ACTA SCIENTIARUM POLONORUM *Oeconomia 7 (4) 2008, 137–145*

PURPOSE OF THE RISK EVALUATION[1]

Štefan Majtán, Daniela Rybárová
University of Economics, Bratislava, Slovak Republic

Abstract. Different people will have different views of the impact of a particular risk – what may be a small risk for one person may destroy the livelihood of someone else. The first stage of a risk analysis is to identify threats. The next step is to work out the likelihood of the threat being realized and to assess its impact. One approach to this is to make the best estimation of the probability of the event occurring, and to multiply this by the amount it will cost to set things right if it happens. This gives a value for the risk.

Key words: Risk Evaluation, Risk Tolerance, Risk Appetite

INTRODUCTION

Risk management ensures that an organization identifies and understands the risks to which it is exposed. Risk management also guarantees that the organization creates and implements an effective plan to prevent losses or reduce the impact if a loss occurs. **The risk evaluation supports in clearly defining insurance needs**. Insurance is a valuable risk-financing tool. Few organizations have the reserves or funds necessary to take on the risk themselves and pay the total costs following a loss. The risk evaluation can determine appropriate threshold level, when the risk or event should be escalalated to the insurance. Purchasing insurance, however, is not risk management. Risk management also addresses many risks that are not insurable, including brand integrity, potential loss of tax-exempt status for volunteer groups, public goodwill and continuing donor support. An effective risk management practice does not eliminate risks. However, having an effective and operational risk management practice shows an insurer that organization is committed to loss reduction or prevention.

[1]This article is a part of VEGA project number 1/4579/07
Corresponding author – Adres do korespondencji: Štefan Majtán, Ekonomická univerzita v Bratislave, KPH, e-mail: majtan@dec.euba.sk; Daniela Rybárová, Ekonomická univerzita v Bratislave, KPH, e-mail: rybarova@dec.euba.sk

ROLE OF RISK EVALUATION IN RISK MANAGEMENT PROCESS

The risk evaluation is one of steps of the risk management process. The purpose of the risk evaluation is to categorize each identified risk using defined risk categories and parameters, and determine its relative priority. Each risk is evaluated and assigned values according to defined risk parameters. The assigned risk parameter values can be integrated to produce additional measures, such as risk exposure, which can be used to prioritize risks for handling. Collectively, the activities of risk evaluation, categorization, and prioritization are sometimes called a risk assessment or risk analysis. The risk management process consists of a series of steps that, when undertaken in sequence, enable continual improvement in decision-making. The risk management process is described for example in **Risk Management Guide for Small Business[2].** It guides the operator through the steps of understanding the environment in which the business operates, identifying, analyzing and evaluating risks, and considering the options for treatment. Steps of the risk management according to this guide are Communicate and consult, Establish the context, Identify the risks, Analyze the risks, Evaluate the risks, Treat the risks and Monitor and review.

Fig. 1. illustrates the components of each step of the risk management process and illustrates the cyclical nature of the process.

In accordance with Risk management guide for small business risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria, and deciding whether these risks require treatment. **The result of a risk evaluation is a prioritized list of risks that require further action.** Organization should be decided whether risks are acceptable or need treatment. Low or tolerable risks may be accepted. Acceptable means the business chooses to accept that the risk exists, either because the risk is at a low level and the cost of treating the risk will outweigh the benefit, or there is no reasonable treatment that can be implemented. A risk may be accepted for the following reasons:

- The cost of treatment far exceeds the benefit, so that acceptance is the only option.
- The level of the risk is so low that specific treatment is not appropriate with available resources.
- The opportunities presented outweigh the threats to such a degree that the risk is justified.
- The risk is such that there is no treatment available, for example the risk that the business may suffer storm damage.

The evaluation of risks is needed to assign a relative importance to each identified risk and is used in determining when appropriate management attention is required. Often it is useful to aggregate risks based on their interrelationships and develop options at an aggregate level. Evaluate identified risks using defined risk parameters. Each risk is evaluated and assigned values according to defined risk criteria. Risk criteria allow a business to clearly define unacceptable levels of risk. Conversely, risk criteria may include the acceptable level of risk for a specific activity or event. At first the risk criteria may be bro-

[2]© 2005 Global Risk Alliance Pty Ltd jointly with NSW Department of State and Regional Development ISBN 0 7313 32490, www.smallbiz.nsw.gov.au

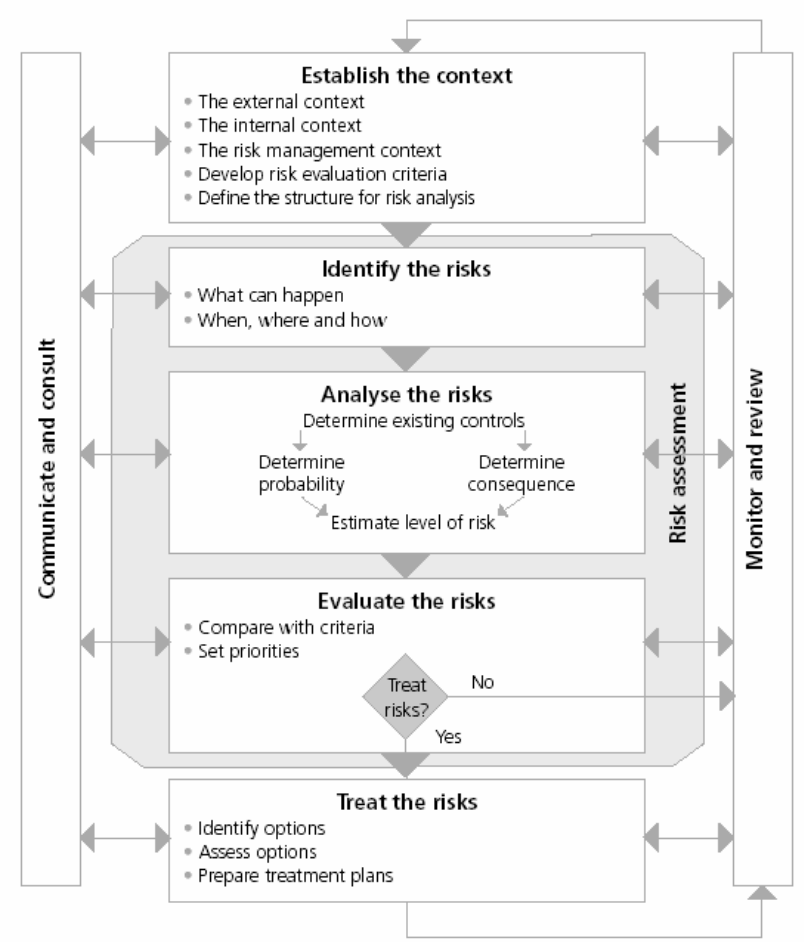

Fig. 1. Details of the risk management process
Rys. 1. Schemat procesu zarządzania ryzykiem
Source: Risk management guide for small business. © 2005 Global Risk Alliance Pty Ltd jointly with NSW Department of State and Regional Development.
Źródło: Risk management guide for small business. © 2005 Global Risk Alliance Pty Ltd jointly with NSW Department of State and Regional Development.

adly defined and then further refined later in the risk management process. These criteria determine if it requires treatment or control. Where a risk exists that may cause any of the objectives not to be met, it is deemed unacceptable and a treatment strategy must be identified. Risk management guide for small business provides a number of examples of risk criteria for a project (table 1).

Risk evaluation is often a difficult and time-consuming task. Specific expertise or group techniques may be needed to assess risks and gain confidence in the prioritization. In addition, priorities may require revaluation as time progresses.

Table 1. Examples of risk criteria and their objectives for a project in small business
Tabela 1. Przykłady kryteriów ryzyka i wynikających z nich przesłanek dla projektów małych firm

Risk criterion	Objective
Safety	Safety must be upheld at all times. No injuries or fatalities will be accepted
Financial impact	Project costs should remain within allocated budget
Media exposure	The project must ensure that the reputation of the business is protected from negative media exposure
Timing	The project must be completed within the contractual timeframe
Staff management	This project must utilise existing staff skills. Where a particular skill set is not available, sub-contracting may be considered
Environment	The project must operate within requirements of environmental legislation and be consistent within the business environmental commitment

Source: Risk management guide for small business. © 2005 Global Risk Alliance Pty Ltd jointly with NSW. Department of State and Regional Development.
Źródło: Risk management guide for small business. © 2005 Global Risk Alliance Pty Ltd jointly with NSW Department of State and Regional Development.

RISK TOLERANCES AND RISK APPETITE

Risk tolerance looks at acceptable/unacceptable deviations from what is expected. **Risk appetite** looks at how much risk a company is willing to accept. Organization must consider the amount of risk it is prepared to tolerate. This will vary according to the perceived importance of particular risks. Organization maybe prepared to take comparatively large risks income areas and none at all in others, such as risks to health and safety.

Defined risk tolerance need:
- Decide or define the acceptable level of risk for each activity
- Determine what is unacceptable
- Clearly identify who is responsible for accepting risk and at what level.

Risk appetite by Mark Carey[3] is a term that is frequently used throughout the risk management community, but it seems that there is a lack of useful information on its application – outside of financial risk areas or other risks that can easily be translated into financial terms. Risk appetite, at the organizational level, is the amount of risk exposure, or potential adverse impact from an event, that the organization is willing to accept/retain. Once the risk appetite threshold has been breached, risk management treatments and business controls are implemented to bring the exposure level back within the accepted range. Mark Carey recommends to define a organization's risk appetite and determine the acceptable level of risk to answer the following questions:
- Where do we feel we should allocate our limited time and resources to minimize risk exposures? Why?
- What level of risk exposure requires immediate action? Why?

[3]Mark Carey is CEO of DelCreo, Inc. www.delcreo.com, DelCreo, Inc. is an enterprise risk management company.

– What level of risk requires a formal response strategy to mitigate the potentially material impact? Why?
– What events have occurred in the past, and at what level were they managed? Why?

Company, DelCreo, has developed a methodology and strategic approach that helps organizations, as well as the security, risk and control functions contained therein, develop and articulate their risk appetite. The key deliverable in this process is the risk appetite table [http://www.delcreo.com/delcreo/free/docs/RiskAppetiteTable.pdf]. The Risk Appetite Table has Impact table, Likelihood table and Risk appetite table.

At first in developing the organisation's risk appetite is to **identify who the key stakeholders** are. Stakeholders can be any person, group or entity that can place a claim on the organisation's attention, resources or output, or is affected by that output. Stakeholders tend to drive decision-making, metrics and measurement, and, of course, risk appetite. They may be internal or external – don't neglect stakeholders that have a direct impact on your salary and performance reviews! Once stakeholders have been identified, list the interests, benefits and outputs that stakeholders demand from your organisation, such as:

– Shareholder value
– Compliance with regulations
– Product safety
– Privacy of personal information

At second in developing the organisation's risk appetite is **identification of key risk indicators** is a three step process:

- Identify and understand value drivers that may be relevant for your business or function. Typically this will involve breaking down the value drivers to the level that will relate to your program.
- Select the key risk indicator metric to be used.
- Determine appropriate thresholds for each key risk indicator.

The risk appetite table is only a risk management tool. It is not the sole decision making device in assessing risk or events. At all times, professional judgment should be exercised to validate the output of the risk appetite table. Also, it is critical that the tables should be reviewed and evolves as the program and the overall business model matures.

Once the development of the risk appetite table is completed, there is still a lot of work ahead. It needs to do the following things:

- Validate the risk appetite table with your management team.
- Communicate the risk appetite table to business units, and your peers within the security, risk and control functions of your organisation.
- Develop incident management and escalation procedures based on your risk appetite
- Test your risk appetite table. Does it make sense? Does it help you determine how to manage risks? Does it provide a useful framework for your team?

In accordance with second author [Miller] the purpose of the risk evaluation is to identify the inherent risk of performing various business functions. Audit resources will be allocated to the functions with the highest risk

The two primary questions to consider when evaluating the risk inherent in a business function are:

- What is the probability that things can go wrong? (the **probability** of one event)
- What is the cost if what can go wrong does go wrong? (the **exposure** of one event)

Risk is evaluated by answering the above questions for various risk factors and assessing the probability of failure and the impact of exposure for each risk factor. **Risk** is the probability times the exposure.

The risk factors inherent in business include the following access risk, business disruption risk, credit risk, customer service risk, data integrity risk, float risk, legal and regulatory risk, financial/external report misstatement risk, fraud risk, physical harm risk. These risk factors cause potential exposures. The potential exposures include (but are not limited to):

– financial loss
– legal and regulatory violations/censorship
– negative customer impact
– loss of business opportunities
– public embarrassment
– inefficiencies in the business process

The evaluation should not consider the effectiveness of the current internal control environment. The evaluation should focus on the risks and exposures inherent to the function being evaluated. However, while performing the risk evaluation, the organization should consider what controls are needed in order to minimize, if not eliminate, the risks and exposures.

Table 2. Definition of scope of the business functions under evaluation
Tabela 2. Definicja zasięgu ocenianych funkcji biznesu

ACCESS RISK	Probability	Exposure
Access risk refers to the impact of unauthorized access to any company assets, such as customer information, passwords, computer hardware and software, confidential financial information, legal information, cash, checks, and other physical assets. When evaluating access risk the nature and relative value of the company's assets need to be considered.	High	High
	Medium	Medium
	Low	Low
	N/A	N/A
BUSINESS DISRUPTION RISK	Probability	Exposure
Business disruption risk considers the impact if the function or activity was rendered inoperative due to a system failure, or a disaster situation. Consideration is given to the impact on Company customers as well as other Company operations.	High	High
	Medium	Medium
	Low	Low
	N/A	N/A

Source: Miller J. - Miller.Jim@amstr.com; http://www.auditnet.org/docs/BusRiskAnal.doc
Źródło: Miller J. - Miller.Jim@amstr.com; http://www.auditnet.org/docs/BusRiskAnal.doc

ILUSTRATION OF PROJECT MANAGEMENT ASSESSMENT IN LARGE FIRM

Project management assessment (PMA) is a diagnostic self-assessment tool and will show the current status of the proposal or the project: **strengths and weaknesses of processes** and **workflows.** It will support the project manager in defining further actions to improve his project. Project management assessment incuding:

- **Opportunity / Risk Management** provides room for manoeuvre and risk-conscious increase of company value.
- **Project Controlling** including obligatory approvals and monthly reports to ensure permanent transparency and steering of projects.
- **Limit of Authority Process** including Risk Review Board as „supervisory body" of projects.

The Limit of Authority Process ensures that all sales opportunities are systematically and adequately reviewed at each key stage in their development during the sales process. The main objectives of the Limits of Authority (LoA) are to:

- ensure **acceptable project results and avoid non-conformance costs** later
- assign **bid resources** only to those bids with high and realistic chance of winning
- ensure conformance with the **business strategy and portfolio**
- contribute to the management of a **well balanced project portfolio**
- ensure the proper **identification/ management of risks** and complexity of an engagement
- ensure that the proposed **solution architecture is deliverable** and its **costing is realistic**
- follow the process defined for approvals and investments of Siemens.

Each project has to be categorized. The project category determines the approval level and the approval body – as well as further reports (monthly reports, annual reviews). The categorization has to be done with the „project categorization sheet".

CONCLUSIONS

Risk management provides a clear and structured approach to identifying risks. Most managers tend to think that having performed risk identification; they have done all that is needed. Ppurposed of the risk evaluation is ensure having a clear understanding of all risks allows an organization to measure and prioritize them and take the appropriate actions to reduce losses. Risk management has other benefits for an organization, including:

- Saving resources: Time, assets, income, property and people are all valuable resources that can be saved if fewer claims occur.
- Protecting the reputation and public image of the organization.
- Preventing or reducing legal liability and increasing the stability of operations.
- Protecting people from harm.
- Protecting the environment.
- Enhancing the ability to prepare for various circumstances.
- Reducing liabilities.
- Assisting in clearly defining insurance needs.

Table 3. Examples of risk class classification for a project in Siemens
Tabela 3. Przykłady klasyfikacji ryzyka w projekcie Siemens

	Project:			**Risk Class (RC)**		
			Comment	**3 Country**	**2 Verticals**	**1 BV**
	Commercial					
C1	Project Size Absolute	One-time Project	TEUR TCV/OV	<5’000	>= 5’000	>= 10’000
		Operation & Outsourcing business	TEUR TCV/OV	<30’000	>= 30’000	>= 100’000
C2	Project Size Relative	One-time Project/ Operation & Outsourcing business	Average contract volume (annual) in percentage of Annual Country Revenue (ACV)	<20%	>=20% to <=40%	>40%
C3	Fixed Price Portion	One-Time Project	TEUR TCV/OV	<2’500	>2’500 to < 5’000	>= 5’000
C4	Take-Over of People *)	FTE	Employees	<20	>=20 to <= 100	>100
C5	Maximum Negative Cash Exposure		TEUR	<= 2’000	>2’000	>= 5’000
C7	Project Profit		% Project Profit Margin	>5%	< 5%	< 5%
					and	and
			TEUR TCV/OV		> 3’000 to < 5’000	=> 5’000

Source: By internal materials - ep@ss Modified account system SAP by Siemens.
Źródło: Na podstawie dokumentacji wewnętrznej - ep@ss Modified account system SAP by Siemens pm@ siemens.

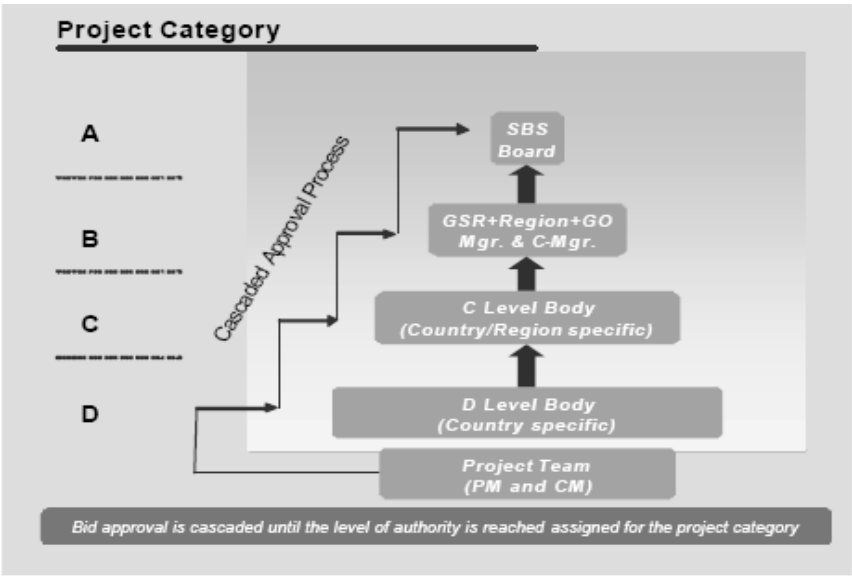

Fig. 2. Illustration of the project category and the approval level
Rys. 2. Schemat kategorii projektu iI akceptowanego poziomu ryzyka
Source: By internal materials – SIS Global Project Categorization Tool.
Źródło: Na podstawie dokumentacji wewnętrznej – SIS Global Project Categorization Tool.

REFERENCES

Bruce T. Barkley: Project Risk Management. McGraw-Hill, New York, 2004. ISBN 0-07-143691-X
http://www.auditnet.org/docs/BusRiskAnal.doc
http://www.delcreo.com/delcreo/free/docs/RiskAppetiteTable.pdf
Internal materials – SIS Global Project Categorization Tool
Miller J. - Miller.Jim@amstr.com
Risk management guide for small business. © 2005 Global Risk Alliance Pty Ltd jointly with NSW Department of State and Regional Development ISBN 0 7313 32490

PRZESŁANKI OCENY RYZYKA

Streszczenie. Ludzie w różnoraki sposób spostrzegają siłę poszczególnych ryzyk – co może stanowić niewielkie ryzyko dla jednej osoby, może zniszczyć życie innej osobie. Pierwszym etapem analizy ryzyka jest identyfikacja zagrożeń. Kolejny etap polega na określeniu prawdopodobieństwa wystąpienia zagrożenia oraz jego stopnia wpływu. Jednym sposobem realizacji tego etapu jest jak najlepsza estymacja prawdopodobieństwa wystąpienia zdarzenia oraz pomnożenie wartości kosztów jakie zostałyby poniesione w przypadku wystąpienia zdarzenia. W ten sposób otrzymujemy wartość ryzyka.

Słowa kluczowe: ocena ryzyka, tolerancja ryzyka, akceptowany poziom ryzyka

Zaakceptowano do druku – Accepted for print: 27.12.2008