Erasmus+

Partnerships to ensure Risk Management in practice (PERM)

Introduction to risk management

Main principles of the risk management process

D. van der Waal & V. Versluis

2017

This text is composed by D. van der Waal and V. Versluis in cooperation with A.F. de Wild. Part of this was translated with the help of S.C. Hassels Mönning and F. van der Werf. A.F. de Wild is applied research professor at the Research Centre for Business Innovation at Rotterdam University of Applied Sciences. All others are lecturers at the School of Financial Management at Rotterdam University of Applied Sciences.

Part of this text was made available by an Erasmus+ grant for Project Partnerships to ensure Risk Management in practice (PERM).
Project number: 2015-1-LV01-KA203-013436

Table of contents

Introduction 1
Chapter 1 History of risk management 3
Chapter 2 Basic concepts 5
2.1 Risk management 5
2.2 Cause and effect 7
2.3 Opportunities and threats 7
Chapter 3 Risk management process 9
3.1 Risk management process 9
3.2 COSO framework 10
Chapter 4 Internal environment and objectives 13
4.1 Internal environment 13
4.2 Objectives 14
Chapter 5 Risk identification 17
5.1 Identification of risks 17
5.2 Tools for identification 19
Chapter 6 Risk assessment 23
6.1 Risk assessment 23
6.2 Modelling risks 24
Chapter 7 Risk evaluation 31
7.1 Prioritising risk 31
7.2 Kinney method 32
7.3 Evaluation with a risk map 34
Chapter 8 Risk response and control measures 37
8.1 Risk response 37
8.2 Control measures 39
Chapter 9 Information, communication and monitoring 45
9.1 Information and communication 45
9.2 Monitoring 46
9.3 Risk policy 47
Chapter 10 Real examples of risk management 49

10.1 Hydro One 49
10.2 University of California 50
10.3 Rio Tinto 50
Concluding remarks 53
List of references 55

Introduction

This text describes the main principles of every step of the risk management process, along with problems and opportunities that arise from this process. The focus will be on Enterprise Risk Management. By following the various steps of the risk management process, an organisation can create awareness of the risks it faces and will be better able to make responsible decisions to control risks.

Nowadays, many organisations are being held accountable for their risk management (processes). This accountability can be applied on a national (for example Code Tabaksblat in The Netherlands) or international level (for example COSO II and Basel II). These companies have to prove that they are in control.

In addition to all kinds of regulations, the turbulence in the financial markets has shown the importance of sound risk management. Structured measures used to control risks will reduce uncertainty and will eventually result in better company performance.

Chapter 1 of this reader will show a short history of risk management. A start on the theory will be made in chapter 2, which focuses on a number of key terms used in the risk management profession. Chapter 3 will link these terms to the risk management process. The various specific parts of this process will be extensively covered in chapter 4 to 9. In chapter 10 three practical examples of successful risk management will be discussed, which will show some specific benefits of risk management.

Chapter 1 History of risk management

One of the first attempts to manage risk dates back to the 17th or 18th century. Japanese rice farmers made agreements with buyers to deliver them a specific amount of rice on a certain date for an already specified price. This is interesting for the farmer, as he knows someone will buy his produce, thereby taking away some of the risk of having produced too much or too little rice. There is also a reason to do this for the buyer, as he knows how much the rice will cost, thereby removing the risk of a possible price increase. In modern times we can recognise this promise as a futures contract in the financial market. In the centuries since, risk management developed much further, but was mainly still applied to the financial and insurance area.

Starting in the 1980s, some large US banks established departments specialised in financial risk management, which indicates the growing importance of risk management. In the 1990s some scandals happened at several institutions and large losses were incurred. One of these scandals happened in 1995 at Barings Bank, a large British bank, where the disapproved actions of one person, along with an earthquake caused the bank to collapse and incur a loss of around 1 billion US dollars. The impact of this scandal could not be exclusively attributed to financial risks, as an employee and a natural disaster were key factors in this risk.

It took scandals, such as at Barings Bank, for risk management to be adopted more widely than just the financial departments and also include risks that originate elsewhere within or outside of the organisation. This is where Enterprise Risk Management (ERM) finds its roots and this is also when a new senior management position emerged at many organisations, the CRO, or Chief Risk Officer. In 2002 the Sarbanes-Oxley act was enacted, which requires publicly traded companies in the US to report on the reliability of their internal controls. In 2004 Basel II was published, which describes the economic capital banks need to hold in order to cover impacts from risks. Both Sarbanes-Oxley and Basel II showed the urgency of risk management for

large organisations. Furthermore, in the same decade several risk management frameworks, standards and guidelines were published. These frameworks, standards and guidelines describe how organisations should approach enterprise-wide risk management, by establishing a structure with criteria, methods and processes to use. One of these frameworks, COSO, is the framework that will be used as a starting point for this book on risk management.

Chapter 2 Basic concepts

This chapter will describe the key terms of the risk management process. The definition of a risk and the importance of objectives will be described, but also other important key terms like cause and will be discussed.

2.1 Risk management

A risk is an uncertain event with consequences for an objective. Risk management is the process by which we try to manage the uncertainty surrounding the objectives. The purpose of the risk management process is to ensure that these objectives are attained.

There is an ongoing debate about the role risk managers ought to play in practice. The opponents of specialised risk managers indicate that these specialists are unnecessary in an organisation. The management of risks is a task of the line managers and adequate risk management is just a matter of good organisation.

In reality the presence of risk managers is usually experienced as unpleasant as these persons would have opposing interests to the relevant department and thus the line managers involved. In this way the presence of risk managers would be counterproductive in realising the objectives of the department or organisation as a whole. Line managers are only interested in achieving the goals on which they will be assessed and for which they will be rewarded. Line managers are responsible for the risks at their department and have good knowledge of most risks because they have to deal with customers and suppliers on a regular basis and know exactly what could go wrong in practice. The task of the line managers is to incorporate risks in the assessment of growth opportunities and in price fixing. What needs to be prevented is that line managers and risk managers are placed on opposite sides of each other.

A potential pitfall is that the controller is the only one made responsible for risk management within an organisation. The reason for this is that risks are usually expressed in terms of financial impact or damage and thus viewed as the responsibility of the controller. However, if risks are expressed on the basis of their cause, the responsible person would probably be the line manager. Even if the cause of the risk lies outside the organisation, the line manager is responsible for signalling it. Therefore, it can be argued that the person made explicitly responsible for managing one or more risks should be the line manager.

The goal of risk management is to create and preserve value through risk control and to be held accountable for this process. In the short run, risk management gives transparency within and outside the organisation by creating awareness for possible, unexpected developments. In the long run, risk management will result in a better efficiency by avoiding losses, a more predictable performance and lower financing costs. This will eventually result in a higher valuation of the organisation as a whole.

Next to risk awareness and value creation, the organisation is able to make better management decisions which results in a better functioning business process. On the other hand, implementing an effective risk management framework can be difficult and requires considerable effort and adjustment. Because of the high costs in terms of time and money, organisations are often reluctant to go through such a change. As these costs will be gained back after a while, the real measurable benefits can only be experienced in the long run.

In addition to the financial hurdle, another drawback is the fact that there will always be risks (unknown unknowns) making it impossible to prove that risk management is effective enough. One cannot foresee everything and the correlation between different types of risks could cause larger problems. The reason for this lies partly in the fact that the decisions that have to be made are based on human judgments.

2.2 Cause and effect

In the pursuit of a certain objective an organisation automatically faces all kinds of risks. Several activities need to be undertaken to ensure the objective is attained. If this is not properly done the achievement of the objective will be endangered. When the objective is realized, in general there will be positive effects. However, these effects will not be there if the objective is not attained.

Under cause a distinction is made between internal and external causes. Internal causes are causes that can be influenced whereas external causes cannot be controlled: i.e. one is simply confronted with it.

When an objective is not attained one will look for the cause of the failure. Both internal and external causes will be examined. In this case the internal causes lie at the bottom of not undertaking the necessary activities.

2.3 Opportunities and threats

Entrepreneurs and investors take risks consciously. They belief that they can earn substantial profits while knowing that they could lose it all when things turn for the worse. To be able to be profitable, entrepreneurs must translate the positive risks into the company's strategy. In this way they protect the company against the downside of the risk while capturing the upside of the risk.

Thus, risk does not always have to be negative. The word risk means that there is uncertainty about the future and that this could result in negative or positive consequences. Managing risks does not imply elimination or minimizing of risk. It's about optimizing the level of uncertainty so that the objective is positively affected while the negative risks will not cause too much damage and is controlled. When an organisation identifies an opportunity, this positive risk will be transferred to the strategic planning

process of the organisation. In case of an identified negative risk all steps of the risk management process need to be followed.

Chapter 3 Risk management process

In chapter 2 some basic terms from the field of risk management were discussed. This chapter will describe the risk management process and its relationship with risk management within the organisation. It will also introduce the COSO framework, which will be used throughout this book.

3.1 Risk management process

The six steps that make up the risk management process are presented in a circle in figure 1. After the sixth step the process continues with the first step.

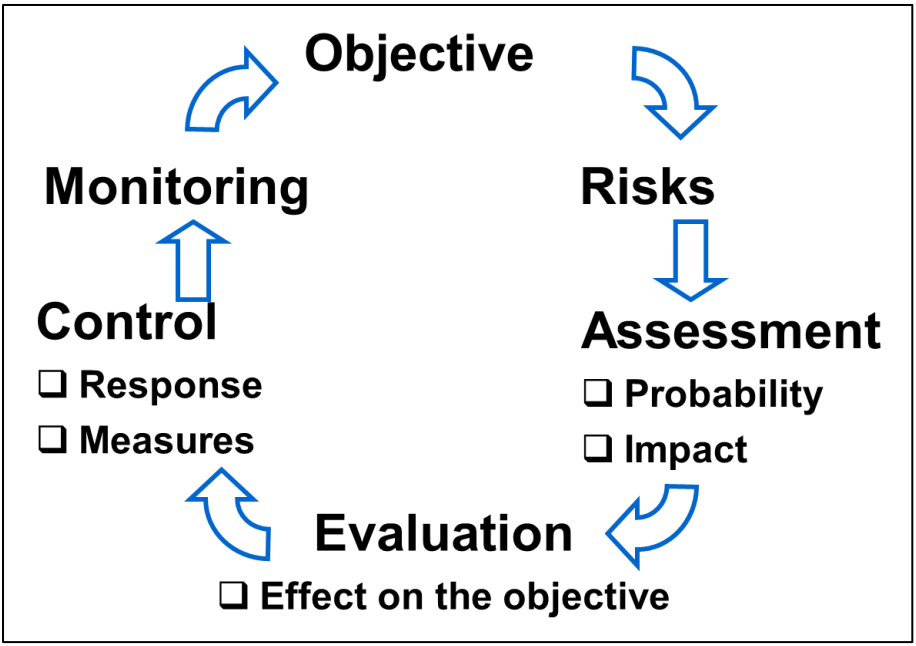

Figure 1 The risk management process

The first step in the risk management process is always to set the objective that needs to be attained. Without a clear objective the rest of the process

cannot be completed. In step two all possible events that may have consequences for this objective are identified. In the third step the probability of occurrence of the risk and its possible consequences for the objective are assessed. In step four the person responsible for attaining the objective evaluates whether the potential effect of the risk on the objective is acceptable. If the effect is not acceptable then a suitable response to the risk is formulated and measures are taken to control the risk. This happens in step five. In the final step of the process, the sixth step called monitoring, it is established whether or not the objective is attained, whether control measures are still effective and in which direction the risk is developing. After step six, the process circle is completed by continuing with the first step of the process. These process circles can be gone through continuously or once in a particular period.

3.2 COSO framework

COSO is a model that is developed by The Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO views the company's risk management as a process that is executed by people (Board of Directors, management teams or other personnel). The model is focussed on attaining the company's objective by applying risk management through the whole organisation and on the strategy of the company. This has the goal of managing the risks within the risk appetite of the organisation. In this way a reasonable degree of certainty is created. The term risk appetite will be more extensively covered in chapter 4.

A number of accounting scandals and cases of fraud in the eighties and nineties was the immediate cause for the invention of COSO. The COSO framework hands recommendations and guidelines regarding the internal control. COSO provides organisations a uniform way of internal control and supports the management of those organisations in the controlling of their internal control systems. Through the years the COSO framework has been further developed and now does not merely focus any longer on internal

control, but on the whole internal control system. This new framework is also known as COSO II or under the aforementioned term Enterprise Risk Management (ERM).

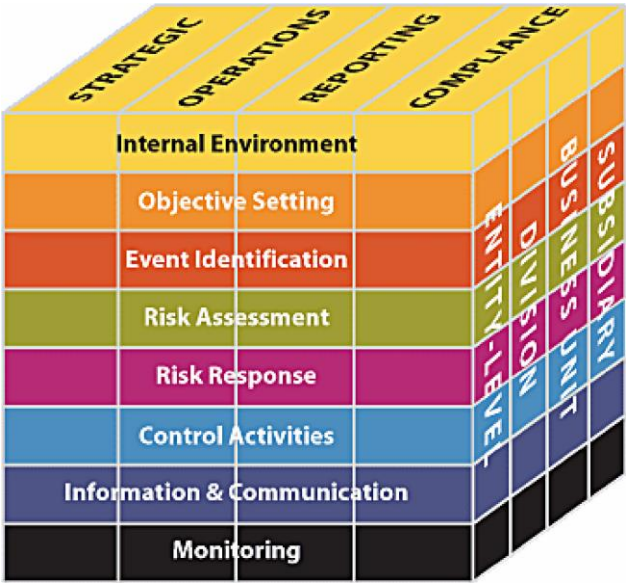

Figure 2 COSO framework

The COSO framework consists of eight layers which correspond with the six steps of the risk management process. In addition to the layers on the front face of the cube, the top face shows the four categories to which the process can be applied (strategic, operational, reporting and compliance). Looking at the side face of the model it becomes clear that the process can also be applied by various groups and levels within the organisation.

In the next chapters the different horizontal layers of the COSO framework will be covered in more depth. The six steps of the risk management process will be used as a guide throughout the rest of this reader.

Chapter 4 Internal environment and objectives

In this chapter the first two layers of the COSO framework will be discussed in more detail, starting with the internal environment, which is followed by objectives.

4.1 Internal environment

The internal environment is where the foundation is laid for the rest of the risk management process. The general philosophy (mission, vision and values) of the organisation needs to be translated to a philosophy regarding risk management.

Risk culture is often cited as a fundamental cause in major world events, such as major industrial accidents and excessive risk taking that caused the 2008 economic crisis. An organisation's risk culture contains the shared beliefs, knowledge and attitudes towards risk of a group of people who share a purpose, which makes it part of the internal environment.

One way an organisation's risk culture expresses itself is in the amount of risk that the people in an organisation are willing to accept, in terms of the maximum amount of acceptable loss. This is known as the organisation's risk appetite. COSO describes risk appetite as:

'The degree of risk, on a broad level, that the organisation is prepared to accept in pursuit of value, it's mission and it's vision'.

See figure 3 below for a simple risk map in which the risk appetite is shown. Chapter 6 on risk assessment and evaluation will elaborate on the various characteristics of the risk matrix.

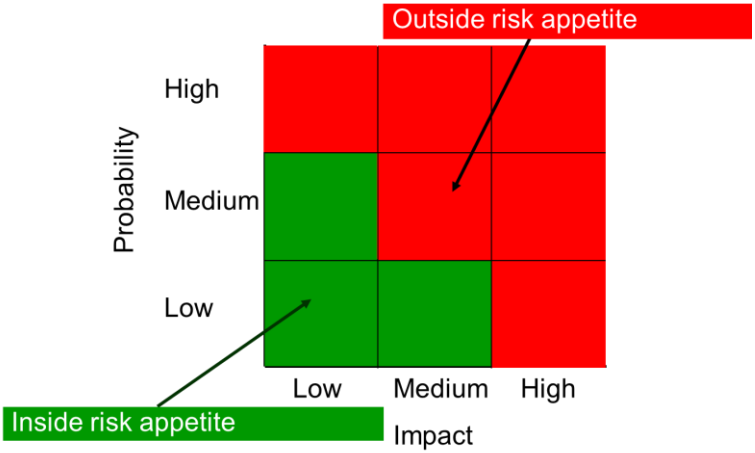

Figure 3 Risk appetite (on a risk map)

The areas in the risk map are coloured to indicate whether the risks that are placed in a particular square fall within or outside the risk appetite. In this way it is clear when an event with a certain likelihood and impact is acceptable or not in terms of (negative) risk. On the impact-axis the effect on the objective is shown. The impact needs to be measurable and often this number will be translated to a certain amount of money (loss).

4.2 Objectives

Organisations define objectives on the basis of their internal environment. In the risk management process (see figure 4) this is shown as the first step, because without objectives there are no risks and without risks no risk management is needed. In this first step the internal environment is taken into account as well.

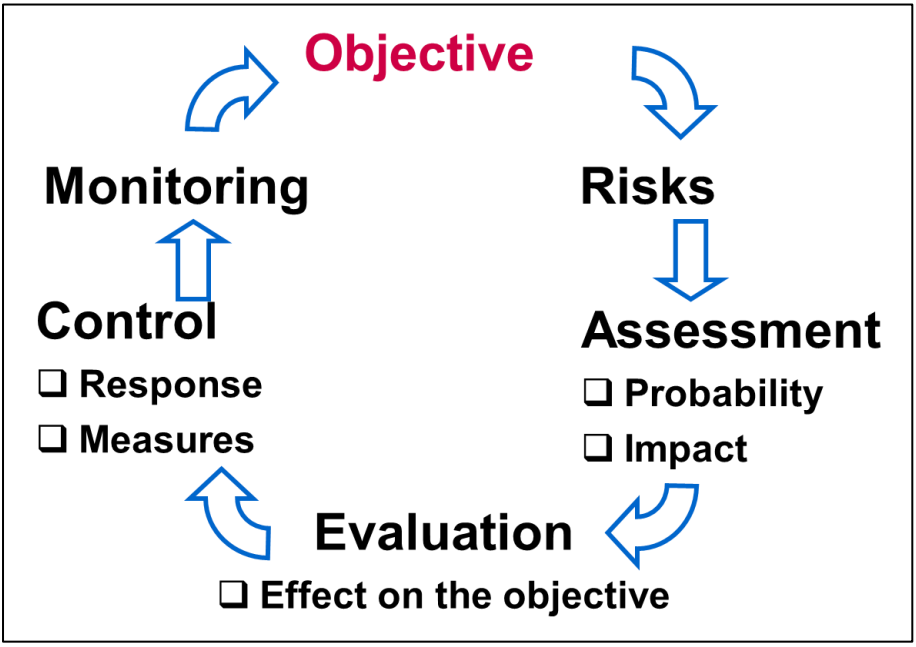

Figure 4 The risk management process

Objectives can be presented as critical success factors (CSF). One can distinguish four types of critical success factors that originate from the four perspectives of the balanced scorecard (BSC) approach:

- financial: e.g. growth, survival;
- customer: e.g. improving service quality, offering a competitive rate;
- internal processes: e.g. optimising the cost level, optimal usage of business resources;
- innovation and learning: e.g. strengthening the market position, improving the time-to-market of new products.

Every critical success factor is measured with one or more key performance indicators (KPI). The performance regarding the success factor growth, for instance, can be measured using the indicator net profit and revenue.

To execute risk management it is important that the objectives are formulated in a SMART way. An objective that is formulated in a SMART way is:

- specific: what exactly needs to be attained?
- measurable: how can you measure whether the objective is attained?
- acceptable: do the stakeholders allow it to be attained?
- reasonable: is it possible to be attained?
- time-bound: within what amount of time does it need to be attained?

It is advisable to start from specific performance indicators to formulate an objective instead of the more general critical success factors. With a SMART-formulated objective it is clear what exactly needs to be attained and how to measure this, and it is easier to identify relevant risks and determine their impact on the objective. When the objective of a business unit is, for example, to realise a profit of € 300.000 in the coming year, one can specifically search for an event that can influence this net profit. Also, the possible impact of these events on the objective can be expressed in a decrease (or increase) in net profit.

Chapter 5 Risk identification

The third step in the COSO framework is the identification of risk. In this chapter several methods and models are presented that can be used as tools to identify risks.

5.1 Identification of risks

Risk identification, also known as risk analysis, is the search for events that have a consequence for the objective. In the COSO framework this step in the risk management process is called event identification. As described in chapter 1, a risk can be defined as a possible event with consequences for the objective. Therefore, the following question can be raised with regards to the identification of negative risks: 'Which events can endanger the objective?'.

A risk cannot exist without an objective. When there is an objective to be attained, something could happen that will influence the desired outcome. However, when there is no objective to be attained, nothing can happen that will affect the target. That is why in the identification of risks it is important in your thoughts and in your expressions to make the relationship with the objective explicit. In the risk management process the risks, or rather the identification of the risks, will follow after the step in which the objective is determined (see figure 5).

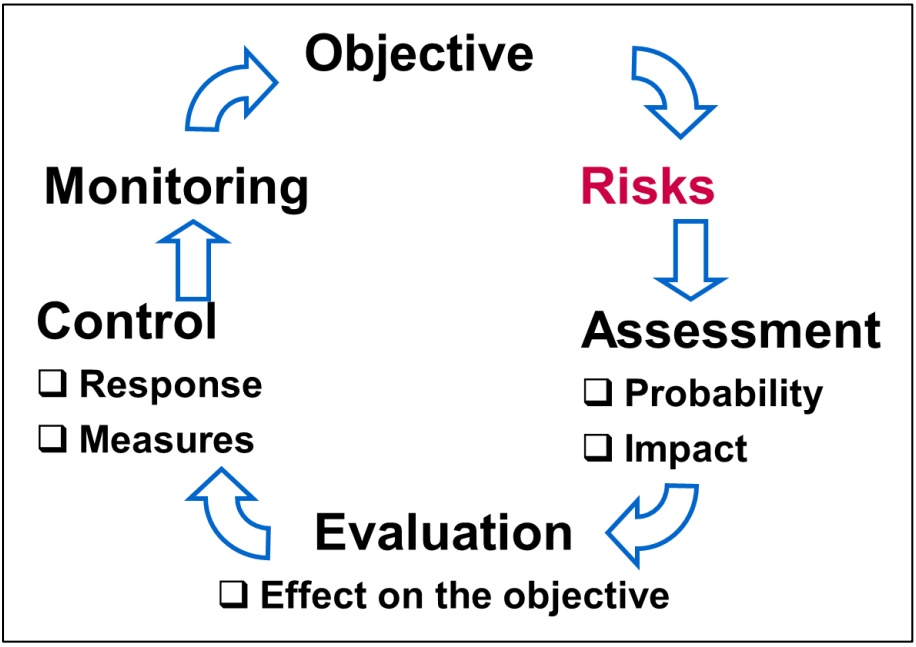

Figure 5 The risk management process

Formulating the events that can endanger the objective in a concrete way will make it easier to come up with suitable measures to control the risk. When thinking in terms of specific events it will also be easier to look for the real cause of the risk. In practice there will often be multiple causes that can be discovered for one single event happening.

In the real world it is rather difficult to formulate a risk as an event. A method that helps to automatically state risks as events is shown in table 1. In this table the earlier mentioned objective maintaining technological competitive advantage is used.

Table 1 A way to formulate risks as an event

Start your formulation with the word 'The'	*The*
Add a verb	*leaking*
Make use of words to clarify the risk	*of innovative ideas to the competitor*
If necessary indicate what the consequences are for the objective	*with the consequence that we lose our advantage*

5.2 Tools for identification

In the identification of risks use can be made of a risk register in which risks and their characteristics can be recorded. Such a risk register in its simplest form can consist of a spreadsheet with the following columns:

- serial number of the risk
- description of the risk
- probability of occurrence of the risk
- consequence of the risk for the objective

Table 2 Risk register

Risk #	Risk description	Prob. (in %)	Impact (in €)
1	*The – verb – risk*	*… %*	*€ …*
2	*Etc.*		

Chapter 5 will elaborate on the subjects of probability of occurrence and impact of the risk on the objective. In the next steps of the risk management process, columns can be added to the risk register, so that it can indicate who

the risk owner is and what measures should be taken to control the risk. Chapter 6 will deal with this last issue.

In the identification of risks checklists are used to determine whether one has considered all relevant angles in the search for risks. Checklists can draw your attention to the external environment (for example PESTEL or DESTEP) or to the internal environment (PIOFACH). The sequence of the words in the checklists is chosen in such a way that the first letters of these words together compose a name that can easily be remembered (this name is called an acronym). Checklists do not indicate what the relationships are between the words in the checklists.

Looking at the internal environment one can think of the employees and the various processes within the organisation. In this case the PIOFACH checklist is used. This checklist considers various internal aspects from which risks could arise. Table 3 shows the content of this checklist.

Table 3 PIOFACH checklist

PIOFACH
P - Personal
I - Information
O - Organisation
F - Financial
A - Administration
C - Communication
H - Housing

When dealing with the external environment the DESTEP or PESTEL checklist is used. The sequence of the words in the checklists is chosen in such a way that the first letters of these words together compose a name that can easily be remembered (i.e. an acronym). Checklists do not indicate what the relationships are between the words in the checklists. Table 4 shows the content of both checklists.

Table 4 DESTEP and PESTEL checklist

DESTEP	PESTEL
D - Demographics	P - Political
E - Economics	E - Economic
S - Society	S - Sociocultural
T - Technology	T - Technical
E - Ecological	E - Environmental
P - Political	L - Legal

Porter's value chain model shows all activities in an organisation that have the objective to add value by producing a product from material resources or by delivering a service through human resources. Both activities in the primary processes and in the processes that have a supporting role have the objective of adding value.

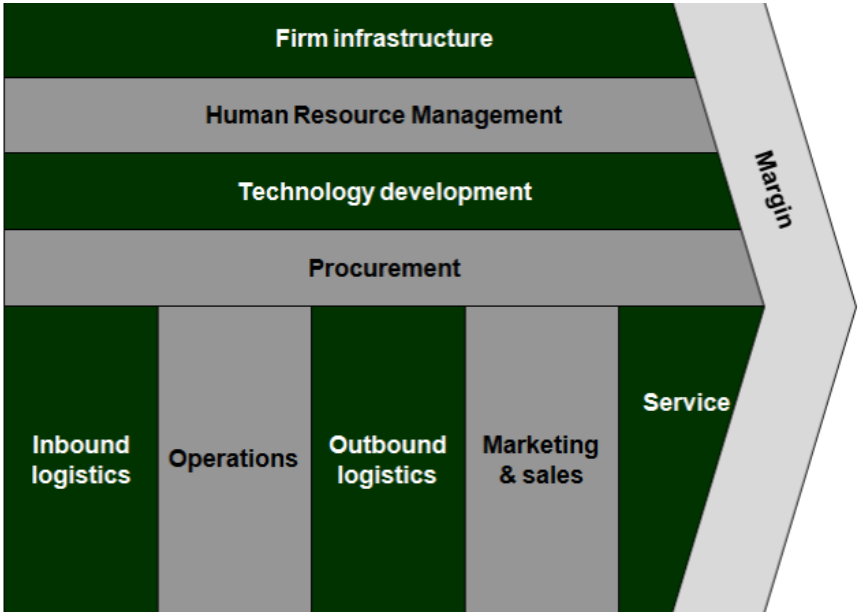

Figure 6 Porter's value chain model

For each of these processes the following questions can be asked, 'What can happen in this process so that the adding of value does not take place?' and 'What event causes the destruction of value in the process?'. This kind of risk identification delivers a list of internal risks. Risk management as such is also referred to as value management.

Porter's five forces model indicates what the balance of power is between the organisation and its current competitors, suppliers and customers. The model also indicates what influence substitutes and new entrants have on the balance of power. On the basis of the model questions can be asked such as, 'What can suppliers do so that our objective is endangered?' or 'What can become a substitute for our product?'. Risk identification on the basis of this model results in a list of external, market-related risks.

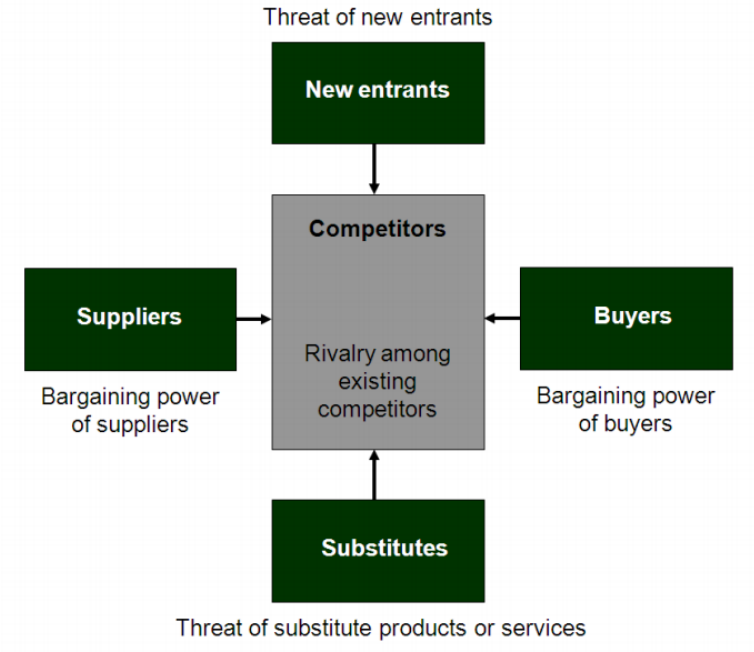

Figure 7 Porter's five forces model

Chapter 6 Risk assessment

After identification of risks, it is important to get a good idea of the size of the risks. In this chapter it will be discussed how the size of risks can be expressed in words and numbers.

6.1 Risk assessment

In the risk management process the logical step after identifying risks is to look at the size of the (negative) risks. However, the size of the resulting expected loss or exposure when the risk does happen, can be split up in two variables: the consequence of the risk on the objective (the impact) and the probability that a risk will materialize (the likelihood).

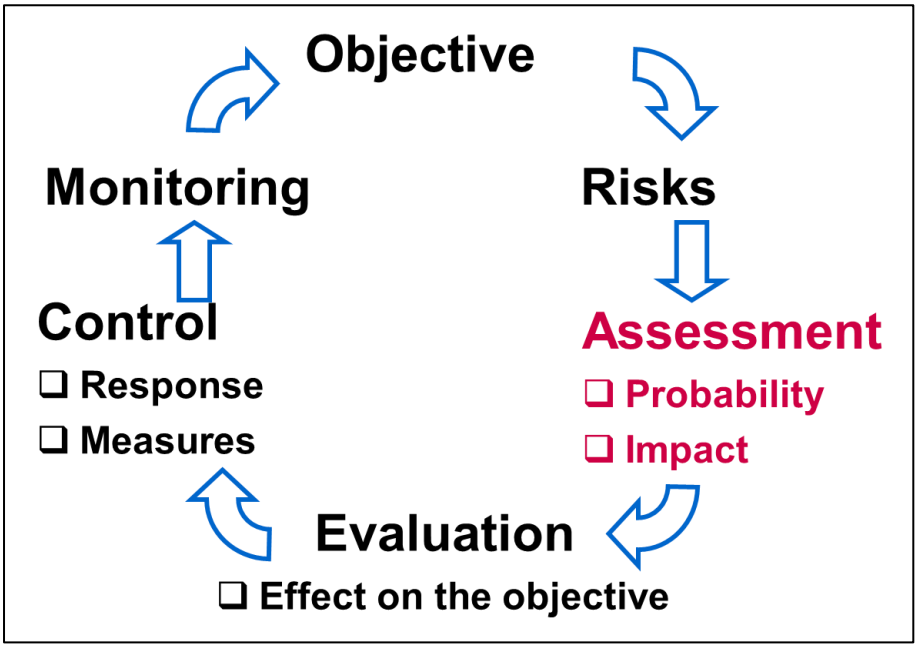

Figure 8 The risk management process

To make an assessment of these variables, one can look at certain known risk occurrences in the past (retrospective). In addition, one has to look how these risk occurrences could develop in the future (prospective). In this respect, it is only possible to predict possible developments.

The likelihood of a risk occurrence can be expressed in several ways. The likelihood can be translated into a probability percentage, as well as into a frequency (of occurrence). In Enterprise Risk Management, the impact is usually expressed in an amount of money.

Probability:

- frequency: 1-in- …
- likelihood: … %

Impact:

- effect on quantitative objective (for example in euro's)

6.2 Modelling risks

Risks can be quantitatively modelled by simplifying them to their basic properties, probability of occurring, the degree an organisation is exposed to the risk and the risk's impact. The probability of a risk is the likelihood that the risk will happen and is expressed as a percentage. For example, a manufacturing organisation needs deliveries of raw materials. There is a 5% chance that a single delivery is incomplete, which means that it can be expected that one in every 20 deliveries is incomplete. To model the probability of this risk, a binomial distribution can be used. This distribution shows how likely it is an event will happen. Graphically, the distribution looks like figure 9.

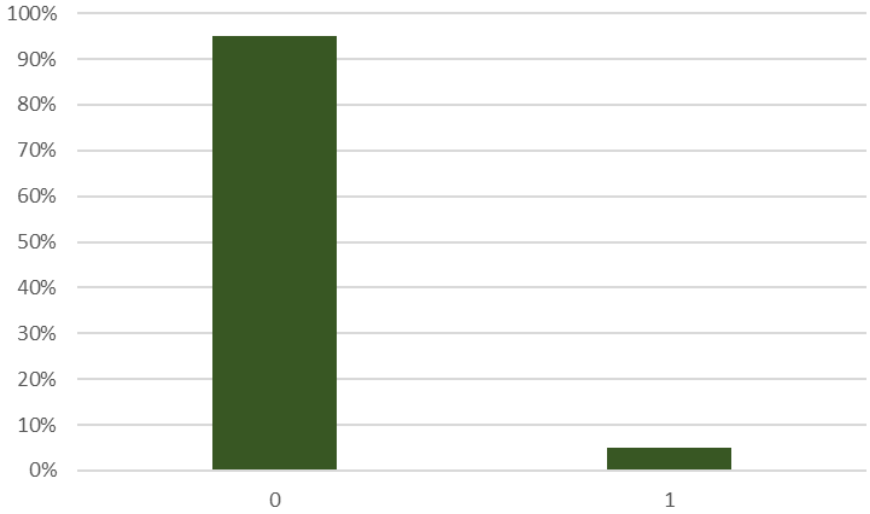

Figure 9 Binomial distribution for a single event with 5% probability

In figure 9 the number of times an event happens can be read along the horizontal axis. The probability of the event can be read along the y axis. In this distribution the probability of the event happening once is 5%, such as in the example.

The exposure of this risk is how often the risk could happen to the organisation. Using the incomplete deliveries example, the organisation has on average 100 deliveries per year, which means the organisation is exposed to the risk of incomplete deliveries 100 times. It is important to realise that this means the risk could happen more than once per year, as every occasion of delivery has a probability of being incomplete.

Combining the probability of the risk and the exposure to the risk over a year, we can expect 5% of all 100 deliveries is incomplete. So, it can be expected that 5 deliveries per year are incomplete. However, the actual number of incomplete deliveries could be higher or lower. The probability of the number of incomplete deliveries can be calculated by extending the binomial

distribution to include not just one event (n=1), but all hundred deliveries (n=100). This is graphically shown in figure 10.

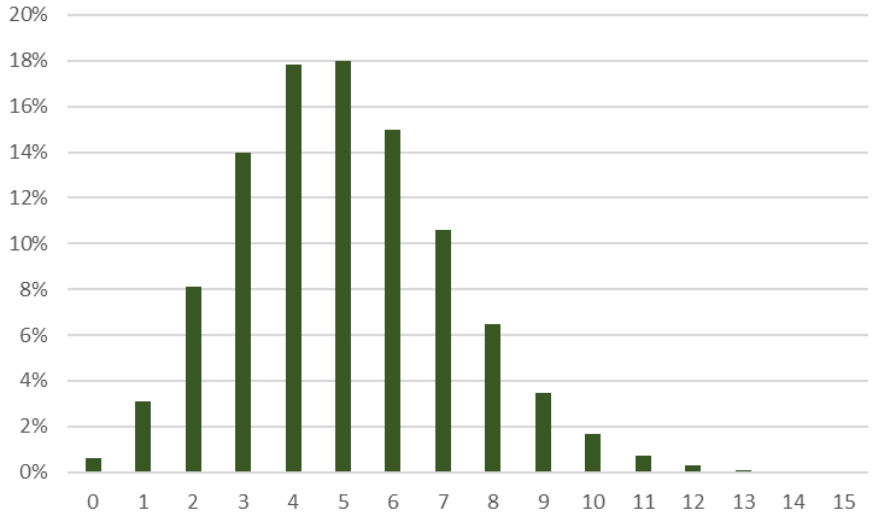

Figure 10 Binomial distribution for 100 events, each with 5% probability

Similar to figure 9, figure 10 shows the probability of a specific amount of incomplete deliveries in one year. It can be seen that although the expected amount of incomplete deliveries is 5, the probability of this is only 18%. Also it is very unlikely (less than 1% probability) that more than 10 deliveries are incomplete in one year.

This can be compared with a series of coin tosses. The amount of tosses is similar to the exposure to a risk. For every toss, the probability of heads is 50%, which is similar to the probability of some risk happening. The probability of four times heads (or the risk happening four times) is 50% * 50% * 50% * 50% = 6,25%.

The impact of a risk is the damage the risk would cause to the organisation. In the deliveries example, the damage would depend on how incomplete the delivery is, which might range from a small portion of the delivery to possibly

the whole delivery. Assume the expressed in financial damage, the impact of an incomplete delivery ranges from €100 at minimum, the value of one missing item, to €10.000, the whole delivery. Assume further that the most likely financial damage for this risk is €2.000. This illustrates that the uncertainty of a risk is not only in the probability, but also shows in the extent of the impact. Of course, this means that two different incomplete deliveries could have very different impacts.

To model the impact of risks in financial damage, it is necessary to use other statistical distributions than used to model probability. There is a wide range of available distributions for this, but only several common or easy to use ones will be discussed.

In business, data on operational risks is usually scarce and relies on estimates. A distribution that is often used in this case is the triangular distribution, which is defined by a minimum, maximum and mode, which is the most likely impact. Typically, this distribution is used if there is only a limited amount of available data, such as for many business related risks. This distribution is helpful to model the example of incomplete delivery, which is shown in figure 11.

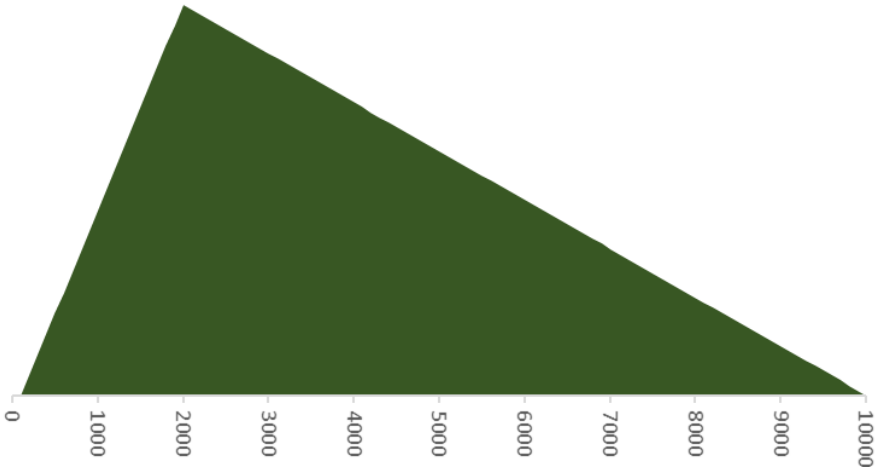

Figure 11 Triangular distribution with a mimimum of 100, mode of 2.000 and maximum of 10.000

Figure 11 is the graphical representation of the possible impact of an incomplete delivery. The most likely outcome of the risk, the mode, is located at the peak of the distribution, where the graph is high. This shows that whenever there is an incomplete delivery, the impact will be around €2.000 most of time. The graph is low around the maximum impact, which means that impacts this large are relatively rare, but might still happen.

Another helpful distribution to model impact is the normal distribution. The specific numbers necessary to use this distribution are the average outcome and its standard deviation, which is a measure for the unpredictability of what is being measured. This distribution is often used if a reasonable amount of historical data is available. It is therefore often used by banks to model fluctuations of currency values. Characteristically outcomes of this distribution are found near the average outcome, though sometimes the outcomes are much higher or lower. Figure 12 illustrates this property of the

normal distribution by showing an example of the possible impact of holding 10.000 US dollars for a company that usually takes payment euros.

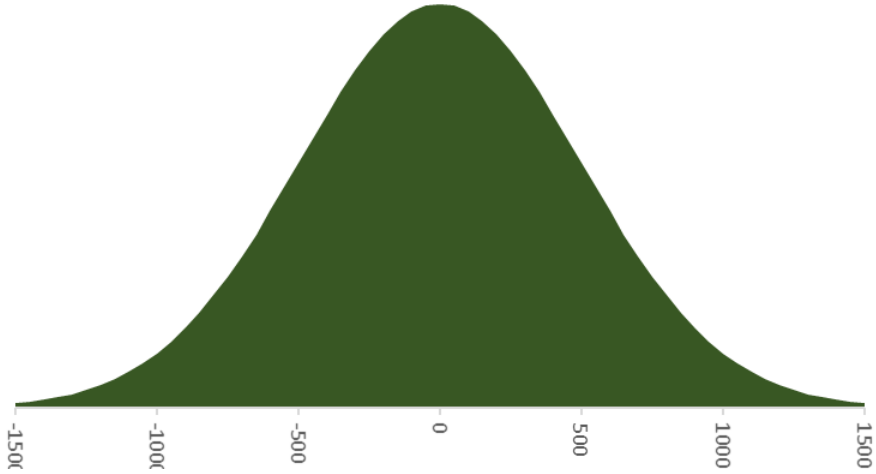

Figure 12 Normal distribution with a mean of 0 and standard deviation of 500

The figure shows that as the exchange price of the currency goes up or down, the value of the cash money changes. Just like in the triangular distribution, the most likely outcome is located where the graph is high. For the normal distribution this is the average. In this case, the exchange price fluctuation is zero, which means it is expected that the value of the cash dollars will be the same over a period of time. However, there is some uncertainty of this, which is shown as the standard deviation. In this case, it is realistic that the value of the dollars might change and will be worth 500 euros less. Reading the graph, it is possible the dollars might be worth 1.000 less, although this is not very likely. Also, this means the risk might actually have a positive outcome, which happens if the value of dollar to euro goes up.

Insurable risks with low probability but high possible impact are often modelled by using the gamma distribution. This distribution is used by insurers to model insurance claims for risks such as fire and flooding. Typically the outcomes of this distribution are relatively small, however in

some cases the impact can be extreme. Figure 13 shows an example of the gamma distribution.

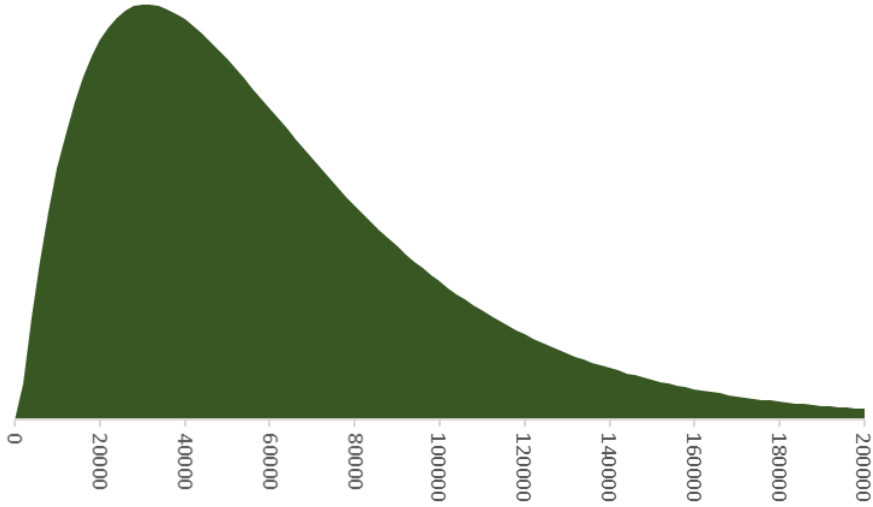

Figure 13 Gamma distribution which shows the relative rarity of high impacts versus small impacts

In figure 13 the difference between small and large impacts can be seen by comparing where the graph is high to where it is low. This example might show the impact of a house fire, which is usually relatively small. The damage of around €40.000 in this case could include the loss of some valuables and repairs for damage to the house, which can still be used after these repairs. Only if a fire goes out of hand, the impact is very large, which could mean a whole house worth €200.000 is destroyed.

Chapter 7 Risk evaluation

After assessing the size of the risks in the previous chapter, this chapter will focus on the further evaluation of risks.

7.1 Prioritising risk

Based on the estimated likelihood and impact it is possible to rank the various identified risks in terms of level of significance: which risks are significant and which are not.

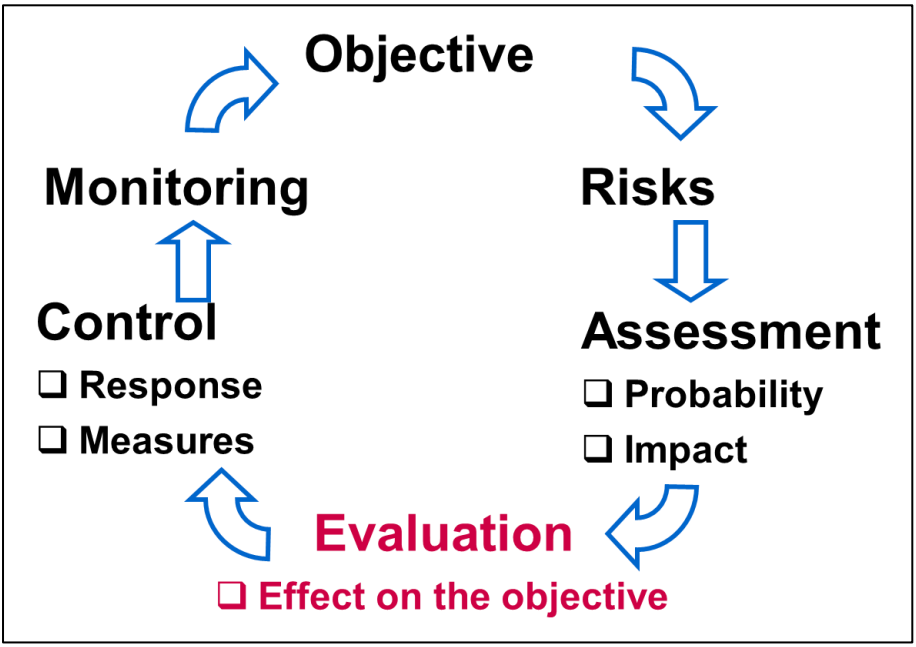

Figure 9 The risk management process

The ranking can be done by multiplying probability by impact. In this way the expected value of the risk can be determined:

Expected value = probability (in %) X impact (in €)

The risk with the highest expected value is the most significant risk and has priority when it comes to finding controls to manage the risk. These controls will be discussed later in chapter 8. In this phase of the risk management process the risk register will look like table 5 and contains the following columns:

- risk number
- risk description
- probability of occurrence
- impact of the risk on the objective (gross risk)
- expected value (probability x impact)

Table 5 Risk register

Risk #	Risk description	Prob. (in %)	Impact (in €)	Expected value
1	*The – verb – risk*	*… %*	*€ …*	*(% x €)*
2	*Etc.*			

7.2 Kinney method

In practice it is not always possible to determine an exact probability and amount of money (impact). To overcome this problem it is possible to use the Kinney method, for which exact numbers are not necessary, but instead uses an estimate of their magnitude.

To assess and rank the risks, a certain value will be assigned to the probability of the risk occurrence and to the impact of the damage caused when the risk materialises. To these two factors the exposure to the risk is often added, which shows the difference between risks that can happen for example only once every few years and risks that happen weekly.

These factors are multiplied and this results in the following formulas:

1. risk (exposure) = impact x probability

2. risk (exposure) = impact x probability x exposure

By assigning a value to the factors mentioned, one can calculate a certain risk value. Based on this value the risks can be ranked and action can be undertaken. Table 6 shows an example of values that can be assigned to the risk factors.

Table 6 An example of values used in the Kinney method

Impact		
1	Insignificant	Injury without delay
3	Important	Injury with delay
7	Severe	Invalidity, irreversible damage
15	Very severe	One death
40	Disaster	Several deaths

Probability	
0,1	Almost unthinkable
0,2	Practically impossible
0,5	Thinkable but improbable
1	Improbable but possible
3	Unusual
6	Great probability
10	Practically sure

Exposure		
0,5	Very rare	Less than once a year
1	Rare	A few times a year
2	Rarely	Monthly
3	Now and then	Weekly
6	Regularly	Daily
10	Constantly	A few times a day

Score		
≤ 20	code 1	No action
> 20	code 2	Needs attention
> 70	code 3	Controls required, can be planned
> 200	code 4	Immediate improvement
> 400	code 5	Stop work

In the example it shows that a risk with a severe impact, possible probability and weekly exposure scores 7 x 1 x 3 = 21. This means attention is needed.

7.3 Evaluation with a risk map

Based on the ranking established before it is possible to place the risks on the risk map. The risk map is an overview of the probability on the vertical axis and the impact on the horizontal axis. In practice these axes can also be shown inversely without causing any problem, provided that the axes are correctly defined. In addition to the term risk map, terms like risk matrix, impact-likelihood diagram or probability-impact diagram will often be used.

Each axis of the risk map is split up into several categories, dividing the risk map into several squares. In figure 10 a simple example of a risk map is shown.

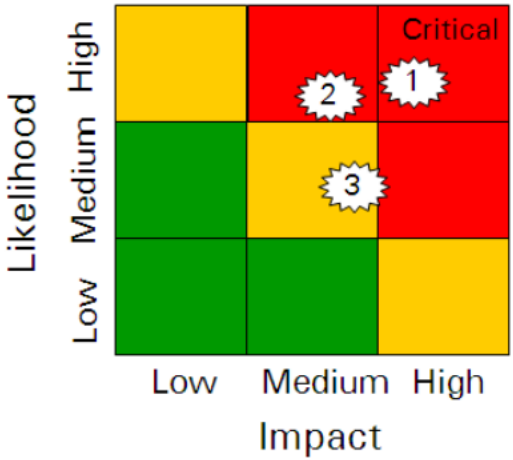

Figure 10 Simplified display of a risk map

In the risk map the axes are qualitatively defined. In the example above this qualitative scaling is realised by simply categorizing the axes into low, medium and high. In practice, this has to be done more specifically.

On a risk map the risk appetite will often be shown by three colours: green, yellow/orange and red, such as can be seen in figure 10.

Green tells you a certain area is acceptable. This is not to say that there are no risks, but the situation is in control. Monitoring is still needed to see whether a certain risk will migrate to the yellow/orange or even the red area.

The yellow/orange area indicates that an area is temporarily acceptable. This means that one is aware of the risk, but the risk is still acceptable for the time being. Risks in this area need to be reduced to an acceptable level. In any case one has to ensure that the risk does not increase and become unacceptable.

The red area indicates that the risk is unacceptable. In this case the organisation has to mitigate the risk by reducing likelihood, impact or both.

The colour distribution and level of risk appetite can be compared to a traffic light. When the light is green you may cross the street but you still have to look around to check whether the situation is completely safe (acceptable). When the traffic light turns yellow/orange the advice is to stop, but it is permitted to cross the street only if there is no other possibility. When the light turns red you have to stop.

In reality some people cross the street when the traffic light is red and take the (unnecessary) risk of endangering one's own or another person's life, or of having to pay a fine. The same goes for organisations. When a risk is in the red area the organisation can choose to do nothing, but simply runs too much (unnecessary) risk. Sometimes luck is on your side but more often there will be (considerable) damage done.

In addition to a qualitative scaling of the axes, a quantitative scaling must be used in order to prevent ambiguity in relation to the extent of a qualitative definition. Terms like possible or probable and average or catastrophic can mean different things for each person. When using a qualitative scaling a measurable factor needs to be included.

Because risk management assumes a central objective, the negative effect of each event on the objective will be shown on the impact axis. When dealing

with Enterprise Risk Management this will in most cases imply a translation into an amount of money. As described earlier in this chapter, the likelihood (in terms of percentage) or the frequency (1 out of a number of cases) will be shown on the probability axis.

In the next example (see figure 11) the axes have been scaled in a linear way and the probability axis is shown in percentages. To make sure the risk map can be read correctly it is necessary to use qualitative as well as quantitative scaling.

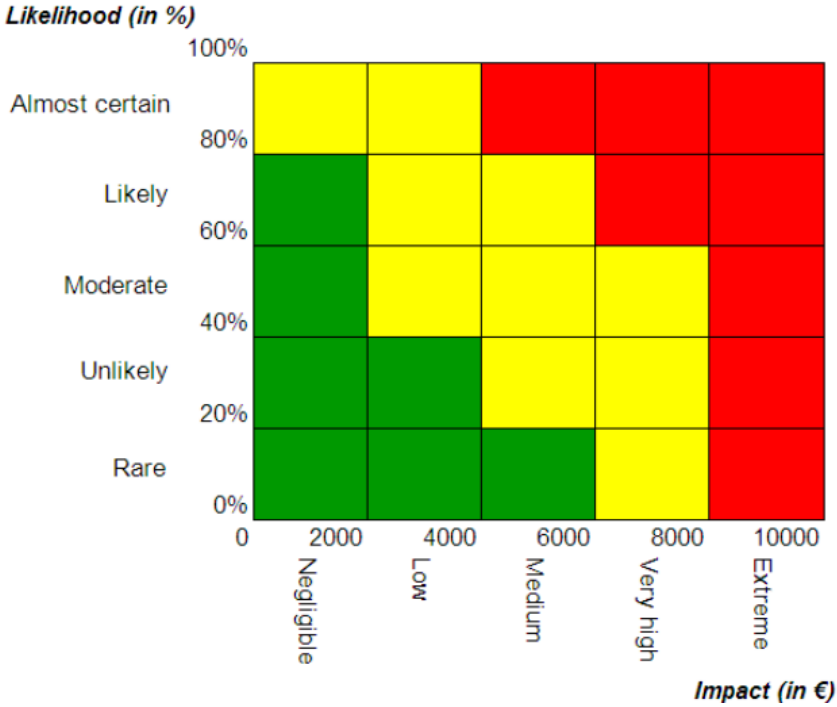

Figure 11 Complete framework of a risk map (linear scaling)

Chapter 8 Risk response and control measures

This chapter describes how to respond to risk and which specific control measures to take, after risks have been assessed and prioritised.

8.1 Risk response

After the assessment of the risks one can decide how to deal with the risks. This decision will be partly based on the risk assessment already executed. When a certain risk is thought to be very small, the organisation could accept this kind of risk. However, this is not the case when we talk about bigger risks that have a higher probability of occurrence, a bigger impact or both. The organisation would want to mitigate these risks by reducing the probability of occurrence or impact after the risk has happened.

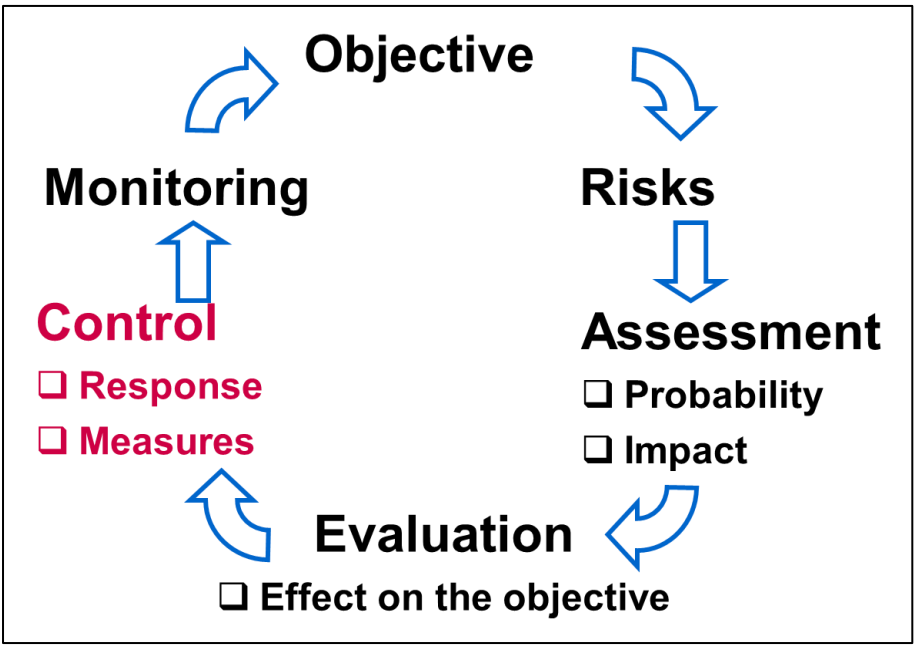

Figure 12 The risk management process

In relation to risk response, we speak of the 4 T's: treat, transfer, terminate and take. Each risk response will lead to another (re)action. In case the risk response is control the risk will be dealt with by the organisation itself and control measures will be taken. These measures can be preventive or repressive in nature. Preventive measures are measures that are implemented before the risk occurs and will focus on reducing the probability of occurrence. Repressive measures are measures applied to mitigate the impact of a risk, after a risk has already occurred. By applying effective control measures the probability of occurrence and/or the actual impact will be reduced. A control measure is effective when the risk is mitigated to an acceptable level.

In case of a transfer the risk is not personally dealt with, but transferred to a third party. The most common situation in transferring a risk is the purchase of an insurance. By insuring a risk, the financial part of the risk (the larger part of it) is transferred to the insurance company. In transferring through insurance, the impact of the risk is reduced: the eventual financial damage is lower. However, the probability of occurrence is not reduced. Next to insurance, outsourcing a risk to a third party is another way of transferring a risk.

In addition to control and transfer one can also choose to avoid a risk. This risk response implies that there will be no risk to bear anymore. This is because the risk no longer exists as the relevant activity is terminated. However, avoiding risks does not belong to the core business of an organisation. Applying the risk response avoid should be considered in each separate case. Finally one can choose to accept the risk. Nothing will be done with the risk as there will be no control measures taken whatsoever. The risk is accepted, because it falls within the risk appetite of the organisation or because the costs of the control measures are higher than the benefits of covering the risk. Thus, there is no efficient measure available.

In avoiding or accepting a risk one does not make use of any control measures. When the risk response is to avoid, the activity is closed so measures will not be necessary anymore. And if we accept the risk, we decide to do nothing.

8.2 Control measures

Based on the risk reaction one can establish control measures and implement these within the organisation. As mentioned in the last paragraph, an organisation can only establish control measures in case of two possible risk reactions, control and transfer. As a consequence of the chosen risk reaction(s) one will assess within the organisation which measures will be most effective when dealing with a certain risk. The organisation will assess whether the risk can be controlled internally or if it is better to transfer (a part of) the risk to a third party. Depending on the control measures taken the policy and the procedures within the organisation are adapted.

Control measures can be characterised as hard or soft controls. Hard controls are measurable agreements and guidelines of which can be objectively checked whether these have been followed. Contrastingly, soft controls intervene or appeal to employees' individual performance and behaviour by influencing their conviction and attitudes and are more difficult to objectively check. Security checks at airports is a good example of a hard control, before being allowed to enter the waiting area, passengers' belongings have to be checked. Only if the box 'passengers' belongings have been checked' can be ticked, the passenger is allowed to go through. Because of wide media coverage of fraud and corruption scandals, such as at Enron, the need for soft controls in addition to hard controls has become more apparent since the 2000s.

Part of risk culture, as discussed in chapter X, is employees' attitude towards taking risk. This itself might be a risk as well. If an organisation's board notices that too much risk is being taken by employees, it might be useful to

attempt to change risk culture as a control measure. To achieve this, soft controls could be used. Although changing a risk culture within an organisation would take a long time, if an attempt is made, attention should be paid to:

- Adopting a clear and compelling vision and strategy that people understand and can buy into;
- Articulating the desired culture at the highest level of the organization;
- Paying attention to the side of culture that is hidden beneath the surface, people's personal concerns, interests and fears;
- Realising that existing systems, processes and policies support the status quo and they should be reviewed and changed if necessary.

Next to controlling the risks internally, an organisation can also choose to involve third parties in the risk management process. Here a distinction can be made between one's own choice and a (forced) choice of outsourcing the risk. An organisation can choose to outsource certain processes to other organisations so that the organisation can concentrate on the primary processes. In some cases, the organisation will be forced to hire third parties, for example an insurance company.

Based on the determined risk reaction and possible control measures, we can add two columns to the risk register that was shown before. In addition, we can also look at the total costs of occurrence of a risk. As described earlier in this chapter, when establishing and implementing control measures, the costs of these measures have to be compared with the benefits of covering the risk. Also, a risk will not be actively controlled when the costs of the control measures outweigh the cost when a risk occurs. Table 7 shows the risk register with the two additional columns.

Table 7 Risk register (inherent risks)

Risk #	Risk description	Prob. (in %)	Impact (in €)	Expected value	Risk response	Control measures
1	*The – verb – risk*	*… %*	*€ …*	*(% x €)*	*(4T's)*	*… + …*
2	*Etc.*					

After implementing the control measures, an improved risk register can be created, such as can be seen in table 8. In the new register the residual risks are shown and therefore also the residual likelihood and the residual impact.

Table 8 Risk register (residual risks)

Risk #	Risk description	Control measures	Prob. (in %)	Impact (in €)	Expected value
1	*The – verb – risk*	*… + …*	*… %*	*€ …*	*(% x €)*
2	*Etc.*				

List of references

Chapter 9 Information, communication and monitoring

The last layers of the COSO framework consist of information, communication and monitoring, which will be discussed in this chapter.

9.1 Information and communication

Within an organisation it is important that the right people get the necessary information in time and in a clear way. Internal communication plays an important factor here. This holds true for all daily, regular activities, but also for risk management.

There is a variety of ways to show the results, through different diagrams and other presentations. This can vary between the well-known line chart, the histogram and a pie-diagram. Combining this information can eventually result in a so-called digital dashboard. A digital dashboard is meant to provide a clear visualisation of the KPI's and related information to mangers and other responsible persons. In this way one can quickly see what the current state of affairs is, which makes it possible to take quick decisions.

In paragraph 4.2 it was described how each critical success factor is measured by one or more key performance indicators. These KPIs are related to the performance of the organisation. However, because performance can only be measured afterwards, adjustment based on KPIs alone will be a challenging task. The moment these performance indicators are revealed it could be already too late to take the necessary measures. To get an early warning signal of whether the objectives will be attained or not, organisations use key risk indicators (KRIs) and key control indicators (KCIs). Both are so-called early warning indicators (EWI) that will generate a warning in an early stage. KRIs give warning of risks that are increasing in potential impact and KCI's give warning if key control measures are not fully effective. With these three types of indicators the organisation will be able to decide whether it is in control to ultimately attain its objectives. By regularly identifying risks and

assessing the probabilities and impacts, the risk profile can be clearly monitored.

9.2 Monitoring

Based on the results an organisation can determine whether the organisational objectives are attained or not. In fact, the organisation is monitoring the operating result. It may come as no surprise that the term 'monitoring' is a key component in (the) risk management (process).

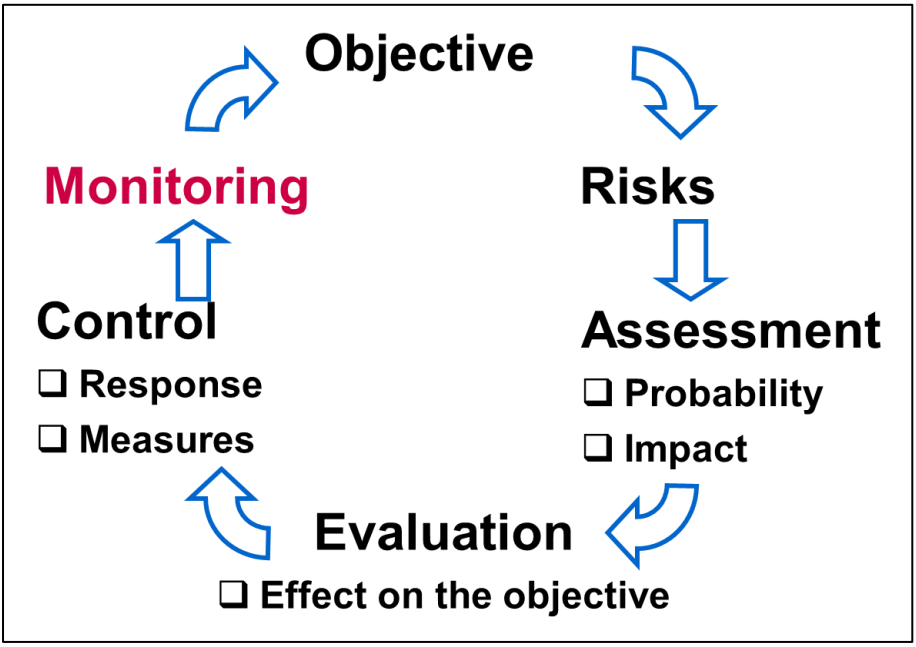

Figure 13 The risk management process

The steps in risk identification that have been followed in the risk management process, to the implementation of control measures, are all meant to manage the internal and external environmental factors that affect the company's objectives. In the last step of the process, called monitoring, one will look whether the control measures are still effective and in what

direction (the) risks will develop. The process circle is rounded when after the step monitoring, the process starts all over again with the first step. These process circles can be followed continuously or periodically.

9.3 Risk policy

The previous chapters show that in every step of the risk management process there are various available tools and techniques. For different organisations some of these tools and techniques might be more important than others, while some tools or elements thereof, might not be applicable. For example, if risks are identified for a school of finance and the DESTEP checklist is used, it would be reasonable to decide that the element "environment" is not as important as the element "political", as the school might likely rely on government funding.

Which tools and techniques are important in the process steps for a specific organisation is usually described in an internal document, called a risk policy. This risk policy is used as a guide for risk management and should be available to all people involved in the risk management process. Typically a risk policy would describe:

- which objectives risks are managed for
- what the organisation's risk appetite is
- what the organisation's risk matrix looks like
- who are involved in the risk management process
- which tools and techniques are used to identify risks
- which numbers are used to measure probability and impact
- who are responsible for risk control (risk owner)
- how often the risk management process is reviewed

In paragraph 10.3 the use of a real risk policy is discussed in more depth.

Designing a risk management process and describing it in a risk management policy takes considerable effort. When the risk management policy is

finished, it is usually accompanied by a statement by the person with the final responsibility for risk management within the organisation. Within many corporations this is usually a senior director with the specific portfolio of risk management, the Chief Risk Officer (CRO), or a CEO or CFO.

Chapter 10 Real examples of risk management

This chapter will provide several summarised examples that shed some light on the potential benefits from risk management.

10.1 Hydro One

Hydro One is a Canadian public company that is responsible for the delivery of electricity for the province of Ontario. In North America it ranks within the top 10 largest organisations of its kind, with a revenue of CA$ 6.5B in 2015. Within five years of starting risk management, the most tangible result was a better coordinated process for allocating capital and an increase of Hydro One's credit rating by Standard & Poor's, which reduced cost of capital.

In 1999 Hydro One appointed a Chief Risk Officer as head of the Corporate Risk Management Group, whose role is that of an independent risk management facilitator. In the next year they produced a risk management policy, which outlines the governing principles and responsibilities for risk management activities, and a risk management framework, which describes the details of the risk management process.

In the risk management process context, Hydro One's main financial objective is earnings stability over time, whereas a secondary objective is to maintain its reputation and public profile. Typically around 60 risks are identified that could harm Hydro One's business. These are then reduced to a top 10 through interviews, workshops and focus groups, by concentrating on a combination of probability and impact per risk. By plotting the top 10 risks on a risk matrix, it is possible to see where priorities lie and how a risk evolves over time. After formulating controls for each risk, a list of residual risks is assembled and a risk owner is assigned. The risk owner then decides if the risk is properly controlled, or if more risk mitigation is necessary. Hydro One sees monitoring as necessary as the impact and probability of risks change over time.

10.2 University of California

The University of California (UC) is a university with a US$ 28.5B budget in 2016, which serves over 250.000 students. In 2010 Standard & Poor's recognised the UC's risk management program as one of the reasons to award a higher credit rating. This lowered cost of capital by 0,1% due to decreased interest, which amounts means $14M savings.

UC keeps data to track the impact of hazard risks, such as insurable risk and liabilities. Direct costs attributable claims for hazard risks per $1.000 revenue have dropped from $18,64 in 2003 to $13,31 in 2010, a decrease of 29%. UC ascribes this drop to cheaper insurance premiums due to effective enterprise risk management.

In 1996 UC started to develop their own risk management system and by 2005 university founded its Office of Risk Services. This department is responsible for creating the current risk system, which is modelled on the COSO 2004 framework. Risk management is done by different campuses and medical centres which formed over a dozen individual risk management groups. The individual groups are supported by the Office of Risk Services through a publicly available toolbox. This toolbox contains generic tools for risk identification, assessment, control measure evaluation and monitoring.

10.3 Rio Tinto

Rio Tinto is one of the largest mining corporations in the world, with a revenue of US$ 33.8B in 2016. Though Rio Tinto has not publicly specified the tangible benefits from enterprise risk management, they do report that it has a positive influence on operational performance and supports delivery of strategic objectives.

Rio Tinto has described their approach to the risk management in a document referred to as a *Risk policy and standard*. The policy states that Rio Tinto fosters a risk aware culture in decision making, manages risk proactively

and applies risk analysis to all facets of its business. The standard describes the process in more detail. Every business unit is to perform risk analysis, which is initiated by one person who leads the process.

During initiation it is determined what the scope of the analysis is, which objectives are evaluated, which methods, tools and techniques are used, who participates, everyone's roles and responsibilities, which metrics are used to measure risk, what the risk acceptance threshold is, how to report and when to update.

Risk identification at Rio Tinto is done through a workshop with key stakeholders at a minimum, additional techniques can be used, if the process initiator finds it necessary. A description of these techniques can be found in Rio Tinto's intranet. After risks are identified, possible risk aggregation is evaluated, if several risks happen at the same time. If any of these risks exist, they are labelled for urgent assessment.

Following identification, every risk is assessed for its impact and probability by internal stakeholders with relevant experience and expertise. Both impacts and probabilities are assessed on a predefined scale. Impacts can be defined as financial or non-financial impact. The assessed risks are further classified as Class I (low risk) to Class IV (urgent), after which they are plotted on a risk matrix. It is preferred to use a risk matrix with four impact and four probability categories. If a risk is characterized by a very large impact and very low probability, it needs immediate treatment.

Possible control measures for the risks are formulated by experts in the relevant area, who can find guidance in Rio Tinto's intranet. After determining cost effectiveness for every control measure, the control measure is allocated to a risk owner, who monitors the risk. The results from the risk analysis are reported in a risk register, which contains at least a reference number, date of last risk update, title of the risk, description of the risk, probability, impact, classification, control measure and risk owner.

Monitoring is done through risk updates, which needs to reflect the results of control measures and additional risks.

Concluding remarks

This text discussed in brief the main principles and elements of the risk management process. Knowledge of these elements allows one individually or with a team to quickly start putting risk management to practice.

Risk management is more of an art than a science. It is therefore crucial to put the knowledge from this text into practice quickly in order for it to become valuable. This can be done using low-tech methods such as writing risks on post-its and plotting them on a risk map, hand drawn on a sheet of whiteboard paper. An alternative is to practice risk management using the high-tech Risk Management Simulation game developed in the Erasmus+ Partnerships to ensure Risk Management in practice (PERM) project. This game can be played using the URL:

http://www.perm.lv/simulation-game/

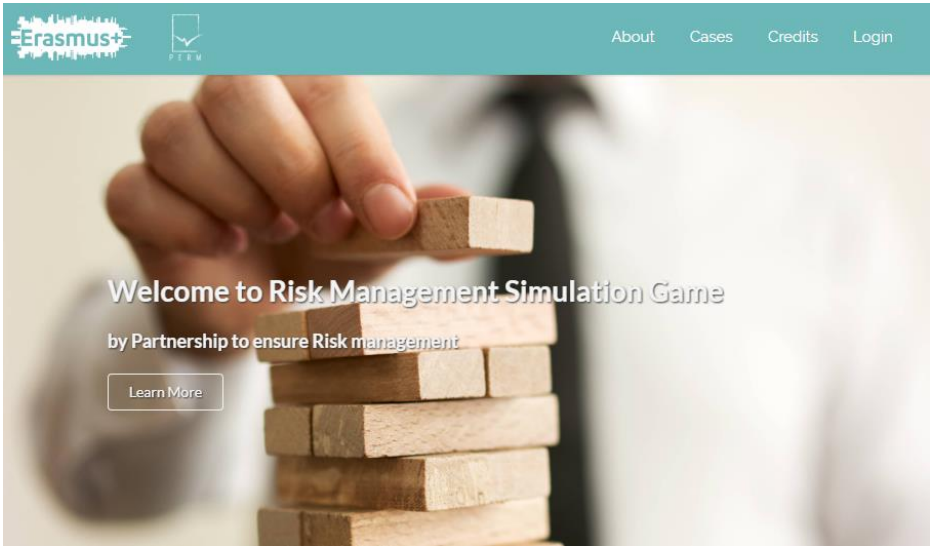

Figure 14 Opening website page of the PERM Simulation Game

Under guidance of a facilitator the game accommodates several players and simulates in several playing rounds the occurrence of risky events in a particular case setting. At the end of each playing round players receive feedback on their risk management performance and prepare for the next round by making alterations in their risk management choices. The game allows players to think through the risk management process steps in multiple rounds in a case setting.

1. Objective: What is the objective of the case company? What activities does it perform and which are the resources used? What is a sound risk appetite for the case company?
2. Risks: Which risky events impact these activities, resources and, in the end, the objective of the case company?
3. Assessment: What is the likelihood and impact of these risks on the case company's objective?
4. Evaluation: What priority level needs to be assigned to the risks in order for the case company to remain within its risk appetite?
5. Control: Which control measures need to be selected to remain within the risk appetite?
6. Monitoring: Are we, when we assess the risks that actually did and did not occur, still in control? Are the chosen control measures effective? Do we need to alter our controls?

Prior to starting the game, the facilitator provides players access to a description of a company case and defines in the software which risks occur, what their likelihood and impact levels are and which set of control measures is available to the players to mitigate these risks. The simulation game uses these inputs to simulate in every new playing round a new set of events that materializes and damages the case company objective.

The tool contributes to learning risk management skills in a very short period of time, in a fashion that resembles reality as closely as possible. More information on how to play or moderate the simulation game is provided on the website.

List of references

Aabo, T., Fraser, J. R., & Simkins, B. J. (2005). The rise and evolution of the chief risk officer: enterprise risk management at Hydro One. *Journal of Applied Corporate Finance*, 17(3), 62-75.

Baker, A., Navarro, E. O., & Van Der Hoek, A. (2005). An experimental card game for teaching software engineering processes. *Journal of Systems and Software*, *75*(1), 3-16.

Bugalla, J. & Narvaez, K. (2012). The University of California ERM program reduces the costs of risk and borrowing. *Government Finance Review*, June 2012.

Burgos, D., Tattersall, C., & Koper, R. (2006). Can IMS Learning Design be used to model computer-based educational games?.

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review*, *16*(2), 147-166.

Greener, I. (2006). Nick Leeson and the collapse of Barings Bank: socio-technical networks and the 'rogue trader'. *Organization*, *13*(3), 421-441.

Guo, Q. L. (2001). Development of risk analysis models for decision-making in project management (Doctoral dissertation, Edinburgh Napier University).

Heus, R. de, & Stremmelaar, M. (2000). *Auditen van soft controls.* Deventer: Kluwer.

ISO/IEC 31010:2009 Ed. 1.0: Risk Management - Risk Assessment Techniques

Kaplan, R., & Mikes, A. (2016). Risk Management – the Revealing Hand. *Journal of Applied Corporate Finance,* 28(1), 8-18.

Klassen, K., & Willoughby, K. (2003). In-class simulation games: Assessing student learning. *Journal of Information Technology Education: Research*, *2*(1), 1-13.

Kober, R., & Tarca, A. (2002). For fun or profit? An evaluation of an accounting simulation game for university students. *Accounting Research Journal*, *15*(1), 98-109.

KPMG Review. (1999). Internal Control: A Practical Guide

Lam, J. (2001). The CRO is here to stay. *Risk Management*, *48*(4), 16.

Law, A. K. (1991). Simulation modeling and analysis. New York: McGraw-Hill.

Packová, V., & Brebera, D. (2015). Loss Distributions in Insurance Risk Management. *Business Administration*, 17.

PwC. (2009). Auditing risk culture – Art or science?

RIMS. (2011). An overview of widely used risk management standards and guidelines.

Rio Tinto. (2009). Risk policy and standard.

Rio Tinto. (2015). Sustainable development 2015. Working for mutual benefit.

Rio Tinto. (2017). 2016 annual report.

Simkins, B., & Ramirez, S. A. (2007). Enterprise-wide risk management and corporate governance. *Loy. U. Chi. LJ*, *39*, 571.

The IIA. (2015). *Discussion paper, Soft controls, What are the starting points for the internal auditor?*

The IRM. (2012). Risk Culture.

University of California. (2010). Enterprise Risk Management Report to the Vice Chancellors of Administration and Medical Center CEOs.

University of California. (2012). Enterprise Risk Management Report.

University of California. (s.d.). Risk Assessment Toolbox. Retrieved March 3, 2017.

Wall, K. (2009). Thinking about Risk: Definition, Assessment, and Management. *The Armed Forces Comptroller*, Summer 2009: 8-13.

Willis Towers Watson. (2016). Risk culture start to come of age.