POLISH ACADEMY OF SCIENCES
COMMITTEE OF TRANSPORT

ARCHIVES OF TRANSPORT

QUARTERLY

ARCHIWUM TRANSPORTU

Indeks 201901

ISSN 0866-9546

volume 24
issue 1
Warsaw 2012

POLISH ACADEMY OF SCIENCES
COMMITTEE OF TRANSPORT

ARCHIVES OF TRANSPORT

QUARTERLY

ARCHIWUM TRANSPORTU

ISSN 0866-9546

volume 24
issue 1
Warsaw 2012

Contents

THE ARCHIVES OF TRANSPORT

VOL. XXIV NO 1 2012

10.2478/v10174-012-0003-7

Selected Tools for Risk Analysis in Logistics Processes

Ewa Kulińska*

Received January 2011

Abstract

As each organization aims at managing effective logistics processes, risk factors can and should be controlled through proper system of risk management. Implementation of complex approach to risk management allows for the following:
– evaluation of significant risk groups associated with logistics processes implementation,
– composition of integrated strategies of risk management,
– composition of tools for risk analysis in logistics processes.

1. Introduction

Risk analysis – upon its assessment, it is necessary to have in mind two basic parameters: the financial consequences and the probability of an event – it closes the summary of all the risks of a given venture, project or company and it evaluation. Usually risk assessment takes the form of a figure or table – different environments use different names there (risk map, risk matrix, risk model, risk profile) – but they all are reduced to one thing: bring all the risks to a common denominator, and comparing this at first sight seems to be impossible. In terms of mapping, literature presents almost the same achievement as in the processes mapping.

2. Risk Management in Logistics Processes

Effective managing risk should be carried out upon close examination of the factors affecting its occurrence in logistic processes. Factors risk has outside cha-

* The Opole University of Technology, Waryńskiego 4 Street, Opole, Poland

racter sticking in surrounding enterprise and internal, associated with its activity. It is possible to distinguish external factors like in groups presented in Table 1.

Table 1

External risk factors of logistics processes

FACTOR	MEANING	KIND OF THE RISK
Macroeconomic	The states associated with the economic policy	– Change in purchasing domestic products; – Change in market value parameters: currency exchange rates, market interest rates, changes in market values securities; – Country's budget deficits and public debt.
Regulatory	Associated with changes in regulation of law and tax	– Changes in regulation law; – Changes in regulation tax.
Globalization	Liberalization of international markets	– Increased competition – limited possibility of customer choice, – Risk dependence – adverse phenomena in one country or industry through specific reactions, can lead to crisis and bring negative effects.
Demand	Associated with increased customer care	– Increase in customers significance; – Increase in customers awareness; – Offer of product/services according to customers expectations.
Product	Associated with broad product offer of competing companies	– Widening range of products available on markets; – Necessity of simultaneous considering different types of risk in frames of the same product.
Other external factors	About diversified specificity	– Phenomena about the demographic capacity e.g. aging societies; – Natural disasters; – Thefts; – Terrorist attacks.

Source: [10]

Apart from all factors mentioned above, that characterize by external character, risk processes are affected by internal factors, which can be grouped under two categories [10]:

- Human factor, decisions and behavior of employees of the organization affecting it's functioning, resulting not only from the classification, but also from character, honesties and professional approach to duties.
- Technical factor, which has the influence on risk processes is noticed on time, making enterprises conditional on electronic systems data processing, completion of the production, etc.

At present, companies face requirements concerning shortening of testing period – for example, from the time of project development to the time of product introduction to market usually takes several month. In these new conditions, organizations can lower costs of individual transactions, but from the other side they are exposed to such threats, like an equipment malfunctions, thefts, hackers activity and computer viruses, that can ruin the system of the register accountant which is fully computerized. The role of technical factor in to generate risk processes

and to discernible in the context of dynamical developing of systems of Internet sale which should be appropriately protected, so that customers shall not be afraid of unauthorized trades made by intruders. Presented range of factors depicts risks completion of logistic processes and illustrates how complex and multifaceted is the management when the enterprise melts in the face threats which result from acting few impulses simultaneously, having a completely different specificity. It is impossible to underestimate the role that effective risk management in maximizing the enterprise profits, shaping its competitive position and realization of other majorities of smaller purposes.

A crucial task is, therefore, a risk evaluation accompanying the completion of logistic processes. This analysis is performed due to the suitable system which monitors risk, and is associated with individual areas constituting base activities. This system is designed to identify opportunities and threats, based on the evaluation, in definite areas and aims to minimize the risk.

The identification of the risk generated in areas of logistic processes is the first stage of analysis. Individual types of the risk are identified according to the accepted ranking. The method of the identification of risk groups processes are presented in the Table 2.

Table 2

Identification of logistics processes risk

TYPES OF LOGISTICS PROCESSES	RISK GROUPS
completion of customer orders	inappropriate time of orders completion, fall in the number of orders, defect in the orders completion
completion of the logistic customer service	underdeveloped solutions, equipment failure, lack of experience
offering additional values for the customer	changes in value
lead to a reduction in the price range, product and service	worsening of quality, loss in elite customers
accepting and shipment of products due to the completion of transport, trans-shipment, storing, packing and marking products	failure to perform orders, fall in the number of orders, lack of integration between processes production, distribution and the transport
ensuring required level of the logistic customer service	inappropriate level of provided services, process service in the insufficient step orientated to the customer, failure to perform contracts by the carriers, logistics operators, etc., failure to perform orders by suppliers, system of the quality control, deliveries performed on time
analysis and forecast of market--connected logistics situations	disabled system of the logistic information
identification of customer preference and expectations in scope of the logistic service	problem with identifying key customers or buyers groups, inaccurate identification of customer needs,

Continued Table 2

identification of logistic market segments	inappropriate offer of logistic benefits to the section, lack of integration of all activities associated with given logistics section
design and development of logistics strategies	failure in the selection of management strategies channels of distribution delayed appearance of new product
developing a set of components and structure of logistics-mix	decisions concerning the service level, planning demand, issuing orders, forecasting of supply, location of compositions and warehouses, division into sales and packing units, decisions concerning the type of transport, scheduling, service level, planning demand
protecting and development classification staff within the scope of competence in the design and completion of logistics processes	inappropriate planning of production
protecting the quality of providing services	inappropriate level of provided services
protecting the quality of purchase and sale products	wrong estimation of the materials quality, mistake in the assessment of suppliers, incorrect suppliers choice, imperfect test evaluation of the quality of finished products
management of products flow through development processes, transport, trans-shipment, storing, packing and marking goods	lack of integration of internal and external supply chain management,
the issue of disposal orders concerning realization and customers orders	delays in information flow, unintelligibility information, incorrect interpretation of orders
identification of purposes and development assumptions of the performance of customer service	inefficient ability of partners to response to unexpected orders (low elasticity, slow adaptation to the requirements)
protecting ability and potentials to create added value	lack of innovative solutions, no strategy of implementing plans into practice, limits in propagating slogans – lack of realization, the impact of promotion and advertising
the examination and development of logistics infrastructure	changes in supply conditions, inappropriate planning of production, lack of flexibility in the manufacturing process
development of the IT technology	lack or insufficient flow of information on demand from outlets and key customers, inappropriate methods of forecasting demand, problems within the scope flow information
shaping and keeping relationships and relation with the environment	imbalance between customers expectations and possibilities of all supplies chain links, the incomprehension of market needs, lack of integration with customers, changes in demand, affairs with contracting parties, competing on the market, market potential,

Continued Table 2

waste, packages, permanently damaged products management	lack of recycling of waste distribution, insufficient ecological awareness, lack of system regulations of dangerous waste, lack of legal requirements concerning stockpiles, lack of waste selection
protecting sale and completion trades	mistakes in planning demand, keeping inessential supplies
protecting financial logistics aspects (realization of customers accounts)	mistake in estimating customer profitability, market's estimate service changes in prices, underestimation of anticipated costs

Source: [1], [2], [3], [5], [6], [7], [10], [11], [14], [15], [16], [18], [20], [21].

The identification allows for determining the level of risk to which enterprise is exposed to. Upon recognizing and estimating the risk level it is necessary to supervise it. Therefore, two approaches are possible: passive or active. Managing passive risk management establishes the ability of logistic process to its generation and determines the acceptable level in the future. Active management of risk consists, that is used by the logistic process fact existence of risk and deliberate conducting of operations generating risk in order to gain extra profits. The second approach is more difficult for enterprises but also brings better results. That is why, active management of risk doesn't lead to undertaking too risky tasks, it is necessary to establish the level of acceptable risk. In the risk analysis the control is placed as the last. This control should be conducted regularly, additionally at moments preceding increase in risk level.

Analysis within the scope of planning, described analysis helps to develop long-term strategy. It serves the fundamental purpose of policy development which was described by the managing staff. Projecting the financial result at establishing influence is a basic task of various positive and negative risk factors in the company's policy.

Paying attention to risks identification allows to the following [10]:

- precise identification of risk in the given area;
- establishing the most important issues to be taken into consideration in strategy development;
- establishing the processes that are worth allocating to spend greater financial resources for the purpose of securities before appearance of undesirable phenomena;
- establishing the processes that are worth to allocate greater financial resources;
- establishing the method to limit the effects of threat;
- establishing the method to reduce effects of threat;
- working out common, transparent criteria of evaluation, possibility of comparison and abilities responding to risks concerning specific area of essential processes;

– defining relations between the effectiveness of risk management processes and optimum structure processes in the horizontal organization

Tools enabling the analysis of determined risk factors are essential.

3. Overview of Risk Maps

One of the simplest tools to create risk maps is 2×2 matrix showing risk as a function of the probability of occurrence of an adverse event and the effect volume (impact) of its appearance on the process course, schematically illustrated in the Fig. 1.

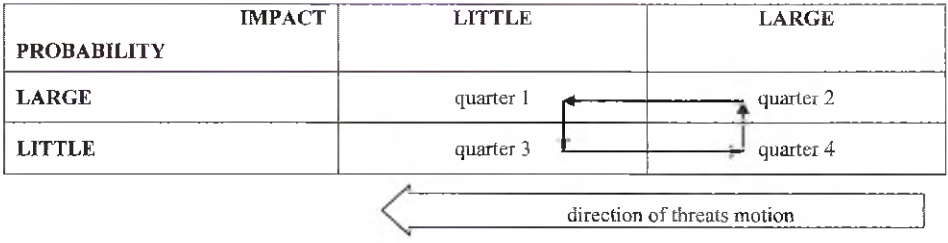

Fig. 1. Matrix 2×2
Source: [10], [17].

2×2 matrix is one of the simplest techniques of risk management. It shall be completed upon previous identification of potential threats and elaboration of their list, then we enter each of them depending on the probability of appearance and the volume of potential losses that may result in the appropriate quarters of the matrix. The following parts of this technique determine [17]:

– 1st quarter – an area with high risks probability and little consequences. Dangerous for the process course may be the accumulation of many threats in this part of the matrix,
– 2nd quarter – an area with high risks probability and simultaneous large negative impacts on the process,
– 3rd quarter – risks area of little probability of occurrence of the little negative consequences for the process. This is the area of the least dangerous threats. The purpose of the risk management process is the process of relocation of all possible threats in the direction of the quarter,
– 4th quarter – the area with little probability of occurrence and large consequences adverse for the process. Threats from this area may be rare but their impact is very detrimental to the process course.

More developed is the matrix of the probability and threats impacts – the Fig. 2. It constitutes a development of 2×2 matrix concept. It is characterized by increased going into subject of probability assessment and its effects.

Probability	Effects				
	Minimal	Small	Middle	Large	Extreme
Very high 0,8-1					
High 0,6-0,8					
Middle 0,4-0,6					
Small 0,2-0,4					
Very small 0-0,2					

Fig. 2. Matrix of probability and threats results
Source: [10], [17].

Probability	Effects				
	Minimal	Small	Middle	Large	Extreme
Very high 0,8-1				3	1
High 0,6-0,8					4
Middle 0,4-0,6			1		4
Small 0,2-0,4		3			2
Very small 0-0,2		2	5	5	

Fig. 3. Risk changes distribution as a result of preventive actions
Source: [10], [17].

Individual threats are entered into the corresponding fields. After entering all identified threats in the process, you should plan preventive actions aimed at removing the most serious threats. The ultimate aim of management of process risk is the relocation of threats most probable and most dangerous to other areas of the matrix – Fig. 3. These activities form the basis of management of processes risks.

Appropriately modified matrix of probability and risk effects can be used to calculate the total tangible risk of a process. The modification consists in ordering to individual links the threats importance expressing the volume of given threat probability and the volume of its potential effects.

Each identified threat that may arise during the process of implementation should be attributed to an adequate matrix box. Then, you should multiply the importance of a given box [WZ] by the number of the threats [LZ] assigned to it, and then you should sum up all numbers received in this way and divide by the number of threats. The obtained numerical value is the total amount of risk [RC] of the analyzed process.

$$RC = \Sigma[(WZ * LZ)/LZ] \quad (1)$$

Probability	Effects				
	Minimal	Small	Middle	Large	Extreme
Very high 0,8-1	2,0	3,5	7,0	8,0	9,0
High 0,6-0,8	1,5	2,0	5,0	7,0	8,0
Middle 0,4-0,6	1,2	1,8	4,0	5,0	7,0
Small 0,2-0,4	1,0	1,5	3,0	4,0	5,0
Very small 0-0,2	0,5	1,0	1,5	3,0	4,0

Fig. 4. Risk weights for a matrix of probability and threats effects
Source: [10], [17].

Thanks to the introduced importances we can also evaluate the effectiveness of planned preventive actions. For that purpose, after the relocation of risks in the matrix, we should re-calculate the total risk of the project and compare it with the original result. With these calculations, you will be able to obtain a numerical value expressing the change at the risk level caused by preventive actions.

Another form of a matrix to map the risks was suggested by Heeg [4]. His technique consists of three stages: risk identification, risk assessment and selection. The basis of the presented technique is to identify the risks specific to the process. According to the author, the identification of risk sources may be carried out by various methods. One of them commonly used is the technique of the analysis of the packets of tasks described, for example, using WSB (*Work Breakdown Structure*). The example is presented in the Table 3.

After identification of threats of activities groups and going into subject of potential sources of risk that may adversely affect the process, it is necessary to determine the probability of specified risks occurrence (Table 3, column 3). Then you should determine the expected costs associated with claim settlement (Table 3, column 4). The last column of table 3 presents likely costs of levelling damage.

Calculated in this way the volume of the likely costs should be sorted descendingly and specify a group of tasks for which the sum of the volumes in the column 5 of Table 3 shall constitute 75% of the total probable costs of the analyzed process risk [4]. Specified set of tasks should become the object of special attention to the managers of the process. With regard to them we should consider the possibility of protective actions. Other activities groups, not placed in the table may be adopted without any special precautionary measures.

There is a technique proposed by Maylor, relating to the effects analysis of failures [4]. In this technique there are considered three parameters characterizing all tasks being part of the process. Each of these parameters must be expressed in numbers.

Table 3

The analysis result

TASK OR GROUP OF TASKS	POTENTIAL THREATS	PROBABILITY OF OCCURRENCE	LIVELLING COSTS [PLN]	PROBABLE COSTS [PLN]
Database modelling	redundancy	0,2	6000	1200
	improperly designed relationships	0,3	8000	2400
Integration of performed basedata procedures	Lack of transmission of all data between functions	0,4	6000	2400
	incompatibility of declared variables	0,3	6000	1800
Computer network construction	problems with wiring assembly in the building	0,6	5000	3000
Server installation	Problems with connection to domain	0,2	600	120
	problems with the transfer of users' accounts	0,6	900	540
data entry into the web site database	introduction of erroneous data	0,6	1100	660

We adopt the scale of points for all parameters. The popular volumes are:

- the importance of the implementation failure of the problem (breakdown), the scale from 1 to 10 [ZN],
- the probability that failure will not be noticed – i.e. that the action was realized, but the person controlling is not able to properly assess whether if it is correct or not – the scale from 1 to 10 [PN],
- the probability of failure occurrence during the implementation of a given action – the risk of breakdown occurrence – the scale from 1 to 10 [PW].

Each of the parameters must be considered individually. The aim of the presented analysis is to calculate the overall risk for a given task being the function depending on three parameters characterized above. Risks in demand are calculated in the following dependence:

$$R = ZN * PN * PW \tag{2}$$

The higher value in the last column, the greater the risk associated with a given task. For activities of the highest risk we should take additional measures in order to mitigate potential damage.

The described technique of estimation and the risk classification is used in practice for several years, particularly in the IT sector. It fulfills well its task when

Table 4

Analysis of failure effects for the sample design tasks

TASK NAME	BREAKDOWN SIGNIFICANCE	PROBABILITY OF UNNOTICING BREAKDOWN	PROBABILITY OF BREADOWN OCCURRENCE	RISK (PRODUCT)
database modeling	3	4	3	36
integration of database's performed procedures	4	4	4	64
construction of IT network	3	1	2	6
server's installation	3	1	2	6
data implementation to www network service	4	2	4	32

Source: [4], [10].

there is a necessity to choose one of the few manners to implement the selected activity. Then, the application of the analysis of the failures effects makes legible the selection of a profitable policy option.

Mapping the risk is reduced mainly to two parameters [19]:

- maximum effect of threat occurrence,
- probability of threat.

The effect should be a reflection of the consequences of the worst of real existing scenarios, while the probability is the ratio depending on the nature of the threat as a phenomenon and the environment in which the supply chain functions. These two parameters are not only helpful in quantifying, but prove indispensable in constructing risk maps. Their aim is to reduce all risks to a common denominator, so that their comparison becomes possible.

Constructing maps of the risk occurring in a given process of the supply chain consists in introducing the specific threats on a system of coordinates, where X coordinates correspond to the value of the probability [expressed, e.g. in %] and Y coordinates result [expressed, e.g. in €]. Figure 5 presents an example of a risk map.

The risk placing in two opposite corners of the presented map clearly requires different responses. The threats in the upper right corner require immediate and active action, leading to unambiguous reduction of the possible effects and the probability of the event. Whereas, the threats in the lower left corner does not bring with them serious consequences and their probability of occurrence is insignificant. Phenomena placed in the middle field of the map on the left require treatments to reduce the possible effects and construct emergency plans. The lower right corner

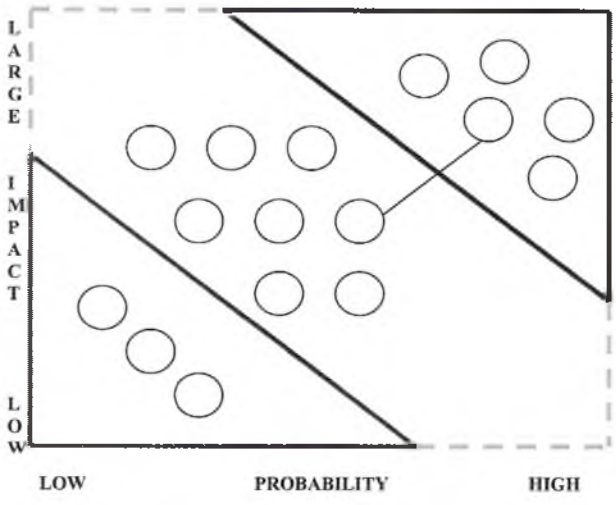

Fig. 5. Risk map for logistics process
Source: [8], [9], [19].

presents the risk associated mostly with imperfection of processes, organization and management culture. They require long-term, systemic approach ordering co-operation and action within and between different activities in the processes. The risks placing closer to each of the corners of the matrix require separate response strategies (*risk treatment*) [13]:

- risks in the upper right corner require promptly and active action leading to simultaneously reduce the possible effects and the probability of the event, also we may consider the abandonment of the company activity, which connects with such risks,
- risks in the upper left corner, as they are unlikely, they are less urgent than those previous and require treatments aiming to reduce the possible effects and construct emergency plans (reference to crisis management),
- risk in the lower right corner of the frictional forces occurring in each company: imperfections of processes, organization, management culture requiring a long-term, systemic approach, ordering the daily work of the company.

Risk maps creation gives a precise picture of the threats in a given area of the process implementation. It eliminates the necessity to browse each time the whole catalogue of the negative phenomena, which becomes significant in case of the necessity to undertake fast actions while breakdown [13]:

- complex areas and functions within the company may require more specialized analytical tools;
- processes mapping;
- *flow charts* – analysis of the amount and type of materials of passing through the company infrastructure business in terms of the mutual influence on the outcome (efficiency) and production bottlenecks;

– methods of HAZOP (Hazard and Operability Studies), HAZID, Fault Tree Analysis, Root Cause Analysis method BowTie, analysis of ALARP.

The risk map used in the internal audit shows the distribution (profile) of risks for the company, resulting from a careful analysis of individual risks. Risks lying above matrix are more acute in terms of the consequences, financial losses, and located closer to the right side are more probable.

IMPACT						
	EXTREME	5	10	15	20	25
	SERIOUS	4	8	12	16	20
	MIDDLE	3	6	9	12	15
	LOW	4	4	6	8	10
	SLIGHT	1	2	3	4	5
		RARE	UNLIKELY	AVERAGE	PROBABLE	ALMOST CERTAIN
		PROBABILITY				

Fig. 6. Matrix of scoring-based risk assessment
Source: [13]

Given these two regularities, it is relatively easy to identify critical risks for an enterprise – those near the upper right corner and the risks relatively unlikely but extremely painful, as well as the risks common but relatively minor.

The analysis demonstrated in the Fig. 6 is facilitated by the imposition of colours on the map created in that way. The gray determines the low risk, scores from 1 to 4 – a level of tolerance for risk, so the level of risk that we are able to accept in a given year. The light gray colour – average risk, the score from 5 to 10 – there will be undertaken additional control mechanisms, there will be built processes diagrams for the purpose of the proper management of these risk areas and the elimination of undesirable phenomena. The dark gray colour – high risk, the score from 12 to 25 – in the first place you should manage these areas, eliminate the disorderly phenomena, they are some of the most important areas of the organization activity or areas having an impact on key objectives pursued by the organization [13].

Within the framework of risk management, you should develop a timetable for the process implementation and determine persons responsible for processes

implementation. Not undertaking activities could lead to exposure of the process to irreparable financial losses and damage connected with the organization functioning. Therefore, risks identification in a proper time and their effective management may improve its functioning. You should not believe that the creation of a single risk map creation is sufficient because it is a dynamic image – like the whole company – and the risk introduced on it is moving. The continuity of risk management consists in this, which requires constant monitoring and improvement.

Mapping processes in small and medium enterprises are relatively simple. However, in large enterprises is essential not only to support software but the mapping and risk management.

At the most developed markets as far as culture and technology of risk management is considered, software offer supporting the different stages and risk management systems is very large. There are 21 companies – mainly from New Zealand, England and Australia – offering 27 different applications. While deciding on the selection of software for the British Ministry of Defense more than 200 items were examined [19]. They are often applications based on MySQL server and workstation with access to web servers using the network and a simple browser. Options available in these applications form a cross-section of all functions of risk management, taking into account the initial risk analysis, risk measurement, creating register and many others. The relevant functions include those functions which enable tracking threats and exchange of information about them up to the automatic generation of reminders or alarms to the risk owners in case of exceeding the time limit, or the level of risk.

These programmes meet the legal requirements, standards, recommendations or good national practice, or international, as well-known examples: SOX, BaselII, IS017799, COSO, Turnbull, AS/NZS 4360 or less common ASX Guidelines (Australia), Cobit, COSA, and COCO (US), HIPAA, Bill C6 (PIPEDA) and the Gramm-Leach-Bliley Act (Canada) or the King Report (Republic of South Africa) [19].

The software is sold in different versions for different numbers of users, ranging from single-user version to solutions of customer/server based on ODBC technology (Open Database Connectivity), or solutions based on web network. The consequence of diversity is also considerable differences in purposes and complexity degree of these packages. This software can be as an example, exclusively an electronic risk register or provide support for basic risk management functions, or may be enriched with additional components concerning issues, such as so-called *compliance* (compliance with the law requirements), internal audit, so-called *knowledge base,* speculative risk analysis (success/failure), project management support, construction of quantitative risk models or the costs analysis of that risk.

The examples of programmes are as follows [19]:

- *Enterprise Risk Assessor, Methodware*, New Zealand,
- *Risk Register, Noweco*, New Zealand,
- *J-Port, Portiva*, Canada,
- *Securac, Acertus*, Canada,

- *Know Risk, CorProfit*, Australia,
- *Risk Decisions, Predictl*, Great Britain,
- *International Security Technology, CORA*, US.

The main advantages emphasized by software producers that process automation, actions automation, common to several users of the database, the possibility to configure and monitor key risk factors or automatic operation of cost and benefit analysis. The principal advantages from the perspective of managers are the following: the ability of great number of programmes to adapt flexibly to the nature and size of the company, consolidation, monitoring and documention and reporting of risk information, to the flexible visualization of the risk or filter risks or multilingualism of several versions [19].

These programmes are divided into several modules- but the division is only logical (a package divided into functions) or physical (individual modules).

The configuration module is used to describe the unique context of the company and its environment. At this stage, prioritizing of risk areas, defining terminology, description of the fields occurring in the programme, the classification of risks and calibration of scales. Some of them allow you to create relations between business goals and risks, and most of them can import information from existing systems in the company database. The risk identification module – registers the results of the risk identification and allows you to assign the owner to the particular risks. The assessment module (usually qualitative) of the risk is used to determine the effect and the probability according to previously defined scales at the stage of configuration.

The result of risk evaluation (assigning measurement to them) is the risk map – programmers showed at this stage the greatest imagination offering a range of different versions of risk maps: maps that describe the risk with numerical values, classic maps of 5×5 squares, developed (up to 10×10 squares), dynamic risk maps showing in one diagram how a given risk evolves over time or at the end of the risk map settling down small business units (branches, divisions, sub-processes) in the risks of large business units. These programmes offer mostly the possiblity to differentiate between the original risk and this risk already controlled. The differentiation of these risks is expressed in change of one or both risk parameters.

The minimization module of the risk control allows you to define aims and then track corrective actions, their status or priority. The module is conjuged with the function of accounting the risk owner or the risk control programme performer for their actions and decisions, and the function of tracking *key risk indicators* status with the possibility of e.g. determining the upper and lower tolerance threshold while exceeding them so-called alerts are activated.

The *Risk Register* programme of the NOWECO company supports for example, up to four separate techniques of dealing with risk: prevention actions, transfer, crisis actions and actions aiming at restoring the business operation.

The monitoring module automatically monitors the status (including the status and the size) of the risk and the status of progress and effectiveness of operations

results controlling the risk. The function mentioned above acts as a sensor. The reporting module offers customarily from from tens up to even hundreds of ready designs of the report, which can be freely modified by users. The most frequent forms of reports are te following: PDF, html, MS Excel, Word, Access. The reporting module obviously includes advanced functions of graphics, filtering and risks sorting, their owners, the threats balance of elements of the company assets. It is understandable that with such diversity it is difficult to clearly define the boundaries between modules and compulsory and optional functions. Less common modules – we call them optional, are briefly characterized below.

Optional events register module (damage, accidents, breakdown) takes into account the effects of both financial (measurable) and non-financial events and allows you to connect with each other and to prepare preventive measures (response to loss trends). The optional consolidation module helps to check and compare risks in different parts or the company branches, or their changes over time. It facilitates the unambiguous identification of the priority risks in interdisciplinary terms (e.g. when different parts of the company or the holding run different type of business activity). Several other interesting additional features that appear to be most useful are the following [10]:

- *Enterprise Risk Assessor, Methodware*: change of risk over time presented on a dynamic risk map, any changes in field names and their descriptions (prompts), the introduction of secure access and diversification of access rights for users;
- *Know – Risk, CorProfit*: change of the screen appearance and free defining what information is visible, which is not, own filters building to sort information;
- *Securac, Acerturs*: analysis simulator of '*what if*'.

The offer existing at the moment is very rich, but there are no equivalents in Polish. Unfortunately, to make the right choice will not be an easy task.

4. Conclusions

In the scope of risk management it is necessary to develop a schedule of implementation and to appoint people responsible for a system of risk management. Failure to undertake activities can be a result of exposing logistics processes to huge financial losses and those connected with the organization operation. Therefore, the identification of risk factors in due time can influence on the improvement in functioning of logistics processes and the company as well.

You should not surrender to the illusion that the creation of risk map is sufficient, as this is dynamic picture – as the whole company – and applied risk factors moves. This is the essence of risk management that requires the repeatability.

References

1. Blaik P.: Logistyka. Koncepcja zintegrowanego zarządzania. PWE, Warszawa 2001 (wydanie II).
2. Christopher M.: Sieci i logistyka. Zarządzanie relacjami w ramach łańcucha dostaw, [in book:] Zarządzanie Łańcuchem Dostaw, materiały konferencyjne LOGISTICS '98, Katowice 1998, tom I.
3. Coyle J., Bardi E., Langley C.: The Management of Business Logistics, West Publishing Company, St. Paul 1996.
4. Frączkowski K.: Zarządzanie projektem informatycznym, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2003.
5. Hammer M.: Reinżynieria i jej następstwa. Jak organizacje skoncentrowane na procesach zmieniają naszą pracę i nasze życie, PWN, Warszawa 1999.
6. Krawczyk S.: Logistyka w zarządzaniu marketingiem, AE, Wrocław 1998.
7. Krawczyk S.: Zarządzanie procesami logistycznymi, PWE, Warszawa 2001.
8. Kulińska E.: Ocena wpływu logistycznej struktury horyzontalnej na efektywność funkcjonowania przedsiębiorstw produkcyjnych, Wydawnictwo Politechniki Warszawskiej, Warszawa 2003.
9. Kulińska E.: Zarządzanie ryzykiem a optymalizacja łańcucha dostaw, Monografia Instytutu Inżynierii Zarządzania Politechniki Poznańskiej, Poznań 2006.
10. Kulińska E.: Aksjologiczny wymiar zarządzania ryzykiem procesów logistycznych. Modele i eksperymenty ekonomiczne. Oficyna Wydawnicza Politechniki Opolskiej – *w druku.*
11. Kulińska E.: Meaning of orientation on processes in creation and realization of the value added, Foundations of Management, vol.2/2009.
12. Kulińska E.: Risk management versus value of logistics processes, [in book:] Advanced Logistics Solutions, (ed. by:) V. Modrak, Presov 2008.
13. Kulińska E., Dornfeld A.: Zarządzanie ryzykiem procesów. Identyfikacja – Modelowanie-Zastosowanie, Wydawnictwo Politechniki Opolskiej, Opole 2009.
14. Kulińska E.: Risk management relation surplus value change of logistics processes, [in book:] Invence – Inovace – Investice, od recese k prosperitě, Vydavatel Vysoká Škola Báňska, Republika Czeska, Ostrava 2009.
15. Kupczyk A., Korolewska-Mróz H., Czerwonka M.: Radykalne zmiany w firmie od reengineeringu do organizacji uczącej się, Wydawnictwo Prawno – Ekonomiczne Infor, Warszawa 1998.
16. Manganelli R., Klein M.: Reengineering. Metoda usprawniania organizacji, PWE, Warszawa 1998.
17. Pawlak M.: Zarządzanie projektami, Wydawnictwo Naukowe PWN, Warszawa 2006.
18. Perechuda K.: Zarządzanie przedsiębiorstwem przyszłości – koncepcje, modele, metody. Formy i narzędzia skutecznego zarządzania przedsiębiorstwem, Agencja Wydawnicza Placet, Warszawa 2000.
19. Rudnicki R.: Zarządzanie ryzykiem dla członków zarządu, www.rudnicki.pl.
20. Rummler G., Brache A.: Podnoszenie efektywności organizacji. Jak zarządzać „Białymi Plamami" w strukturze organizacyjnej? PWE, Warszawa 2000.
21. Zieniewicz K.: Współczesne koncepcje i metody zarządzania, PWE, Warszawa 1999.