities do not start or do not continue. With smart decisions, risks can also be maintained. Residual risk is that which remains even after the risk treatment. (ISO 31000, 2009)

1.3 Risk catalogue in supply chains

The final product of conventional risk identification and assessment is a risk catalogue for supply chains that contains all the identified and described risks of a specific organization(Jereb & Cvahte, 2012). A more advanced version is the risk catalogue that contains the risks on the level of the entire supply chain. The risk catalogue is an important and useful tool in risk management, since its use significantly shortens the process of risk identification. It is designed so broadly that it is useful in various organizations, notably in terms of the guidelines for the identification of risk and as a checklist.

Every leader in supply chains should be aware of the importance of cooperation between organizations, since a single organization can never identify as many risks as a group of organizations, especially with regards to risks in supply chains. Organizations often start the process of risk management alone, although very often they do not start even such a project. In such circumstances, the Faculty of Logistics of the University of Maribor, in the context of the activities of the Laboratory of Informatics, created an online risk catalogue for supply chains, through which organizations can carry out important steps in the process of risk assessment. (Jereb, 2014, p. 87-89)

This model of risk catalogue includes the principles of ISO 31000, ISO 31010 and ISO 28000. This is online risk catalogue for supply chains is available on the website http://labinf.fl.uni-mb.si/risk-catalog/. It can be used as a checklist of pos-

sible risks, and reflects a widely used model for risk management in supply chains (Jereb, Ivanuša & Rosi, 2013, p. 68).

When considering the risk management model, which is provided by ISO 31000, we can see that the processes that are involved in risk assessment, particularly the identification and analysis of risks, are the key processes in the whole risk management process. We should be aware that the risks that are not detected in the process of risk identification, are later not discussed and incorporated into the risk management; therefore, they are overlooked so we cannot be prepared for them. The identification of risks should be concluded with the creation of a risk catalogue, in which each risk is classified in categories according to its fundamental dimensions. Later in the process, it is necessary to introduce additional dimensions that are specific to each organization (Jereb, 2014, p. 81-82).

When classifying risks into basic dimension, the online risk catalogue can be used. In it, the fundamental dimensions of the risks coincide with the areas of risks, as defined by ISO 28000 (See Figure 3). Because some risks are more complex, it is illogical to classify them into only one group or dimension; thus, some risks are classified into two categories: primary and secondary (Jereb, 2014, p. 82-83).

Every organization that deals with risk assessment by using this risk catalogue must implement all those dimensions required by the specific requirements of the organization. This is mostly dependent on the type of goods or services offered by the supply chain, but there are also universal risks that occur in all supply chains (Jereb, 2014, p. 86-87).

In addition to the list of dimensions, the model of Risk Catalogue also contains the list of affected publics, the list of affected logistics resources, the list of supply chain risk origins, as well as the list of the levels of logistics planning (‘Risk Catalogue’, [labinf.fl.uni-mb.si]).

Figure 1.3: A section of the risk catalogue: dimensions of risk definition

Dimensions of risk definition

List of groups by ISO 28000

This model is structured so that it complements 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. Each identified risk is placed in one of these groups.

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

Source: Risk Catalogue [labinf.fl.uni-mb.si].

Figure 1.4: The section of Risk catalog: Data

Risk	Group according to ISO 28000	Secondary group according to ISO 28000	Primary logistics resource	Secondary logistics resource	Primary public	Secondary public	Origin of risk	Level of logistics planning
Limited or no access to the key locker	a.PHY		ISL		OPE		COM	OPL
Fall of wall/ceiling	a.PHY		ISL		IMP	OPE	OSC	TPL
Collapse of tent	a.PHY		ISL		IMP	OPE	OSC	TPL
Planted bomb or explosive	a.PHY		ALS		ALL		OSC	OPL
Damage to the forklift ramp	a.PHY		ISL	FLW	OPE		COM	OPL
Damage of cranes, lifts	a.PHY		ISL	FLW	MNG	OPE	COM	OPL
Collapse of the roof (snow)	a.PHY		ISL	FLW	IMP	OPE	OSC	TPL
Destruction or reduction of value of goods	a.PHY		ISL		MNG	CCU	COM	TPL

Source: 'Risk Catalogue' [labinf.fl.uni-mb.si].

The Risk Catalogue is published under a Creative Commons license that allows interested users to use it, download and share it 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 the catalogue is an ever growing publication, all users should be able to contribute, comment or add to its content. This is achieved by submitting ideas to the editorial board, which assesses the contributions and incorporates them in the catalogue when appropriate. Submissions are expected via email sc.riskcatalog@gmail.com.

1.4 The principle of modelling risks with respect to segmentation of the public

The described model is sufficiently general in order to be useful in various situations and fields where risk is encountered. Although the model described in this chapter can be used in a wide array of fields, the example of a business process model is presented below. Depending on the particular field in which the risk are to be modelled, the importance of a particular part of the model (various public, internal vs. external, dynamic behaviour in time, etc.) may differ; however, it can seldom happen that an individual part of the model is completely negligible in a particular case (Jereb, 2014, 70-71).

1.4.1 The presentation of the processes

Business processes are represented by process graphs, i.e. mathematical structures in which the nodes represent a particular process, while the link between two nodes represents their relation.

The process graph *PG* is defined as a directed graph (Jereb, 2009):

$$\begin{gathered} PG = \{P, E\} = \{P, (P_k, P_l), (P_m, P_n) \ldots (P_q, P_r)\}; \\ k, l, m, n, q, r = \{1,2,3,\ldots, (PG)\} \end{gathered} \tag{1}$$

where P represents a set of resources of any kind (goods, services, information, etc.) and their mixture; E represents a set of edges representing the flow of any kind of resources, in which particular processes from P are the sources and destinations, respectively, of such flows. E is a set of ordered pairs, in which the pair (P_x, P_y) is considered to be directed from the process P_x to the process P_y. It represents the output resources flow for the process P_x and the input resources flow for the

process P_y. Each pair (P_x, P_y) represents the information on the mutual relationship between the process P_x and P_y. P_x is a direct predecessor of P_y and vice versa, P_y is a direct successor of P_x. In our model, both P and E are finite sets.

The behaviour of the process P_k is influenced by its input, denoted by *Input(P_k)*.

The output of the process P_k is denoted by *Output(P_k)* and it is generated according to the following items:

a) its current status (or state in which the process is),
b) its current input, and
c) the rules for generating the output according to the status and input.

The calculation of the process states described by parameters is further explained in the paper.

The definitions of the process P_k input and output are, as follows:

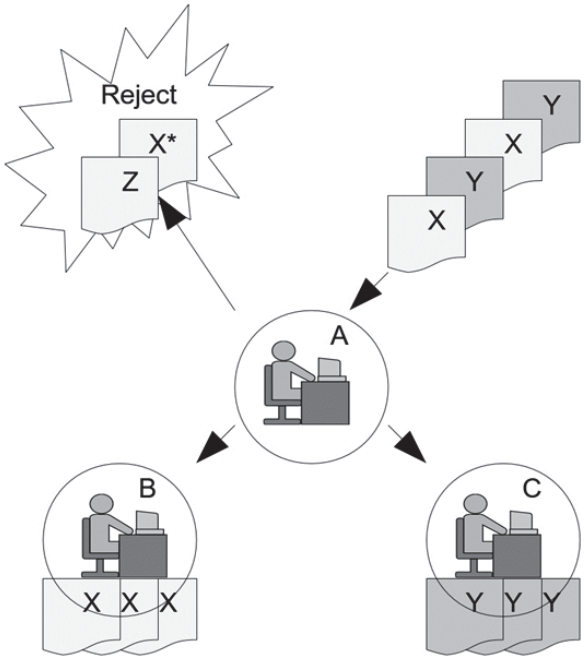
$$Input(P_k) = \{(P_x, P_k)\} = \{Inp_{k,1}, Inp_{k,2}, ..., Inp_{k,n}\} \tag{2}$$

$$Output(P_k) = \{(P_k, P_y)\} = \{Out_{k,1}, Out_{k,2}, ..., Out_{k,n}\} \tag{3}$$

Example Clerk A regularly receives documents of two types: Document X and Document Y. Upon receipt, Clerk A, performing the Business Process A, establishes whether the documents are adequate for further processing. If any document is not adequate, Clerk A rejects it, producing Explanation Z, including a request for the amendment of the document. If the document is adequate for further processing, it is recorded in Incoming Mail and forwarded to other clerks: Type X documents are forwarded to Clerk B, performing Business Process B; and Type Y documents are forwarded to Clerk C, performing Business Process C.

Figure 1.5 illustrates this simplified example of business processes.

Figure 1.5: A simplified business process in which Clerk A reviews and sorts / classifies the received documents and forwards them to the Business Processes B (Clerk B) and C (Clerk C)



Source: Jereb, 2014, p. 72.

1.4.2 Description of the status of the process parameters and time dimension of the model

The state of each process and its specific properties are described according to parameter: the process time parameters, the maturity level, sensibility to some types of risks, the period of the year in which its importance may be low or high, the risk acceptance, the impact acceptance, and other parameters. The model does not define what each parameter actually represents, nor does it define the number of parameters. The most important aspect of the parameters is that they allow the accumulation of the previous life cycles of each business process within them; this accumulated information is then used to accumulate the impacts and new business process parameter values. In this way, modelling also comprises the 'history' of the modelled system. These parameters include the accumulated history of past mo-

ments and accordingly, the past combinations of risks and other impacts relevant to the business process (Jereb, 2014, p. 71-72).

Example In our business processes example, the Process A parameter could be the number of delays involved in forwarding or rejecting any document by Clerk A (the clerk acts later than required by the respective regulations). If Clerk A never makes a mistake, Type X documents are sent to Clerk B. However, the clerk could make a mistake and send an incorrect document to Clerk B. A document may also be ambiguous, and it may only later become evident that it is of a different type than initially believed by Clerk A. In the first or second case, the document sent to Clerk B is of the wrong type. Within Process B, the number of incorrect documents received can be measured and recorded in a particular parameter of Process B.

Example In the above example, each individual delay could be insignificant, but a number of delays could have adverse consequences. It is, therefore, not only necessary to record individual delays, but also the total sum of all delays. This is an example of an additional process parameter.

The model should include the dimension of time, which introduces non-determinism. In many real situations, some or all processes include the time dimension in their input, output, or in the manner in which the following state of a process is calculated.

The state of the process P_k is described by the following equation:

$$State(P_k, t) = \{Par_{k,1}(t), Par_{k,2}(t), ..., Par_{k,m}(t)\} \tag{4}$$

In which $Par_{k,x}(t)$ denotes the value of the parameter x of the process P_k in time t.

In addition, there is the function Φ_{SC} that calculates new values of the process parameters (i.e. the new state) in each discrete (temporal) moment, based on:

a) Business process input $Input(P_k,t)$;
b) Current values of business process parameters $State(P_k,t)$.

$$State(P_k, t+\Delta) = \Phi_{SC}\begin{bmatrix} Input(P_k, t), \\ State(P_k, t) \end{bmatrix} \tag{5}$$

Equation (4) represents the state of the process P_k, which is changing through time. In the case of discrete simulation, the new state of the P_k is evaluated for every single time segment Δ by the function Φ_{SC}, which calculates new states as represented by Equation (5). The $State(P_k, t)$ comprises all accumulated influences spread from P_k in the future. These influences are based on the past combinations

of inputs and states of the P_k. In other words, it represents a kind of accumulated history of the P_k, which could be reflected in the future by generated impacts.

In the above-explained equations. we still do not consider the following described segmentations, including the risks and segments of the public.

1.4.3 Segmentation with respect to different publics

Simulations should be conducted for each segment of the public separately. The view given throughout this article, however, justifies the calculation of risk, process states and consequences for each particular segment of the public.

$$\begin{gathered} GeneralInput\left(P_k, Public_l, t\right) = \\ Input\left(P_k, Public_l, t\right) - Risk\left(P_k, Public_l, t\right) \end{gathered} \tag{6}$$

Equation (6) for calculating risks conducting the segment of the public is expressed as:

$$\begin{gathered} Risk\left(P_k, Public_l, t\right) = \\ \Phi_{RC}\begin{bmatrix} Uncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{bmatrix} = \\ \Phi_{RC}\begin{bmatrix} ObjUncertainty\left(P_k, Public_l, t\right), \\ SubUncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{bmatrix} \end{gathered} \tag{7}$$

Whereby in (7):

a) P_k is process *k.*
b) *Uncertainty* (P_k,*Public, t)* is the uncertainty in the process P_k at time *t.*
c) Sub*Uncertainty* (P_k, *t)* is the subjective uncertainty in the process P_k at time *t*.
d) *Exposure* (P_k , *Public, t)* is the exposure in the process P_k with respect to the segment of *Public* at time *t*.
e) Particular risks for the process *Pk* are represented by a set of *m* risks $\{R_{k,1}(t), R_{k,2}(t), \ldots, R_{k,m}(t)\}$ at time *t*.
f) Function Φ_{RC} calculates risks.

Equation (8) for calculating processes considering (6) the state conducting the segment of the public and segmenting input to risks, uncertainty and exposure is:

$$
\begin{aligned}
&State\left(P_k, Public_l, t+\Delta\right) = \\
&\Phi_{SC}\left[\begin{array}{c} Input\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{array}\right] = \\
&\Phi_{SC}\left[\begin{array}{c} Risk\left(P_k, Public_l, t\right), \\ GeneralInput\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{array}\right] = \\
&\Phi_{SC}\left[\begin{array}{c} \Phi_{RC}\left[\begin{array}{c} ObjUncertainty\left(P_k, Public_l, t\right), \\ SubUncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{array}\right], \\ GeneralInput\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{array}\right]
\end{aligned}
\tag{8}
$$

Equation (9) for calculating consequences, considering (7), (8) and conducting the segment of the public, is:

$$
\begin{aligned}
&Consequence\left(P_k, Public_l, t+\Delta\right) = \\
&\Phi_{IC}\left[\begin{array}{c} Input\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{array}\right] = \\
&\Phi_{CC}\left[\begin{array}{c} Risk\left(P_k, Public_l, t\right), \\ GeneralInput\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{array}\right] = \\
&\Phi_{CC}\left[\begin{array}{c} \Phi_{RC}\left[\begin{array}{c} ObjUncertainty\left(P_k, Public_l, t\right), \\ SubUncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{array}\right], \\ GeneralInput\left(P_k, Public_l, t\right), \\ State\left(P_k, Public_l, t\right) \end{array}\right]
\end{aligned}
\tag{9}
$$

Considering Equations (7), (8), (9) and conducting segments of the public risks should be expressed with Equation (10):

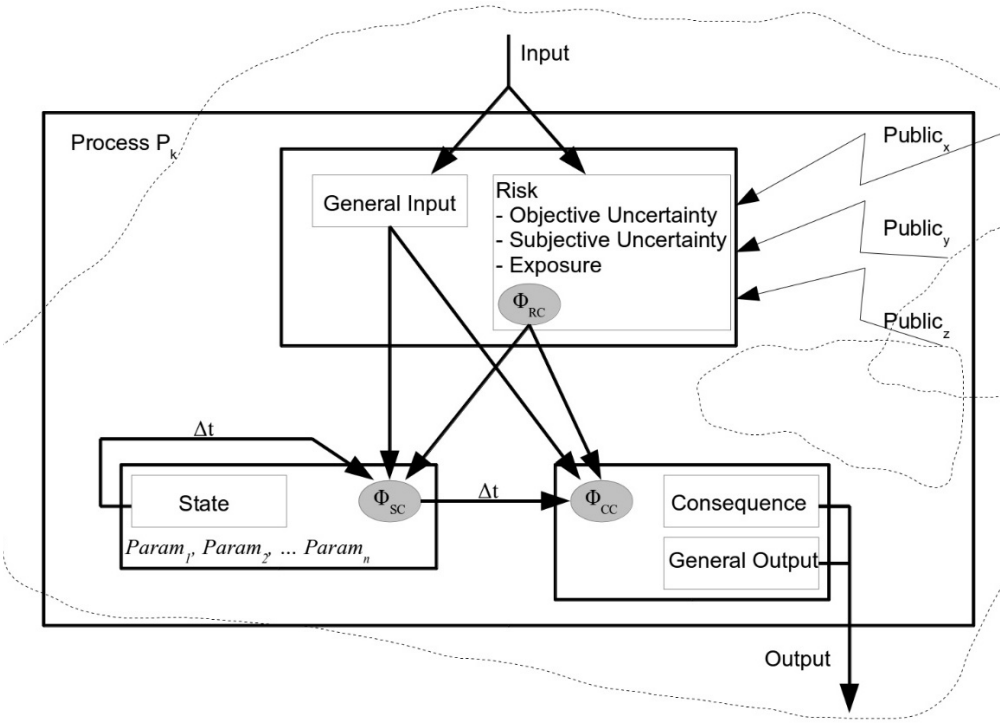
$$
\begin{aligned}
&Consequence\left(P_k, Public_l, t+\Delta\right) = \\
&\Phi_{CC}\left[\begin{array}{l}
\Phi_{RC}\left[\begin{array}{l} ObjUncertainty\left(P_k, Public_l, t\right), \\ SubUncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{array}\right], \\
GeneralInput\left(P_k, Public_l, t\right), \\
State\left(P_k, Public_l, t\right)
\end{array}\right] \\
&\Phi_{CC}\left[\begin{array}{l}
\Phi_{RC}\left[\begin{array}{l} ObjUncertainty\left(P_k, Public_l, t\right), \\ SubUncertainty\left(P_k, Public_l, t\right), \\ Exposure\left(P_k, Public_l, t\right) \end{array}\right], \\
GeneralInput\left(P_k, Public_l, t\right), \\
\Phi_{SC}\left[\begin{array}{l}
\Phi_{RC}\left[\begin{array}{l} ObjUncertainty\left(P_k, Public_l, t-\Delta\right), \\ SubUncertainty\left(P_k, Public_l, t-\Delta\right), \\ Exposure\left(P_k, Public_l, t-\Delta\right) \end{array}\right], \\
GeneralInput\left(P_k, Public_l, t-\Delta\right), \\
State\left(P_k, Public_l, t-\Delta\right)
\end{array}\right]
\end{array}\right]
\end{aligned}
\tag{10}
$$

Equation (7) shows how to calculate risk, which is the input to a business process based on objective and subjective uncertainty and exposure at a point in time.

Equation (8) shows how to calculate process states based on known risks, general inputs, and process states recorded for a prior time segment at a certain point in time. Equation (9) explains the calculation of the impact based on the same inputs as for internal process states. Equation (10) gives the calculation of consequences using a transitive relation for the calculation of internal process states in a prior time segment by taking into consideration risks, general input and internal process states in the time segment prior to the previous time segment. All equations include business processes and segments of the public.

These equations constitute the foundation of the algorithm for the calculation of the consequences in a model. The impact calculation is central to risk management modeling, and is illustrated by Figure 1.6.

Figure 1.6: The main elements of the risk management model



Source: Jereb, 2009, p.30.

1.4.4 Acceptance border

For risks, the acceptance border is calculated in Equation (11), using the function Φ_{RAB}; the acceptance border for the consequences is defined with Equation (12) by the function Φ_{CAB}; the acceptance border for the process states is defined with Equation (13) by the function Φ_{SAB}.

$$\begin{gathered} RiskAcceptanceBorder\left(P_k, Public_l, t\right) = \\ \left\{RAB_{k,l,1}\left(t\right), RAB_{k,l,2}\left(t\right), ..., RAB_{k,l,m}\left(t\right)\right\} = \\ \Phi_{RAB}\left(Risk\left(P_k, Public_l, t\right)\right) \end{gathered} \tag{11}$$

$$\begin{gathered} ConsequenceAcceptanceBorder\left(P_k, Public_l, t\right) = \\ \left\{CAB_{k,l,1}\left(t\right), CAB_{k,l,2}\left(t\right), ..., CAB_{k,l,m}\left(t\right)\right\} = \\ \Phi_{CAB}\left(Consequence\left(P_k, Public_l, t\right)\right) \end{gathered} \tag{12}$$

$$\begin{gathered} StateAcceptanceBorder\left(P_k, Public_l, t\right) = \\ \left\{SAB_{k,l,1}\left(t\right), SAB_{k,l,2}\left(t\right), ..., SAB_{k,l,m}\left(t\right)\right\} = \\ \Phi_{SAB}\left(State\left(P_k, Public_l, t\right)\right) \end{gathered} \tag{13}$$

In Equations (14), (15) and (16), tolerable or acceptable values for risk, consequences, and values of the process states are defined according to the given acceptance borders.

$$\begin{gathered} AcceptedRisks\left(P_k, Public_l, t\right) = \\ \left\{R_{k,l,x}\left(t\right); x = 1,2,..., m \,\square\, R_{k,l,x}\left(t\right) < RAB_{k,l,x}\left(t\right)\right\} \end{gathered} \tag{14}$$

$$\begin{gathered} AcceptedConsequences\left(P_k, Public_l, t\right) = \\ \left\{C_{k,l,x}\left(t\right); x = 1,2,..., m \,\square\, C_{k,l,x}\left(t\right) < CAB_{k,l,x}\left(t\right)\right\} \end{gathered} \tag{15}$$

$$\begin{gathered} AcceptedStates\left(P_k, Public_l, t\right) = \\ \left\{Param_{k,l,x}\left(t\right); x = 1,2,..., m \,\square\, Param_{k,l,x}\left(t\right) < SAB_{k,l,x}\left(t\right)\right\} \end{gathered} \tag{16}$$

Equations (17), (18), and (19) define the unacceptable (intolerable) values, which represent a set of values that is equal to the set of all possible values minus the set of acceptable values.

$$\begin{gathered} NotAcceptedRisks\left(P_k, Public_l, t\right) = \\ Risk\left(P_k, Public_l, t\right) - AcceptedRisks\left(P_k, Public_l, t\right) \end{gathered} \tag{17}$$

$$NotAcceptedConsequences\left(P_k, Public_l, t\right) = Consequence\left(P_k, Public_l, t\right) - AcceptedConsequences\left(P_k, Public_l, t\right) \tag{18}$$

$$NotAcceptedStates\left(P_k, Public_l, t\right) = State\left(P_k, Public_l, t\right) - AcceptedStates\left(P_k, Public_l, t\right) \tag{19}$$

Example For Business Process A (see Figure 5) and for all segments of the public, it is true that risks and acceptance borders do not change over time. The risks that accompany business processes should be:

a) R_1 – poorly legible received document.
b) R_2 – delays resulting from untimely forwarding or rejection of a document by Clerk A.
c) R_3 – wrong type of the document sent from Clerk A to Clerk B.

The following individual segments of the public have been observed:

a) SJ1 – employees who carry out Business Process A.
b) SJ2 – owners of Business Process A.
c) SJ3 – users of Business Process A.

Objective and subjective uncertainty, exposure and risks have the following set of four values: {Ø – zero value, S – relatively small values, M – middle values, H – relatively high values}. Although the same designations of values are used, they have different implications for uncertainty, exposure and risks. Tables 1.1 to 1.3 show values that change in simulations.

Table 1.1: Objective uncertainty as to the individual risk and segment of the public.

	SJ_1	SJ_2	SJ_3
R_1	S	S	Ø
R_2	M	M	Ø
R_3	S	S	Ø

Table 1.2: Subjective uncertainty as to the individual risk and segment of the public

	SJ_1	SJ_2	SJ_3
R_1	Ø	S	S
R_2	Ø	H	H
R_3	Ø	M	H

Table 1.3: Exposure to the individual risk and segment of the public

	SJ_1	SJ_2	SJ_3
R_1	S	M	S
R_2	S	M	H
R_3	M	H	H

Table 1.4 shows the calculated risks by using a function (see Equation (6)). In this case, the function is simplified in order to calculate risk as the worst option in the Cartesian product between objective and subjective uncertainty, and the exposure.

Table 1.4: Calculated risks for an individual segment of the public

	SJ_1	SJ_2	SJ_3
R_1	S	M	S
R_2	M	H	H
R_3	M	H	H

If the acceptance borders were such that acceptable risks are as described in Table 1.5, the risk R_3 would be unacceptable to all segments of the public and the risk R_2 would be unacceptable to SJ_2, while the remaining risks are acceptable.

Table 1.5: Accepted risks for an individual segment of the public

	SJ_1	SJ_2	SJ_3
R_1	S,M	S,M	S,M
R_2	S,M	S,M	S,M,H
R_3	S	S	S,M

In practice, we need to decide what to do with these risks. If we want to reduce them, it is necessary to take steps towards reducing uncertainty and/or exposure. In a similar way, we should calculate and assess the business processes' states and the corresponding impacts.

References

Creative Commons 2011. Attribution – NonCommercial - NoDerivs 3.0 Unported. Accessed 28 August 2015 on: http://creativecommons.org/licenses/by-nc-nd/3.0/

Holton, G. A. (2004). Defining Risk. *Financial Analyst Journal*, Vol. 60, No. 6. CFA Institute.

IEC/FDIS 31010. (2009). *Risk management – Risk assessment techniques*. Geneve: ISO.

ISACA 2007. *Cobit 4.1.* International Systems audit and Control association.

ISO 28000. (2007). *Specification for security management systems for the supply chain*. Geneve: ISO.

ISO 31000. (2009). *Risk management – Principles and guidelines*. Geneve: ISO.

Jereb, B. & Cvahte, T. (2012). *Risk catalog*. Accessed 10 September 2015 on: http://labinf.fl.uni-mb.si/risk-catalog

Jereb, B., Cvahte, T. & Rosi, B. (2012). Mastering supply chain risks. *Serbian Journal of Management*, Vol. 7, No. 2, 271-285.

Jereb, B., Ivanuša, T. & Rosi, B. (2013). Systemic thinking and requisite holism in mastering logistics risks: the model for identifying risks in organizations and supply chains. *Amfiteatru Economic*, Vol. 15, No. 33, 56-73.

Jereb, B. (2009). Segmenting risks in risk management. *Logistics and sustainable transport*, 06-04-09, Vol. 1, No. 4, 1-31.

Jereb, B. (2011). Standarda za upravljanje tveganj: ISO 31000:2009 in ISO/IEC 31010:2009 = Risk management standards: ISO 31000:2009 and ISO/IEC 31010:2009. *Zbornik referatov 19. Mednarodne konference o revidiranju in*

kontroli informacijskih sistemov, Ptuj, 27. in 28. september 2011, 199-215). Ljubljana: Slovenski inštitut za revizijo.
Jereb, B. (2014). *Upravljanje tveganj*. Celje: University of Maribor, Fakulty of logistics.
Lakshmi, S. D. & Mathew, K. (2013). Handling of Uncertainty – A Survey. *International Journal of Scientific and Research Publications*, Vol. 3, No. 1, 1-4.
Risk catalog, [labinf.fl.uni-mb.si]. Accessed 28 August 2015 on: http://labinf.fl.uni-mb.si/risk-catalog/doku.php?id=risk_catalog
Tokyo Gas CSR Report 2014 [*Tokyo Gas*], (2014). Accessed 10 September 2015 on: http://www.tokyo-gas.co.jp/csr/report_e/7_management/compliance.html