Supply Chain Risk Management Using Software Tool

Matotek Marija, Barać Ivan, Regodić Dušan

Singidunum University, 32 Danijelova St., 11000 Belgrade, Republic of Serbia, matotek@vts-zr.edu.rs; dregodic@singidunum.ac.rs

Grubor Gojko

Sinergija University, Raje Banjičića St., 76300 Bijeljina, Bosnia & Herzegovina, ggrubor@sinergija.edu.ba

Abstract: Risk management is an integrating part of every supply chain aspect. Unsuccessful risk management can have negative economic and ecologic consequences and cause total or partial lost in the business of a company. Supply Chain Risk Management (SCRM) technology helps managers plan for and handle disruptions in the supply chain. Companies that invest in the emerging field of SCRM technology are less likely to sustain costly supply disruptions or negative press because of the actions of their suppliers. In this paper a model of risk management in supply chain is suggested, according to the international standard ISO 31000:2009 recommendation. An automatic risk evaluation has been performed by software application and as a result 2393 individual risk assessments have been obtained. In this case study the levels of risk factors obtained by risk treatment have been accepted. In order to lessen the subjectivity of the analysts it is necessary to use the same methodology for risk assessment by more than one risk analysts and then to compare their results to provide an objective risk assessment, a key phase in risk management.

Keywords: risk; risk management; software tool; supply chain

1 Introduction

As a general answer to the question "What is management risk?" the theory offers [1] the following answer: "To many analysts, politicians and academics it is the management of the natural environment and of technology-generated macro-risks that appear to threaten our existence! In general, risk management can be defined as a life discipline which considers the likelihood of future events causing unwanted effects. However, risk may not be considered as an avoidable category.

According to the ISO 31000 standard risk management consists of risk identification, risk assessment, risk prioritization, and effectively allocate and using resources for risk treatment in order to minimize, monitor and control likelihood or impact of the unwanted events, and to maximize realization of the expected successes.

In theory, supply chains work as a cohesive, singularly competitive unit, accomplishing what many large, vertically integrated firms tried and failed to accomplish in years past. The difference is that independent companies in a supply chain are relatively free to enter and leave a supply chain relationship if these relationships are no longer proving beneficial; it is this free market alliance – building that allows supply chains to operate more effectively than vertically integrated conglomerates [2]. A supply chain risk appraisal process can help make strategic decisions and operational plans to reduce the quantity of supply chain defects [3]. The identified compliance issues require response strategies, in the form of developing policies and procedures, to address compliance risks effectively. Infrastructure and resources (including material, human, IT, financial, technical) have to be provided and assigned to enforce the program. To illustrate the high-complexity of compliance management, consider that, to manage for example "product liability compliance" the following business functions could be related: engineering, procurement, manufacturing, quality control, sales and distribution, and more. To ensure product compliance the organization needs a certain level of control across the entire supply chain [4].

Economic globalization and the resultant complexity of the supply chain network plus the uncertainty of the environment makes risk and vulnerability a major challenge to related firms [5]. The risk assessment segment in the supply chain management is a rather devalued research field. In this paper the authors will present a risk management model in supply chains. The preliminary results of the risk assessment shown in this paper, suggest that the software tool application in risk assessment can be useful, mainly for decreasing overall total risk. Thus, risk management is getting simpler and more effective requiring less bureaucracy.

2 Historical Perspective of Risk Management

Risk management has been familiar to humanity since ancient times. The authors of the article [6] reported that the first risk assessment was recorded with the Asipu group who lived in the Tigris-Euphrates valley in 3200 BC. They tried to make contributions to risk assessment in construction businesses, business start – ups, and even concerning marriage arrangements. The Asipu analyzed available risk factors suggesting alternatives and proposing the best solution for quantitative risk mitigation [6]. In 792 BC bottomry contracts were used in order to mitigate risk. This form consisted of three elements: loan, interest rate and risk premium. In

this period, the concept of general average was also developed, only to evolve into insurance concept. Apparently, insurance is one of the oldest forms of the risk mitigation strategy. The advance in probability theory development in the 17th and 18th Centuries made it an important tool which can be used for risk management. Since the nineteenth century, probability theory continues in many disciplines, using specific tools and methods from finance to system engineering disciplines.

3 Basic Elements of Supply Chains Management

According to [7], the supply chain is a set of physical elements, in which their activities and processes are related to their mutual interactions. The executive part of this chain consists of appropriate ways and rules of realization related to logistic activities and processes, and it is an operative part by its nature. The management of the executive part and determination of the fixed part of the supply chain both constitute the supply chain management used to define its performance (for example, costs and service levels). In [8], the authors developed the framework for supply chains management including three basic elements (Figure 1):

- supply chain structure (defining the key elements of supply chain which will be connected through business processes)
- business processes (defining the business processes used to connect certain elements of supply chain) and
- managing components (defining the level of integrated management for each business process).

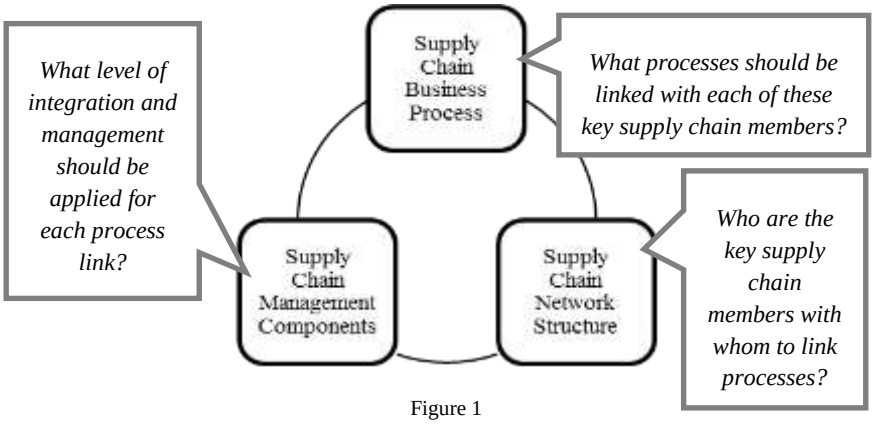


Figure 1
Supply chain management framework: Elements and key decisions [8]

Each of these elements is directly related to the degree of fulfillment of end-user demands, taking into account the key performance indicators. They refer to a relatively small number of critical dimensions of business which have a huge impact on the success in the market. Key performance indicators compare the efficiency and / or effectiveness of a system with standardized or target (desired) values. A well-defined set of performance indicators of the supply chain can help identify technological reserves in key logistics processes and their later utilization.

Companies have reacted to the apparent opportunities and threats of globalization through various global production practices that have increased supply chain complexity and various forms of risk. Through increasing supply chain integration, companies have attempted to manage this increased level of complexity. Supply chain integration has been identified as a key practice to manage supply chains and achieve superior performance [9].

4 Risk Taxonomy in The Supply Chain

Risk taxonomy in the supply chain is possible according to several criteria. According to the exposure area, the following assets are exposed to the risk:

- people,
- technologies,
- environment and
- business processes.

Risk management concept in the supply chain can be defined as exposure to the risky events that have negative impact to the supply chain operability and performances such as service level, costs or possibility of the fast response. The spectrum of the risky events that can affect supply chain operability is very large going from external risk factors (e.g. supply chain environment) to inter-organization and intra-organization risk factors. The consequences of these risk factors can be categorized according to duration, intensity and likelihood of occurrence as follows:

(1) from short-term to long-term;

(2) from small intensity ones to high intensity ones, and

(3) from very rare to very common ones.

From the logistic point of view, the interaction among supply chain members becomes more and more complex due to the growing uncertainty as a result of the new business models applied to increase logistic efficacy and competitiveness.

Therefore, with the main risk sources in the supply chains the following types of interactions can be identified:

(1) occurring between supply chain members and the environment, and

(2) occurring between individual members inside the supply chain.

The traditional method of management of these risks requires the engagement of additional material and time. However, what the companies really need, in the supply chain, is proactive risk management.

When, considering risk control tools, making decisions on appropriate measures for risk treatment and performing their implementation among partners, they become obvious complex tasks, even though within the supply chain a consistent risk management policy is present. In a supply chain, an internal audit entity can develop an appropriate risk management program providing risk assessment by continual monitoring and auditing. However, before a company can conceive a methodology for risk mitigation, the managers have to understand the risk categories, events and conditions that generate risks (Tab. 1). Therefore, using the knowledge about these key risk factors, the companies can choose the most efficient risk mitigation strategy. To mitigate risks by intelligent positioning and dimensioning without profit reduction is a great challenge for management.

Table 1

Risk categories and its expression in the supply chain

Risk category	**Risk expression**
Disorder/ interruption	Natural disaster. Business dispute. Supplier bankruptcy. War and terrorism. Dependency on one supply source, and alternative supplier response ability.
Delay	High utilization of the capacity on the chain source Supply source inflexibility. Bad quality and contribution on the chain source Border crossing or mode of transport change.
Systems	ICT infrastructure breakdown. ICT system integration or excessive networking. E-business.
Prediction	Incorrect prediction due to long terms, short life cycle, and small clients data base. “Bullwhip effect” or information distortion due to sale promotion, incentive, lack of visibility, and excessive demand during shortages of products.
Intellectual property	Vertical integration of the supply chain. Global market and outsourcing.
Procurement	Exchange rate risk. Percentage of the key components or raw materials that are supplied from one source. Large utilization of the industrial capacity. Long terms vs. short terms contracts.

Demand	Number of consumers. Finance strength of consumers.
Inventory	Products rate of obsolescence. Holding costs. Value of the products. Uncertainty of the supply and demand.
Capacity	Capacity costs. Capacity flexibility.

5 Supply Chain Risk Management – Case Study

This chapter summarizes the results of the case studies in which the process of risk management in supply chains is implemented in accordance with the recommendations of international, globally accepted, standards ISO 31000 : 2009, Risk management - Principles and guidelines.

Risk management process is a systematic application of management policies, procedures and practices of communication activities, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk [10].

Figure 2 shows the block diagram of the process of risk management. The case study did not discuss the following blocks: "Establishing the context", "Communication and consultation" and "Monitoring and review" because it was assumed that the risk management framework had already been established, including the specified sub-processes. Within the study, emphasis is given to the assessment of risk (comprising the steps of risk identification, risk analysis and risk assessment) and treatment of risk. For the automation purposes of the abovementioned sub – processes and the qualitative analysis the application, whose results were used solely for scientific purposes, was used.

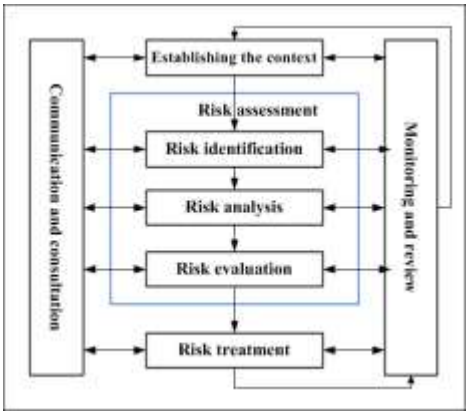


Figure 2
Risk management process (Adapted from [10])

Table 2 shows the basic concepts and definitions needed for a description of the risk management process. Most of the concepts and definitions have been taken from ISO 31000:2009 [10] standard, and the rest from ISO/IEC 27005 [11] which gives the recommendations for risk assessment in ISMS.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation [10].

The risk assessment used the statistics and numerical approximations or qualitative methods, defining the values on the basis of quality. As the output from the phase of the risk assessment, the obtained parameters were used in the treatment of stage risk (reducing the risk to an acceptable level). The control measures to be implemented in order to improve supply chain risk through treatment were identified.

Table 2
The basic terms and definition [10], [11]

Terms	**Definition**
risk	effect of uncertainty on objectives
risk management	coordinated activities to direct and control an organization with regard to risk
assets/ resource	the organization should allocate appropriate resources for risk management
threat/ risk source	element which alone or in combination has the intrinsic potential to give rise to risk
vulnerability	intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence
risk criteria	terms of reference against which the significance of a risk is evaluated
level of risk	magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood
residual risk	risk remaining after risk treatment
control	measure that is modifying risk
risk assessment	overall process of risk identification, analysis and risk evaluation
risk identification	process of finding, recognizing and describing risks
risk analysis	process to comprehend the nature of risk and to determine the level of risk
risk evaluation	risk evaluation process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
risk treatment	process to modify risk

5.1 Risk Management Methodologies

The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources.

Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy, be defined at the beginning of any risk management process and be continually reviewed [10].

Table 3 presents the basic concepts and criteria that are defined in the methodology for risk management, which is defined before the phase of risk assessment and cannot be altered during the phase of risk assessment and risk treatment. The validity of the methodology can be analyzed during and upon completion of the above two stages in risk management, and it can be changed for future risk assessment (the block diagram in Figure 1 "Monitoring and review").

Table 3 shows that the risk is calculated through the influence of the three characteristics of the supply chain (impact on confidentiality (e.g., information), integrity (of the supply chain as a whole) and availability (e.g., the services offered through the supply chain). In the considered case study, the risk actually represents the probability that a particular threat risk source will exploit the vulnerability of the assets / resource, which is demonstrated through the loss of confidentiality, integrity or availability of the supply chain.

Table 3

Risk management methodologies terms and criteria [10]

Term	**Description of criteria**		
T_v -threat value	(1-low; 2-medium and 3-high)		
V_v -vulnerability value			
$P = T_v \times V_v$ – probability P_l – level of risk	$\forall P \in \{1,2,3,4\} \Rightarrow P_l = P;$ $\forall P \in \{6,9\} \Rightarrow P_l = 5;$		
I_{vx} - impact value (x= confidentiality, integrity or availability)	(1- very low; 2- low; 3- medium; 4- high; 5- very high)		
$R_x = I_{vx} \times P_l$ - Risk (x= confidentiality, integrity or availability)	risk level	action	risk treatment
$1 \le R_x \le 2$	very low	not require any action	risk retention
$3 \le R_x \le 4$	low	required monitoring of risk	risk retention
$5 \le R_x \le 10$	medium	need some action and monitoring risk	risk retention
$12 \le R_x \le 16$	high	necessary actions	risk reduction
$20 \le R_x \le 25$	very high	necessary actions	risk reduction

The case study used a modified version of the software tools Hestia Risk (Croatian company that distributes Bluefield Ltd.), integrated software solution for managing risks by using a qualitative methodology, which is based on the application of international standards ISO 31000, and other related standards such as ISO / IEC 27005, ISO 22301 and others. The authors have taken advantage of the flexibility and parametrization software to adjust for risk assessment in SCM. The authors define a list of vulnerabilities, threats list, their relations, the key processes in the SCM, as well as measures to be implemented to mitigate the risk. In addition, this defines the method of risk assessment which is later used in the case study.

5.2 Risk Identification

The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis [10].

Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered [10].

5.2.1 Assets

Consideration should be given to the following: people, skills, experience and competence; resources needed for each step of the risk management process; the organization's processes, methods and tools to be used for managing risk; documented processes and procedures; information and knowledge management systems; and training programmes [10].

Figure 3 shows the review of 27 processes in supply chains, which are grouped into nine specific groups. Each process was analyzed individually in order to investigate the effect of the potential risks on confidentiality, integrity and availability. After analysis, each group processes were associated with certain risk groups.

5.2.2 Threats/Risk Sources

A risk source can be tangible or intangible [10]. Threats have the power to damage the information, assets, process or system. Threats may arise from natural or human origin and can be accidental or intentional. It should identify sources of accidental and intentional threats, as well as to estimate how their occurrence probability is. It is necessary to expect threats, because failure to do so may cause a risk to the organization. The level of threat is defining for each of the identified threats. This study deals with 73 different kinds of threats and risk sources according to confidentiality, integrity and availability in supply chains.

	IMPACTS		
	Confidentiality	Integrity	Availability
COMMUNICATION WITH THE REGION AND THE LEGAL PROCEDURES AND			
COMMUNICATION	2	2	3
COMPLIANCE WITH LEGAL PROCEDURES AND STANDARDS	3	2	3
DESIGN PROCESS			
DELEGATION OF AUTORITY	2	1	4
DEPARTMENTALIZATION	1	1	2
ESTABLISHING A RANGE OF CONTROLS	2	2	4
IDENTIFICATION AND ARANGEMENT OF JOBS	1	2	3
FINANCIAL MANAGEMENT			
JOBS OF ACQUISITION AND PLACEMENT OF FUNDS	3	5	3
JOBS OF FINANCIAL MANAGEMENT	5	4	3
JOBS OF PAYMENT AND LIQUIDATION	5	4	3
INFORMATION MANAGEMENT			
COLLECTION AND PROCESSING OF INFORMATION	4	3	4
INFORMATION USAGE	5	4	5
MATERIAL MANAGEMENT			
PLANNING OF MATERIALS	1	4	4
PRODUCTION CONTROLS	3	4	5
PURCHASE OF MATERIALS	1	2	3
STORAGE	1	3	4
PLANNING AND DEMANDS ANTICIPATION			
DISTRIBUTION PLANNING	4	5	3
PLANNING AND DEMANDS ANTICIPATION	4	4	2
PLANNING SECURITY STOCKS	3	2	1
SUPPLY NETWORK PLANNING	5	5	3
PRODUCTION PROCESS			
EXECUTION OD PRODUCTION	3	4	5
FINALISATION	3	4	4
PREPARATION OF PRODUCTION	3	4	5
RETURN PROCESSES			
REPLACEMENT	1	2	1
RETURN	1	1	1
THE TRANSPORT PROCESS			
LOADING	2	2	4
TRANSPORT	2	2	4
UNLOAD	2	1	4

Figure 3
List of supply chain processes

5.2.3 Vulnerabilities

Vulnerability is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats [11]. The vulnerability factors of supply chains may be classified into five groups [12], which may be complemented by two further risk sources [13]:

- disturbances in the value-added process (manufacturing, purchasing, storage, delivery, scheduling),
- control (non-existence or failure),

- demand (lack of information, unpredictability, unexpected events),
- supply (unreliability, lack of capacity, vis major),
- environmental (economic and political events, accidents, natural disasters),
- enterprise structure (if non-conformance with enterprise processes) and
- a supply or sale chain or a "network" composed of several individual companies (disturbances in communication or uncertainties in cooperation).

These seven points embrace virtually all security perspectives and thus may serve as a foundation for our security model with respect to enterprise functional risk analysis [14].

The study deals with 67 different types of vulnerabilities in supply chain processes.

5.2.4 Group of Risks

After the analysis, the threats were divided into four risk groups (human factor, processes, system and external factors). Each group process is associated with one or more risk groups. At the stage of risk assessment, risks for each process are analyzed by each individual threat that is associated with the risk groups.

5.2.5 Controls

Controls include any process, policy, device, practice, or other actions which modify risk. Controls may not always exert the intended or assumed modifying effect [11].

The study defined 76 – control measures to be applied in order to reduce the level of risk to an acceptable one after the risk treatment phase. Control-measures can be organizational, procedural and technical.

5.3 Risk Analysis

Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk [8].

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified.

Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account [10].

5.4 Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered. Decisions should take account the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk. Decisions should be made in accordance with legal, regulatory and other requirements [10].

This application was used for automatic evaluation of risk, and as a result 2393 individual risk assessments were obtained. Risk assessments are divided according to levels of risk (risk level "5" - 1084 risks; level "4" - 709; the level of "3" - 537; the level of "2" – 50; level "1" - 13 risk).

The methodology for risk management in the supply chain was used to define that only "4" and "5" risk levels would be treated, which makes the total of 1793 different risks in this study with all controls - measures for reducing risk used up in the risk treatment phase. Figure 4 shows the list of risk levels.

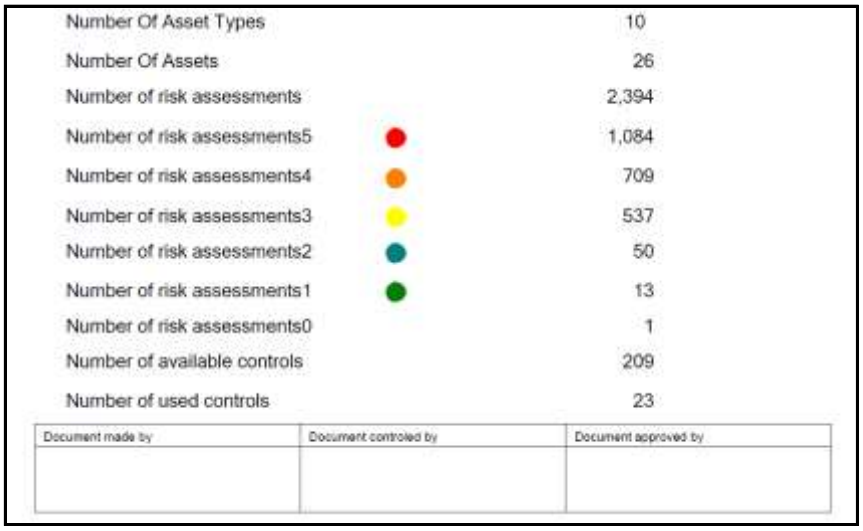


Figure 4
List of risk levels

5.5 Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls [10].

In the risk evaluation phase, it was determined that all the available control – measures would be used in order to reduce the risks levels "4" and "5". The principle that the application of each control – measure reduces the level of individual threats for value 1 was used.

Figure 5 shows part of the risk treatment plan. By applying the defined control / measures of risk treatment plan the risk levels "4" and "5" are reduced.

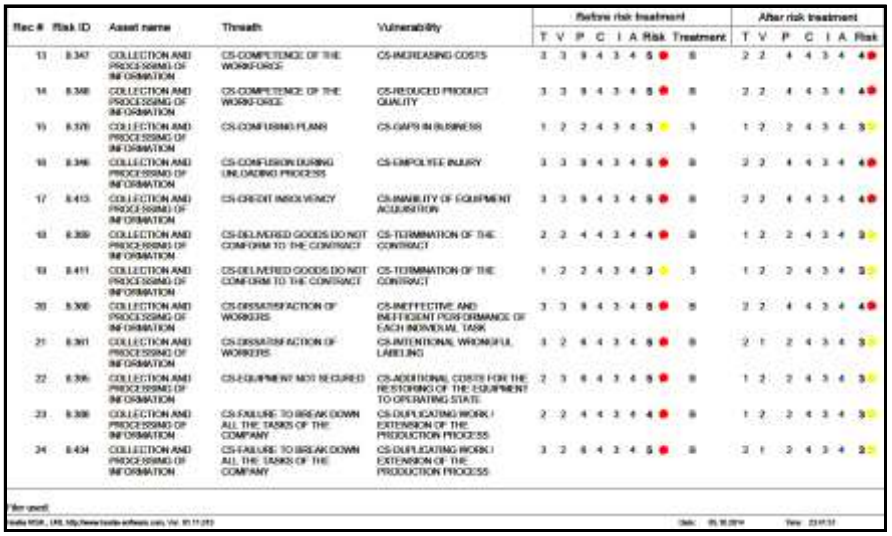
ISO 27001:2005 Controls			Treatment ID	Budget	Pearson responsible	Implementation dates		Finished
Clause	Section	Control				Start	End	
	10.1.3.	EDUCATION OF EMPLOYEES	2.410	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.4.	ESTABLISHMENT OF THE PRICE FOR CERTAIN PRODUCTS THAT ENABLE THE IMPLEMENTATION OF BUSINESS PLANS	176	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.5.	FORMATION OF A UNIFIED INTERNAL REGISTER TO STORE THE ORIGINAL COPY OF THE CONTRACT, ANNEXES, DECISIONS, STATEMENTS	194	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.6.	FORMING A WORKING UNIT	20	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.7.	DO NOT USE INFORMATION ON BUSINESS SECRETS FOR THE PURPOSE OF ADVERTISING THROUGH PUBLIC SOCIAL NETWORKS	82	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.8.	INNOVATION IN P / D AND MONITORING TRENDS	80	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.9.	INTERNAL CONTROL	20	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.10.	EXPLORE THE MARKET AND CONSUMER NEEDS	4	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.11.	RESEARCH AND ADAPTING TO MARKET NEEDS	85	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.12.	MARKET RESEARCH	60	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.13.	EXPLORE THE MARKET AND CONSUMER NEEDS	75	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.14.	CREATING A STRATEGIC PLAN FOR INTER-INSTITUTIONAL COOPERATION	163	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.15.	DEVELOPMENT, ADOPTION AND COMPLIANCE WITH THE FINANCIAL PLAN FOR EACH YEAR / QUARTER	586	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.17.	CLEARLY DEFINED DESCRIPTION OF THE POSITION, RIGHTS AND OBLIGATIONS OF EMPLOYEES	137	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.19.	CLEARLY DEFINE PRIORITIES	530	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	
	10.1.20.	CONTROL OF CONGRUENCE OF THE GOODS AND DISPATCH NOTES	97	100,000.00 €	Ivan Banac	4.10.2014	31.12.2014	

Figure 5
Risk treatment plan

Figure 6 shows part of the risk list before risk treatment, and risk – treated values after applying controls – measures, i.e., the reduction of threat levels for value 1.

After the risk treatment phase had been completed, 85 risk levels "5" remained (reduced by 999 risks) and 203 risk levels "4" (reduced by 506 risks).

By analyzing the results of the risk level "5", and after completion of the risk evaluation phase the following processes were identified as the most critical in the supply chain: "distribution planning", "production control" and "supply networking planning" - 15 risks; "information usage" - 13 risks; "execution of production", "jobs of acquisition and placement of funds" and "preparation of production" - 9 risks each at level "5".



Rec #	Risk ID	Asset name	Threath	Vulnerability	Before risk treatment								After risk treatment						
					T	V	P	C	I	A	Risk	Treatment	T	V	P	C	I	A	Risk
13	8.347	COLLECTION AND PROCESSING OF INFORMATION	CS-COMPETENCE OF THE WORKFORCE	CS-INCREASING COSTS	3	3	3	4	3	4	5	5	2	2	4	4	3	4	4
14	8.348	COLLECTION AND PROCESSING OF INFORMATION	CS-COMPETENCE OF THE WORKFORCE	CS-REDUCED PRODUCT QUALITY	3	3	3	4	3	4	5	5	2	2	4	4	3	4	4
15	8.370	COLLECTION AND PROCESSING OF INFORMATION	CS-CONFUSING PLANS	CS-GAPS IN BUSINESS	1	2	2	4	3	4	3	3	1	2	2	4	3	4	3
16	8.346	COLLECTION AND PROCESSING OF INFORMATION	CS-CONFUSION DURING UNLOADING PROCESS	CS-EMPOLYEE INJURY	3	3	3	4	3	4	5	5	2	2	4	4	3	4	4
17	8.415	COLLECTION AND PROCESSING OF INFORMATION	CS-CREDIT INSOLVENCY	CS-INABILITY OF EQUIPMENT ACQUISITION	3	3	3	4	3	4	5	5	2	2	4	4	3	4	4
18	8.359	COLLECTION AND PROCESSING OF INFORMATION	CS-DELIVERED GOODS DO NOT CONFORM TO THE CONTRACT	CS-TERMINATION OF THE CONTRACT	2	2	4	4	3	4	4	5	1	2	2	4	3	4	3
19	8.411	COLLECTION AND PROCESSING OF INFORMATION	CS-DELIVERED GOODS DO NOT CONFORM TO THE CONTRACT	CS-TERMINATION OF THE CONTRACT	1	2	2	4	3	4	3	3	1	2	2	4	3	4	3
20	8.368	COLLECTION AND PROCESSING OF INFORMATION	CS-DISSATISFACTION OF WORKERS	CS-INEFFECTIVE AND INEFFICIENT PERFORMANCE OF EACH INDIVIDUAL TASK	3	3	3	4	3	4	5	5	2	2	4	4	3	4	4
21	8.361	COLLECTION AND PROCESSING OF INFORMATION	CS-DISSATISFACTION OF WORKERS	CS-INTENTIONAL WRONGFUL LABELING	3	2	4	4	3	4	5	5	2	1	2	4	3	4	3
22	8.356	COLLECTION AND PROCESSING OF INFORMATION	CS-EQUIPMENT NOT SECURED	CS-ADDITIONAL COSTS FOR THE RESTORING OF THE EQUIPMENT TO OPERATING STATE	2	3	4	4	3	4	5	5	1	2	2	4	3	4	3
23	8.368	COLLECTION AND PROCESSING OF INFORMATION	CS-FAILURE TO BREAK DOWN ALL THE TASKS OF THE COMPANY	CS-DUPLICATING WORK / EXTENSION OF THE PRODUCTION PROCESS	2	2	4	4	3	4	4	5	1	2	2	4	3	4	3
24	8.434	COLLECTION AND PROCESSING OF INFORMATION	CS-FAILURE TO BREAK DOWN ALL THE TASKS OF THE COMPANY	CS-DUPLICATING WORK / EXTENSION OF THE PRODUCTION PROCESS	3	2	4	4	3	4	5	5	2	1	2	4	3	4	2

Figure 6

List of risk, before and after risk treatment

The next step includes deciding as to whether to accept the estimated levels of risk or to implement the new controls / measures; next, it is necessary to re – execute the risk evaluation phase. In this study, the levels obtained by risk evaluation were accepted.

Conclusions

Nowadays, decreasing the frequency and probability of risks occurring – from internal and environmental processes – can greatly reduce tensions within companies. Those reductions prepare conditions for formulating proper and operational strategies, thus, securing the continuation of those companies within the global markets.

Handling or managing risk is becoming a necessary and an objective assumption of business success and successful, risk management should provide continuous existence of the system. The documentation resulting from the risk management process enables the process of accreditation and authorization of the risk management process. Risk management should not be linked only to organizations, but it should apply to all individual activities of short-term or long-term nature.

The concept of supply chain management brings additional risks, which in accordance with the objective of management increases the level of integration and coordination among supply chain partners, and should be dealt with concurrently. These risks include the internal risks in the supply chain, such as co-operative and operational risks.

Risk management should be extended from the financial and corporate perspective, to the domain of logistics and inter-organizational cooperation. However, although it sounds simple, the problems to be solved are:

- the challenge of transforming risk management from legal obligations into a tool for planning;
- identification of hidden risks and their dissolution;
- quantification and the probability of the level of damage;
- application of bottom - up risk management in supply chains in order to avoid overloading the top management, as is the case in the top - down management.

Segments of the supply chain simulation by stochastic modeling in order to support mapping of risk impact assessment of different risk parameters variation may represent an elegant but a complicated task. Therefore, supply chain partners need to develop an understanding of the importance of the process of identification of the structure of key risks. Efficient security and the protection of the supply chain include basic standards for physical security, access control, personnel security, education and training, procedural security, IT security, business partners, as well as the safe transfer from point of origin to the final destination within the supply chain [15].

This paper describes the process of risk management in the supply chain by application of software tools. The disadvantage of the methodology used in this case study is the use of qualitative methods for risk assessment, which entails a certain degree of subjectivity of risk analysts and greatly depends on their experience. To minimize this subjectivity, it is necessary to use the same methodology, to have the risk assessed by several analysts and to compare their results to ensure a more objective assessment which is the key phase in the supply chain risk management.

This is an assignment project that was conducted at the University Singidunum (Belgrade, Serbia) by PhD students and their mentors. Contribution of authors can be seen in the detailed description of the risk assessment process in SCM, an adaptation of a software tool Hestia Risk, enabling the assessment of the risks as much as possible automate, accelerate and make more objective. Outputs from these case study can be used for educational purposes, as well as real-SCM system. Further research projects will be expanded by creating new Web applications to risk assessment in SCM, based on experiences and results of conducted case studies.

References

[1] F. H. Kloman (1999) Risk Management Agonistes, *Risk Analysis Journal*, 10(2): 201

[2] J. Wisner, K. C. Tan, G. Leong (2015) *Principles of Supply Chain Management: A Balanced Approach*, Cengage Learning

[3] Zurich Insurance Company, *Supply Chain Risk Assessment*, Zurich, Switzerland (2010)

[4] P. Benedek (2012) *Compliance Management – a New Response to Legal and Business Challenges*, Acta Polytechnica Hungarica, 9(3): 135

[5] Y. Yu, W. Xiong, Y. Cao (2015) A Conceptual Model of Supply Chain Risk Mitigation: The Role of Supply Chain Integration and Organizational Risk Propensity. *Journal of Coastal Research: Special Issue 73* - Recent Developments of Port and Ocean Engineering: 95

[6] V. T. Covello, J. Mumpower (1985) Risk Analysis and Risk Management: An Historical Perspective, *Risk Analysis*, 5(2): 103

[7] M. Maslarić (2014) *Development of Model for Logistics Risk Management in Supply Chains*, PhD Thesis, Faculty of Technical Sciences, Novi Sad, Serbia

[8] M. Cooper, D. Lambert, J. Pagh (1997) Supply Chain Management: More Than a New Name for Logistics. *The International Journal of Logistics Management*, 8(1): 1

[9] F. Wiengarten, P. Humphreys, C. Gimenez, R. McIvor (2015) Risk, Risk Management Practices, and the Success of Supply Chain Integration, *International Journal of Production Economics*

[10] International Organization for Standardization, *ISO 31000 – Risk management – Principles and guidelines* (2009)

[11] International Organization for Standardization, *ISO/IEC 27005-Information technology – Security techniques – Information security risk management* (2011)

[12] M. Christopher, H. Peck (2004) Building the Resilient Supply Chain, *International Journal of Logistics Management*, 15(2): 1

[13] G. Smith, K. Watson, W. Baker, J. Pokorski (2007) A Critical Balance: Collaboration and Security in the IT-enabled Supply Chain, *International Journal of Production Research*, 45(11): 2595

[14] P. Michelberger Jr., C. Lábodi (2012) After Information Security – Before a Paradigm Change (A Complex Enterprise Security Model), *Acta Polytechnica Hungarica*, 9(4): 101

[15] M. Matotek, D. Regodić (2015) Human Resource Risk Management in Supply Chain, *Dyna Management*, 3(1): 1